EXACT 2-DIVISIBILITY OF EXPONENTIAL SUMS ASSOCIATED TO BOOLEAN FUNCTIONS

FRANCIS N. CASTRO, LUIS A. MEDINA, AND IVELISSE M. RUBIO

Abstract. In this paper we extend the covering method for computing the exact 2-divisibility of exponential sums of Boolean functions, improve results on the divisibility of the Hamming weight of deformations of Boolean functions, and provide criteria to obtain non-balanced functions. In particular, we present criteria to determine cosets of Reed-Muller codes that do not contain any balanced function, and to construct deformations of symmetric functions that are not balanced. The use of the covering method together with classifications of cosets of Reed-Muller codes obtained by the action of linear groups can improve the search of balanced functions in Reed-Muller codes dramatically.

1. Introduction

The divisibility of exponential sums has been used to characterize and prove properties in coding theory and cryptography (see [3], [14], [20], [22], [23], [24], [26]). The computation of bounds or the exact 2-divisibility of exponential sums of Boolean functions gives information on the Hamming weight of the function, and can be used to obtain information on the covering radius and the weight distribution of certain codes, which are properties that are important for the analysis of decoding algorithms. Moreover, these properties are also related to cryptography as they can be used to study the non-linearity and balancedness of Boolean functions.

In general, algebraic methods to estimate the p-divisibility of exponential sums over finite fields are non-elementary. The covering method [5, 8, 9, 10, 23, 24] provides an elementary and intuitive way to estimate or compute the exact p-divisibility of exponential sums, which is particularly convenient in the applications. For example, the use of the covering method together with classifications of cosets of Reed-Muller codes obtained by the action of linear groups [18] can improve the search of balanced functions in Reed-Muller codes dramatically.

In this paper we follow the approach in [10] and extend the results of [8] to study the exact 2-divisibility of exponential sums of polynomials whose minimal coverings might not be unique. The paper is self contained and the results provide an elementary condition on the minimal coverings that allows us to construct families of Boolean functions for which the "greater than or equal to" relation obtained in the classical results on 2-divisibility is replaced by either equality or strict inequality. In addition to study families of non balanced functions, we study and, in certain cases improve, the 2-divisibility of the difference of the Hamming weights of the Boolean functions F and deformations $F+G$, refining a version of Katz's theorem for Boolean functions obtained by Canteaut in [3].

2. Preliminaries

Let $\mathbb{F}$ be the binary field, $\mathbb{F}^n = \{(x_1, \ldots, x_n) \,|\, x_i \in \mathbb{F}, i = 1, \ldots, n\}$, and $F = F(x_1, \ldots, x_n)$ be a polynomial in n variables over $\mathbb{F}$. Sometimes we use $\mathbf{x}$ instead of $(x_1, \ldots, x_n)$. Without loss of generality, we assume throughout the rest of the paper that F is not a polynomial in some subset of the variables $x_1, \ldots, x_n$.

Any Boolean function $f : \mathbb{F}^n \longrightarrow \mathbb{F}$ can be identified with a unique Boolean polynomial $F = x_{11}^{e_{11}} \cdots x_{n1}^{e_{n1}} + \cdots + x_{1N}^{e_{1N}} \cdots x_{nN}^{e_{nN}}$, where $e_{ij} \in \{0, 1\}$. The exponential sum of a polynomial F over $\mathbb{F}$ is $S(F) = \sum_{\mathbf{x} \in \mathbb{F}^n} (-1)^{F(\mathbf{x})}$.

Our aim is to compute the highest power of 2 dividing $S(F)$ and apply the results to the computation of Hamming weights, and to the determination of deformed Boolean functions that are not balanced. In general, if m is a non-zero integer, we denote this highest power of 2 by $\nu_2(m)$, where $m = 2^{\nu_2(m)}a$ and a is not divisible by 2. We also refer to $\nu_2(m)$ as the *exact 2-divisibility* of m.

Date: August 27, 2017.

2010 *Mathematics Subject Classification.* 05E05, 11T23, 06E30.

Key words and phrases. 2-divisibility, Hamming weight, exponential sums, balanced Boolean functions, Reed-Muller codes.

One of the advantages of working over $\mathbb{F}$ is the identities $(-1)^{\mathbf{x}} = 1 - 2\mathbf{x}$, $\mathbf{x}^d = \mathbf{x}$, where $d > 0$, $\mathbf{x} \in \mathbb{F}^n$. Therefore

$$S(F) = \sum_{\mathbf{x}\in\mathbb{F}^n} (-1)^{F(\mathbf{x})} = 2^n + \sum_{\lambda} (-2)^{m_\lambda} \sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x}). \tag{2.1}$$

Here, $(-2)^{m_\lambda} f_\lambda(\mathbf{x})$ are monomials that are products of all possible choices of terms $2x_{1i}^{e_{1i}} \cdots x_{ni}^{e_{ni}}$ in the factors $1 - 2x_{1i}^{e_{1i}} \cdots x_{ni}^{e_{ni}}$ and m_λ is the number of terms in that choice. It is clear that

$$\nu_2\left(S(F)\right) \geq \nu_2\left(\sum_{\lambda} (-2)^{m_\lambda} \sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})\right).$$

It is important to note that

$$\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x}) = 2^l,$$

where l is the number of variables that are missing in f_λ. Hence, the exact 2-divisibility of $S(F)$ can be determined if we are able to "control" the smallest sets of monomials of F needed to cover all the variables.

Definition 2.1. Let $\mathcal{C}$ be a minimal set of monomials of F covering all variables. This is, every variable x_i is in at least one monomial of $\mathcal{C}$, and $\mathcal{C}$ is minimal with this property. We call this set $\mathcal{C}$ a *minimal covering* of F.

Example 2.2. For $F = x_1x_2x_3 + x_1x_2x_4 + x_1x_4 + x_2x_4 \in \mathbb{F}[x_1, \ldots, x_4]$, $\{x_1x_2x_3, x_1x_4\}$ and $\{x_1x_2x_3, x_1x_2x_4\}$ are minimal coverings of cardinality 2.

