EXACT DIVISIBILITY OF EXPONENTIAL SUMS OVER THE BINARY FIELD VIA THE COVERING METHOD

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

Abstract. Boolean functions are one of the most studied objects in mathematics. In this paper, we use the covering method to compute the exact 2-divisibility of exponential sums of boolean functions with prescribed leading monomials. Our results generalize those of [4] and [8] for the binary field. As an application of our findings, we provide families of boolean functions that are not balanced, and give sufficient conditions for the solvability of systems of boolean equations.

1. Introduction

Boolean functions are one of the most studied objects in mathematics. They are important in many applications, for example, in the design of stream ciphers, block and hash functions. These functions play a vital role in cryptography as they are used as filter and combination generator of stream ciphers based on linear feedback shift registers. The case of boolean functions of degree 2 has been intensively studied because of its relation to bent functions.

One can find many papers discussing the properties of boolean functions. The subject can be studied from the point of view of complexity theory or from the algebraic point of view as we do in this paper, where we compute the exact 2-divisibility of exponential sums of families of boolean functions.

Divisibility of exponential sums have been used to characterize properties of functions, as it was done, for example, by Canteaut, Charpin, and Dobbertin in [2]. In [1], Adolphson-Sperber used Newton polyhedra to improve Ax-Katz's result on the divisibility of exponential sums. In [6], Moreno-Moreno gave an estimate for the divisibility of exponential sums that, in many cases, improve Adolphson-Sperber's result (and hence Ax-Katz's result) when the degree of the polynomial is greater than the characteristic of the finite field.

In [5], Moreno-Moreno introduced the covering method, which provides an elementary way to estimate the divisibility of exponential sums over the binary field. Using this method, they gave an improvement to Ax's theorem for the binary case. In [7], Moreno-Castro-Mattson used the covering method to give an elementary proof to Moreno-Moreno's result ([6]) for finite fields of characteristic 2. Recently, in [3], Castro-Randriam-Rubio-Mattson generalized the use of the covering method to any finite field providing an elementary approach to compute the p-divisibility of exponential sums of polynomials over prime fields. The authors obtain several bounds which unify and improve a number of previous results in this direction.

Date: May 6, 2010 and, in revised form, XXXX..

2010 *Mathematics Subject Classification.* Primary 11T06 ; Secondary 11T23 .

Key words and phrases. exponential sums, systems of polynomial equations, covering, 2-divisibility.

In this paper, we use the covering method to compute the exact 2-divisibility of exponential sums of boolean functions with prescribed leading monomials. Our results generalize those of [4] and [8] for the binary field. As an application of our findings, we provide families of boolean functions that are not balanced, and give sufficient conditions for the solvability of systems of boolean equations.

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 $F(\mathbf{X}) = F(X_1, \ldots, X_n)$ 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 can assume throughout the rest of the paper that $F(\mathbf{X})$ is not a polynomial in some subset of the variables $X_1, \ldots, X_n$.

The exponential sum associated to F over $\mathbb{F}$ is:

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

Our aim is to compute the exact 2-divisibility of these exponential sums, this is, to compute the highest power of 2 dividing $S(F)$. We denote the highest power of 2 dividing a number N by $\nu_2(N)$.

One of the advantages of working over $\mathbb{F}$ is that one has the following identities:

$$(-1)^x = 1 - 2x \quad \text{and} \quad x^d = x$$

for $d > 0$, $x \in \mathbb{F}^n$. Therefore if

$$F(\mathbf{X}) = X_{11}^{e_{11}} \cdots X_{n1}^{e_{n1}} + \cdots + X_{1N}^{e_{1N}} \cdots X_{nN}^{e_{nN}},$$

then

$$\begin{aligned} S(F) &= \sum_{\mathbf{x} \in \mathbb{F}^n} (-1)^{F(\mathbf{x})} \\ &= \sum_{\mathbf{x} \in \mathbb{F}^n} (1 - 2x_{11}^{e_{11}} \cdots x_{n1}^{e_{n1}}) \cdots (1 - 2x_{1N}^{e_{1N}} \cdots x_{nN}^{e_{nN}}) \\ &= \sum_{\mathbf{x} \in \mathbb{F}^n} \left(1 + \sum_{\lambda} (-2)^{m(\lambda)} g_\lambda(\mathbf{x}) \right), \\ &= 2^n + \sum_{\lambda} (-2)^{m(\lambda)} \sum_{\mathbf{x} \in \mathbb{F}^n} g_\lambda(\mathbf{x}), \end{aligned} \tag{2.2}$$

