RECURRENCES IN TERMS OF SPECIAL POLYNOMIALS FOR EXPONENTIAL SUMS OF ELEMENTARY SYMMETRIC POLYNOMIALS OVER FINITE FIELDS

Axel O. Gómez-Flores
Department of Mathematics, The Ohio State University, Columbus, Ohio
gomez-flores.1@osu.edu

Luis A. Medina
Department of Mathematics, University of Puerto Rico, San Juan, Puerto Rico
luis.medina17@upr.edu

Luisiany Pomales
Department of Mathematics, University of Puerto Rico, San Juan, Puerto Rico
luisiany.pomales@upr.edu

Carlos F. Santiago-Calderón
Department of Mathematics, University of Puerto Rico, San Juan, Puerto Rico
carlos.santiago66@upr.edu

Received: 3/31/22, Accepted: 1/17/23, Published: 1/27/23

Abstract

It is known that exponential sums of symmetric Boolean functions are linear recurrent. The characteristic polynomial of the homogeneous linear recurrence that they satisfy can be expressed in terms of cyclotomic polynomials. In this work, we study the general recurrence for q-ary functions and, in the case of 3-ary functions, we express the characteristic polynomial of the recurrence in terms of some special polynomials.

1. Introduction

Exponential sums are beautiful mathematical objects that lie in the intersection of combinatorics and number theory. These objects can be used on various problems, for example, to determine if a system of polynomial equations have solutions over a finite field and to detect when a particular function is balanced. This last property (balancedness) is very useful in some cryptographic applications [6, 7, 8, 9, 10, 13,

DOI: 10.5281/zenodo.7569270

14]. Classical examples of exponential sums include the Gauss sum, Kloosterman sums, and Weyl sums.

In this work, we consider exponential sums of the following type. Let $q = p^r$ where p is prime and r is a positive integer. Let $\mathbb{F}_q$ be the field of q elements. An n-variable q-ary function is a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$. The set of all n-variable q-ary functions is denoted by $\mathcal{B}_{n,q}$. The *exponential sum* of $f \in \mathcal{B}_{n,q}$ is defined by

$$S_{\mathbb{F}_q}(f) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} \xi_p^{\mathrm{Tr}(f(\mathbf{x}))}, \tag{1}$$

where $\xi_n = \exp(2\pi i/n)$ and $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ is the field trace function. The *field trace function* is explicitly given by

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \sum_{j=0}^{r-1} \alpha^{p^j}, \tag{2}$$

with arithmetic done in $\mathbb{F}_q$. When $q = 2$, we call these functions Boolean functions. The set $\mathcal{B}_{n,2}$ is denoted by $\mathcal{B}_n$ and the exponential sum of a Boolean function f is denoted by $S(f)$ instead of $S_{\mathbb{F}_2}(f)$.

Exponential sums that look like the right-hand side of Equation (1) have been extensively studied when the characteristic of the field is 2 because of their cryptographic applications, see [4, 5, 6, 9, 10, 13, 14, 19]. In the binary case, it is known that, under certain conditions, exponential sums of symmetric Boolean functions are linear recurrent (this is also true for other types of functions).

An n-variable Boolean function $f(\mathbf{X})$ is called symmetric if it is fixed under the action of the symmetric group of n symbols, that is, if

$$f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n) \tag{3}$$

for every $\sigma \in S_n$ (here S_n represents the symmetric group of n symbols). Every n-variable Boolean function can be identified with a multi-variable polynomial. This polynomial is known as the *algebraic normal form* (or ANF for short) of the Boolean function. In the particular case of symmetric Boolean functions, every such function can be identified with an expression of the form

$$\boldsymbol{e}_{n,k_1} \oplus \cdots \oplus \boldsymbol{e}_{n,k_s}, \tag{4}$$

where $0 \le k_1 < \cdots < k_s$ are integers, $\boldsymbol{e}_{n,k}$ represents the n-variable *elementary symmetric polynomial* of degree k and $\oplus$ represents addition modulo 2. The polynomial $\boldsymbol{e}_{n,k}$ is formed by adding together all distinct products of k distinct variables in $\{X_1, \ldots, X_n\}$. For example,

$$\boldsymbol{e}_{5,2} = X_1X_2+X_1X_3+X_1X_4+X_1X_5+X_2X_3+X_2X_4+X_2X_5+X_3X_4+X_3X_5+X_4X_5.$$

We use the notation $\boldsymbol{e}_{n,[k_1,\ldots,k_s]}$ to represent the normal form displayed in (4).

As mentioned earlier, under some circumstances, exponential sums of symmetric Boolean functions are linear recurrent. The recurrence they satisfy is very elegant and the characteristic polynomial of the recurrence can be expressed in terms of some known polynomials. Explicitly, let $0 \leq k_1 < \cdots < k_s$ be fixed integers and $r = \lfloor \log_2(k_s) \rfloor + 1$. The sequence $\{S(\boldsymbol{e}_{n,[k_1,\ldots,k_s]})\}_{n\in\mathbb{N}}$ satisfies the homogeneous linear recurrence whose characteristic polynomial is given by

$$(X-2)\Phi_4(X-1)\cdots\Phi_{2^r}(X-1),$$

where $\Phi_n(X)$ represents the n-th cyclotomic polynomial. This result is a consequence of the following theorem of Cai et al. ([4]).

Theorem 1 ([4]). *Let $1 \leq k_1 < \cdots < k_s$ be fixed integers and $r = \lfloor \log_2(k_s) \rfloor + 1$. The value of the exponential sum $S(\boldsymbol{e}_{n,[k_1,\cdots,k_s]})$ is given by*

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

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

$$c_j(k_1,\cdots,k_s) = \frac{1}{2^r}\sum_{t=0}^{2^r-1}(-1)^{\binom{t}{k_1}+\cdots+\binom{t}{k_s}}\zeta_j^{-t}. \tag{5}$$

Recently, some cryptographic applications beyond characteristic 2 have been found. That has prompted new research in exponential sums that look like the right-hand side of Equation (1) and some of the results available for the binary field have been extended to other finite fields [11, 12, 15, 16, 17, 18]. In particular, in [12], Theorem 1 was extended to general finite fields.

