NEW FAMILIES OF BALANCED SYMMETRIC FUNCTIONS AND A GENERALIZATION OF CUSICK, LI AND STĂNICĂ'S CONJECTURE

RAFAEL A. ARCE-NAZARIO, FRANCIS N. CASTRO, OSCAR E. GONZÁLEZ, LUIS A. MEDINA, AND IVELISSE M. RUBIO

Abstract. In this paper we provide new families of balanced symmetric functions over any finite field. We also generalize a conjecture of Cusick, Li, and Stănică about the non-balancedness of elementary symmetric Boolean functions to any finite field and prove part of our conjecture.

1. Introduction

A function is said to be balanced if its values are equally distributed. This is an important property for functions that are used in cryptographic applications, so they are resistant to algebraic attacks. Much research has been done on balanced Boolean functions and some of the ideas have been extended to characteristic $p > 2$.

Symmetric functions are functions whose values remain the same when the entries of the inputs are permuted. This presents an advantage in implementation complexity and also for systems with memory constrains. In this paper we provide new families of balanced symmetric functions over finite fields of any characteristic.

In 2008, Cusick, Li and Stănică [10] presented a conjecture about the non-balancedness of elementary symmetric Boolean functions that can be phrased as follows:

Conjecture 1.1 (CLS, [10])**.** *The only nonlinear balanced elementary symmetric Boolean functions are those with degree $k = 2^l$ and $n = 2^{l+1}D - 1$ variables, where l, D are positive integers.*

Conjecture 1.1 essentially states that there are very few balanced elementary Boolean functions and gives precise formulas for the parameters n, k of these balanced functions. In [10, 9, 12, 14, 5], several cases of this conjecture are tackled. All the advances in proving the conjecture up to 2013 can be found in [14]. In 2015, many of the boundary cases of Cusick, Li and Stănică's conjecture were shown to be true in [4].

Some authors have been studying the balancedness of symmetric functions over finite fields of odd characteristic. In [10, 13, 11] lower bounds on the number of n-variable balanced symmetric functions over $\mathbb{F}_p$ were presented, but no explicit new families of balanced symmetric functions were given. In 2015, Arce-Nazario, Castro and Rubio [1, 2] generalized the conjecture of Cusick, Li and Stănică on Boolean elementary symmetric functions to elementary symmetric functions over $\mathbb{F}_p$.

Conjecture 1.2 (ACR, [2])**.** *The only nonlinear balanced elementary symmetric functions over $\mathbb{F}_p$ are those with degree $k = p^l$ and $n = p^l D - 1$ variables, where $l, D \in \mathbb{N}, D \not\equiv 1 \pmod p$.*

After getting partial results on this conjecture, we realized that it can be generalized to any finite field:

Conjecture 1.3. *The only nonlinear balanced elementary symmetric Boolean functions over $\mathbb{F}_q$, $q = p^f$ are those with degree $k = p^l$ and $n = p^l D - 1$ variables, where $l, D \in \mathbb{N}, D \not\equiv 1 \pmod p$.*

Conjecture 1.3 is an extension of Conjecture 1.1 because for $q = p = 2, D \not\equiv 1 \pmod 2$ implies that $n = 2^{l+1}D' - 1$, where $D' = \frac{D}{2}$ is a positive integer, and hence we obtain the original conjecture. Note that our conjecture only depends on the characteristic of the field, not on the degree of the extension. Hence, if Conjecture 1.3 were true, for a fixed p, the number nonlinear balanced elementary symmetric Boolean functions over is the same regardless of the size of the field.

We used computers to verify Conjecture 1.3 for the following cases:

Date: October 18, 2016.

2010 *Mathematics Subject Classification.* Primary 33E20 , 33B15.

Key words and phrases. Elementary symmetric functions, Balanced functions.

- $q = k = 3, \quad n \leq 85,000$;
- $q = 3, \quad k = 9, \quad n \leq 10,000$;
- $q = 3, \quad 2 \leq k \leq 50, \quad n \leq 650$;
- $q = 4, \quad k = 2, \quad n \leq 150,000$;
- $q = 4, \quad k = 4, \quad n \leq 50,000$;
- $q = k = 5, \quad n \leq 3000$;
- $3 \leq p \leq 11, \quad 2 \leq k \leq 10, \quad n \leq 100$.