where $(-2)^{m(\lambda)} g_\lambda(\mathbf{x})$ are monomials that are products of all possible choices of terms $2x_{1i}^{e_{1i}} \cdots x_{ni}^{e_{ni}}$ for the factors $(1 - 2x_{1i}^{e_{1i}} \cdots x_{ni}^{e_{ni}})$ and $m(\lambda)$ is the number of terms in that choice. Note that $\sum_{\mathbf{x} \in \mathbb{F}^n} g_\lambda(\mathbf{x}) = 2^l$, where l is the number of variables that are missing in g_λ. Hence, the exact 2-divisibility of $S(F)$ can be determined if we are able to "control" the sets of monomials of F needed to cover all the variables.

Let $\mathcal{C}$ be a minimal set of monomials of F covering all variables, that is, every variable X_i is in at least one monomial of $\mathcal{C}$, and $\mathcal{C}$ is minimal with that property. We call this set $\mathcal{C}$ a *minimal covering* of F and we assume that its cardinality is r.

Example 2.1. Let $F(X_1, X_2, \ldots, X_6) = X_1X_2X_3 + X_4X_5 + X_5X_6 + X_1 + \cdots + X_6$ be a polynomial over $\mathbb{F}$. $\{X_1X_2X_3, X_4X_5, X_5X_6\}$ and $\{X_1X_2X_3, X_4X_5, X_6\}$ are the minimal coverings of F with cardinality 3.

In [5], Moreno-Moreno used minimal coverings to prove the following improvement to the binary Ax's theorem.

Theorem 2.2. *Let $F(\mathbf{X})$ be a polynomial over $\mathbb{F}$ and let $\mathcal{C}$ be a minimal covering of F. If $|\mathcal{C}| = r$, then*

$$\nu_2(S(F)) \geq r.$$

The relation between an exponential sum $S(F) = \sum_{\mathbf{x}\in\mathbb{F}^n}(-1)^{F(\mathbf{x})}$ and the number of zeros of a system of polynomials $F_1(\mathbf{X}), \cdots, F_t(\mathbf{X})$ is given by the following lemma.

Lemma 2.3. *Let $F_1(\mathbf{X}), \cdots, F_t(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ and N be the number of common zeros of $F_1, \cdots, F_t$. Then,*

$$N = 2^{-t} S\left(Y_1 F_1(\mathbf{X}) + \cdots + Y_t F_t(\mathbf{X})\right).$$

3. Exact 2-divisibility of exponential sums and solvability of systems of equations

In the next lemmas we give conditions on a covering $\mathcal{C}$ of a boolean function F that will allow us to determine the 2-divisibility of certain products of monomials in F. We show that the only product of monomials in F for which the corresponding term $\sum_{\mathbf{x}\in\mathbb{F}^n} g_\lambda(\mathbf{x})$ in (2.2) is not divisible by 2^{r+1} is the product of the r monomials in $\mathcal{C}$. Hence, the exact 2-divisibility of $S(F)$ is 2^r.

Lemma 3.1. *Let $F(\mathbf{X})$ be a polynomial over $\mathbb{F}$, and $\mathcal{C}$ be a minimal covering of F, $|\mathcal{C}| = r$, such that each monomial in $\mathcal{C}$ has at least two variables that are not contained in the set of all other monomials in $\mathcal{C}$. With notations as in (2.2), if g_λ is a product of $m(\lambda) < r$ monomials in $\mathcal{C}$, then*

$$2^{r+1} | 2^{m(\lambda)} \sum_{\mathbf{x}\in\mathbb{F}^n} g_\lambda(\mathbf{x}).$$

Proof. Suppose that g_λ is the product of $m(\lambda) < r$ monomials of F. Then g_λ misses $l \geq 1$ variables and $2^l | g_\lambda$. Let $\mathcal{C} = \{a_1(\mathbf{X}), \ldots, a_r(\mathbf{X})\}$ be a minimal covering of F, where each monomial has at least two variables that are not contained in the other monomials of $\mathcal{C}$. Consider

$$2^{m(\lambda)} \sum_{\mathbf{x}\in\mathbb{F}^n} g_\lambda(\mathbf{x}) = 2^{m(\lambda)} \sum_{\mathbf{x}\in\mathbb{F}^n} \prod_{j=1}^{m(\lambda)} a_{i_j}(\mathbf{x}). \tag{3.1}$$