In [24], Moreno-Moreno used minimal coverings to prove the following improvement to the binary Ax's theorem [2]. In Section 3 we refine this theorem by providing sufficient conditions for the exponential sum of a Boolean polynomial to have exact 2-divisibility.

Theorem 2.3. *Let F be a polynomial over $\mathbb{F}$ and $\mathcal{C}$ be a minimal covering of F. Then,*

$$\nu_2\left(S(F)\right) \geq |C|.$$

3. Using coverings to compute the 2-divisibility of exponential sums

To obtain the results in this paper we need to study the 2-divisibility of the terms $\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})$ in the expansion of the exponential sum of F (2.1). In Lemma 3.1, proved in [8], we present conditions so that the only term $\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})$ that is not divisible by $2^{|\mathcal{C}|+1}$ is the term where f_λ is the product of all the monomials in $\mathcal{C}$, where $\mathcal{C}$ is a minimal covering of F. This result, together with Lemma 3.2, will allow us to determine the exact 2-divisibility of the exponential sum of F or to improve the existing bounds.

Lemma 3.1. *Let F be a polynomial over $\mathbb{F}$, and $\mathcal{C}$ be a minimal covering of F such that each monomial in $\mathcal{C}$ has at least two variables that are not contained in any of the other monomials in $\mathcal{C}$. With the notation of (2.1), if f_λ is a product of $m_\lambda < |\mathcal{C}|$ monomials in $\mathcal{C}$, then*

$$2^{|\mathcal{C}|+1} \mid 2^{m_\lambda} \sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x}).$$

Lemma 3.2. *Let F be a polynomial over $\mathbb{F}$, and $\mathcal{C}_1, \ldots, \mathcal{C}_c$ be all the minimal coverings of F. With the notation of (2.1), if f_λ is a product of m_λ monomials in F such that not all of them belong to the same minimal covering $\mathcal{C}_i$, then*

$$2^{|\mathcal{C}_i|+1} \mid 2^{m_\lambda} \sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x}).$$

Proof. If $m_\lambda > |\mathcal{C}_i|$ the result is clear. Let $T = 2^{m_\lambda} \sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})$ be such that f_λ is a product of $m_\lambda \leq |\mathcal{C}_i|$ monomials in F and not all of them belong to the same minimal covering. If $m_\lambda = |\mathcal{C}_i|$, then f_λ misses at least one variable because otherwise the monomials in the product would form another minimal covering of F. Therefore $2^{|\mathcal{C}_i|+1} \mid T$.

If $m_\lambda < |\mathcal{C}_i|$, then f_λ misses $l \geq |\mathcal{C}_i| - m_\lambda + 1$ variables. Otherwise, if $l \leq |\mathcal{C}_i| - m_\lambda$, one can construct a covering $\mathcal{C}'$ of F in the following way: for each missing variable in f_λ, we select a monomial in $\mathcal{C}_1$ containing the missing variable (it could happen that the same monomial in $\mathcal{C}_1$ contains more than one of the missing

variables). The new covering $\mathcal{C}'$ is the set of all the m_λ monomials of F that formed f_λ and at most $l \leq |\mathcal{C}_i| - m_\lambda$ monomials from the covering $\mathcal{C}_1$ containing the missing variables. This implies that $|\mathcal{C}'| \leq m_\lambda + |\mathcal{C}_i| - m_\lambda = |\mathcal{C}_i|$. If $|\mathcal{C}'| = |\mathcal{C}_i|$, then, since the coverings $\mathcal{C}_1, \ldots, \mathcal{C}_c$ are all the minimal coverings, $\mathcal{C}' = \mathcal{C}_j$, for some $1 \leq j \leq c$, and the monomials that formed f_λ would all be from the same covering, which is a contradiction. If $|\mathcal{C}'| < |\mathcal{C}_i|$, we found a covering smaller than the minimal, which is also a contradiction. □

□

The estimates on the p-divisibility of exponential sums over finite fields given by the results of Ax [2] and Katz [21] are general and tight in the sense that there are examples that attain their bounds. This implies that improvements are possible only if additional conditions are imposed. For example, by considering the binary case and using the covering method Moreno and Moreno were able to improve Ax's result [24].

In the next theorem, the simple condition of each monomial in $\mathcal{C}_i$ having at least two variables that are not contained in the other monomials of $\mathcal{C}_i$ provides families of Boolean functions for which the "greater than or equal to" relation obtained in the classical results on 2-divisibility is replaced by either equality or strict inequality. This key result is a generalization of Proposition 3.3 in [8] and it allows us to construct families of non-balanced functions.

Theorem 3.3. *Let F be a polynomial over $\mathbb{F}$, and $\mathcal{C}_1, \ldots, \mathcal{C}_c$ be all the minimal coverings of F. If, for any $1 \leq i \leq c$, each monomial in $\mathcal{C}_i$ has at least two variables that are not contained in the other monomials of $\mathcal{C}_i$, then $\nu_2(S(F)) = |\mathcal{C}_i|$ if c is odd, and otherwise $\nu_2(S(F)) \geq |\mathcal{C}_i| + 1$.*

Proof. Products of the monomials f_λ in each covering produce terms in (2.1) with

$$2^{m_\lambda} \sum_{\mathbf{x} \in \mathbb{F}^n} f_\lambda(\mathbf{x}) = 2^{|\mathcal{C}_i|} \sum_{\mathbf{x} \in \mathbb{F}^n} x_1 \cdots x_n = 2^{|\mathcal{C}_i|}.$$

Using Lemmas 3.1 and 3.2 we see that combinations of any other monomials produce terms with

$$2^{m_\lambda} \sum_{\mathbf{x} \in \mathbb{F}^n} f_\lambda(\mathbf{x}) = 2^{a_\lambda},$$

where $a_\lambda > |\mathcal{C}_i|$. Therefore,

$$S(F) = 2^n + 2^{|\mathcal{C}_i|} \cdot c + \sum_\lambda 2^{a_\lambda}, \ a_\lambda > |\mathcal{C}_i|$$

and the result follows. □ □

The above theorem refines Moreno-Moreno's Theorem 2.3 in certain cases. With it, if one can guarantee that a Boolean polynomial F has an odd number of minimal coverings with certain property, then one can compute the exact 2-divisibility of $S(F)$. Although, in general, it is not an easy task to find all the minimal coverings of a given polynomial, one can easily construct polynomials for which one knows all the minimal coverings and hence knows the exact 2-divisibility. We do this in Section 4 for several families of polynomials. In particular, in Subsection 4.1.1 we use this method to construct cosets of Reed-Muller codes that do not contain any balanced function and reduce the search for balanced functions dramatically.