In this paper we prove that the functions that are said to be balanced in Conjecture 1.3 are in fact balanced. This provides new families of balanced symmetric functions for $\mathbb{F}_{2^f}$, $f \neq 1$ and for any field of characteristic $p > 2$. We also show how the covering method of [3, 8] can be used to find many examples of specific families of non-balanced symmetric functions that confirm the conjecture.

2. Preliminaries

From now on, let p be a prime, $q = p^f$, $\mathbb{F}_q$ be the finite field with q elements, and $\mathbb{F}_q^n = \{(x_1, \ldots, x_n) \,|\, x_i \in \mathbb{F}_q, i = 1, \ldots, n\}$. Let $\mathbf{x} = (x_1, \ldots, x_n)$. We use capital letters X_i to represent variables in polynomials or functions, and lowercase letters x_i to represent the elements of a set.

Definition 2.1. A function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ is **balanced** if its values are uniformly distributed. This is, if F takes each value of $\mathbb{F}_q$ exactly q^{n-1} times.

The n-variable elementary symmetric function of degree k is

$$\sigma_{n,k} = \sigma_k(X_1, X_2, \ldots, X_n) = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} X_{i_1} \cdot X_{i_2} \cdots X_{i_k}.$$

To prove the balancedness of the functions prescribed by our conjecture we use the base p expansion of non-negative integers and Lucas' theorem.

The **base p expansion** of a non-negative integer k is $k = k_r p^r + \cdots + k_2 p^2 + k_1 p + k_0 = (k_r k_{r-1} \cdots k_1 k_0)_p$, where $0 \leq k_i < p$. The p-weight of k, $s_p(k)$, is defined as the sum of the digits in the base p expansion of k: $s_p(k) = k_0 + k_1 + \cdots + k_r$. The **exact p-divisibility** of a non-zero integer k, $v_p(k)$, is the exponent on the highest power of p dividing k. It is known that

$$\nu_p(k!) = \frac{k - s_p(k)}{p - 1}. \tag{2.1}$$

Theorem 2.2 (Lucas)**.** *Let p be a prime, and let n be a positive integer with $n = (n_r n_{r-1} \cdots n_0)_p$. Let k be a positive integer less than n. If $k = (k_r k_{r-1} \cdots k_0)_p$, then*

$$\binom{n}{k} \equiv \prod_{j=0}^{r} \binom{n_j}{k_j} \pmod{p},$$

where $\binom{0}{0} = 1$ and $\binom{n_j}{k_j} = 0$ if $n_j < k_j$.

The main tool that we use to prove the non-balancedness of some families of symmetric functions is exponential sums.

2.1. Exact p-divisibility of exponential sums to prove non-balancedness.

Let ζ be a primitive p-th root of unity over $\mathbb{Q}$, and $\mathrm{Tr} : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ be the trace map. The exponential sum associated to a function $F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ is

$$S(F) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} \zeta^{\mathrm{Tr}(F(\mathbf{x}))}.$$

If F is balanced, then $F(\mathbf{x}) = b \in \mathbb{F}_q$ for q^{n-1} elements $\mathbf{x} \in \mathbb{F}_q^n$ and $S(F) = q^{n-1} \sum_{b \in \mathbb{F}_q} \zeta^{\mathrm{Tr}(b)} = 0$.

If $S(F)$ has exact p-divisibility $\nu_p S(F)$ and $S(F) \neq 0$. Hence, if we can compute the exact p-divisibility of $S(F)$, we are proving that F is not balanced.

The covering method for polynomials over the prime field $\mathbb{F}_p$ was introduced in [3, 8] as an elementary method to compute exact p-divisibility of exponential sums. The elementary statements obtained in these papers have been extended in [7] to any field $\mathbb{F}_q$, but their proofs are not elementary. We now summarize the concepts and results that are needed for the proofs in Section 4.

Definition 2.3. Let $F(\mathbf{X}) = a_1F_1 + a_2F_2 + \cdots + a_NF_N$. A set $\mathcal{C} = \{F_1^{v_1}, \ldots, F_N^{v_N}\}$ of powers of the monomials in F is a $(q-1)$**-covering of** F if, in the product $F_1^{v_1} \cdots F_N^{v_N}$, the exponent of each variable is a positive multiple of $q-1$.