Theorem 2 ([12]). *Let n and $k > 1$ be positive integers, p be a prime and $q = p^r$ with $r \geq 1$. Let $D = p^{\lfloor \log_p(k) \rfloor + 1}$. 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

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

$\xi_m = \exp(2\pi i/m)$, $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ and $F^{(p)}_{k;\mathbb{F}_q}(b_1, \cdots, b_{q-1})$ represents the value of $\boldsymbol{e}_{n,k}$ on a tuple $\mathbf{x} \in \mathbb{F}_q^n$ with the property that $\mathbf{x}$ has b_j entries equal to α_j where $\mathbb{F}_q = \{0, \alpha_1, \alpha_2, \cdots, \alpha_{q-1}\}$. 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

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

Our goal in this work is to express $P_{q,k}(X)$ in terms of known polynomials (as it was in the binary case). That is a very challenging problem, but a useful one. Knowing the explicit coefficients of the characteristic polynomial will allow us to better implement the recurrences on the machine. That, in turn, will allow us to explore cryptographic properties of these functions when the number of variables grows.

We study first the case $q = 3$ and then move to other examples. Some simple knowledge of Galois theory is required to read this article.

2. The Simple Cases

The goal is to express $P_{3,k}(X)$ in terms of some known polynomials. Observe that in order to achieve this goal, we must calculate the minimal polynomial over $\mathbb{Q}$ for each $1 + \xi_D^a + \xi_D^b$ where $D = 3^{\lfloor \log_3(k) \rfloor + 1}$ and $0 \le b \le a \le D - 1$.

Calculating these minimal polynomials can be a challenge. However, some cases are simple. We start with them. Before we proceed, observe that the minimal polynomial of $1 + \xi_D^a + \xi_D^b$ is a shift of the minimal polynomial of $\xi_D^a + \xi_D^b$, and thus, in some instances we will work with $\xi_D^a + \xi_D^b$.

Let $r = \lfloor \log_3(k) \rfloor + 1$. The first simple case is when $a = b$. In that case, we are working with the algebraic integer $1 + 2\xi_{3^r}^a$. If $a = 0$, then it is clear that the minimal polynomial is $X - 3$ and therefore, $X - 3$ is a factor of $P_{3,k}(X)$. When $a \ge 1$ the analysis is reduced to finding the minimal polynomials of $1 + 2\xi_{3^\ell}$ for $1 \le \ell \le r$. The minimal polynomial of $2\xi_{3^\ell}$ over $\mathbb{Q}$ is given by $2^{2 \cdot 3^{\ell-1}} \Phi_{3^\ell}(X/2)$ and therefore

$$2^{2 \cdot 3^{\ell-1}} \Phi_{3^\ell}\left(\frac{X-1}{2}\right)$$

is the minimal polynomial of $1 + 2\xi_{3^\ell}$ and a factor of $P_{3,k}(X)$ for $\ell = 1, \ldots, r$.

Another simple case is when the algebraic number in consideration is $2 + \xi_{3^r}^a$. This case is reduced to finding the minimal polynomial of $2 + \xi_{3^\ell}$ for $1 \le \ell \le r$. The minimal polynomial of $2 + \xi_{3^\ell}$ over $\mathbb{Q}$ is given by $\Phi_{3^\ell}(X - 2)$ and therefore

$$\Phi_{3^\ell}(X - 2)$$

is a factor of $P_{3,k}(X)$ for $\ell = 1, \ldots, r$.

Since all these polynomials are relatively prime to each other, then we have the following result.

Proposition 1. *Let $k > 1$ and $r = \lfloor \log_3(k) \rfloor + 1$. Then,*

$$(X-3)\prod_{\ell=1}^{r} 2^{2\cdot 3^{\ell-1}} \Phi_{3^\ell}\left(\frac{X-1}{2}\right) \prod_{\ell=1}^{r} \Phi_{3^\ell}(X-2) \tag{6}$$

divides $P_{3,k}(X)$.

Observe that in the general case, that is, when $q = p^t$ with p prime and we are working over $\mathbb{F}_q$, we are interested in finding the minimal polynomials of algebraic integers of the form

$$1 + \xi_D^{a_1} + \cdots + \xi_D^{a_{q-1}}, \tag{7}$$

where $D = p^{\lfloor \log_p(k) \rfloor + 1}$ and $0 \leq a_{q-1} \leq a_{q-2} \leq \cdots \leq a_2 \leq a_1 \leq D-1$. Of course, the algebraic integers

$$s + (q-s)\xi_D^a, \tag{8}$$

where $1 \leq s \leq q-1$, are of the same type as the algebraic integers in (7). Therefore, the same argument as before leads to the following result.

Proposition 2. *Let p be a prime, $q = p^t$, $k > 1$ and $r = \lfloor \log_p(k) \rfloor + 1$. Then,*

$$(X-q)\prod_{s=1}^{q-1}\prod_{\ell=1}^{r} (q-s)^{(p-1)\cdot p^{\ell-1}} \Phi_{p^\ell}\left(\frac{X-s}{q-s}\right) \tag{9}$$

divides $P_{q,k}(X)$.

The remaining cases are not as simple of the ones discussed already. Again, we work first over $\mathbb{F}_3$. The remaining cases are reduced to study the minimal polynomials of $\xi_{3^m}^a + \xi_{3^l}^b$ for $\gcd(a,3) = \gcd(b,3) = 1$ and $1 \leq \ell \leq m \leq r$. From now on, we use Galois Theory in our study. This is standard when studying minimal polynomials.

3. The Case of $\xi_{3^m} + \xi_{3^\ell}$ When $1 \leq l < m \leq r$

Let $\alpha_{m,\ell} = \xi_{3^m} + \xi_{3^\ell}$ and let $\mu_{\alpha_{m,\ell};\mathbb{Q}}(X)$ be the minimal polynomial of $\alpha_{m,\ell}$ over $\mathbb{Q}$. The first step in our analysis is to find the degree of $\mu_{\alpha_{m,\ell};\mathbb{Q}}(X)$.