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, we cannot guarantee the exact 2-divisibility of $S(F)$.

Example 3.4. Consider $F = x_1 \cdots x_{n-1} + x_1 + \cdots + x_n$. This polynomial has exactly one minimal covering (of cardinality 2) but, since $S(F) = 0$, $\nu_2(S(F)) \neq 2$.

3.1. **2-Divisibility of deformations.** Sometimes the 2-divisibility of the exponential sum of a deformation $F + G$ of a polynomial F can be obtained by only studying the 2-divisibility of the exponential sum of F. By providing conditions on the coverings we can obtain information about families of polynomials $F + G_i$ by just studying the polynomial F. This can be used to study cosets of certain sets of polynomials, as we do in Section 4. We now study the 2-divisibility of deformations of Boolean functions $F + G$ and, in Subsection 3.2, apply the results to compare the Hamming weights of Boolean functions F to the Hamming weight of deformations $F + G$. In Section 4 we apply the results to Reed-Muller codes and symmetric functions to determine non-balanced functions.

Theorem 3.5. *Let F and G be Boolean functions. Suppose that the minimal coverings of F are the minimal coverings of $F+G$ and each monomial in a minimal covering C_F has at least two variables that are not contained in the other monomials of C_F. Then,*

$$S(F+G) \equiv S(F) \pmod{2^{|\mathcal{C}_F|+1}}.$$

Moreover, if the number of minimal coverings is odd, then

$$\nu_2\left(S(F+G)\right) = \nu_2\left(S(F)\right) = |\mathcal{C}_F|.$$

Proof. Suppose that the minimal coverings of $F+G$ and F are the same and each monomial in a minimal covering has at least two variables that are not contained in the other monomials. If the number of minimal coverings of F is odd, then, by Theorem 3.3,

$$\nu_2\left(S(F+G)\right) = \nu_2\left(S(F)\right) = |\mathcal{C}_F|.$$

This implies that

$$S(F) = 2^{|\mathcal{C}_F|}k_F \text{ and } S(F+G) = 2^{|\mathcal{C}_F|}k_{F+G},$$

where k_F, k_{F+G} are odd numbers. Therefore

$$S(F) - S(F+G) = 2^{|C_F|}\left(k_{F+G} - k_F\right) = 2^{|C_F|+1}k,$$

$k \in \mathbb{Z}$, because $k_{F+G} - k_F$ is an even number. Hence, $S(F+G) \equiv S(F) \pmod{2^{|\mathcal{C}_F|+1}}$.

If the number of minimal coverings is even, Theorem 3.3 implies that $2^{|C_F|+1}$ divides $S(F)$ and $S(F+G)$. Hence, $S(F+G) \equiv S(F) \pmod{2^{|\mathcal{C}_F|+1}}$. □ □

If the number of minimal coverings of F is odd, Theorem 3.5 provides conditions so that the 2-divisibility of $S(F+G) - S(F)$ is greater than the 2-divisibility of $S(F)$. In [19, Theorem 1.2], using a result from [4], Hou presented a characterization for when the 2-divisibility of $S(F+G) - S(F)$ is greater than the 2-divisibility of $S(F)$, where G is a linear polynomial. It is important to note that the method in [19] depends on the deformation $F+G$ being done by a linear polynomial G, whereas in Theorem 3.5, G is not restricted to be linear. Also, Theorem 3.5 provides conditions for when $\nu_2\left(S(F+G)\right) = \nu_2\left(S(F)\right) = |\mathcal{C}_F|$, and get that $F+G$ is non-balanced.

The intuitive and simple condition of the deformations having the same coverings as the original function has useful applications to the determination of non-balanced functions. This will be seen in Theorem 4.2 and Corollary 4.3, which are applied in Example 4.4 to explain the non existence of balanced functions in certain cosets of Reed-Muller codes, and answers a question of Cusick and Cheon [11].

To get more precise approximations of the 2-divisibility of deformations one has to study the terms of the expansion of the exponential sum of specific deformations as we do in the next proposition.

Proposition 3.6. *Let F and G be Boolean functions where G is linear and no term of G is a term in F. Suppose that $\mathcal{C}_1, \ldots, \mathcal{C}_c$ are all the minimal coverings of F. If, for any $1 \le i \le c$, each monomial in $\mathcal{C}_i$ has at least two variables that are not contained in the other monomials of $\mathcal{C}_i$, and if any set of $|\mathcal{C}_i|$ or less monomials of $F+G$ does not cover $n-1$ variables unless they form a minimal covering, then $\nu_2\left(S(F+G) - S(F)\right) = |\mathcal{C}_i| + 1$ if c and the number of terms in G are odd, and otherwise $\nu_2\left(S(F+G) - S(F)\right) \ge |\mathcal{C}_i| + 2$.*

Proof. Using the notation of (2.1) we have

$$\begin{aligned} S(F+G) &= 2^n + \left[\sum_{\lambda}(-2)^{m_\lambda}\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})\right] + \left[\sum_{\lambda'}(-2)^{m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} g_{\lambda'}(\mathbf{x})\right] + \\ &\quad + \left[\sum_{\substack{\lambda \\ m_\lambda \ge 1}}\sum_{\substack{\lambda' \\ m_{\lambda'} \ge 1}} (-2)^{m_\lambda + m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})g_{\lambda'}(\mathbf{x})\right] \\ &= S(F) + \sum_{\lambda'}(-2)^{m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} g_{\lambda'}(\mathbf{x}) + \sum_{\substack{\lambda \\ m_\lambda \ge 1}}\sum_{\substack{\lambda' \\ m_{\lambda'} \ge 1}} (-2)^{m_\lambda + m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})g_{\lambda'}(\mathbf{x}). \end{aligned}$$

