Contemporary Mathematics

Exact Divisibility of Exponential Sums and Some Consequences

Francis N. Castro, Raúl Figueroa, and Luis A. Medina

Abstract. In this paper we compute the exact divisibility of some exponential sums over $\mathbb{F}_p$. Our results imply that these families of polynomials are not permutation polynomials of $\mathbb{F}_p$. Also, we apply our results to the Waring problem.

1. Introduction

Exponential sums have been applied in many areas of mathematics. Divisibility of exponential sums is an area of the theory of exponential sums that has received considered attention. Many authors have studied the p-adic divisibility of the roots of L-function associated to the exponential sum. That information is encoded in the Newton polygon of the L-function ([**20, 24, 22, 25**]). As the value of an exponential sum is equal to the sum of the roots of the L-function associated to it, any estimates in those imply an estimate for the divisibility of the exponential sum. Sometimes some of the roots of the L-function associated to the exponential sum have the same p-divisibility and when added together, the p-divisibility of the exponential sum increases. In this paper we are interested in the divisibility of the exponential sums associated to polynomials over a finite field of odd characteristic.

In general, there are very good estimates for the divisibility of exponential sums (for example [**21, 1, 15, 16, 2**]). In this paper, we address the question of computing the exact divisibility of exponential sums associated to polynomials over $\mathbb{F}_p$. This is a difficult question, but in some cases it can be computed. Everytime we compute the exact divisibility of a family of exponential sums we can conclude two things. First, that each value of the exponential sum is not equal to zero and second, that the polynomial associated to the exponential sum is not a permutation of the finite field. In this paper we compute exact divisibility of families of exponential sums associated to the following polynomials:

(1) $F(X) = aX^{d_1} + bX^{d_2}$,
(2) the polynomials containing monomials of type X^{d_1} and X^{d_2} satisfying $d_1 + d_2 = p - 1$,

2010 *Mathematics Subject Classification.* Primary 11L07 ; Secondary 11P05 .

Key words and phrases. p-divisibility of exponential sum, Waring Problem, Permutation Polynomials.

under some natural conditions.

The original Waring's problem is to find the minimum number of variables such that the equation $X_1^d + \cdots + X_n^d = a$ has at least one solution for any natural number a. This minimum number is called the *Waring number* associated to d. Many authors have considered the Waring problem over finite fields. There are many bounds for Waring numbers and some can be found in [**23, 10, 4**]. Many of these bounds are consequences of good estimates of the absolute value of Gauss sums ([**11**], [**8**]) or methods of arithmetic combinatorics [**4**], [**18**].

In the literature of the Waring problem over finite fields, the following generalization has been considered: Given a polynomial $F(X)$ over $\mathbb{F}_p$, estimate the minimum number of variables such that

$$F(X_1) + \cdots + F(X_n) = a \tag{1}$$

has at least one solution over $\mathbb{F}_p$ for any $a \in \mathbb{F}_p$. We denote this number by $\gamma(F, q)$. The above problem can be related to the following problem: Given polynomials $F_1(X_1), \ldots, F_n(X_n)$ over $\mathbb{F}_p$, find conditions such that every $a \in \mathbb{F}_p$ can be written as

$$a = F_1(x_1) + \cdots + F_n(x_n), \tag{2}$$

where $x_1, \ldots, x_n \in \mathbb{F}_p$. In [**5**], Carlitz et. al. proved that given $F_1(X_1), \ldots, F_n(X_n)$ polynomials over $\mathbb{F}_p$ of degree $d_1, \ldots, d_n$, every element $a \in \mathbb{F}_p$ can be written as $a = F_1(x_1) + \cdots + F_n(x_n)$, provided that

$$\sum_{i=1}^{n} \left[\frac{p-1}{d_i} \right] + t > p,$$

where t is the number of F_i's which are neither of degree $p-1$ nor of the form $\alpha(X_i - \beta)^{\frac{1}{2}(p-1)} + \lambda$. In [**3**], Cochrane et. al. use estimates for exponential sums to prove that (1) has at least one solution for every $a \in \mathbb{F}_p$, whenever $r_1 + \cdots + r_{\gamma(F,p)} \geq \log p$, where the absolute value of the exponential sum corresponding to each r_i is less than or equal to $p(1 - r_i)$. Note that these results are for polynomials over $\mathbb{F}_p$. Recently in [**18**], [**9**], they considered the Waring problem when $F = F_1 = \cdots = F_n$ and F is a Dickson polynomial over finite fields. Finally, in this paper we apply our results about divisibility of exponential sums to obtain estimates for the generalization of the Waring problem given in (1).