It is well-known from Galois Theory that

$$G = \mathrm{Gal}(\mathbb{Q}(\xi_{3^m})/\mathbb{Q}) \simeq \mathbb{Z}_{3^m}^{\times},$$

where $\mathbb{Z}_{3^m}^{\times}$ represents the group of units modulo 3^m. This implies that the degree of the extension $\mathbb{Q}(\xi_{3^m})/\mathbb{Q}$ is given by

$$[\mathbb{Q}(\xi_{3^m}) : \mathbb{Q}] = |\mathbb{Z}_{3^m}^{\times}| = \varphi(3^m) = 2 \cdot 3^{m-1}.$$

Suppose that $\sigma_j \in G$ is such that $\sigma_j(\xi_{3^m}) = \xi_{3^m}^j$ where $1 \leq j < 3^m$ is relatively prime to 3. Note that

$$\sigma_j(\alpha_{m,\ell}) = \xi_{3^m}^j + \xi_{3^\ell}^j \tag{10}$$

because σ_j is a $\mathbb{Q}$-automorphism. Thus, $\xi_{3^m}^j + \xi_{3^\ell}^j$ is a conjugate of $\xi_{3^m} + \xi_{3^\ell}$. Observe that if j, k are integers relatively prime to 3 and let

$$\xi_{3^m}^j + \xi_{3^\ell}^j = \xi_{3^m}^k + \xi_{3^\ell}^k, \tag{11}$$

then it must be true that $j \equiv k \mod 3^m$. This implies that $\alpha_{m,\ell}$ has at least $2 \cdot 3^{m-1}$ conjugates, that is,

$$[\mathbb{Q}(\alpha_{m,\ell}) : \mathbb{Q}] \geq 2 \cdot 3^{m-1}.$$

But it is clear that $\mathbb{Q}(\alpha_{m,\ell}) \subseteq \mathbb{Q}(\xi_{3^m})$, and thus

$$[\mathbb{Q}(\alpha_{m,\ell}) : \mathbb{Q}] = 2 \cdot 3^{m-1}.$$

We conclude that $\deg(\mu_{\alpha_{m,\ell};\mathbb{Q}}(X)) = 2 \cdot 3^{m-1}$.

The next step is to calculate $\mu_{\alpha_{m,\ell}}(X)$. It turns out that in some instances, like the one we are going to present, it is easier to calculate the product of some minimal polynomials than calculating them individually. We start with the following standard result from Galois Theory.

Lemma 1. *Suppose that $f(X) \in \mathbb{Z}[X]$ and let α be an algebraic integer over $\mathbb{Q}$. Suppose that*

$$\alpha = \alpha_1,\ \alpha_2, \cdots, \alpha_r$$

are all the conjugates of α. Then,

$$\prod_{j=1}^{r} f(X - \alpha_j) \in \mathbb{Z}[X].$$

Proof. As just mentioned, this is a standard result from Galois Theory. Suppose that $m_\alpha(X)$ is the minimal polynomial of α over $\mathbb{Q}$ (which has coefficients in $\mathbb{Z}$). Let $G = \mathrm{Gal}_{\mathbb{Q}}(m_\alpha(X))$ and let

$$g(X) = \prod_{\sigma \in G} f\left(X - \sigma(\alpha)\right).$$

Observe that if $\tau \in G$, then

$$\begin{aligned}\tau(g(X)) &= \prod_{\sigma\in G} f\left(X - \tau\sigma(\alpha)\right)\\ &= \prod_{\sigma\in G} f\left(X - \sigma(\alpha)\right)\\ &= g(X).\end{aligned}$$

That implies that the coefficients of $g(X)$ are fixed for every $\tau \in G$ and therefore they must belong to $\mathbb{Q}$. The assumption of α implies that they are actually in $\mathbb{Z}$. This conclude the proof. □

Proposition 3. *Let $1 \leq \ell < m$ be integers and let j be an integer such that $\gcd(j,3) = 1$. Let $\mu_{\xi_{3^m}+\xi_{3^\ell}^j;\mathbb{Q}}(X)$ be the minimal polynomial of $\xi_{3^m} + \xi_{3^\ell}^j$ over $\mathbb{Q}$. Then,*

$$\prod_{\gcd(j,3)=1}^{3^{\ell-1}} \mu_{\xi_{3^m}+\xi_{3^\ell}^j;\mathbb{Q}}(X) = \prod_{\gcd(j,3)=1}^{3^{\ell-1}} \Phi_{3^m}(X - \xi_{3^\ell}^j). \tag{12}$$

Proof. Consider the polynomial

$$f(X) = \prod_{\gcd(j,3)=1}^{3^{\ell}-1} \Phi_{3^m}(X - \xi_{3^\ell}^j). \tag{13}$$

Since we are running over all the conjugates of ξ_{3^ℓ}, the previous lemma implies $f(X) \in \mathbb{Z}[X]$. But then, $\mu_{\xi_{3^m}+\xi_{3^\ell}^j,\mathbb{Q}}(X)$ divides $f(X)$. The polynomials

$$\mu_{\xi_{3^r}+\xi_{3^\ell}^j,\mathbb{Q}}(X)$$

are relatively prime to each other, and thus

$$\prod_{\gcd(j,3)=1}^{3^{\ell}-1} \mu_{\xi_{3^m}+\xi_{3^\ell}^j,\mathbb{Q}}(X) \text{ divides } f(X) = \prod_{\gcd(j,3)=1}^{3^{\ell}-1} \Phi_{3^m}(X - \xi_{3^\ell}^j). \tag{14}$$

Both polynomials in (14) are monic and of the same degree, therefore

$$\prod_{\gcd(j,3)=1}^{3^{\ell}-1} \mu_{\xi_{3^m}+\xi_{3^\ell}^j,\mathbb{Q}}(X) = \prod_{\gcd(j,3)=1}^{3^{\ell}-1} \Phi_{3^m}(X - \xi_{3^\ell}^j). \tag{15}$$

Thus, multiplying these shifted cyclotomic polynomials gives us the product of the minimal polynomials over $\mathbb{Q}$ of the elements $\xi_{3^m} + \xi_{3^\ell}^j$ □

An immediate consequence of the previous result is the following.