Therefore, $\nu_2\left(S(F+G)-S(F)\right)$

$$= \nu_2\left(\sum_{\lambda'}(-2)^{m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} g_{\lambda'}(\mathbf{x}) + \sum_{\substack{\lambda\\ m_\lambda\geq 1}}\sum_{\substack{\lambda'\\ m_{\lambda'}\geq 1}}(-2)^{m_\lambda+m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})g_{\lambda'}(\mathbf{x})\right).$$

If $m_\lambda + m_{\lambda'} \geq |\mathcal{C}_i|+2$, it is clear that

$$\nu_2\left((-2)^{m_\lambda+m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})g_{\lambda'}(\mathbf{x})\right) \geq |C_i|+2.$$

Suppose that $m_\lambda + m_{\lambda'} < |\mathcal{C}_i|+1$. Then $f_\lambda g_{\lambda'}$ misses at least $|\mathcal{C}_i|+2-m_\lambda-m_{\lambda'}$ variables. Otherwise it misses at most $|\mathcal{C}_i|+1-m_\lambda-m_{\lambda'}$ variables. In this case, we could construct a set $\mathcal{C}$ with the monomials in $f_\lambda g_{\lambda'}$, and $|\mathcal{C}_i|-m_\lambda-m_{\lambda'}$ monomials from a covering $\mathcal{C}_i$, each of them containing at least a missing variable. This set $\mathcal{C}$ would have $|\mathcal{C}_i|$ monomials that cover at least $n-1$ variables. If $\mathcal{C}$ is not a covering, there is a contradiction to the assumption that any set of $|\mathcal{C}_i|$ or less monomials do not cover $n-1$ variables. If $\mathcal{C}$ forms a covering, it would be minimal and contains a monomial of G, contradicting that each monomial in any minimal covering contains at least two variables that are not contained in the other monomials. Therefore, $f_\lambda g_{\lambda'}$ misses at least $|\mathcal{C}_i|+2-m_\lambda-m_{\lambda'}$ variables and

$$\nu_2\left((-2)^{m_\lambda+m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})g_{\lambda'}(\mathbf{x})\right) \geq m_\lambda+m_{\lambda'}+|\mathcal{C}_i|+2-m_\lambda-m_{\lambda'} = |\mathcal{C}_i|+2.$$

Suppose that $m_\lambda + m_{\lambda'} = |\mathcal{C}_i|+1$ and the monomials in f_λ do not form a covering. Then, the monomials in $f_\lambda g_{\lambda'}$ cannot cover all the variables. Otherwise, we could remove a monomial from $g_{\lambda'}$, and with the remaining monomials and the monomials in f_λ, form a set with $|\mathcal{C}_i|$ monomials from that cover $n-1$ variables and do not form a covering. This contradicts one of the hypotheses. Therefore, there is at least one variable missing in $f_\lambda g_{\lambda'}$, and

$$\nu_2\left((-2)^{m_\lambda+m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})g_{\lambda'}(\mathbf{x})\right) \geq m_\lambda+m_{\lambda'}+1 = |\mathcal{C}_i|+2.$$

The only missing case is when $m_\lambda + m_{\lambda'} = |\mathcal{C}_i|+1$ and the monomials in f_λ cover all the variables. This implies $m_\lambda = |C_i|$, $m_{\lambda'}=1$, and the monomials in f_λ are the monomials in a minimal covering $\mathcal{C}_i$. Then

$$(-2)^{m_\lambda+m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})g_{\lambda'}(\mathbf{x}) = (-2)^{|C_i|+1}.$$

Adding all the terms involving at least one monomial from F we have that

$$\sum_{\lambda}\sum_{\lambda'}(-2)^{m_\lambda+m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} f_\lambda(\mathbf{x})g_{\lambda'}(\mathbf{x}) = (a)(c)2^{|\mathcal{C}_i|+1}+2^{|\mathcal{C}_i|+2}k,$$

where a is the number of terms in G and c is the number of minimal coverings of F.

Now, since G is linear, $g_{\lambda'}$ is missing exactly $n-m_{\lambda'}$ variables and $n=\nu_2\left(\sum_{\lambda'}(-2)^{m_{\lambda'}}\sum_{\mathbf{x}\in\mathbb{F}^n} g_{\lambda'}(\mathbf{x})\right)$. This implies that $\nu_2\left(S(F+G)-S(F)\right) = |C_i|+1$ if and only if c and the number of terms in G are odd. Otherwise we get $\nu_2\left(S(F+G)-S(F)\right)\geq |C_i|+2$. □ □

3.2. **Application to Hamming weights of F and deformations $F+G$.** The Hamming weight of Boolean functions is an important property used in applications to coding theory and cryptography. The *Hamming weight associated with* F, $w(F)$, is the number of $\mathbf{x}\in\mathbb{F}^n$ such that $F(\mathbf{x})=1$. If $w_0(F)$ is the number of $\mathbf{x}\in\mathbb{F}^n$ such that $F(\mathbf{x})=0$, then

$$S(F) = w_0(F) - w(F)$$

and

$$2^n = w(F)+w_0(F).$$

This implies that

$$w(F) = 2^{n-1} - \frac{1}{2}S(F),$$

and this gives a correspondence between results on exponential sums and Hamming weights of Boolean functions.

In [3], Canteaut used the next result to study the weight distribution of cosets of first-order Reed-Muller codes.

Theorem 3.7 (Canteaut). *Let F, G be Boolean functions of degrees d_1 and d_2 respectively, $d_2 < d_1$. Then, $w(F+G) \equiv w(F) \pmod{2^{\lceil \frac{n-d_2}{d_1} \rceil}}$.*

As we mentioned before, estimates on the p-divisibility of exponential sums over finite fields given by the results of Ax [2] and Katz [21] are general and tight in the sense that there are examples that attain their bounds. This implies that improvements are only possible only if some additional conditions are imposed. Canteaut's result is a refinement of Katz's theorem for the Boolean case, and tight for this case. The result can only be improved by imposing additional conditions as we do next.