2. Preliminaries

Let $F(X_1, \cdots, X_n) = \sum_{i=1}^{N} a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}}$ be a polynomial in the variables $X_1, \cdots, X_n$ over $\mathbb{F}_p$. In this paper we consider p to be odd.

Let $\mathbb{Q}_p$ be the p-adic field with ring of integers $\mathbb{Z}_p$, and let $\mathbb{K}$ be the extension over $\mathbb{Q}_p$ obtained by adjoining a primitive $(p-1)$th root of unity in $\overline{\mathbb{Q}}_p$, the algebraic closure of $\mathbb{Q}_p$. The residue class field is isomorphic to $\mathbb{F}_p$. Let $\mathcal{T}$ denote the Teichmüller representatives of $\mathbb{F}_p$ in $\mathbb{K}$. Denote by ξ a primitive pth root of unity in $\overline{\mathbb{Q}}_p$. Define $\theta = 1 - \xi$ and denote by v_θ the valuation over θ. Note that $v_\theta(p) = p - 1$ and $v_p(x) = \frac{v_\theta(x)}{p-1}$.

Let $\psi : \mathbb{F}_p \to \mathbb{Q}(\xi)$ be a nontrivial additive character. The exponential sum associated to F is defined as follows:

$$S(F) = \sum_{x_1, \ldots, x_n \in \mathbb{F}_p} \psi(F(x_1, \ldots, x_n)).$$

Note that if we are able to compute the exact p-divisibility of the exponential sum $S(F)$, then we know that $S(F)$ will not be divisible by some arbitrary large power of p and therefore $S(F) \neq 0$. The next theorem ([**16**]) gives a bound for the valuation of an exponential sum with respect to θ.

THEOREM 2.1. *Let* $F(X_1, \ldots, X_n) = \sum_{i=1}^{N} a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}}$, $a_i \neq 0$. *If* $S(F)$ *is the exponential sum*

$$S(F) = \sum_{x_1, \cdots, x_n \in \mathbb{F}_p} \psi(F(x_1, \cdots, x_n)), \tag{3}$$

then $v_\theta(S(F)) \geq L$, *where*

$$L = \min_{(j_1, \ldots, j_N)} \left\{ \sum_{i=1}^{N} j_i + (p-1)s \mid 0 \leq j_i < p \right\},$$

for $(j_1, \ldots, j_N)$ *a solution to the system*

$$\begin{cases} e_{11}j_1 + e_{12}j_2 + \ldots + e_{1N}j_N & \equiv 0 \bmod p-1 \\ \vdots & \vdots \\ e_{n1}j_1 + e_{n2}j_2 + \ldots + e_{nN}j_N & \equiv 0 \bmod p-1, \end{cases} \tag{4}$$

and s *the number of expressions in (4) that are equal to zero.*

Following the notation of [**16**], we expand the exponential sum $S(F)$:

$$S(F) = \sum_{j_1=0}^{p-1} \cdots \sum_{j_N=0}^{p-1} \left[\prod_{i=1}^{N} c(j_i) \right] \left[\sum_{\mathbf{t} \in \mathcal{T}^n} \mathbf{t}^{j_1\mathbf{e}_1 + \cdots + j_N\mathbf{e}_N} \right] \left[\prod_{i=1}^{N} a_i'^{j_i} \right], \tag{5}$$

where a_i''s are the Teichmüller representatives of the coefficients a_i of F, and $c(j_i)$ is defined in Lemma 2.2 below. Each solution $(j_1, \cdots, j_N)$ to (4) is associated to a term T in the above sum with

$$\begin{aligned} v_\theta(T) &= v_\theta \left(\left[\prod_{i=1}^{N} c(j_i) \right] \left[\sum_{\mathbf{t}} \mathbf{t}^{j_1\mathbf{e}_1 + \cdots + j_N\mathbf{e}_N} \right] \left[\prod_{i=1}^{N} a_i'^{j_i} \right] \right) \\ &= \sum_{i=1}^{N} j_i + (p-1)s, \end{aligned} \tag{6}$$

where s is the number of expressions in (4) that are equal to zero for the vector $(j_1, \cdots, j_N)$.