Corollary 1. *Let $k > 1$ and $r = \lfloor \log_3(k) \rfloor + 1$. The polynomial*

$$\prod_{m=2}^{r} \prod_{\ell=1}^{m-1} \prod_{\gcd(j,3)=1}^{3^\ell - 1} \Phi_{3^m}(X - 1 - \xi_{3^\ell}^j) \tag{16}$$

divides $P_{3,k}(X)$.

These results can be extended to $\mathbb{F}_q$, q odd, without too much effort. Observe that the algebraic integers

$$s + \left(\frac{q-s}{2}\right) \xi_{p^m} + \left(\frac{q-s}{2}\right) \xi_{p^\ell}^j, \tag{17}$$

where $s = 1, 3, 5, \ldots, q-2$, $1 \leq \ell < m$, and $\gcd(j, p) = 1$, are of the same type as expression (7). Therefore, the same argument as before yields

$$\prod_{\gcd(j,p)=1}^{p^\ell - 1} \mu_{\left(\frac{q-s}{2}\right)\xi_{p^m} + \left(\frac{q-s}{2}\right)\xi_{p^\ell}^j, \mathbb{Q}}(X) = \tag{18}$$
$$\prod_{\gcd(j,p)=1}^{p^\ell - 1} \left(\frac{q-1}{2}\right)^{(p-1)p^{m-1}} \Phi_{p^m}\left(\frac{2X}{q-1} - \xi_{p^\ell}^j\right).$$

That leads to the following result.

Corollary 2. *Let p be an odd prime, $q = p^t$, $k > 1$ and $r = \lfloor \log_p(k) \rfloor + 1$. The polynomial*

$$\prod_{m=2}^{r} \prod_{\ell=1}^{m-1} \prod_{s=1,odd}^{q-2} \prod_{\gcd(j,p)=1}^{p^\ell - 1} \left(\frac{q-s}{2}\right)^{(p-1)p^{m-1}} \Phi_{p^m}\left(\frac{2(X-1)}{q-s} - \xi_{p^\ell}^j\right) \tag{19}$$

divides $P_{q,k}(X)$.

These results take care of the case considered in this section. Observe that we are still missing the case when the algebraic integer in consideration is $1 + \xi_{3^m}^a + \xi_{3^m}^b$ with $\gcd(a, 3) = \gcd(b, 3) = 1$.

4. The Case of $\xi_{3^m} + \xi_{3^m}^j$ with $\gcd(j, 3) = 1$

Let $1 \leq a, b < 3^m$ be integers such that $\gcd(a, 3) = \gcd(b, 3) = 1$ and let $\beta_{a,b} = \xi_{3^m}^a + \xi_{3^m}^b$. As before, let $G = \mathrm{Gal}(\mathbb{Q}(\xi_{3^m})/\mathbb{Q}) \simeq \mathbb{Z}_{3^m}^\times$. Let $\sigma_k \in G$ with $\gcd(k, 3) = 1$ be such that

$$\sigma_k(\xi_{3^m}) = \xi_{3^m}^k.$$

Then,

$$\sigma_k(\beta_{a,b}) = \xi_{3^m}^{ak} + \xi_{3^m}^{bk} \tag{20}$$

and $\xi_{3^m}^{ak} + \xi_{3^m}^{bk}$ is a conjugate of $\beta_{a,b}$ for every k such that $\gcd(k,3) = 1$.

Suppose that k, ℓ are integers such that $\gcd(k,3) = \gcd(\ell,3) = 1$ and

$$\xi_{3^m}^{ak} + \xi_{3^m}^{bk} = \xi_{3^m}^{a\ell} + \xi_{3^m}^{b\ell}.$$

Then, it must be true that either $k \equiv \ell \mod 3^m$, which is trivial, or

$$\begin{aligned} ak &\equiv b\ell \mod 3^m \\ bk &\equiv a\ell \mod 3^m. \end{aligned}$$

This system of congruences implies that $k \equiv a^{-1}b\ell \mod 3^m$ and so $a^2 \equiv b^2 \mod 3^m$. Therefore, if

$$a \not\equiv -b \mod 3^m,$$

then $[\mathbb{Q}(\beta_{a,b}) : \mathbb{Q}] = 2 \cdot 3^{m-1}$. On the other hand, if $a \equiv -b \mod 3^m$, then $[\mathbb{Q}(\beta_{a,-a}) : \mathbb{Q}] = 3^{m-1}$.

We discuss the case $\xi_{3^m}^{a} + \xi_{3^m}^{-a}$ later. For the case $a \not\equiv \pm b \mod 3^m$, Galois Theory tells us that

$$\mu_{\beta_{a,b};\mathbb{Q}}(X) = \prod_{\gcd(j,3)=1}^{3^m-1} (X - \xi_{3^m}^{aj} - \xi_{3^m}^{bj}). \tag{21}$$

Expressing this polynomial in terms of special polynomials or writing its coefficients explicitly in $\mathbb{Z}$ is not an easy task. There are, however, some instances in which that can be achieved.

Consider the case when

$$b = a\left(3^{m-1} + 1\right),$$

where $\gcd(a,3) = 1$. Since the numbers $\xi_{3^m}^{a} + \xi_{3^m}^{(3^{m-1}+1)a}$, for $a \in \mathbb{Z}_{3^m}^{\times}$, are conjugates, it is sufficient to work with the algebraic integer $\xi_{3^m} + \xi_{3^m}^{3^{m-1}+1}$.