Using that

$$w(F+G) - w(F) = -\frac{1}{2}\left(S(F+G) - S(F)\right),$$

we have $S(F+G) \equiv S(F) \pmod{2^r}$ if and only if $w(F+G) \equiv w(F) \pmod{2^{r-1}}$, and the results in Section 3.1 can be used to estimate the Hamming weight of deformations. The next results are direct consequences of Theorem 3.5 and Proposition 3.6.

Theorem 3.8. *Let F and G be Boolean functions. Suppose that the minimal coverings of F are the minimal coverings of $F+G$ and each monomial in a minimal covering C_F has at least two variables that are not contained in the other monomials of C_F. Then,*

$$w(F+G) \equiv w(F) \pmod{2^{|\mathcal{C}_F|}}.$$

Moreover, if the number of minimal coverings is odd, then

$$\nu_2\left(w(F+G)\right) = \nu_2\left(w(F)\right) = |\mathcal{C}_F| - 1.$$

Since $|\mathcal{C}_F| \geq \lceil \frac{n-d_2}{d_1} \rceil$, there are cases when the above result improves Theorem 3.7 as it is illustrated in the next example.

Example 3.9. Consider

$$F = x_1x_2x_3x_4 + x_3x_4x_5 + x_5x_6x_7 + x_7x_8x_9$$

and

$$G = x_1 + \cdots + x_9.$$

Both F and $F+G$ have the same unique minimal covering

$$\mathcal{C} = \{x_1x_2x_3x_4, x_5x_6x_7, x_7x_8x_9\}.$$

Theorem 3.8 gives $w(F+G) \equiv w(F) \pmod 8$, but Theorem 3.7 gives $w(F+G) \equiv w(F) \pmod 4$. Moreover, we get that the exact 2-divisibility of $w(F+G)$ is 2. It can be verified that $w(F) = 132$, $w(F+G) = 260$ and $w(F+G) - w(F) = 2^7$.

In some special cases one can refine the results by obtaining exact divisibility or improving the divisibility obtained in previous results.

Proposition 3.10. *Let F and G be Boolean functions where G is linear and no term of G is a term in F. Suppose that $\mathcal{C}_1, \ldots, \mathcal{C}_c$ are all the minimal coverings of F. If, for any $1 \leq i \leq c$, each monomial in $\mathcal{C}_i$ has at least two variables that are not contained in the other monomials of $\mathcal{C}_i$, and if any set of $|\mathcal{C}_i|$ or less monomials of $F+G$ does not cover $n-1$ variables unless they form a minimal covering, then*

$$\nu_2\left(w(F+G) - w(F)\right) = |\mathcal{C}_F|$$

if c and the number of terms in G are odd, and otherwise $\nu_2\left(w(F+G) - w(F)\right) \geq |\mathcal{C}_F| + 1$.

Example 3.11. Consider the polynomial F of degree 5 and $n = 11$ variables,

$$F = x_1x_2x_3x_4x_5 + x_4x_5x_6 + x_1x_2x_7 + x_8x_9x_{10} + x_6x_7x_{11}$$

and

$$F + G_{a_1,\ldots,a_{10},a_{11}} = x_1x_2x_3x_4x_5 + x_4x_5x_6 + x_1x_2x_7 + x_8x_9x_{10} + x_6x_7x_{11} + \sum_{i=1}^{11} a_ix_i.$$

We have

$$w(F+G)-w(F)\in\{216,264,312,360,376,392,408,424,456,504\}$$

whenever $\sum_{i=1}^{11}a_i$ is odd, and

$$w(F+G)-w(F)\in\{288=2^5\cdot 9, 336=2^4\cdot 21, 368=2^4\cdot 23, 384=2^7\cdot 3,$$
$$400=2^4\cdot 25, 416=2^5\cdot 13, 432=2^4\cdot 27, 480=2^5\cdot 15, 528=2^4\cdot 33\}.$$

if $\sum_{i=1}^{11}a_i$ is even. Note that Proposition 3.10 predicts the 2-divisibility of

$$\nu_2\left(w(F+G)-w(F)\right)=3$$

if $\sum_{i=1}^{11}a_i$ is odd and

$$\nu_2\left(w(F+G)-w(F)\right)\geq 4$$

if $\sum_{i=1}^{11}a_i$ is even. Note that, in the latter case, $\nu_2(w(F+G)-w(F))\in\{4,5,7\}$.

Corollary 3.12. *Let $F=F_1+\cdots+F_r$ be such that the F_i's are monomials of disjoint support, of degree greater than or equal to 2, and G be linear. Then, $\nu_2\left(w(F+G)-w(F)\right)=r$ if the number of terms in G is odd, and otherwise $\nu_2\left(w(F+G)-w(F)\right)\geq r+1$.*

4. Non-balanced functions in Reed-Muller codes and symmetric functions

A Boolean function F in n variables is said to be *balanced* if the function is equal to one in half of the values of $\mathbf{x}\in\mathbb{F}^n$. It is easy to see that this happens if and only if $S(F)=0$. If one can compute the exact 2-divisibility of $S(F)$, then $S(F)\neq 0$ and F is not balanced. Hence, if one can describe Boolean functions satisfying some of the conditions of Theorem 3.3, one is describing Boolean functions that are not balanced.

4.1. **Families of non-balanced functions in Reed-Muller codes.** The *k-th order Reed-Muller code of length 2^n*, $R(k,n)$, can be identified with the set of Boolean functions in n variables and degree less than or equal to k. A Boolean function in $R(k,n)$ is balanced if and only if its Hamming weight is 2^{n-1}. Much work has been done studying the weight distribution of these codes but no general formula is known for $3\leq k\leq n-4$.

The 2-divisibility of the elements in cosets of first-order Reed-Muller codes has been studied in many papers, for example [3, 16, 17]. In [18] Hou counted the number of orbits when the general linear group $GL(n,2)$ acts on $R(k,n)/R(k-1,n)$ for $6\leq n\leq 11$. Cosets of $R(k-1,n)$ belonging to the same orbit have the same weight distribution and hence the same number of balanced functions. This implies that to know the number of balanced functions of all the cosets in an orbit, it is enough to study a coset representative for the orbit. In the same paper, Hou presented representatives for each of the different orbits in $R(k,n)/R(k-1,n)$ for $k=3,\ 6\leq n\leq 8$.