The **size** of the covering $\mathcal{C}$ is $\sum_{i=1}^{N} s_p(v_i)$. The covering is **minimal** if for any other $(q-1)$-covering $\mathcal{C}' = \left\{F_1^{v_1'}, \ldots, F_N^{v_N'}\right\}$ of F, $\sum_{i=1}^{N} s_p(v_i') \geq \sum_{i=1}^{N} s_p(v_i)$. We denote by $\kappa_{q-1}(F)$ the size of a minimal $(q-1)$-covering of F.

The next lemma is a generalization of Lemma 2.2 in [8]:

Lemma 2.4. *Suppose that each minimal $(q-1)$-covering $\mathcal{C}_i = \{F_1^{v_{i1}}, \ldots, F_N^{v_{iN}}\}$ of a polynomial $F = a_1F_1 + a_2F_2 + \cdots + a_NF_N$ is such that each monomial has at least two variables that are not included in any other monomial of $\mathcal{C}_i$. Let $\mathcal{C}_1, \ldots, \mathcal{C}_c$ be all the minimal $(q-1)$-coverings of F. If r_i is the number of $vij \neq 0$ for $j = 1, \ldots, N$, then*

$$\nu_p(S(F)) \text{ is } \begin{cases} = \kappa_{q-1}(F)/(p-1) & \text{if } \sum_{i=1}^{c} \frac{(-1)^{r_i} a_1^{v_{i1}} \cdots a_N^{v_{iN}}}{\rho(v_{i1}) \cdots \rho(v_{iN})} \not\equiv 0 \bmod p \\ > \kappa_{q-1}(F)/(p-1) & \text{otherwise} \end{cases},$$

where $\rho(a) = a_0!a_1! \cdots a_l!$ with $a = a_0 + a_1p + \cdots + a_lp^l$.

3. New families of balanced symmetric functions

In this section we provide new families of balanced symmetric functions for fields of any characteristic. This includes extension fields of characteristic 2 and hence extends the results in [10]. We first prove that all the functions that are said to be balanced in Conjecture 1.3 are in fact balanced.

Throughout this section, let $k = p^l$ and $n = p^lD - 1$, where $l, D \in \mathbb{N}$ and $D \not\equiv 1 \pmod{p}$. We begin with a lemma regarding the number of terms $\binom{n}{k} = \binom{p^lD-1}{p^l}$ in $\sigma_{n,k}$. The lemma applies to any $D \in \mathbb{N}$, but our usage will be restricted to $D \not\equiv 1 \pmod{p}$.

Lemma 3.1. *We have*

$$\binom{p^lD-1}{p^l} \equiv D - 1 \pmod{p}.$$

Proof. Let $D - 1 = a + hp$, where $0 \leq a \leq p-1, h \in \mathbb{Z}$. Then, $a \equiv D - 1 \pmod{p}$, and, by Lucas' theorem,

$$\binom{p^lD-1}{p^l} = \binom{hp^{l+1} + ap^l + (p^l - 1)}{p^l} \equiv \binom{a}{1} \equiv \binom{D-1}{1} \pmod{p}.$$

□

We need another preparatory lemma.

Lemma 3.2. *For $1 \leq r \leq k-1$, we have $\binom{n-r}{k-r} \equiv 0 \pmod{p}$.*

Proof. Since $D > 1$, we can write $D = D' + 1$ for some $D' \in \mathbb{N}$. Then,

$$\binom{n-r}{k-r} = \binom{p^lD' + \left(p^l - r - 1\right)}{p^l - r},$$

and, to apply Lucas' theorem, we need to compare the base p expansion of $p^l - r - 1$ and $p^l - r$.