Proposition 4. *Let $m > 1$ be a positive integer. The minimal polynomial of $\gamma_m = \xi_{3^m} + \xi_{3^m}^{3^{m-1}+1}$ over $\mathbb{Q}$ is given by*

$$\mu_{\gamma_m;\mathbb{Q}}(X) = \Phi_{2\cdot 3^m}(X) = X^{2\cdot 3^{m-1}} - X^{3^{m-1}} + 1.$$

Proof. We first show that γ_m is a root of unity. Observe that

$$\begin{aligned} \gamma_m &= \xi_{3^m} + \xi_{3^m}^{3^{m-1}+1} \\ &= \cos\left(\frac{2\pi}{3^m}\right) + i\sin\left(\frac{2\pi}{3^m}\right) + \cos\left(\frac{2\pi}{3^m}(3^{m-1}+1)\right) + i\sin\left(\frac{2\pi}{3^m}(3^{m-1}+1)\right) \\ &= \cos\left(\frac{2\pi}{3^m}\right) + i\sin\left(\frac{2\pi}{3^m}\right) + \cos\left(\frac{2\pi}{3^m} + \frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3^m} + \frac{2\pi}{3}\right) \\ &= \cos\left(\frac{2\pi}{3^m}\right) + i\sin\left(\frac{2\pi}{3^m}\right) - \sin\left(\frac{2\pi}{3^m} + \frac{\pi}{6}\right) + i\cos\left(\frac{2\pi}{3^m} + \frac{\pi}{6}\right), \end{aligned}$$

where the last equality is a consequence of the identities

$$\cos\left(\theta+\frac{2\pi}{3}\right)=-\sin\left(\theta+\frac{\pi}{6}\right) \text{ and } \sin\left(\theta+\frac{2\pi}{3}\right)=\cos\left(\theta+\frac{\pi}{6}\right).$$

The well-known identities

$$\begin{aligned}\sin(\alpha+\beta) &= \sin(\alpha)\cos(\beta)+\cos(\alpha)\sin(\beta)\\ \cos(\alpha+\beta) &= \cos(\alpha)\cos(\beta)-\sin(\alpha)\sin(\beta),\end{aligned}$$

imply

$$\begin{aligned}\sin\left(\frac{2\pi}{3^m}+\frac{\pi}{6}\right) &= \frac{\sqrt{3}}{2}\cdot\sin\left(\frac{2\pi}{3^m}\right)+\frac{1}{2}\cdot\cos\left(\frac{2\pi}{3^m}\right)\\ \cos\left(\frac{2\pi}{3^m}+\frac{\pi}{6}\right) &= \frac{\sqrt{3}}{2}\cdot\cos\left(\frac{2\pi}{3^m}\right)-\frac{1}{2}\cdot\sin\left(\frac{2\pi}{3^m}\right),\end{aligned}$$

and therefore

$$\gamma_m = \frac{1}{2}\cos\left(\frac{2\pi}{3^m}\right)-\frac{\sqrt{3}}{2}\sin\left(\frac{2\pi}{3^m}\right)+i\left(\frac{1}{2}\sin\left(\frac{2\pi}{3^m}\right)+\frac{\sqrt{3}}{2}\cos\left(\frac{2\pi}{3^m}\right)\right).$$

A straightforward calculation leads to $|\gamma_m|=1$. Thus, γ_m is a root of unity.

The next step is to calculate the argument of γ_m. Recall that if $z=x+iy\in\mathbb{C}$, then

$$\arg(z)=\tan^{-1}(y/x).$$

The imaginary part of γ_m over its real part is given by

$$\begin{aligned}\frac{1/2\cdot\sin(2\pi/3^m)+\sqrt{3}/2\cdot\cos(2\pi/3^m)}{1/2\cdot\cos(2\pi/3^m)-\sqrt{3}/2\cdot\sin(2\pi/3^m)} &= \frac{\tan(2\pi/3^m)+\sqrt{3}}{1-\sqrt{3}\cdot\tan(2\pi/3^m)}\\ &= \frac{\tan(2\pi/3^m)+\tan(\pi/3)}{1-\tan(\pi/3)\tan(2\pi/3^m)}.\end{aligned}$$

The identity

$$\tan(\alpha+\beta)=\frac{\tan(\alpha)+\tan(\beta)}{1-\tan(\alpha)\tan(\beta)}$$

implies

$$\arg(\gamma_m)=\tan^{-1}\left(\tan\left(\frac{(3^{m-1}+2)\pi}{3^m}\right)\right)=\frac{(3^{m-1}+2)\pi}{3^m}.$$

All of the above implies that

$$\gamma_m=\exp\left(\frac{(3^{m-1}+2)\pi i}{3^m}\right)$$

and thus γ_m is a root of the polynomial $X^{3^m}+1$. Recall that

$$X^{3^m}+1=\prod_{j=0}^{m}\Phi_{2\cdot 3^j}(X).$$

Since $[\mathbb{Q}(\gamma_m):\mathbb{Q}]=2\cdot 3^{m-1}$, it is clear that γ_m is not a root of $\Phi_{2\cdot 3^j}(X)$ for $0\leq j\leq m-1$. Therefore γ_m must be a root of

$$\Phi_{2\cdot 3^m}(X)=X^{2\cdot 3^{m-1}}-X^{3^{m-1}}+1.$$

Since $[\mathbb{Q}(\gamma_m),\mathbb{Q}]=2\cdot 3^{m-1}$, then $\mu_{\gamma_m;\mathbb{Q}}(X)=\Phi_{2\cdot 3^m}(X)$. This concludes the proof. □

Corollary 3. *Let $k>1$ be an integer and $r=\lfloor\log_3(k)\rfloor+1$. Then,*

$$\prod_{\ell=1}^{r}\Phi_{2\cdot 3^\ell}(X-1) \tag{22}$$

divides $P_{3,k}(X)$.

The above result depends heavily on the fact that we are working with the prime $p=3$, and thus it cannot be extended to the general case of $\mathbb{F}_q$. It can be extended, however, to the case when q is a power of three.

Corollary 4. *Let $k>1$ be an integer, $q=3^t$ and $r=\lfloor\log_3(k)\rfloor+1$. Then,*

$$\prod_{s=1,odd}^{q-2}\prod_{\ell=1}^{r}\left(\frac{q-s}{2}\right)^{2\cdot 3^{\ell-1}}\Phi_{2\cdot 3^\ell}\left(\frac{2(X-1)}{q-s}\right) \tag{23}$$

divides $P_{q,k}(X)$.

