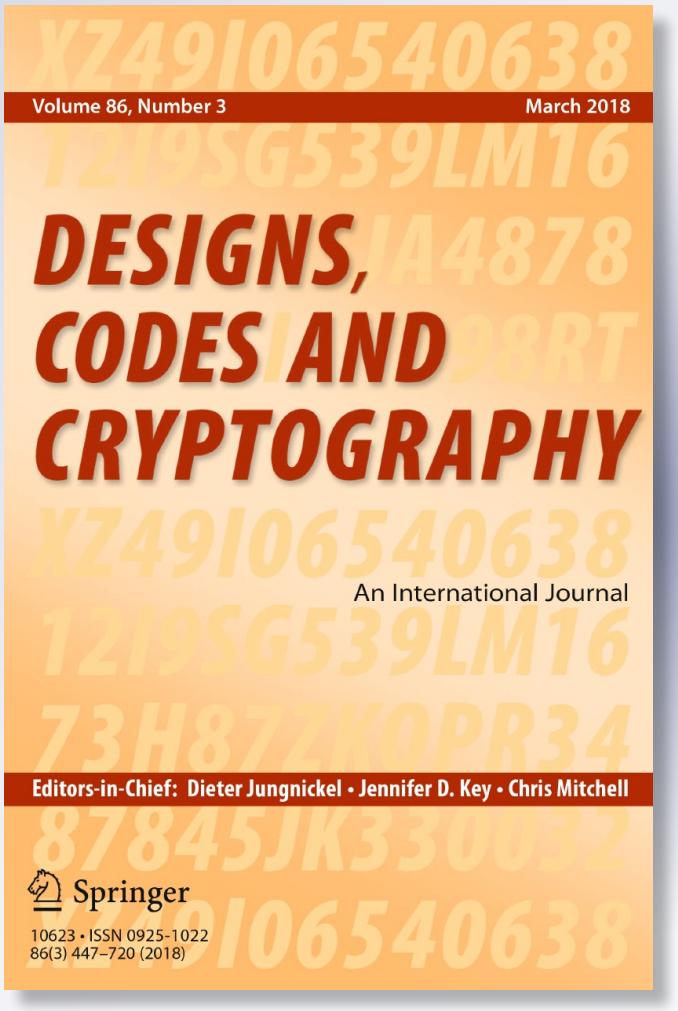
New families of balanced symmetric functions and a generalization of Cusick, Li and St#nic#'s conjecture

Rafael A. Arce-Nazario, Francis N. Castro, Oscar E. González, Luis A. Medina & Ivelisse M. Rubio

Designs, Codes and Cryptography
An International Journal

ISSN 0925-1022
Volume 86
Number 3

Des. Codes Cryptogr. (2018) 86:693-701
DOI 10.1007/s10623-017-0351-7



Springer

Des. Codes Cryptogr. (2018) 86:693–701
https://doi.org/10.1007/s10623-017-0351-7

New families of balanced symmetric functions and a generalization of Cusick, Li and Stănică's conjecture

Rafael A. Arce-Nazario[1] · Francis N. Castro[2] · Oscar E. González[2] · Luis A. Medina[2] · Ivelisse M. Rubio[1]

Received: 27 August 2016 / Revised: 1 March 2017 / Accepted: 4 March 2017 /
Published online: 11 March 2017

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.

Keywords Elementary symmetric functions · Balanced functions

Mathematics Subject Classification 33E20 · 33B15

1 Introduction

A function is said to be balanced if its values are equally distributed. This is a desirable property for functions that are used in cryptographic applications. 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. These functions can be represented in compact ways, reducing the amount of memory needed for storing and simplifying hardware implementations. Hence, the use of symmetric functions presents advantages in implementation, specially in environments with limited resources. In this paper we provide new families of balanced symmetric functions over finite fields of any characteristic.

Communicated by A. Pott.

✉ Francis N. Castro
franciscastr@gmail.com

[1] Department of Computer Science, University of Puerto Rico, PO Box 70377, San Juan, PR 00936-8377, USA

[2] Department of Mathematics, University of Puerto Rico, PO Box 70377, San Juan, PR 00936-8377, USA

In 2008, Cusick, Li and Stănică [9] presented a conjecture about the non-balancedness of elementary symmetric Boolean functions that can be phrased as follows:

Conjecture 1 (CLS, [9]) *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 essentially states that there are very few balanced elementary symmetric Boolean functions and gives precise formulas for the parameters n, k of these balanced functions. In [4,8,9,11,15], several cases of this conjecture are tackled. All the advances in proving the conjecture up to 2013 can be found in [15]. In 2015, many of the boundary cases of Cusick, Li and Stănică's conjecture were shown to be true as reported in [3].