Let $p^l - r = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_ip^i$, where $b_i \neq 0$. If $i = 0$, then, $p^l - r - 1 = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_0 - 1$. If $i > 0$, then, $p^l - r - 1 = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + (b_i - 1)\,p^i + a_{i-1}p^{i-1} + \cdots + a_1p + (p-1)$. In any case, there is a digit in the base p expansion of $p^l - r - 1$ that it is smaller than the corresponding digit in the base p expansion of $p^l - r$. Therefore, $\binom{n-r}{k-r} \equiv 0 \pmod{p}$. □

The key to prove that the functions in Conjecture 1.3 are balanced is Lemma 3.5 below, that relates $\sigma_{n,k}(X_1 + \alpha, \ldots, X_n + \alpha)$, $\alpha \in \mathbb{F}_q$, to $\sigma_{n,k}(X_1, X_2, \ldots, X_n)$. To prove Lemma 3.5 we need Corollary 3.4 that follows from the following known result about elementary symmetric functions.

Lemma 3.3 (Vieta)**.** *Let $\lambda \in \mathbb{F}_q^*$. Then,*

$$\prod_{j=1}^{m} (\lambda - X_j) = \lambda^m - \sigma_{m,1}\lambda^{m-1} + \sigma_{m,2}\lambda^{m-2} + \cdots + (-1)^m\sigma_{m,m}.$$

Writing $\prod_{j=1}^{m}(\lambda - X_j) = \sum_{j=0}^{m}(-1)^j \lambda^{m-j}\sigma_{m,j}$, and letting $\prod_{j=1}^{m}(X_j+\alpha) = -\prod_{j=1}^{m}(-\alpha - X_j)$, we get

Corollary 3.4. *Let $\alpha \in \mathbb{F}_q$. Then,*

$$\prod_{j=1}^{m}(X_j+\alpha) = \sum_{j=0}^{m}(-1)^{m+1}\alpha^{m-j}\sigma_{m,j}.$$

Lemma 3.5. *Let $\alpha \in \mathbb{F}_q$. Then,*

$$\sigma_k(X_1+\alpha,\ldots,X_n+\alpha) \equiv \sigma_k(X_1,\ldots,X_n) + (-1)^{p^l+1}(D-1)\alpha^k \pmod p.$$

Proof. Expanding

$$\begin{aligned}\sigma_k(X_1+\alpha,\ldots,X_n+\alpha) &= \sum_{1\le i_1<\cdots<i_k\le n}(X_{i_1}+\alpha)(X_{i_2}+\alpha)\cdots(X_{i_k}+\alpha)\\ &= \prod_{j=1}^{k}(X_{1i_j}+\alpha) + \prod_{j=1}^{k}(X_{2i_j}+\alpha) + \cdots + \prod_{j=1}^{k}\left(X_{\binom{n}{k}i_j}+\alpha\right), \qquad (3.1)\end{aligned}$$

where X_{hi_j} is the variable X_{i_j} in the h monomial of the sum in (3.1). Hence,

$$\begin{aligned}\sigma_k(X_1+\alpha,\ldots,X_n+\alpha) = \sum_{j=0}^{k}(-1)^{p^l+1}\alpha^{k-j}\sigma_j(X_{1i_1},\ldots,X_{1i_k}) + \cdots\\ + \sum_{j=0}^{k}(-1)^{p^l+1}\alpha^{k-j}\sigma_j\left(X_{\binom{n}{k}i_1},\ldots,X_{\binom{n}{k}i_k}\right). \qquad (3.2)\end{aligned}$$

For $j=0$ we get a term α^k in each of the $\binom{n}{k}$ terms of (3.2); which adds to $\binom{n}{k}\alpha^k$. Also, for $j=k$, we get a term $\sigma_k(X_{hi_1},\ldots,X_{hi_k})$ for each $1\le h\le\binom{n}{k}$; which adds to $\sigma_{n,k}$. Therefore, by Lemma 3.1,

$$\begin{aligned}\sigma_k(X_1+\alpha,\ldots,X_n+\alpha) &= \sigma_{n,k} + (-1)^{p^l+1}\binom{n}{k}\alpha^k + H\\ &\equiv \sigma_{n,k} + (-1)^{p^l+1}(D-1)\alpha^k + H \pmod p,\end{aligned}$$

where H are the terms in (3.2) with $0<j<k$. We now see that $H\equiv 0 \pmod p$.