Since there are $r - m(\lambda)$ monomials of the covering that are not included in the product, g_λ is missing at least $l = 2(r - m(\lambda))$ variables. Therefore $m(\lambda) + l \geq m(\lambda) + 2r - 2m(\lambda) \geq 2r - m(\lambda) > 2r - r = r$. This implies that 2^{r+1} divides (3.1). □

Lemma 3.2. *Let $F(\mathbf{X})$ be a polynomial over $\mathbb{F}$, and $\mathcal{C}$ be a unique minimal covering of F, $|\mathcal{C}| = r$. With notations as in (2.2), if g_λ is a product of $m(\lambda) \leq r$ monomials in F such that not all of them belong to $\mathcal{C}$, then*

$$2^{r+1} | 2^{m(\lambda)} \sum_{\mathbf{x}\in\mathbb{F}^n} g_\lambda(\mathbf{x}).$$

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

If $2^{m(\lambda)+l}|T$, where $m(\lambda) + l = a \leq r$, and $l \geq 1$ are the missing variables in g_λ, then one can construct a covering of F in the following way: for each missing variable in g_λ, we select a monomial in $\mathcal{C}$ containing the missing variable. The new covering $\mathcal{C}'$ is the set of all the $m(\lambda)$ monomials of F that formed g_λ and the l monomials from the covering $\mathcal{C}$ containing the missing variables. This implies that $|\mathcal{C}'| = a \leq r$. If $|\mathcal{C}'| = r$, then, since the covering $\mathcal{C}$ is unique, the monomials that formed g_λ were all from $\mathcal{C}$, which is a contradiction. If $|\mathcal{C}'| < r$, we found a covering smaller than the minimal, which is also a contradiction.

□

The next proposition gives sufficient conditions on the covering $\mathcal{C}$ of a boolean function in order to compute the exact 2-divisibility of the exponential sum of the function. As a consequence we get conditions for a boolean function F being not balanced, this is, conditions for F with $S(F) \neq 0$.

Proposition 3.3. *Let $F(\mathbf{X})$ be a polynomial over $\mathbb{F}$, and let $\mathcal{C}$ be a unique minimal covering of F such that each monomial in $\mathcal{C}$ has at least two variables that are not contained in the set of all other monomials in $\mathcal{C}$, and $|\mathcal{C}| = r$. Then, $\nu_2(S(F)) = r$. In particular, $S(F) \neq 0$.*

Proof. Let $\mathcal{C} = \{a_1(\mathbf{X}), \ldots, a_r(\mathbf{X})\}$, and

$$T = 2^{m(\lambda)} \sum_{\mathbf{x}\in\mathbb{F}^n} g_\lambda(\mathbf{x}).$$

It is clear that if $m(\lambda) > r$, then $2^{r+1}|T$. By Lemmas 3.1 and 3.2, if g_λ is a product of $m(\lambda) \leq r$ monomials in F such that not all of them belong to $\mathcal{C}$, or g_λ is a product of less than r monomials in $\mathcal{C}$, then $2^{r+1}|T$. The result follows when one notice that $\prod_{i=i}^{r} a_i(\mathbf{X}) = X_1 \cdots X_n$ is the only monomial g_λ with

$$2^{m(\lambda)} \sum_{\mathbf{x}\in\mathbb{F}^n} g_\lambda(\mathbf{x}) = 2^{m(\lambda)} \sum_{\mathbf{x}\in\mathbb{F}^n} x_1 \cdots x_n = 2^r.$$

□

With the above proposition, if one can guarantee that a boolean function F has a unique minimal covering with certain property, then one can compute the exact 2-divisibility of the exponential sum of F. But, in general, it is not an easy task to find all the minimal coverings of a polynomial. In the following theorem, which is our main result, we give sufficient conditions to construct boolean functions with the appropriated coverings and hence be able to compute the exact 2-divisibility of their exponential sums. Essentially the theorem give us sufficient conditions on a set $\mathcal{C}$, so one can construct boolean functions with $\mathcal{C}$ as the appropriated covering. This is a generalization of Theorem 4.1 of [4] and [8] for the binary case. Also the technique in the next proof is completely different as it only requires an argument related to the covering whereas the proofs in [4] and [8] required more sophisticated machinery.