Some authors have been studying the balancedness of symmetric functions over finite fields of odd characteristic. In [9,10,13] 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 et al. [1,2] generalized the conjecture of Cusick, Li and Stănică on Boolean elementary symmetric functions to elementary symmetric functions over $\mathbb{F}_p$.

Conjecture 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 could be generalized to any finite field:

Conjecture 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 3 is an extension of Conjecture 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 3 were true, for a fixed p, the number of nonlinear balanced elementary symmetric Boolean functions over a field of characteristic p is the same, regardless of the size of the field.

We used computers to verify Conjecture 3 for the following cases:

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

In this paper we prove that the functions that are said to be balanced in Conjecture 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 [6,7] 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 $\mathbb{F}_q^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{F}_q, i = 1, \ldots, n\}$. 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 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

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

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 $0 \le k_i < p$. 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, $\nu_p(k)$, is the exponent on the highest power of p dividing k. It is known that

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

The exact p-divisibility can be extended to $\mathbb{Q}$ via

$$\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b). \tag{2}$$

It can also be extended to $\mathbb{Q}(\zeta)$, where ζ is a p-root of unity. See [12,14] for more details.

Theorem 1 *(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 a, one has that $p^{a+1} \nmid S(F)$ 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 [6,7] as an elementary method to compute exact p-divisibility of exponential sums. The elementary statements obtained in these papers were extended in [5] 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 Sect. 4.

Definition 2 Let $F(\mathbf{X}) = a_1F_1 + a_2F_2 + \cdots + a_NF_N \in \mathbb{F}_q[\mathbf{X}]$ be a polynomial that contains all the n variables, and the F_i's are monomials. A set $\mathcal{C} = \left\{F_1^{v_1}, \ldots, F_N^{v_N}\right\}$ of powers of the monomials in F is a $(q-1)$**-covering of** F if, in the product $F_1^{v_1} \ldots F_N^{v_N}$, the exponent of each variable is a positive multiple of $q-1$.

Remark 1 Some of the exponents v_i of the monomials in the covering might be equal to zero. Sometimes, if $v_i = 0$, we do not include the monomial $F_i^{v_i}$ in the covering.

Example 1 Let

$$F(\mathbf{X}) = X_1^2X_2^3X_3^3 + X_1^3X_2^3X_3^3 + X_4^2X_5^2 + X_1X_4^3X_5^3 \in \mathbb{F}_7[X_1, \ldots, X_5].$$

Then, $\mathcal{C}_1 = \left\{\left(X_1^2X_2^3X_3^3\right)^6, \left(X_4^2X_5^2\right)^3\right\}$, $\mathcal{C}_2 = \left\{\left(X_1^2X_2^3X_3^3\right)^2, \left(X_1X_4^3X_5^3\right)^2\right\}$, $\mathcal{C}_3 = \left\{\left(X_1^3X_2^3X_3^3\right)^2, \left(X_4^2X_5^2\right)^3\right\}$ are some of the 6-coverings of F.

A $(q-1)$-covering of a polynomial $F = a_1F_1 + a_2F_2 + \cdots + a_NF_N$ always exists: we can take as covering the set $\mathcal{C} = \left\{F_1^{q-1}, \ldots, F_N^{q-1}\right\}$. 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, $\sum_{i=1}^N s_p\left(v_i'\right) \geq \sum_{i=1}^N s_p(v_i)$. We denote by $\kappa_{q-1}(F)$ the size of a minimal $(q-1)$-covering of F.

The next lemma is a generalization of [6, Lemma 2.2]. We do not include the proof here because it requires some more background and we want to keep the focus of the paper on Conjecture 3. A proof can be found in [5].

Lemma 1 *Let $F(\mathbf{X}) : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $F = a_1F_1 + a_2F_2 + \cdots + a_NF_N$ be a polynomial with coefficients in $\mathbb{F}_p$. Suppose that each minimal $(q-1)$-covering $\mathcal{C}_i = \{F_1^{v_{i1}}, \ldots, F_N^{v_{iN}}\}$ of F 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 $v_{ij} = q-1$ for $j = 1, \ldots, N$, then*

$$v_p(S(F)) \begin{cases} = \kappa_{q-1}(F)/(p-1) \ \text{ if } \ \sum_{i=1}^c (-1)^{fr_i} \dfrac{\prod_{j=1}^N a_j^{v_{ij}}}{\prod_{v_{ij} \neq q-1} \rho(v_{ij})} \not\equiv 0 \pmod{p} \\ > \kappa_{q-1}(F)/(p-1) \ \text{ otherwise,} \end{cases}$$

where $\rho(k) = k_0!k_1! \cdots k_l!$ with $k = k_0 + k_1p + \cdots + k_lp^l$.