Sometimes one does not have equality on the valuation of $S(F)$ because it could happen that there is more than one solution $(j_1, \ldots, j_N)$ that gives the minimum value for $\sum_{i=1}^{N} j_i$ and, for example, when the associated terms are similar some could cancel and produce higher powers of θ dividing the exponential. However, there are situations on which one is able to compute the exact divisibility. The situation that we considered in this paper is when there is a unique solution $(j_1, \ldots, j_N)$ in (4). In this case the exact divisibility of $S(F)$ is obtained. This was used in [**6**], [**7**], [**19**] to obtain that $v_\theta(S(F)) = L$ for infinite families of polynomials.

From now on we call any solution $(j_1, \cdots, j_N)$ of (4) that has $v_\theta(T)$ of minimum value a *minimal solution*. In the cases considered in this paper we have $s = 0$. We use the following lemma and Stickelberger's Theorem to compute exact divisibility.

LEMMA 2.2 ([**16**]). *There is a unique polynomial* $C(X) = \sum_{j=0}^{p-1} c(j)X^j \in \mathbb{K}(\xi)[X]$ *of degree* $p-1$ *such that*

$$C(t) = \xi^{tr_{\mathbb{K}/\mathbb{Q}_p}(t)}, \quad \text{for all } t \in \mathcal{T}.$$

Moreover, the coefficients of $C(X)$ *satisfy*

$$\begin{aligned} c(0) &= 1 \\ (p-1)c(p-1) &= -p \\ (p-1)c(j) &= g(j) \qquad \text{for } 0 < j < p-1, \end{aligned}$$

where $g(j)$ *is the Gauss sum,*

$$g(j) = \sum_{t \in \mathcal{T}^*} t^{-j} \xi^{tr_{\mathbb{K}/\mathbb{Q}_p}(t)}.$$

THEOREM 2.3 (Stickelberger [**17**]). *For* $0 < j < p-1$,

$$\frac{g(j)j!}{\theta^j} \equiv -1 \bmod \theta. \tag{8}$$

The non-zero elements in the Teichmüller set $\mathcal{T}$ satisfy the following relation:

LEMMA 2.4. *Suppose that* $e_1, e_2, \cdots, e_n$ *are non-negative integers such that* r *of them are non-zero and let* $\mathbf{e} = (e_1, \cdots, e_n)$. *Then,*

$$\sum_{\mathbf{t} \in \mathcal{T}^n} \mathbf{t}^{\mathbf{e}} = \begin{cases} (p-1)^r p^{n-r} & \text{if all } e_i \text{ are divisible by } p-1 \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

Next we state a theorem about permutation polynomials. This theorem is going to be used in the next section.

THEOREM 2.5 ([**13**]). *A polynomial* $F(X)$ *over* $\mathbb{F}_p$ *in one variable over* $\mathbb{F}_p$ *is a permutation polynomial of* $\mathbb{F}_p$ *if and only if* $S(F) = \sum_{x \in \mathbb{F}_p} \psi(F(x)) = 0$ *for all nontrivial additive character of* $\mathbb{F}_p$.

Theorem 2.5 implies that if $S(F) \neq 0$ for some nontrivial additive character, then F is not a permutation polynomial of $\mathbb{F}_p$.

3. Exact Divisibility of Exponential Sums in One Variable over $\mathbb{F}_p$

In this section we compute the p-divisibility of some exponential sums in one variable over $\mathbb{F}_p$. We apply our results about exact divisibility of exponential sums to solutions of equations. Let $F(X)$ be a polynomial over $\mathbb{F}_p$, where p is an odd prime. If $F(X) = a_1X^{d_1} + a_2X^{d_2} + \cdots + a_rX^{d_r}$, we need to compute

$$L = \min\{j_1 + j_2 + \cdots + j_r\}.$$

for any $0 \leq j_1, j_2, \ldots, j_r \leq p-1$ satisfying

$$d_1j_1 + d_2j_2 + \cdots + d_rj_r \equiv 0 \bmod p-1 \tag{10}$$

and prove this minimum is unique to conclude $v_\theta(S(F)) = L$. In particular this implies that $S(a_1X^{d_1} + \cdots + a_rX^{d_r}) \neq 0$ and $F(X) = a_1X^d + a_2X^{d_2} + \cdots + a_rX^{d_r}$ is not a permutation polynomial of $\mathbb{F}_p$. We assume through the paper that $p-1 > d_1 > d_2 > \cdots > d_r \geq 1$ and $a_1 \neq 0$. It is known that if d_1 divides $p-1$, then $\nu_\theta(S(F)) = \dfrac{p-1}{d_1}$.