Theorem 3.4. *Let $\mathcal{C} = \{a_1(\mathbf{X}), \ldots, a_r(\mathbf{X})\}$ be a set of monomials covering all the variables and with degrees greater than 1. If any monomial in $\mathcal{C}$ has at least $s \geq 2$ variables that are not contained in the set of all the other monomials in $\mathcal{C}$, then*

$$\nu_2\left(S\left(F\right)\right) = r,$$

where

$$F = \sum_{i=1}^{r} a_i(\mathbf{X}) + G(\mathbf{X}),$$

and $deg(G) < s$. In particular $S\left(F\right) \neq 0$.

Proof. By Proposition 3.3 we only have to prove that $\mathcal{C}$ is a unique minimal covering of F. It is clear that any set of less than r monomials in $\mathcal{C}$ is not a covering of F. Any monomial $a_i(\mathbf{X})$ in $\mathcal{C}$ has at least $s \geq 2$ variables that are not covered by the other monomials in $\mathcal{C}$, and, since $deg(G) \leq s-1$, if one substitutes a monomial in $\mathcal{C}$ by a monomial in G there is at least one variable that it is not covered. Therefore $\mathcal{C}$ is minimal and unique. □

The next example shows that, to compute the exact 2-divisibility, it is necessary that each monomial in the covering contributes with at least two new variables to the covering.

Example 3.5. Consider $F = X_1X_2X_3+X_3X_4X_5+X_5X_6X_7$. Then $\mathcal{C} = \{X_1X_2X_3, X_3X_4X_5, X_5X_6X_7\}$ is the unique minimal covering of F. Note that $X_3X_4X_5$ has only one variable that it is not contained in $\{X_1X_2X_3, X_5X_6X_7\}$ and the theorem does not apply. One can verify that $S(F) = 2^6$.

Corollary 3.6. *With the notations of Theorem 3.4, we have that*

$$|S(F)| \geq 2^r.$$

The next example shows that even though boolean functions with the same unique minimal covering have the same 2-divisibility, there is an ample spectrum for the exact value of $S(F)$.

Example 3.7. Consider $F = X_1X_2X_3X_4 + X_4X_5X_6X_7 + X_7X_8X_9$ and $F' = X_1X_2X_3X_4+X_4X_5X_6X_7+X_7X_8X_9+X_1+X_2+X_3+X_4+X_5+X_6+X_7+X_8+X_9$. Then $S(F) = 8 \cdot 3 \cdot 13$, and $S(F') = 8$.

Corollary 3.8. *Let $\mathcal{C} = \{a_1(\mathbf{X}), \ldots, a_r(\mathbf{X})\}$ be a set of monomials covering all the variables and with degrees $1 < d_i < n$. If any monomial in $\mathcal{C}$ has at least $s \geq 2$ variables that are not contained in the set of all the other monomials in $\mathcal{C}$, then*

$$|S\left(X_1 \cdots X_n + a_1(\mathbf{X}) + \cdots + a_r(\mathbf{X}) + G(\mathbf{X})\right)| = 2m,$$

where $|m| \geq 2^{r-1} - 1$, m odd, and $deg(G) < s$.

Proof. Let $F = X_1 \cdots X_n + a_1(\mathbf{X}) + \cdots + a_r(\mathbf{X}) + G(\mathbf{X})$ and $F' = a_1(\mathbf{X}) + \cdots + a_r(\mathbf{X}) + G(\mathbf{X})$. By Theorem 3.4, we have that $S(F) = 2m$ and $S(F') = 2^r m'$,

where m and m' are odd. Note that

$$\begin{aligned} S(F) &= \sum_{\substack{\mathbf{x}\in\mathbb{F}^n \\ x_1\cdots x_n=0}} (-1)^{F(\mathbf{x})} + (-1)^{F(1,\ldots,1)} \\ &= \sum_{\substack{\mathbf{x}\in\mathbb{F}^n \\ x_1\cdots x_n=0}} (-1)^{F'(\mathbf{x})} + (-1)^{F(1,\ldots,1)} \\ &= \sum_{\mathbf{x}\in\mathbb{F}^n} (-1)^{F'(\mathbf{x})} - (-1)^{F'(1,\ldots,1)} + (-1)^{F(1,\ldots,1)} \\ &= S(F') - 2(-1)^{F'(1,\ldots,1)}. \end{aligned}$$

Hence $2m = 2^r m' - 2(-1)^{F'(1,\ldots,1)}$ and $m = 2^{r-1}m' - (-1)^{F'(1,\ldots,1)}$. This implies that $|m| = |2^{r-1}m' - (-1)^{F'(1,\ldots,1)}| \geq 2^{r-1}|m'| - |\pm 1| \geq 2^{r-1} - 1$. □

Theorem 3.4 give sufficient conditions to guarantee the solvability of systems of binary equations and the computation of the exact 2-divisibility of the number of solutions.