Remark 2 Since $S(F) \in \mathbb{Q}(\zeta)$, we are working with the extension of $v_p(\cdot)$ and $v_p(S(F))$ might not be an integer.

Example 2 Consider the polynomial F of Example 1. The size of $\mathcal{C}_1$ is 9, the size of $\mathcal{C}_2$ is 4, and the size of $\mathcal{C}_3$ is 5. The unique minimal covering of F is $\mathcal{C}_2$. Note that $\left(X_1^2X_2^3X_3^3\right)^2$ contains the variables X_2, X_3, which are not contained in $\left(X_1X_4^3X_5^3\right)^2$, and $\left(X_1X_4^3X_5^3\right)^2$

contains the variables X_4, X_5, which are not contained in $\left(X_1^2 X_2^3 X_3^3\right)^2$. Therefore, the exact p-divisibility of F is $\frac{4}{6}$.

The next example shows that, if we drop the condition of each monomial in the covering having at least two variables that are not contained in the set of other monomials in the covering, we cannot guarantee exact p-divisibility.

Example 3 Consider $F(\mathbf{X}) = X_1X_2+X_1+X_2+X_3 \in \mathbb{F}_2[X_1, X_2, X_3]$. The unique minimal covering of F is $\mathcal{C} = \{X_1X_2, X_3\}$. Note that, since $S(F) = 0$, we have $\nu_2(S(F)) \neq 2$, even with F having a unique minimal covering.

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 [9]. We first prove that all the functions that are said to be balanced in Conjecture 3 are in fact balanced.

Throughout this section, let $k = p^l$ and $n = p^l D - 1$, where $l, D \in \mathbb{N}$ and $D \not\equiv 1 \pmod{p}$. We begin with a lemma regarding the number of terms $\binom{n}{k} = \binom{p^l D-1}{p^l}$ 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 2 *We have*

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

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,

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

□

We need another preparatory lemma.

Lemma 3 *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,

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

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

Let $p^l - r = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_i p^i$, 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, $p^l - r - 1 = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + (b_i - 1)\, p^i + a_{i-1}p^{i-1} + \cdots + a_1 p + (p - 1)$. 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 3 are balanced is Lemma 5 below, which 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 5 we need Corollary 1 which follows from the following known result about elementary symmetric functions.

Lemma 4 (Vieta) *Let $\lambda \in \mathbb{F}_q^*$. Then,*

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

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

Corollary 1 *Let $\alpha \in \mathbb{F}_q$. Then,*

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

Lemma 5 *Let $\alpha \in \mathbb{F}_q$. Then,*

$$\sigma_k\left(X_1 + \alpha, \ldots, X_n + \alpha\right) = \sigma_k\left(X_1, \ldots, X_n\right) + (D-1)\alpha^k$$

Proof Expanding

$$\begin{aligned}\sigma_k\left(X_1 + \alpha, \ldots, X_n + \alpha\right) &= \sum_{1 \le i_1 < \cdots < i_k \le n} \left(X_{i_1} + \alpha\right)\left(X_{i_2} + \alpha\right) \cdots \left(X_{i_k} + \alpha\right) \\ &= \prod_{j=1}^{k} \left(X_{1 i_j} + \alpha\right) + \prod_{j=1}^{k} \left(X_{2 i_j} + \alpha\right) + \cdots + \prod_{j=1}^{k} \left(X_{\binom{n}{k} i_j} + \alpha\right), \end{aligned} \tag{3}$$

where $X_{h i_j}$ is the variable X_{i_j} in the h monomial of the sum in (3). Hence,

$$\begin{aligned}\sigma_k\left(X_1 + \alpha, \ldots, X_n + \alpha\right) = &\sum_{j=0}^{k} \alpha^{k-j} \sigma_j\left(X_{1 i_1}, \ldots, X_{1 i_k}\right) \\ &+ \cdots + \sum_{j=0}^{k} \alpha^{k-j} \sigma_j\left(X_{\binom{n}{k} i_1}, \ldots, X_{\binom{n}{k} i_k}\right). \end{aligned} \tag{4}$$

For $j = 0$ we get a term α^k in each of the $\binom{n}{k}$ terms of (4); which adds to $\binom{n}{k}\alpha^k$. Also, for $j = k$, we get a term $\sigma_k\left(X_{h i_1}, \ldots, X_{h i_k}\right)$ for each $1 \le h \le \binom{n}{k}$; which adds to $\sigma_{n,k}$. Therefore, by Lemma 2,

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

where H are the terms in (4) with $0 < j < k$. We now see that $H = 0$ in $\mathbb{F}_q$.