We now discuss the case $\xi_{3^m}^a+\xi_{3^m}^{-a}$ for $a\in\mathbb{Z}_{3^m}^\times$. Again, since $\xi_{3^m}^a+\xi_{3^m}^{-a}$'s are all conjugates of $\xi_{3^m}+\xi_{3^m}^{-1}$, it is enough to study this last algebraic integer. We start with the following result from Abhyankar, Cohen, and Zieve [2].

Theorem 3 ([2])**.** *Let $n>3$ be an odd integer. The minimal polynomial of $\xi_n+\xi_n^{-1}$ is a factor of*

$$U_{(n-1)/2}\left(\frac{X}{2}\right)+U_{(n-3)/2}\left(\frac{X}{2}\right)$$

where $U_m(X)$ represents the m-th Chebyshev polynomial of the second kind, that is,

$$\sin((m+1)\theta)=U_m(\cos(\theta))\sin(\theta).$$

Proof. The argument of this proof is from [2]. We decided to include it in order to get insight on the machinery used.

Recall that

$$\xi_n + \xi_n^{-1} = 2\cos\left(\frac{2\pi}{n}\right). \tag{24}$$

The m-th Chebyshev polynomial of the first kind $T_m(X)$ satisfies

$$\cos(m\theta) = T_m(\cos(\theta)). \tag{25}$$

Therefore,

$$T_m\left(\frac{\xi_n + \xi_n^{-1}}{2}\right) = T_m\left(\cos\left(\frac{2\pi}{n}\right)\right) = \cos\left(\frac{2\pi m}{n}\right) = \frac{\xi_n^m + \xi_n^{-m}}{2}. \tag{26}$$

Observe that this implies that

$$T_m\left(\frac{X + X^{-1}}{2}\right) = \frac{X^m + X^{-m}}{2} \tag{27}$$

for infinite values of X, and thus they must be equal as rational functions. In particular,

$$T_n\left(\frac{\xi_n + \xi_n^{-1}}{2}\right) = \frac{\xi_n^n + \xi_n^{-n}}{2} = 1, \tag{28}$$

Therefore, $\gamma_n = \xi_n + \xi_n^{-1}$ is a root of $T_n(X/2) - 1$.

Observe that

$$T_n\left(\frac{X + X^{-1}}{2}\right) + 1 = \frac{1}{2}\left(X^{1/2} - X^{-1/2}\right)^2 \left(\frac{X^{n/2} - X^{-n/2}}{X^{1/2} - X^{-1/2}}\right)^2. \tag{29}$$

The first factor can be written as

$$\frac{1}{2}\left(X^{1/2} - X^{-1/2}\right)^2 = \frac{1}{2}\left(X - 2 + X^{-1}\right) = \frac{1}{2}\left(X + X^{-1}\right) - 1. \tag{30}$$

For the second one, observe that

$$\begin{aligned} \frac{X^{n/2} - X^{-n/2}}{X^{1/2} - X^{-1/2}} &= \left(\frac{X^{n/2} - X^{-n/2}}{X^{1/2} - X^{-1/2}}\right)\left(\frac{X^{1/2} + X^{-1/2}}{X^{1/2} + X^{-1/2}}\right) \\ &= \frac{X^{(n+1)/2} - X^{(1-n)/2} + X^{(n-1)/2} - X^{(-1-n)/2}}{X - X^{-1}} \\ &= \frac{X^{(n+1)/2} - X^{(-1-n)/2}}{X - X^{-1}} + \frac{X^{(n-1)/2} - X^{(1-n)/2}}{X - X^{-1}}. \end{aligned} \tag{31}$$

An argument similar to the one given for the m-th Chebyshev polynomial of the first kind shows that the m-th Chebyshev polynomial of the second kind satisfies the functional equation

$$U_m\left(\frac{X + X^{-1}}{2}\right) = \frac{X^{m+1} - X^{-1-m}}{X - X^{-1}}. \tag{32}$$

Thus, Equations (31) and (32) imply that

$$\frac{X^{n/2}-X^{-n/2}}{X^{1/2}-X^{-1/2}} = U_{(n-1)/2}\left(\frac{X+X^{-1}}{2}\right) + U_{(n-3)/2}\left(\frac{X+X^{-1}}{2}\right). \tag{33}$$

Therefore, Equations (29), (30) and (33) imply that

$$\begin{aligned} T_n\left(\frac{X+X^{-1}}{2}\right)+1 &= \left(\frac{1}{2}\left(X+X^{-1}\right)-1\right)\times \\ &\quad \left(U_{(n-1)/2}\left(\frac{X+X^{-1}}{2}\right) + U_{(n-3)/2}\left(\frac{X+X^{-1}}{2}\right)\right)^2 \end{aligned} \tag{34}$$

The change of variable $t = X + X^{-1}$ gives us

$$T_n(t/2)+1 = \frac{1}{2}(t-2)\left(U_{(n-1)/2}(t/2) + U_{(n-3)/2}(t/2)\right)^2. \tag{35}$$

Since $\xi_n \neq -1$, then γ_n is a root of

$$U_{(n-1)/2}\left(\frac{X}{2}\right) + U_{(n-3)/2}\left(\frac{X}{2}\right). \tag{36}$$

Therefore, the minimal polynomial of $\gamma_n = \xi_n + \xi_n^{-1}$ is a factor of the polynomial in (36). This concludes the proof. □

This result can be used to identify factors of $P_{3,k}(X)$, in particular, we have the following result. The result is written in general form, that is, for $p > 2$ odd.