We start our study with exponential sums associated to $F(X) = aX^{d+1} + bX^d$, where $ab \neq 0$.

THEOREM 3.1. *Let d be a positive integer greater than 1. Let k be the smallest positive integer such that $c(p-1)/(d+1)$ and $c(p-1)/d$ are not integers for $c > 0$ and $[c(p-1)/(d+1)] = [c(p-1)/d]$, for $c < k$.*

- *Then*
$$\nu_\theta(S(aX^{d+1} + bX^d)) = \lceil \frac{k(p-1)}{d+1} \rceil,$$
if $k(p-1)/(d+1)$ and $k(p-1)/d$ are not integers and $[k(p-1)/(d+1)] \neq [k(p-1)/d]$.
- *If only one of $k(p-1)/(d+1)$ or $k(p-1)/d$ is an integer, then the value of $\nu_\theta(S(aX^{d+1} + bX^d))$ is such integer.*
- *If $k(p-1)/(d+1)$ and $k(p-1)/d$ are integers, then $\nu_\theta(S(aX^{d+1} + bX^d))$ is the minimum of such integers.*

PROOF. Let j_1, j_2 be integers, $0 \leq j_1, j_2 \leq p-2$, such that

$$j_1(d+1) + j_2 d = c(p-1)$$

for some integer $c \geq 0$. We rewrite this equation as $Sd + j_1 = c(p-1)$, where $S = j_1 + j_2$. Let $m > 0$ denote the smallest sum $j_1 + j_2$. Notice that if j_1', j_2' is another solution of the modular equation associated to $aX^{d+1} + bX^d$ and $S = j_1 + j_2 = j_1' + j_2'$, then $j_1 - j_1' = (c - c')(p-1)$ so $j_1 = j_1'$ and $j_2 = j_2'$. Thus, there exists a unique pair j_1, j_2 such that $m = j_1 + j_2$. Assume first that $j_1 \neq 0 \neq j_2$. From $Sd < Sd + j_2 = c(p-1) < Sd + S$ we get

$$\frac{c(p-1)}{d+1} < S < \frac{c(p-1)}{d}$$

Let k be the smallest integer such that $c(p-1)/(d+1)$ and $c(p-1)/d$ are not integers (for $c > 0$) and $[c(p-1)/(d+1)] = [c(p-1)/d]$ for $0 \leq c < k$. If $k(p-1)/(d+1)$ and $k(p-1)/d$ are not integers and $[k(p-1)/(d+1)] \neq [k(p-1)/d]$, then clearly $m = [k(p-1)/(d+1)] + 1$. If either $k(p-1)/(d+1)$ or $k(p-1)/d$ is an integer then m is that integer value. □

EXAMPLE 3.2. Two examples:

- If $d = 51$ and $p = 757$, we have $\nu_\theta(S(aX^{52} + bX^{51})) = 44$ since $k = 3$.
- If $d = 31$ and $p = 61$, we have we have $\nu_\theta(S(aX^{32} + bX^{31})) = 15$. Note that $c(p-1)/32$ and $c(p-1)/31$ are not integers for $c \leq 7$. In this case $[c(p-1)/32] = [c(p-1)/31]$ for $c \leq 8$ but $8(p-1)/32 = 15$ is an integer. The exact 61-divisibility of the number of solutions of $F(X_1) + \cdots + F(X_{4m}) = a$ is 61^m, for $a \in \mathbb{F}_{61}$, where $F(X) = aX^{32} + bX^{31}$.

COROLLARY 3.3. *With notation Theorem 3.1, we have*

$$S(aX^{d+1} + bX^d) \neq 0.$$

COROLLARY 3.4. *Suppose that $d > 1$ is positive integer dividing $p-1$. Then*

$$\nu_\theta\big(S(aX^{d^2} + bX^{d+1})\big) \begin{cases} \min\{\frac{p-1}{d+1}, \frac{p-1}{d(d, \frac{p-1}{d})}\} & \text{if } d+1 \mid p-1 \\ \frac{p-1}{d(d, \frac{p-1}{d})} & \text{otherwise} \end{cases}$$