The next example illustrates how one can use classifications of cosets and Theorem 3.3 to limit the search for balanced functions in $R(k,n)/R(k-1,n)$.

Example 4.1. Consider the classification of the cosets of $R(3,8)/R(2,8)$ presented in Table 2 of [18]. By inspection, we can identify 15 coset representatives where at least half of the functions in each coset are not balanced and provide constructions for these non-balanced functions. To illustrate some of the constructions, let $1\leq a_i,b_i\leq n$ and $G(x_{a_1}x_{b_1},x_{a_2}x_{b_2},\ldots,x_{a_t}x_{b_t})\in R(2,n)$ be a polynomial that does not have $x_{a_i}x_{b_i}$ as a term for $1\leq i\leq t$.

(1) Let F_6 be the representative of an orbit of $R(3,8)/R(2,8)$ included in Table 2 of [18]: $F_6=x_1x_2x_3+x_1x_4x_5+x_2x_4x_6+x_3x_5x_6+x_4x_5x_6$. Then, any polynomial of the form $F_6'=F_6+x_7x_8+G(x_7x_8)$ has a unique minimal covering $\mathcal{C}=\{x_1x_2x_3,x_4x_5x_6,x_7x_8\}$. Theorem 3.3 implies that $\nu_2\left(S(F_6')\right)=3$, and therefore F_6' is not balanced. There are $2^{\binom{8}{2}-1+\binom{8}{1}}=2^{35}$ non-balanced polynomials of this form associated to F_6.

(2) Let F_{15} be the representative of an orbit of $R(3,8)/R(2,8)$ included in Table 2 of [18]: $F_{15}=x_1x_2x_3+x_2x_4x_5+x_6x_7x_8+x_1x_4x_7$. Then, any polynomial of the form $F_{15}'=F_{15}+G(x_4x_5,x_1x_3)$ has a unique minimal covering $\mathcal{C}=\{x_1x_2x_3,x_2x_4x_5,x_6x_7x_8\}$. Therefore F_{15}' is not balanced and there are $2^{\binom{8}{2}-2+\binom{8}{1}}=2^{34}$ polynomials of this form.

Also, any polynomial of the form $F_{15}''=F_{15}+x_1x_3+x_4x_5+G(x_4x_5,x_1x_3)$ has exactly three minimal coverings $\mathcal{C}_1=\{x_1x_2x_3,x_2x_4x_5,x_6x_7x_8\}$, $\mathcal{C}_2=\{x_2x_4x_5,x_6x_7x_8,x_1x_3\}$, $\mathcal{C}_3=\{x_2x_4x_5,x_6x_7x_8,x_4x_5\}$.

Therefore F''_{15} is not balanced and there are $2^{\binom{8}{2}-2+\binom{8}{1}} = 2^{34}$ non-balanced polynomials of this form. There are 2^{35} non-balanced polynomials of the form F'_{15} or F''_{15} associated to the representative F_{15}.

Note that the form of the non-balanced polynomials can be used, together with the group action, to determine what types of polynomials to avoid in the search for balanced functions.

One can give general descriptions of functions in cosets of Reed-Muller codes that are not balanced as is illustrated in the next theorem.

Theorem 4.2. *Let $k \geq 2$, $n = ks + r$, $r = 0$ or $2 \leq r < k$. Let $F_1, \ldots, F_s$ be monomials of degree k and disjoint support, $M = \{x_{i_1}, \ldots, x_{i_r}\}$ be the set of variables not covered by any monomial $F_1, \ldots, F_s$, and H_{m_i} be a monomial of degree k_i, $r \leq k_i < k$ that contains all the variables in M. Let F be a polynomial where each term does not contain at least one of the variables in M, $\deg(F) \leq k$, and each term of F has at least one variable in common with any other term in $F+F_i$, for $1 \leq i \leq s$. If $F' = F_1+\cdots+F_s+H_{m_1}+\cdots+H_{m_h}+F \in R(k,n)$, for h an odd integer, and $x_{i_1}x_{i_2}\cdots x_{i_r}$ is not a term in $G \in R(k-l,n)$, where $1 \leq k-l \leq r$ if $r \neq 0$, then $F'+G$ is not balanced.*

Proof. If $r = 0$, then $\mathcal{C} = \{F_1, \ldots, F_s\}$ is the unique minimal covering of F'. If $2 \leq r < k$, then $\mathcal{C}_i = \{F_1, \ldots, F_s, H_{m_i}\}$ forms a minimal covering of F' for each $1 \leq i \leq h$. Any covering containing monomials from F will not be minimal. The number of minimal coverings of F is odd because h is odd.

Since $\deg(G) < k$, any minimal covering of $F'+G \in F'+R(k-l,n)$ will contain $F_1, \ldots, F_s$. Since $X_{i_1}X_{i_2}\cdots X_{i_r}$ is not a term in G, no single term of G will contribute the r missing variables and we would need more than one term from G to form a covering of $F'+G$. Therefore, any covering of $F'+G$ that includes terms from G cannot be minimal. This implies that the minimal coverings of F' and $F'+G$ are the same. Since each monomial in the covering contributes at least two new variables, and the number of minimal coverings is odd, by Theorem 3.5, $\nu_2(S(F'+G)) = |\mathcal{C}_i|$ and therefore $F'+G$ is not balanced. □ □

4.1.1. *Cosets of Reed-Muller codes that do not contain any balanced function.* A coset $F + R(k-1,n)$ of $R(k,n)/R(k-1,n)$ is a set of deformations of the Boolean function F. Combining classifications of the cosets in $R(k,n)/R(k-1,n)$ with the results in Section 3 one can improve the search for balanced functions dramatically. Cusick and Cheon [11] studied the number of balanced functions in representatives of the cosets of $R(k,n)/R(k-1,n)$ for $k = 3, n = 6, 7$. They found interesting to note the "uneven distribution of the balanced functions in the cosets of $R(2,6)$ (where two cosets have no balanced functions at all), ...". If one can describe Boolean functions F such that $F+G$ satisfy the conditions of Theorem 3.5 for all $G \in R(k-l,n)$, one gets that the coset $F+R(k-l,n)$ does not contain any balanced function. The next Corollary explains the behavior noticed by Cusick and Cheon, and, in general, can be used to determine a priori cosets that do not contain any balanced functions, saving computational time.