Proposition 5. *Let $p > 2$ be a prime and $r > 1$ an integer. Then,*

$$\prod_{m=1}^{r} \mu_{\xi_{p^m}+\xi_{p^m}^{-1};\mathbb{Q}}(X) = U_{(p^r-1)/2}\left(\frac{X}{2}\right) + U_{(p^r-3)/2}\left(\frac{X}{2}\right). \tag{37}$$

Proof. Let $1 \leq m \leq r$. Observe that

$$T_{p^r}\left(\frac{\xi_{p^m}+\xi_{p^m}^{-1}}{2}\right) = \frac{\xi_{p^m}^{p^r}+\xi_{p^m}^{-p^r}}{2} = 1. \tag{38}$$

Therefore, $\xi_{p^m} + \xi_{p^m}^{-1}$ is a root of

$$T_{p^r}(X/2) = \frac{1}{2}(X-2)\left(U_{(p^r-1)/2}(X/2) + U_{(p^r-3)/2}(X/2)\right)^2, \tag{39}$$

and thus a root of

$$U_{(p^r-1)/2}(X/2) + U_{(p^r-3)/2}(X/2). \tag{40}$$

This implies that $\mu_{\xi_{p^m}+\xi_{p^m}^{-1};\mathbb{Q}}(X)$ divides the polynomial in (40) for every $1 \leq m \leq r$ and thus

$$\prod_{m=1}^{r} \mu_{\xi_{p^m}+\xi_{p^m}^{-1};\mathbb{Q}}(X) \tag{41}$$

divides the polynomial in (40). However, we know that

$$[\mathbb{Q}(\xi_{p^m} + \xi_{p^m}^{-1}) : \mathbb{Q}] = \frac{p^{m-1}(p-1)}{2}$$

therefore,

$$\begin{aligned} \deg\left(\prod_{m=1}^{r} \mu_{\xi_{p^m}+\xi_{p^m}^{-1};\mathbb{Q}}(X)\right) &= \sum_{m=1}^{r} \frac{p^{m-1}(p-1)}{2} \\ &= \frac{p^r-1}{2}. \end{aligned} \tag{42}$$

Since the polynomials in (40) and in (41) are of the same degree, both are monic and the polynomial in (41) divides the polynomial in (40), we conclude that they are equal. □

Corollary 5. *Let $p > 1$ be a prime and $r > 1$ an integer. Then,*

$$\mu_{\xi_{p^m}+\xi_{p^m}^{-1}}(X) = \frac{U_{(p^r-1)/2}(X/2) + U_{(p^r-3)/2}(X/2)}{U_{(p^{r-1}-1)/2}(X/2) + U_{(p^{r-1}-3)/2}(X/2)}, \tag{43}$$

where $U_n(X)$ represents the n-th Chebyschev polynomial of the second kind.

Corollary 6. *Let $k > 1$ be an integer and $r = \lfloor \log_3(k) \rfloor + 1$. Then,*

$$U_{(3^r-1)/2}\left(\frac{X-1}{2}\right) + U_{(3^r-3)/2}\left(\frac{X-1}{2}\right), \tag{44}$$

where $U_n(X)$ represents the n-th Chebyschev polynomial of the second kind, divides $P_{3,k}(X)$.

This result can be extended to $\mathbb{F}_q$. Observe that the algebraic integers

$$s + \left(\frac{q-s}{2}\right)\xi_{p^m} + \left(\frac{q-s}{2}\right)\xi_{p^m}^{-1}, \tag{45}$$

where $s = 1, 3, 5, \ldots, q-2$, are of the same type as the algebraic integers in (7). Therefore, we have the following result.

Corollary 7. *Let p be an odd prime, $q = p^t$, $k > 1$ be an integer and $r = \lfloor \log_p(k) \rfloor + 1$. Then,*

$$\prod_{s=1,odd}^{q-2} \left(\frac{q-s}{2}\right)^{\frac{p^r-1}{2}} \left(U_{(p^r-1)/2}\left(\frac{X-s}{q-s}\right) + U_{(p^r-3)/2}\left(\frac{X-s}{q-s}\right)\right), \tag{46}$$

where $U_n(X)$ represents the n-th Chebyschev polynomial of the second kind, divides $P_{q,k}(X)$.

We are still missing the minimal polynomials of $\xi_{3^m}+\xi_{3^m}^a$ where

$$a \in \mathbb{Z}_{3^m}^\times \setminus \{1, 3^m-1, 3^{m-1}+1, 2\cdot 3^{m-1}+1\}.$$

Let

$$T_m := \mathbb{Z}_{3^m}^\times \setminus \{1, 3^m-1, 3^{m-1}+1, 2\cdot 3^{m-1}+1\}.$$

These polynomials are hard to calculate explicitly. Of course, using Galois theory we can state that

$$\mu_{\xi_{3^m}+\xi_{3^m}^a;\mathbb{Q}}(X) = \prod_{\gcd(j,3)=1}^{3^m-1} \left(X-\xi_{3^m}^j-\xi_{3^m}^{aj}\right). \tag{47}$$

and we may be tempted to say

$$\prod_{m=1}^{r}\prod_{a\in T_m}\prod_{\gcd(j,3)=1}^{3^m-1}\left(X-1-\xi_{3^m}^j-\xi_{3^m}^{aj}\right) \tag{48}$$

divides $P_{3,k}(X)$. However, we must be careful because the expression in (48) is not square-free. That is because if $a\in T_m$ and a^{-1} represents the inverse of a as an element of $\mathbb{Z}_{3^m}^\times$, then

$$\prod_{\gcd(j,3)=1}^{3^m-1}\left(X-1-\xi_{3^m}^j-\xi_{3^m}^{aj}\right) = \prod_{\gcd(j,3)=1}^{3^m-1}\left(X-1-\xi_{3^m}^j-\xi_{3^m}^{a^{-1}j}\right) \tag{49}$$

because $1+\xi_{3^m}+\xi_{3^m}^a$ and $1+\xi_{3^m}+\xi_{3^m}^{a^{-1}}$ are conjugates (apply to $1+\xi_{3^m}+\xi_{3^m}^a$ the $\mathbb{Q}$-automorphism that sends ξ_{3^m} to $\xi_{3^m}^{a^{-1}}$). Therefore, once we choose $a\in T_m$ and calculate

$$\prod_{\gcd(j,3)=1}^{3^m-1}\left(X-1-\xi_{3^m}^j-\xi_{3^m}^{aj}\right)$$

we ignore the polynomial produced by choosing a^{-1}.