PROOF. If d^2 divides $p-1$, then $\nu_\theta\big(S(aX^{d^2}+bX^{d+1})\big) = \dfrac{p-1}{d^2}$. Suppose that $d^2 \not| p-1$. The modular equation associated to the exponential sum is $d^2 j_1 + (d+1)j_2 \equiv 0 \bmod p-1$. Let $j_1' = dj_1 \bmod p-1$. We obtain the following modular equation $dj_1' + (d+1)j_2 \equiv 0 \bmod p-1$. The minimal solution of this modular equation is $\min\{\frac{p-1}{d+1}, \frac{p-1}{d}\}$ by Theorem 3.1. □

EXAMPLE 3.5. If $d=3$ and $p=61$, we have we have $\nu_\theta(S(aX^9+bX^4)) = 15$ since $\min\{\frac{p-1}{d+1}, \frac{p-1}{d(d,\frac{p-1}{d})}\} = \min\{15, 20\} = 15$.

Consider polynomials of degree $p-2$ over $\mathbb{F}_p$. In [**12**], Koyangin confirmed the common belief that almost all permutation polynomials have degree $q-2$. The following theorem provides families of polynomials that cannot be permutation polynomials of $\mathbb{F}_p$.

THEOREM 3.6. *Let $p-2 = d_1 > d_2 > \cdots > d_r = 2$ be positive integers satisfying $d_2 < \lfloor \frac{p-1}{3} \rfloor$. Then*

$$v_\theta(S(a_1X^{p-2} + a_2X^{d_2} + \cdots + a_rX^2)) = 3,$$

where $a_1a_r \neq 0$. In particular $S(F) \neq 0$ and F is not a permutation polynomial of $\mathbb{F}_p$.

PROOF. Note that we do not have a minimal solution of $(p-2)j_1 + \cdots + 2j_r \equiv 0 \bmod p-1$ with value ≤ 2. We are going to prove that the unique minimal solution of $(p-2)j_1 + \cdots + 2j_r \equiv 0 \bmod p-1$ is $j_1 = 2, j_r = 1$ and $j_2 = \cdots = j_{r-1} = 0$. Note that $d_{i_1} + d_{i_2} + d_{i_3} < p-1$ for $i_1, i_2, i_3 > 1$, $p-2+2d_{i_1} \not\equiv 0 \bmod p-1$ and $2(p-2) + d_{i_1} \not\equiv 0 \bmod p-1$ except when $d_{i_1} = 2$. This completes the proof. □

Now we apply Theorem 3.8 to the Waring problem over $\mathbb{F}_p$.

COROLLARY 3.7. *Let $p-2 = d_1 > d_2 > \cdots > \cdots > d_{r-1} > d_r = 2$ be positive integers satisfying $d_2 < \lfloor \frac{p-1}{3} \rfloor$ and $F(X) = a_1X^{d_1} + a_2X^{d_2} + \cdots + \cdots + a_rX^{d_r}$. Then $F(X_1) + \cdots + F(X_s) = a$ is solvable for any $a \in \mathbb{F}_p$ whenever $s \geq \frac{p-1}{3}$ and $p \equiv 1 \bmod 3$.*

PROOF. Let N be the number of solutions of the equation $F(X_1) + \cdots + F(X_s) = a$ over $\mathbb{F}_p$. Using the identity $N = \frac{1}{p}\sum_{x_1,\ldots,x_s,y\in\mathbb{F}_p} \psi(y(F(x_1) + \cdots + F(x_s) - a))$, we obtain the following system of modular equations:

$$\begin{aligned}
(p-2)j_{11} + d_2j_{21} + \cdots + d_{r-1}j_{r-11} + 2j_{r1} &\equiv 0 \bmod p-1\\
&\vdots \cdots\\
(p-2)j_{1s} + d_2j_{2s} + \cdots + d_{r-1}j_{r-1s} + 2j_{rs} &\equiv 0 \bmod p-1\\
j_{11} + \cdots + j_{rs} + j &\equiv 0 \bmod p-1
\end{aligned}$$

The first s-modular equations have an unique minimal solution: $j_{11} = \cdots = j_{1s} = 2, j_{r1} = \cdots = j_{rs} = 1$, the other j_i's equal to zero. Taking $s = \frac{p-1}{3}$, we obtain a minimal solution of the modular system. Therefore p does not divide the number of solutions of $F(X_1) + \cdots + F(X_s) = a$. Hence, $F(X_1) + \cdots + F(X_s) = a$ is solvable over $\mathbb{F}_p$. □

The following theorem gives a condition for a polynomial not to be a permutation polynomial of $\mathbb{F}_p$, where the exponents of the polynomial satisfy some conditions.