Corollary 4.3. *Suppose that $F' = F_1+\cdots+F_s+H_{m_1}+\cdots+H_{m_h}+F \in R(k,n)$, satisfies the conditions of Theorem 4.2. Then, the coset $F'+R(k-l,n) \in R(k,n)/R(k-l,n)$ does not contain any balanced function, where $1 \leq k-l < r$ if $r \neq 0$.*

Proof. Just note that, since $k-l$ is strictly less than r, $x_{i_1}x_{i_2}\cdots x_{i_r}$ is not a monomial in G for any $G \in R(k-l,n)$. □ □

This corollary can be used to construct cosets that do not contain any balanced function, as we see in the next example.

Example 4.4. Inspecting Table 1 of [11] one notices that $F_4 = x_1x_2x_3+x_4x_5x_6$ and $F_6 = x_1x_2x_3+x_4x_5x_6+x_1x_4x_5+x_2x_4x_6+x_3x_5x_6$ satisfy the conditions of the previous corollary and hence, the cosets $F_4+R(2,6)$ and $F_6+R(2,6)$ do not contain any balanced functions. This explains the behavior noticed by Cusick and Cheon. Note that these are 2 of the 6 cosets of $R(3,6)/R(2,6)$ in the classification in [18]. Any other coset in their orbits will behave in the same way. From (6.16) in [18] we get that 523,776 of the 1,048,576 cosets in $R(3,6)/R(2,6)$ do not contain any balanced functions; almost half of the search for balanced functions could have been avoided by using the covering method.

Corollary 4.5. *Suppose that $n = ks, k \geq 2$, $l \geq 1$. Then, any coset of the form $F_1+\cdots+F_s+R(k-l,n)$, where $F_1, \ldots, F_s$ are monomials of degree k and disjoint support, does not contain any balanced function.*

It is not difficult to find other sufficient conditions that guarantee cosets of Reed-Muller codes that do not contain any balanced function. Constructing polynomials with certain minimal coverings gives lower bounds on the number of cosets in $R(k,n)/R(k-l,n)$ that consist only of non-balanced functions.

Example 4.6. Let $k \geq 2,\ n = 2k$ and $c = \dfrac{\binom{2k}{k}}{2}$. Then, there are at least

$$2^{c-1} + \sum_{j=0}^{\lfloor \frac{c-1}{2} \rfloor} \binom{c}{2j+1} \left(\binom{2k}{k} - 4j - 2 \right)$$

cosets in $R(k,2k)/R(k-1,2k)$ that do not contain any balanced functions.

4.2. **Deformations of elementary symmetric Boolean functions that are not balanced.** Symmetric Boolean functions in n variables are Boolean functions whose value do not depend on the permutation of its input. These functions are simpler to study and easier to implement. Elementary symmetric Boolean functions are the building blocks for all symmetric Boolean functions. There is a unique elementary symmetric Boolean function $\sigma_{n,k}$ in n variables and degree k. From now on, $k \geq 2$ and we use σ_k to denote $\sigma_{n,k}$. This is, $\sigma_k = \sigma_{n,k} = \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq n} x_{j_1} \cdots x_{j_k}$.

It has been proved that almost all the elementary symmetric Boolean functions are non-balanced ([6], [7], [12], [13], [15], [25]), and Cusick-Li-Stănică conjectured that the only nonlinear balanced elementary symmetric Boolean functions are of degree $k = 2^t$ and have $n = 2^{t+1}D - 1$ variables, where D is odd. This conjecture has been generalized to fields of any characteristic in [1].

To use the covering method to provide families of deformations $F = \sigma_k + G$ of elementary symmetric Boolean functions that are non-balanced, we need to find conditions so that the minimal coverings of $F = \sigma_k + G$ and σ_k are the same. We also need to compute the number of minimal coverings of σ_k. Imposing conditions on the degree of G we can easily obtain that the minimal coverings of $F = \sigma_k + G$ and σ_k are the same.

Lemma 4.7. *Let $n = ks + r,\ k, s > 1,\ 0 \leq r < k$, and $F = \sigma_k + G$. Suppose that $\deg(G) < k$ if $k \mid n$, and $\deg(G) < r$ if $k \nmid n$. Then $\mathcal{C}$ is a minimal covering of F if and only if $\mathcal{C}$ is a minimal covering of σ_k.*

In general, it is hard to count the number of minimal coverings for arbitrary σ_k. But writing $n = ks + r$, where $0 \leq r < k$, one can divide the problem in cases and find sufficient conditions so that one can compute the number of minimal coverings. We illustrate this by presenting results when $r = 0, k-1$.

Lemma 4.8. *Let $n = ks,\ k, s > 1$. The number of minimal coverings of σ_k is*

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

Using the 2-divisibility of c, Lemma 4.7, and Theorem 3.3, one can prove the next results.

Proposition 4.9. *Let $n = ks,\ k, s > 1$, and $F = y\sigma_k(x_{m+1}, \cdots, x_{m+n}) + G$, where $y = 1$ if $m = 0$ and otherwise $y = x_1 \cdots x_m$, and $\deg(G) < k+m$. Then, $\nu_2(S(F)) = s$ if $k = 2^l$, and otherwise $\nu_2(S(F)) \geq s+1$. In particular, if $k = 2^l$, then F is not balanced.*

Suppose that $n = ks + k - 1$, where $s \geq 1, k > 2$, and consider $F = \sigma_k + G$, where $\deg(G) < k - 1$. With a counting argument we get that number of minimal coverings of σ_k is

$$c = \frac{ks\binom{n}{k}\binom{n-k}{k}\binom{n-2k}{k}\cdots\binom{2k-1}{k}}{2(s!)} = \frac{ks(n!)}{2(s!)(k!)^s(k-1)!}.$$

Proposition 4.10. *Let $n = ks + k - 1,\ s \geq 1,\ k > 2$, and $F = y\sigma_k(x_{m+1}, \cdots, x_{m+n}) + G$, where $y = 1$ if $m = 0$ and otherwise $y = x_1 \cdots x_m$, and $\deg(G) < k + m - 1$. Then, $\nu_2(S(F)) = 2$ if $k = 2^l + 1$ and $s = 1$, and otherwise $\nu_2(S(F)) \geq s + 2$. In particular, if $k = 2^l + 1$ and $s = 1$, then F is not balanced.*

Acknowledgments. The authors appreciate the comments and suggestions to the paper made the referees. They helped us to improve and clarify the presentation of our results.