Theorem 3.9. *Let $\mathcal{C} = \{a_1(\mathbf{X}), \ldots, a_r(\mathbf{X})\}$ be a set of monomials covering all the variables and with degrees greater than 1. If any monomial in $\mathcal{C}$ has at least $s \geq 2$ variables that are not contained in the set of all the other monomials in $\mathcal{C}$, then $\nu_2(N(F_1, \ldots, F_t)) = r - t$, where $N(F_1, \ldots, F_t))$ is the number of common solutions of the following system of polynomial equations:*

$$\begin{aligned} F_1 &= a_1(\mathbf{X}) + \cdots + a_{r_1}(\mathbf{X}) + G_1(\mathbf{X}) = 0 \\ F_2 &= a_{r_1+1}(\mathbf{X}) + \cdots + a_{r_2}(\mathbf{X}) + G_2(\mathbf{X}) = 0 \\ &\vdots \\ F_t &= a_{r_{t-1}+1}(\mathbf{X}) + \cdots + a_r(\mathbf{X}) + G_t(\mathbf{X}) = 0, \end{aligned} \tag{3.2}$$

where $deg(G_i) < s$ for $i = 1, \ldots, t$. In particular system (3.2) is solvable.

Proof. Consider

$$F = Y_1F_1(\mathbf{X}) + Y_2F_2(\mathbf{X}) + \cdots + Y_tF_t(\mathbf{X}).$$

Then, by Lemma 2.3, $N(F_1, \ldots, F_t) = 2^{-t}S(F)$, $v_2(N(F_1, \ldots, F_t)) = v_2(S(F)) - t$ and one just have to prove that $\nu_2(S(F)) = r$ to obtain the result.

Note that

$$\mathcal{C} = \{Y_1a_1(\mathbf{X}), \ldots, Y_1a_{r_1}(\mathbf{X}), \ldots, Y_ta_r(\mathbf{X})\}$$

is a unique minimal covering for F where each monomial has at least two variables that are not contained in the other monomials. The result follows from Proposition 3.3. □

Example 3.10. Let $F(X_1, \ldots, X_{48}) = X_1X_2X_3 + X_4X_5X_6 + \cdots + X_{46}X_{47}X_{48} + G(X_1, \ldots, X_{48})$ be a polynomial over $\mathbb{F}$, where $deg(G) < 3$. Then $N(F - \alpha) = 2^{15} \cdot m$ for $\alpha \in \mathbb{F}$, where m is odd.

To obtain unique minimal coverings it is enough to construct monomials of disjoint support that cover all the variables. The next result gives a simple way to construct boolean functions with exponential sums of exact 2-divisibility.

Corollary 3.11. *Let $\mathcal{C} = \{a_1(\mathbf{X}), \ldots, a_r(\mathbf{X})\}$ be a set of monomials of disjoint support covering all the variables and with degrees greater than 1. Then*

$$\nu_2\left(S\left(F\right)\right) = r,$$

where

$$F = \sum_{i=1}^{r} a_i(\mathbf{X}) + G(\mathbf{X}),$$

and, $deg(G) < \min\limits_{1\leq i\leq r} deg(a_i(\mathbf{X}))$. In particular $S\left(F\right) \neq 0$.

The following corollary determines the exact 2-divisibility of the number of solutions of systems of polynomial equations with conditions similar to the conditions on Corollary 3.11.