First note that $X_{i_1}\cdots X_{i_r}$ is a monomial in H if and only if it is a term in $\sigma_r(X_{hi_1},\ldots,X_{hi_k})$ for some $1\le h\le\binom{n}{k}$ and $r<k$. This happens if and only if $X_{i_1}\cdots X_{i_r}$ divides a term of $\sigma_{n,k}$. The number of times that the term $X_{i_1}\cdots X_{i_r}$ appears in H is the number of terms in $\sigma_{n,k}$ that are divisible by $X_{i_1}\cdots X_{i_r}$. This is the same as the number of ways to choose $k-r$ variables from $n-r$ variables to obtain monomials of degree k with no repeated variables: $\binom{n-r}{k-r}$. This implies that the coefficient of each monomial in H is a multiple of $\binom{n-r}{k-r}$, and, by Lemma 3.2, $H\equiv 0 \pmod p$. □

Lemma 3.6. *Let $\alpha,\beta\in\mathbb{F}_q$. If $(a_1+\alpha,\ldots,a_n+\alpha)\neq(a_1+\beta,\ldots,a_n+\beta)$, then $\sigma_k(a_1+\alpha,\ldots,a_n+\alpha)\neq\sigma_k(a_1+\beta,\ldots,a_n+\beta)$.*

Proof. Suppose $\sigma_k(a_1+\alpha,\ldots,a_n+\alpha)=\sigma_k(a_1+\beta,\ldots,a_n+\beta)$. Then, by Lemma 3.5,

$$(-1)^{p^l+1}(D-1)\alpha^k \equiv (-1)^{p^l+1}(D-1)\beta^k \pmod p.$$

Since, $p\nmid(D-1)$ and $k=p^l$, we have that $p\mid(\alpha-\beta)^{p^l}$. Therefore, $\alpha=\beta$ and this is a contradiction. □

The next theorem proves that the functions predicted in Conjecture 1.3 to be balanced are in fact balanced. The theorem provides new families of balanced elementary symmetric functions for $\mathbb{F}_{2^f}$, $f\neq 1$ and for any field of characteristic $p>2$.

Theorem 3.7. *Let $k=p^l$ and $n=p^lD-1$, where $D\not\equiv 1 \pmod p$. Then, the function $\sigma_{n,k}:\mathbb{F}_q^n\longrightarrow\mathbb{F}_q$ is balanced.*

Proof. Let $(a_{11}, a_{12}, \ldots, a_{1n}) \in \mathbb{F}_q^{\,n}$ and $A_1 := \{(a_{11}+\alpha, a_{12}+\alpha, \ldots, a_{1n}+\alpha) \mid \alpha \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^{\,n}$. Then, by Lemma 3.5,

$$\sigma_k(a_{11}+\alpha, \ldots, a_{1n}+\alpha) \equiv \sigma_{n,k}(a_{11}, \ldots, a_{1n}) + (-1)^{p^l+1}(D-1)\alpha^k \pmod p.$$

By Lemma 3.6 all $\sigma_k(a_{11}+\alpha, \ldots, a_{1n}+\alpha)$ are different for each $\alpha \in \mathbb{F}_q$. This is,

$$V_1 := \{\sigma_k(a_{11}+\alpha, \ldots, a_{1n}+\alpha) \mid \alpha \in \mathbb{F}_q\} = \mathbb{F}_q.$$

Now consider $A_2 := \{(a_{21}+\alpha, a_{22}+\alpha, \ldots, a_{2n}+\alpha) \mid \alpha \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^{\,n}$, where $(a_{21}, a_{22}, \ldots, a_{2n}) \notin A_1$. Note that $A_1 \cap A_2 = \emptyset$. Similarly,

$$V_2 := \{\sigma_k(a_{21}+\alpha, \ldots, a_{2n}+\alpha) \mid \alpha \in \mathbb{F}_q\} = \mathbb{F}_q.$$

Continuing this process until $\cup_i A_i = \mathbb{F}_q^{\,n}$, we get q^{n-1} sets V_i,

$$\left\{\sigma_k(a_1, \ldots, a_n) \mid (a_1, \ldots, a_n) \in \mathbb{F}_q^{\,n}\right\} = \cup_{i=1}^{q^{n-1}} V_i,$$

and each element of $\mathbb{F}_q$ appears q^{n-1} times as an image of $\sigma_{n,k}$. This implies that $\sigma_{n,k}$ is balanced. □

The composition of the trace function with elementary symmetric functions provides more new families of balanced symmetric functions for the cases covered by Theorem 3.7.