THEOREM 3.8. *Let $p-2 \geq d_1 > d_2 > \cdots > d_{r-1} > d_r \geq 1$. If at least one of the following conditions happen $d_{i_1} + d_{i_2} = d_{i_3} + d_{i_4} = \cdots = d_{i_{l-1}} + d_{i_l} = p-1$ for some l or $d_m = \frac{p-1}{2}$, then*

$$v_\theta\big(S(a_1X^{p-2}+a_2X^{d_2}+\cdots+a_{r-1}X^{d_{r-1}}+a_rX^{d_r})\big) \begin{cases} = 2 & 2(a_{i_1}a_{i_2}+\cdots+a_{i_{l-1}}a_{i_l})+ \\ & a_m^2 \not\equiv 0 \bmod p \\ > 2. & \end{cases}$$

In particular, $S(F) \neq 0$ and $F(X) = a_1X^{p-2}+a_2X^{d_1}+\cdots+a_{r-1}X^{d_{r-1}}+a_rX$ is not a permutation polynomial of $\mathbb{F}_p$ whenever $2(a_{i_1}a_{i_2}+\cdots+a_{i_{l-1}}a_{i_l})+a_m^2 \not\equiv 0 \bmod p$.

PROOF. The hypothesis in Theorem 3.8 implies that the minimal solutions of the modular equation $d_1j_1 + d_2j_2 + \cdots + d_rj_r \equiv 0 \bmod p-1$ are of the following two types:

I. $j_{i_k} = j_{i_{k+1}} = 1$ and the rest of the j_i's equal to zero
II. $j_m = 2$ and the rest of the j_i's equal to zero.

The minimal solution $j_{i_k} = j_{i_{k+1}} = 1$ and the rest of the j_i's equal to zero corresponds to $d_{i_k}, d_{i_{k+1}}$ satisfying $d_{i_k} + d_{i_{k+1}} = p-1$. The minimal solution $j_m = 2$ and the rest of the j_i's equal to zero corresponds to $d_m = \frac{p-1}{2}$. The contribution of a minimal solution of type I to the divisibility of $\frac{S(F)}{\theta^2}$ is

$$\begin{aligned}\frac{(p-1)a_{i_k}a_{i_{k+1}}c(1)^2}{\theta^2} &\equiv \frac{(p-1)a_{i_k}a_{i_{k+1}}g(1)^2}{(p-1)^2\theta^2} \bmod \theta \\ &\equiv \frac{a_{i_k}a_{i_{k+1}}}{(p-1)}\left(\frac{g(1)}{\theta}\right)^2 \equiv \frac{a_{i_k}a_{i_{k+1}}}{(p-1)} \bmod \theta.\end{aligned}$$

The contribution of a minimal solution of type II to the divisibility of $\frac{S(F)}{\theta^2}$ is

$$\begin{aligned}\frac{(p-1)a_m^2c(2)}{\theta^2} &\equiv \frac{(p-1)a_m^2g(2)}{(p-1)\theta^2} \bmod \theta \\ &\equiv \frac{a_m^2}{2}\left(\frac{g(2)\cdot 2!}{\theta^2}\right) \equiv -\frac{a_m^2}{2} \bmod \theta.\end{aligned}$$

The total contribution of all the minimal solutions to $\frac{S(F)}{\theta^2}$ is

$$\frac{1}{p-1}(a_{i_1}a_{i_2}+\cdots+a_{i_{l-1}}a_{i_l}) - \frac{a_m^2}{2}.$$

Note that $\frac{1}{p-1}(a_{i_1}a_{i_2}+\cdots+a_{i_{l-1}}a_{i_l}) - \frac{a_m^2}{2}$ is a p-adic integer, hence if $\frac{1}{p-1}(a_{i_1}a_{i_2}+\cdots+a_{i_{l-1}}a_{i_l}) - \frac{a_m^2}{2} \equiv 0 \bmod \theta$, then $\frac{1}{p-1}(a_{i_1}a_{i_2}+\cdots+a_{i_{l-1}}a_{i_l}) - \frac{a_m^2}{2} \equiv 0 \bmod p$. From this our result follows. □

Now we state several corollaries.