Corollary 3.12. *Let $\mathcal{C} = \{a_1(\mathbf{X}), \ldots, a_r(\mathbf{X})\}$ be a set of monomials of disjoint support covering all the variables and with degrees greater than 1. Then $\nu_2\left(N(F_1, \ldots, F_t)\right) = r - t$, where $N(F_1, \ldots, F_t))$ is the number of common solutions of the following system of polynomial equations:*

$$\begin{aligned} F_1 &= a_1(\mathbf{X}) + \cdots + a_{r_1}(\mathbf{X}) + G_1(\mathbf{X}) = 0 \\ F_2 &= a_{r_1+1}(\mathbf{X}) + \cdots + a_{r_2}(\mathbf{X}) + G_2(\mathbf{X}) = 0 \\ &\vdots \\ F_t &= a_{r_{t-1}+1}(\mathbf{X}) + \cdots + a_r(\mathbf{X}) + G_t(\mathbf{X}) = 0, \end{aligned} \tag{3.3}$$

where $deg(G_i) < \min_{1\leq j\leq r} deg\left(a_j(\mathbf{X})\right)$ for $i = 1, \ldots, t$. In particular system (3.3) is solvable.

Example 3.13. The following system of polynomial equations in 13 variables is solvable for any $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}^3$:

$$X_1X_2X_3X_4X_5 + \sum_i X_i = \alpha_1$$

$$X_6X_7X_8X_9 + \sum_{i<j} X_iX_j = \alpha_2$$

$$X_{10}X_{11}X_{12}X_{13} + \sum_{i<j<k} X_iX_jX_k = \alpha_3.$$

Example 3.14. Let $N(\alpha_1, \alpha_2)$ be the number of solutions of the following system of polynomial equations:

$$X_1X_2X_3X_4 + X_5X_6X_7X_8 + \sum_{i<j} X_iX_j = \alpha_1 \tag{3.4}$$

$$X_9X_{10}X_{11}X_{12}X_{13}X_{14} + X_1X_2X_3 + X_3X_4X_5 + \cdots + X_{12}X_{13}X_{14} = \alpha_2.$$

Corollary 3.12 implies that this system is solvable for any (α_1, α_2) and $N(\alpha_1, \alpha_2) = 2m$, where m is odd. The next table shows the exact number of solutions of the system for each (α_1, α_2).

$N(0,0)$	$N(1,0)$	$N(0,1)$	$N(1,1)$
$2 \cdot 3^2 \cdot 293$	$2 \cdot 37 \cdot 67$	$2 \cdot 3^2 \cdot 163$	$2 \cdot 1609$

References

[1] A. Adolphson and S. Sperber, p-adic Estimates for Exponential Sums and the Theorem of Chevalley-Warning, *Ann. Sci. Ec. Norm. Super.*, 4^e série, vol **20**, pp. 545-556, 1987.

[2] A. Canteaut, P. Charpin, and H. Dobbertin, Weight divisibility of Cyclic Codes, Highly Nonlinear Functions on F_{2^m}, and Crosscorrelation of Maximum-Length Sequences, *SIAM J. Discrete Math.*, **13** , pp. 105-138, 2000.

[3] F. N. Castro, H. Randriam, I. Rubio and H. F. Mattson, Jr., Divisibility of Exponential Sums via Elementary Methods, *Journal of Number Theory*, **130** (2010) pp. 1520-1536.

[4] F. N. Castro, I. Rubio and J. Vega, Divisibility of Exponential Sums and Solvability of Certain Equations over Finite Fields, *Quart. J. Math.*, **60**, pp. 169-181, 2009.

[5] O. Moreno and C. J. Moreno, The MacWilliams-Sloane Conjecture on the Tightness of the Carlitz-Uchiyama Bound and the Weights of Dual of BCH Codes, *IEEE Trans. Inform. Theory* **40:6** , pp. 1894-1907, 1994.

[6] O. Moreno and C.J. Moreno, Improvement of the Chevalley-Warning and the Ax-Katz theorems, *Amer. J. Math.* **117:**1 (1995),241-244.

[7] O. Moreno, F. N. Castro and H. F. Mattson jr. Correction, Divisibility Properties for Covering Radius for Certain Cyclic Codes, *IEEE Trans. Inform. Theory*, IEEE Transaction on Information Theory, **52**,(2006), 1798-1799.

[8] I. Rubio and F. N. Castro, Solvability of Systems of Polynomial Equations with Some Prescribed Monomials, accepted for publication in AMS Contemporary Mathematics.

Department of Mathematics, University of Puerto Rico, Río Piedras, Box 23355, San Juan, PR 00931

E-mail address: franciscastr@gmail.com

Department of Mathematics, University of Puerto Rico, Río Piedras, Box 23355, San Juan, PR 00931

E-mail address: luis.medina@uprrp.edu

Department of Computer Science, University of Puerto Rico, Río Piedras, Box 23328, San Juan, PR 00931

E-mail address: iverubio@uprrp.edu