Corollary 3.8. *Let $k = p^l$ and $n = p^l D - 1$, where $D \not\equiv 1 \pmod p$. Then, the function $Tr(\sigma_{n,k}) : \mathbb{F}_q^{\,n} \longrightarrow \mathbb{F}_p$ is balanced over $\mathbb{F}_p$ (each value of $\mathbb{F}_p$ is assumed p^{nf-1} times).*

4. Families of non-balanced elementary symmetric functions

The covering method of Section 2.1 can be used to find many examples of specific families of non-balanced elementary symmetric functions. In this section we present some of these examples.

Proposition 4.1. *Let $n = mk$. Then,*

$$\nu_p(S(\sigma_{n,k})) \text{ is } \begin{cases} = fm & ms_p(k) + s_p(m) = s_p(mk) + m, \\ \geq fm+1 & \text{otherwise.} \end{cases}$$

Proof. It is easy to see that any set of the form

$$\mathcal{C}_i = \left\{(X_{i_{11}} X_{i_{12}} \ldots X_{i_{1k}})^{q-1}, \cdots, (X_{i_{m1}} X_{i_{m2}} \cdots X_{i_{mk}})^{q-1}\right\},$$

where the $X_{i_{j1}} X_{i_{j2}} \cdots X_{j_{ik}}$ have disjoint support, form a minimal $(q-1)$-covering of $\sigma_{n,k}$. Since $q-1 = (p-1)\left(1 + p + \cdots + p^{f-1}\right)$, we have $s_p(q-1) = (p-1)f$, and $\kappa_{q-1}(\sigma_{n,k}) = (p-1)fm$.

By Lemma 2.4, $\nu_p(S(\sigma_{n,k})) = fm$ if and only if

$$\sum_{i=1}^{c} \frac{(-1)^m}{(\rho(q-1))^m} \equiv \frac{c(-1)^m}{(\rho(q-1))^m} \equiv \frac{c(-1)^m}{((p-1)!)^{fm}} \equiv c(-1)^f \not\equiv 0 \pmod p,$$

where c is the number of minimal $(q-1)$-coverings. A simple counting argument shows that the number of minimal coverings of $\sigma_{n,k}$ is

$$c = \frac{\binom{n}{k}\binom{n-k}{k}\binom{n-2k}{k}\cdots\binom{k}{k}}{m!} = \frac{n!}{(k!)^m m!}. \tag{4.1}$$

Now, $c(-1)^f \not\equiv 0 \pmod p$ if and only if $\nu_p\left(\frac{n!}{(k!)^m m!}\right) = 0$. Using (2.1),

$$\nu_p\left(\frac{n!}{(k!)^m m!}\right) = \frac{ms_p(k) + s_p(m) - s_p(mk) - m}{p-1},$$

and therefore $\nu_p(S(\sigma_{n,k})) = fm$ if and only if $ms_p(k) + s_p(m) - s_p(mk) - m = 0$. □

Corollary 4.2. *Let $n = mk$. Then $\sigma_{n,k}$ is non-balanced over $\mathbb{F}_q$ if $ms_p(k) + s_p(m) = s_p(mk) + m$.*

Example 4.3. Let $n = mk$. Then $\sigma_{n,k}$ is non-balanced over $\mathbb{F}_p$ whenever $k = p^s$,or $n < p$, or $m < p$ and $ms_p(k) = s_p(mk)$.

Proposition 4.4. *Let $n = mk + k - 1$. If $n < p$, then $\sigma_{n,k}$ is non-balanced over $\mathbb{F}_p$.*

Proof. The proof is similar to the proof of Proposition 4.1. Just note that the minimal $(q-1)$-coverings of $\sigma_{n,k}$ have the form

$$\mathcal{C}_i = \Big\{ \left(X_{i_{11}} X_{i_{12}} \dots X_{i_{1k}}\right)^{q-1}, \cdots, \left(X_{i_{m1}} X_{i_{m2}} \cdots X_{i_{mk}}\right)^{q-1}, \left(X_{i_{(m+1)1}} X_{i_{(m+1)2}} \cdots X_{i_{(m+1)k}}\right)^{q-1} \Big\},$$

where the $X_{i_{j1}} X_{i_{j2}} \cdots X_{j_{ik}}$ have disjoint support and the number of minimal coverings is

$$c = \frac{kmn!}{2m! \left(k!\right)^m (k-1)!}.$$

Since $n < p$, we can prove that $\nu_p(c) = 0$, and therefore $\nu_p\left(S(\sigma_{n,k})\right) = f(m+1)$ and $\sigma_{n,k}$ is not balanced. □