References

[1] Rafael A Arce-Nazario, Francis N Castro, Oscar E González, Luis A Medina, and Ivelisse M Rubio. New families of balanced symmetric functions and a generalization of Cusick, Li and Stănică's conjecture. *Designs, Codes and Cryptography. (2017). doi: 10.1007/s10623-017-0351-7.*

[2] James Ax. Zeroes of polynomials over finite fields. *Amer. J. Math.*, 86:255–261, 1964.

[3] Anne Canteaut. On the weight distributions of optimal cosets of the first-order Reed-Muller codes. *IEEE Trans. Inform. Theory*, 47(1):407–413, 2001.

[4] Claude Carlet and Philippe Guillot. A new representation of Boolean functions. In *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, volume 1719 of *Lecture Notes in Comput. Sci.*, pages 94–103. Springer, Berlin, 1999.

[5] Francis Castro and Ivelisse M. Rubio. Exact p-divisibility of exponential sums via the covering method. *Proc. Amer. Math. Soc.*, 143(3):1043–1056, 2015.

[6] Francis N. Castro, Oscar E. González, and Luis A. Medina. A divisibility approach to the open boundary cases of Cusick-Li-Stănicăs conjecture. *Cryptography and Communications*, pages 1–24, 2015.

[7] Francis N. Castro and Luis A. Medina. Linear recurrences and asymptotic behavior of exponential sums of symmetric Boolean functions. *Electron. J. Combin.*, 18(2):Paper 8, 21, 2011.

[8] Francis N. Castro, Luis A. Medina, and Ivelisse M. Rubio. Exact divisibility of exponential sums over the binary field via the covering method. In *Groups, algebras and applications*, volume 537 of *Contemp. Math.*, pages 129–136. Amer. Math. Soc., Providence, RI, 2011.

[9] Francis N. Castro, Hugues Randriam, Ivelisse Rubio, and H. F. Mattson, Jr. Divisibility of exponential sums via elementary methods. *J. Number Theory*, 130(7):1520–1536, 2010.

[10] Francis N. Castro and Ivelisse M. Rubio. Construction of systems of polynomial equations with exact p-divisibility via the covering method. *J. Algebra Appl.*, 13(6):1450013, 15, 2014.

[11] Thomas W. Cusick and Younhwan Cheon. Counting balanced Boolean functions in n variables with bounded degree. *Experiment. Math.*, 16(1):101–105, 2007.

[12] Thomas W. Cusick, Yuan Li, and Pantelimon Stănică. Balanced symmetric functions over GF(p). *IEEE Trans. Inform. Theory*, 54(3):1304–1307, 2008.

[13] Thomas W. Cusick, Yuan Li, and Pantelimon Stănică. On a conjecture for balanced symmetric Boolean functions. *J. Math. Cryptol.*, 3(4):273–290, 2009.

[14] Thomas W. Cusick and Pantelimon St˘ anică. *Cryptographic Boolean functions and applications.* Elsevier/Academic Press, Amsterdam, 2009.

[15] Guang-Pu Gao, Wen-Fen Liu, and Xi-Yong Zhang. The degree of balanced elementary symmetric Boolean functions of $4k+3$ variables. *IEEE Trans. Inform. Theory*, 57(7):4822–4825, 2011.

[16] Xiang-dong Hou. The covering radius of $R(1,9)$ in $R(4,9)$. *Des. Codes Cryptogr.*, 8(3):285–292, 1996.

[17] Xiang-dong Hou. On the covering radius of $R(1,m)$ in $R(3,m)$. *IEEE Trans. Inform. Theory*, 42(3):1035–1037, 1996.

[18] Xiang-dong Hou. GL$(m,2)$ acting on $R(r,m)/R(r-1,m)$. *Discrete Math.*, 149(1-3):99–122, 1996.

[19] Xiang-Dong Hou. p-ary and q-ary versions of certain results about bent functions and resilient functions. *Finite Fields Appl.*, 10(4):566–582, 2004.

[20] Daniel J. Katz. Sharp p-divisibility of weights in abelian codes over $\mathbb{Z}/p^d\mathbb{Z}$. *IEEE Trans. Inform. Theory*, 54(12):5354–5380, 2008.

[21] Nicholas M. Katz. On a theorem of Ax. *Amer. J. Math.*, 93:485–499, 1971.

[22] Gary McGuire. An alternative proof of a result on the weight divisibility of a cyclic code using supersingular curves. *Finite Fields Appl.*, 18(2):434–436, 2012.

[23] Oscar Moreno, Francis N. Castro, and H. F. Mattson, Jr. Correction to: "Divisibility properties for covering radius of certain cyclic codes" [IEEE Trans. Inform. Theory **49** (2003), no. 12, 3299–3303; mr2045808] by Moreno and Castro. *IEEE Trans. Inform. Theory*, 52(4):1798–1799, 2006.

[24] Oscar Moreno and Carlos J. Moreno. The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes. *IEEE Trans. Inform. Theory*, 40(6):1894–1907, 1994.

[25] Wei Su, Xiaohu Tang, and Alexander Pott. A note on a conjecture for balanced elementary symmetric Boolean functions. *IEEE Trans. Inform. Theory*, 59(1):665–671, 2013.

[26] Harold N. Ward. Weight polarization and divisibility. *Discrete Math.*, 83(2-3):315–326, 1990.

Department of Mathematics, University of Puerto Rico, San Juan, PR 00936
E-mail address: franciscastr@gmail.com

Department of Mathematics, University of Puerto Rico, San Juan, PR 00936
E-mail address: luis.medina17@upr.edu

Department of Computer Science, University of Puerto Rico, San Juan, PR 00936
E-mail address: iverubio@gmail.com