First note that $X_{i_1} \cdots X_{i_r}$ is a monomial in H if and only if it is a term in $\sigma_r\left(X_{h i_1}, \ldots, X_{h i_k}\right)$ 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, $H = 0$. □

Lemma 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 5,

$$(D-1)\alpha^k = (D-1)\beta^k.$$

Since $p \nmid (D-1)$ and $k = p^l$, we have that $(\alpha-\beta)^{p^l} = 0$ in $\mathbb{F}_q$. Therefore, $\alpha = \beta$ and this is a contradiction. □

The next theorem proves that the functions predicted in Conjecture 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 2 *Let* $k = p^l$ *and* $n = p^l D - 1$, *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 5,

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

By Lemma 6 all $\sigma_k(a_{11}+\alpha, \ldots, a_{1n}+\alpha)$ are different for each $\alpha \in \mathbb{F}_q$. That is,

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

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

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

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 2.

Corollary 2 *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 Sect. 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 1 *Let* $n = mk$, *and* $\sigma_{n,k}$ *an elementary symmetric function in* $\mathbb{F}_q$. *Then,*

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

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

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

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 1, $v_p\left(S\left(\sigma_{n,k}\right)\right) = fm$ if and only if $\sum_{i=1}^{c}(-1)^{fm} \equiv c(-1)^{fm} \not\equiv 0 \pmod{p}$, 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

$$c = \frac{\binom{n}{k}\binom{n-k}{k}\binom{n-2k}{k}\cdots\binom{k}{k}}{m!} = \frac{n!}{(k!)^m m!}. \tag{5}$$

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

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

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

Corollary 3 *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 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 2 *Let $n = mk + k - 1$. If $n < q$, then $\sigma_{n,k}$ is non-balanced over $\mathbb{F}_q$.*

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

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

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

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

Since $n < p$, p does not divide any factor of c, $v_p(c) = 0$, and therefore $v_p\left(S(\sigma_{n,k})\right) = f(m+1)$ and $\sigma_{n,k}$ is not balanced. □

Acknowledgements The authors appreciate the comments and suggestions to the paper made by one of the referees and the additional suggestions and a correction made by Alexander Pott. All of them helped to improve the paper. 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. Arce-Nazario R.A., Castro F.N., Rubio I.M.: Using the covering method to compute p-divisibility of exponential sums of polynomial deformations. Proposal to the National Security Agency (2014).

2. Arce-Nazario R.A., Castro F.N., Rubio I.M.: On a generalization of Cusick-Li-Stănică's conjecture about balanced elementary symmetric Boolean functions. In: Talk given at the 12th International Conference on Finite Fields and Their Applications (2015).
3. Castro F.N., González O.E., Medina L.A.: A divisibility approach to the open boundary cases of Cusick-Li-Stănică's conjecture. Cryptogr. Commun. **7**(4), 379–402 (2015).
4. Castro F.N., Medina L.A.: Linear recurrences and asymptotic behavior of exponential sums of symmetric Boolean functions. Electron. J. Combin. **18**(2), 8,21 (2011).
5. Castro, F.N., Rubio I.M.: Extension of the covering method to any finite field (pre-print), https://franciscastr.files.wordpress.com/2016/01/covering-q-1.
6. Castro F.N., Rubio I.M.: Construction of systems of polynomial equations with exact p-divisibility via the covering method. J. Algebra Appl. **13**(6), 1450013,15 (2014).
7. Castro F.N., Rubio I.M.: Exact p-divisibility of exponential sums via the covering method. Proc. Am. Math. Soc. **143**(3), 1043–1056 (2015).
8. Cusick T., Li Y., Stănică P.: On a conjecture for balanced symmetric Boolean functions. J. Math. Crypt. **3**, 1–18 (2009).
9. Cusick T.W., Li Y., Stănică P.: Balanced symmetric functions over GF(p). IEEE Trans. Inf. Theory **5**, 1304–1307 (2008).
10. Fu S., Li C., Matsuura K., Qu L.: Enumeration of balanced symmetric functions over GF(p). Inform. Process. Lett. **110**(14–15), 544–548 (2010).
11. Gao G., Liu W., Zhang X.: The degree of balanced elemetary symmetric Boolean functions of 4k + 3 variables. IEEE Trans. Inf. Theory **57**, 4822–4825 (2011).
12. Ireland K., Rosen M.: A Classical Introduction to Modern Number Theory, 2nd edn. Springer, New York (1990).
13. Ke P., Huang L., Zhang S.: Improved lower bound on the number of balanced symmetric functions over GF(p). Inf. Sci. **179**(5), 682–687 (2009).
14. Moreno O., Shum K., Castro F.N., Kumar P.V.: Tight bounds for Chevalley-Warning-Ax type estimates, with improved applications. Proc. Lond. Math. Soc. **88**, 545–564 (2004).
15. Su W., Tang X., Pott A.: A note on a conjecture for balanced elementary symmetric Boolean functions. IEEE Trans. Inf. Theory **59**, 665–671 (2013).