There is always the possibility that we choose an $a\in\mathbb{Z}_{3^m}^\times$ that is its own inverse. However, it is not hard to show that $x^2=1$ has only two solutions in $\mathbb{Z}_{3^m}$, i.e. ± 1 and $\pm 1\notin T_m$ by definition. Therefore, for every $a\in T_m$, we have that $a^{-1}\in T_m$ and $a\neq a^{-1}$. Since $|T_m| = 2\cdot 3^{m-1}-4$, write

$$T_m = \{a_1, a_2, \ldots, a_{3^{m-1}-2}, a_1^{-1}, a_2^{-1}, \ldots, a_{3^{m-1}-2}^{-1}\}.$$

and define V_m as

$$V_m := \{a_1, a_2, \ldots, a_{3^{m-1}-2}\}. \tag{50}$$

Then the polynomial

$$\prod_{m=1}^{r}\prod_{a\in V_m}\prod_{\gcd(j,3)=1}^{3^m-1}\left(X-1-\xi_{3^m}^{j}-\xi_{3^m}^{aj}\right) \tag{51}$$

divides $P_{3,k}(X)$.

All the information given so far can be put together to express $P_{3,k}(X)$ in terms of known polynomials. In particular, we have the following result.

Theorem 4. *Let $k>1$ be an integer and $r=\lfloor \log_3(k)\rfloor+1$. The sequence $\{S_{\mathbb{F}_3}(\boldsymbol{e}_{n,k})\}$ satisfies the homogeneous linear recurrence with integer coefficients whose characteristic polynomial is given by*

$$(X-3)\prod_{\ell=1}^{r}2^{2\cdot 3^{\ell-1}}\Phi_{3^\ell}\left(\frac{X-1}{2}\right)\prod_{\ell=1}^{r}\Phi_{3^\ell}(X-2)\prod_{m=2}^{r}\prod_{\ell=1}^{m-1}\prod_{\gcd(j,3)=1}^{3^\ell-1}\Phi_{3^m}(X-1-\xi_{3^\ell}^{j}) \tag{52}$$

$$\times\left(U_{(3^r-1)/2}\left(\frac{X-1}{2}\right)+U_{(3^r-3)/2}\left(\frac{X-1}{2}\right)\right)\prod_{\ell=1}^{r}\Phi_{2\cdot 3^\ell}(X-1)$$

$$\times\prod_{m=1}^{r}\prod_{a\in V_m}\prod_{\gcd(j,3)=1}^{3^m-1}\left(X-1-\xi_{3^m}^{j}-\xi_{3^m}^{aj}\right),$$

where $\xi_n=\exp(2\pi i/n)$, $\Phi_n(X)$ is the n-th cyclotomic polynomial and $U_n(X)$ is the n-th Chebyshev polynomial of the second kind.

For the general case, the results given in this article can be used to find a factor of the polynomial $P_{q,k}(X)$ in terms of known polynomials. A formula for $P_{k,q}(X)$ similar to the one provided on Theorem 4 remains open.

Acknowledgements. The research of the second author was supported by UPR-FIPI 7240022.00 and by The Puerto Rico Science, Technology and Research Trust (PRST) under agreement number 2020-00124. This content is only the responsibility of the authors and does not necessarily represent the official views of The Puerto Rico Science, Technology and Research Trust. The first, third and fourth authors were also supported as students by the same grant (PRST). The first author also acknowledges the support of the project PRLS-AMP. The fourth author also acknowledges the support of the Francis N. Castro Scholarship (NSF-DUE 2030188).

References

[1] O. Aberth, The elementary symmetric functions in a finite field of prime order, *Illinois J. Math.* **8**(1) (1964), 132-138.

[2] S. S. Abhyankar, S. D. Cohen, and M. E. Zieve, Bivariate factorizations connecting Dickson polynomials and Galois theory, *Trans. Amer. Math. Soc.* **352** (2000), 2871-2887.

[3] 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 Cusick, Li and P. Stănică, *Des. Codes, Cryptogr.* **86** (2018), 693-701.

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

[5] A. Canteaut and M. Videau, Symmetric Boolean functions, *IEEE Trans. Inf. Theory* **51**(8) (2005), 2791-2881.

[6] 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.

[7] F. N. Castro and L. A. Medina, Linear recurrences and asymptotic behavior of exponential sums of symmetric Boolean functions, *Electron. J. Combin.* **18** (2011), #P8.

[8] F. N. Castro and L. A. Medina, Asymptotic behavior of perturbations of symmetric functions, *Ann. Comb.* **18** (2014), 397-417.

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

[10] F. N. Castro, L. A. Medina, and P. Stănică, Generalized Walsh transforms of symmetric and rotation symmetric Boolean functions are linear recurrent, *Appl. Algebra Engrg. Comm. Comput.* **29**(5) (2018), 433-453.

[11] 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 Math.* **341**(7) (2018), 1915-1931.

[12] F. N. Castro, L. A. Medina, and L. B. Sepúlveda, Closed formulas for exponential sums of symmetric polynomials over Galois fields, *J. Algebraic Combin.* **50**(1) (2019), 73-98.

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

[14] T. W. Cusick, Y. Li, and P. Stănică, Balanced symmetric functions over $GF(p)$, *IEEE Trans. Inf. Theory* **54**(3) (2008), 1304-1307.

[15] Y. Hu and G. Xiao, Resilient functions over finite fields, *IEEE Trans. Inf. Theory* **49** (2003), 2040-2046.

[16] Y. Li and T. W. Cusick, Linear structures of symmetric functions over finite fields, *Inf. Processing Letters* **97** (2006), 124-127. structure

[17] Y. Li and T. W. Cusick, Strict avalanche criterion over finite fields, *J. Math. Cryptol.* **1**(1) (2007), 65-78.

[18] M. Liu, P. Lu and G.L. Mullen, Correlation-immune functions over finite fields, *IEEE Trans. Inf. Theory* **44** (1998), 1273-1276.

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