In similar ways, we can use the covering method to obtain many more families of unbalanced elementary symmetric functions. For example, the function $\sigma_{n,n-1}$ is non-balanced over $\mathbb{F}_p$, for $p \nmid n(n-3), p$ odd.

Also, using the techniques involving Stickelberger's theorem presented in [6] we can show that Propositions 4.1 and 4.4 are true for extensions of $\mathbb{F}_p$.

Acknowledgments. The third author was partially supported as a student by NSF-DUE 1356474 and the Mellon-Mays Undergraduate Fellowship. The fourth author acknowledges the partial support of UPR-FIPI 1890015.00.

References

[1] R. A. Arce-Nazario, F. N. Castro, and I. M. Rubio. Using the covering method to compute p-divisibility of exponential sums of polynomial deformations. Proposal to the National Security Agency, October 2014.
[2] R. A. Arce-Nazario, F. N. Castro, and I. M. Rubio. On a generalization of Cusick-Li-Stănică's conjecture about balanced elementary symmetric boolean functions. Talk given at the 12th International Conference on Finite Fields and Their Applications, July 2015.
[3] F. Castro and I. M. Rubio. Exact p-divisibility of exponential sums via the covering method. *Proc. Amer. Math. Soc.*, 143(3):1043–1056, 2015.
[4] F. N. Castro, O. E. González, and L. A. Medina. A divisibility approach to the open boundary cases of Cusick-Li-Stănică's conjecture. *Cryptogr. Commun.*, 7(4):379–402, 2015.
[5] F. N. Castro and L. A. Medina. Linear recurrences and asymptotic behavior of exponential sums of symmetric Boolean functions. *Electron. J. Combin.*, 18(2):Paper 8, 21, 2011.
[6] F. N. Castro, I. Rubio, and J. M. Vega. Divisibility of exponential sums and solvability of certain equations over finite fields. *The Quarterly Journal of Mathematics*, 60(2):169–181, 2009.
[7] F. N. Castro and I. M. Rubio. Extension of the covering method to any field (draft).
[8] F. N. Castro and I. M. Rubio. Construction of systems of polynomial equations with exact p-divisibility via the covering method. *J. Algebra Appl.*, 13(6):1450013, 15, 2014.
[9] T. Cusick, Y. Li, and P. Stănică. On a conjecture for balanced symmetric Boolean functions. *J. Math. Crypt.*, 3:1–18, 2009.
[10] T. W. Cusick, Y. Li, and P. Stănică. Balanced symmetric functions over GF(p). *IEEE Trans. on Information Theory*, 5:1304–1307, 2008.
[11] S. Fu, C. Li, K. Matsuura, and L. Qu. Enumeration of balanced symmetric functions over GF(p). *Inform. Process. Lett.*, 110(14-15):544–548, 2010.
[12] G. Gao, W. Liu, and X. Zhang. The degree of balanced elemetary symmetric Boolean functions of 4k + 3 variables. *IEEE Trans. on Information Theory*, 57:4822–4825, 2011.
[13] P. Ke, L. Huang, and S. Zhang. Improved lower bound on the number of balanced symmetric functions over GF(p). *Inform. Sci.*, 179(5):682–687, 2009.
[14] W. Su, X. Tang, and A. Pott. A note on a conjecture for balanced elementary symmetric Boolean functions. *IEEE Trans. on Information Theory*, 59:665–671, 2013.

Department of Computer Science, University of Puerto Rico, San Juan, PR 00931
E-mail address: rafael.arce@upr.edu

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

Department of Mathematics, University of Puerto Rico, San Juan, PR 00931
E-mail address: oscar.gonzalez3@upr.edu

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

Department of Computer Science, University of Puerto Rico, San Juan, PR 00931
E-mail address: iverubio@gmail.com