COROLLARY 3.9. *Let $p-2 \geq d_1 > d_2 > \cdots > d_{r-1} > d_r \geq 1$, and $d_i \neq \frac{p-1}{2}$ for any i. Then*

$$v_\theta(S(a_1X^{d_1}+a_2X^{d_2}+\cdots+a_{r-1}X^{d_{r-1}}+a_rX^{d_r})) = 2,$$

whenever $l = 2$. In particular, $S(F) \neq 0$ and $F(X)$ is not a permutation polynomial of $\mathbb{F}_p$.

PROOF. Suppose (d_{i_1}, d_{i_2}) is the only order pair such that $d_{i_1} + d_{i_2} = p-1$. In this case we have $a_{i_1}a_{i_2} \not\equiv 0 \bmod p$. □

In the next corollary we apply Theorem 3.8 to the Waring problem over $\mathbb{F}_p$.

COROLLARY 3.10. *Let $p-2 \geq d_1 > d_2 > \cdots > d_{r-1} > d_r \geq 1$, and $d_i \neq \frac{p-1}{2}$ for any i and $F(X) = a_1X^{p-2} + \cdots + a_rX^{d_r}$. Then $F(X_1) + \cdots + F(X_s) = a$ is solvable for any $a \in \mathbb{F}_p$ whenever $s \geq \frac{p-1}{2}$, and $l = 2$.*

PROOF. Let N be number the solutions of the equation $F(X_1)+\cdots+F(X_s) = a$ over $\mathbb{F}_p$. Then the following system of modular equations is associated to N:

$$\begin{aligned} d_1j_{11} + d_2j_{21} + \cdots + d_{r-1}j_{r-11} + d_rj_{r1} &\equiv 0 \bmod p-1 \\ &\vdots \cdots \\ d_1j_{1s} + d_2j_{2s} + \cdots + d_{r-1}j_{r-1s} + d_rj_{rs} &\equiv 0 \bmod p-1. \\ j_{11} + \cdots + j_{rs} + j &\equiv 0 \bmod p-1 \end{aligned}$$

This system has a unique minimal solution since $l = 2$. Therefore p does not divide the number of solutions of $F(X_1) + \cdots + F(X_s) = a$. □

REMARK 1. Theorem 3.8 implies that p does not divide the number of solutions of the following system of polynomial equations:

$$\begin{aligned} a_1X_1^d + \cdots + a_{p-1}X_{p-1}^d &= a \\ b_1X_1^{p-1-d} + \cdots + b_{p-1}X_{p-1}^{p-1-d} &= b. \end{aligned}$$

Hence this system is solvable for any $(a, b) \in \mathbb{F}_p^2$.

COROLLARY 3.11. *Let $p-2 = d_1 > d_2 > \cdots > d_m = \frac{p-1}{2} > \cdots > d_{r-1} > d_r = 1$, $d_i + d_j \neq p-1$ for $i \neq j$ and $1 < i, j < r$. Then*

$$v_\theta\big(S(a_1X^{d_1} + \cdots + a_{r-1}X^{d_{r-1}} + a_rX)\big) \begin{cases} = 2 & \text{if } 2a_1a_r + a_m^2 \not\equiv 0 \bmod p \\ > 2 & \text{otherwise.} \end{cases},$$

where $a_1a_ma_r \neq 0$. In particular, $F(X) = a_1X^{p-2} + a_1X^{d_1} + \cdots + a_mX^{\frac{p-1}{2}} + \cdots + a_{r-1}X^{d_{r-1}} + a_rX$ is not a permutation polynomial of $\mathbb{F}_p$ whenever $2a_1a_r + a_l^2 \not\equiv 0 \bmod p$.

PROOF. In this case we have $\frac{a_1a_r}{(p-1)} - \frac{a_m^2}{2} \equiv 0 \bmod p$. From this our result follows. □

COROLLARY 3.12. *Let $p-1 > d_1 > d_2 > \cdots d_m = \frac{p-1}{2} > \cdots > d_{r-1} > d_r \geq 1$, and $d_i + d_j \neq p-1$ for any i, j with $i \neq j$. Then*

$$v_\theta\big(S(a_1X^{d_1} + a_2X^{d_2} + \cdots + a_rX^{d_r})\big) = 2,$$

whenever $a_m \neq 0$. In particular, $S(F) \neq 0$ and $F(X)$ is not a permutation polynomial of $\mathbb{F}_p$.

PROOF. The proof is similar to the proof of Corollary 3.11. □

As in Corollary 3.10, we apply Theorem 3.8 to the Waring problem over $\mathbb{F}_p$.

COROLLARY 3.13. *Let $p-1 > d_1 > d_2 > \cdots > \frac{p-1}{2} = d_m > \cdots > d_{r-1} > d_r \geq 1$, and $d_i + d_j \neq p-1$ for any i, j with $i \neq j$ and $F(X) = a_1X^{d_1} + a_2X^{d_2} + \cdots + a_mX^{\frac{p-1}{2}} + \cdots + a_rX^{d_r}$. Then $F(X_1) + \cdots + F(X_s) = a$ is solvable for any $a \in \mathbb{F}_p$ whenever $s \geq \frac{p-1}{2}$ and $a_m \neq 0$.*

EXAMPLE 3.14. Let $F(X) = X^{p-2} + X^d + X$ be a polynomial over $\mathbb{F}_p$.

- $\gamma(F,11)=2$ for $2\leq d\leq 8$, $d\neq 5$ and $\gamma(F,11)=3$ for $d=5$.
- $\gamma(F,13)=2$ for $2\leq d\leq 10$, $d\neq 6$ and $\gamma(F,11)=3$ for $d=6$.
- $\gamma(F,17)=2$ for $2\leq d\leq 14$.
- $\gamma(F,19)=2$ for $2\leq d\leq 16$.

Now, we compute the exact divisibility of exponential sums of type $S(aX^{d_1}+bX^{d_2})$, where d_1-d_2 divides $p-1$.

THEOREM 3.15. *Let d_1,d_2 be positive integers satisfying $d_1>d_2>0$ and $d_1\not|(p-1)$. Let $F(X)=aX^{d_1}+bX^{d_2}(ab\neq 0)$ be a binomial over $\mathbb{F}_p$ and $(d_1,d_2)=1$. If $d_1-d_2\mid p-1$*

(1) *then $\nu_\theta(S(F))\geq d_1-d_2$.*

(2) *and $\frac{p-1}{d_1-d_2}>d_1-d_2-\overline{d_1}\geq 0$, then $\nu_\theta(S(F))=d_1-d_2$ where $\overline{d_1}$ is the smallest nonnegative integer congruent to d_1 mod $\frac{p-1}{d_1-d_2}$. In this situation, $S(F)\neq 0$ and F does not permute $\mathbb{F}_p$.*

PROOF. We can write the modular equation associated to $S(F)$ as follows $(d_1-d_2)j_1+d_2(j_1+j_2)\equiv 0 \bmod p-1$. Then $d_2(j_1+j_2)\equiv 0 \bmod (d_1-d_2)$. We obtain $j_1+j_2\equiv 0 \bmod (d_1-d_2)$. Hence a minimal solution of $d_1j_1+d_2j_2\equiv 0 \bmod p-1$ is $\geq d_1-d_2$. This completes the proof of the first part of Theorem 3.15.

Let $j_2=\overline{d_1}\equiv d_1 \bmod \frac{p-1}{d_1-d_2}$, and $j_1=d_1-d_2-\overline{d_1}$. We are going to prove that (j_1,j_2) is a minimal solution of $d_1j_1+d_2j_2\equiv 0 \bmod p-1$.

$$d_1j_1+d_2j_2=d_1(d_1-d_2-\overline{d_1})+d_2\overline{d_1}$$
$$d_1(d_1-d_2)+(d_2-d_1)\overline{d_1}=(d_1-d_2)(d_1-\overline{d_1})\equiv 0 \bmod p-1$$

Now we are going to prove that this solution is unique. Suppose that (j_1,j_2) is another minimal solution, i.e., $j_1+j_2=d_1-d_2$. We have $(d_1-d_2)(d_1-d_2-\overline{d_1})+d_2(d_1-d_2)=c_1(p-1),(d_1-d_2)j_1+d_2(d_1-d_2)=c_2(p-1)$. If $c_1=c_2$ then $j_1=d_1-d_2-\overline{d_1}$ and it is unique. If $c_1\neq c_2$, then $j_1=d_1-d_2+\overline{d_1}+(\frac{p-1}{d_1-d_2})l$. If $l\geq 1$, then $j_1\geq d_1-d_2-\overline{d_1}+\frac{p-1}{d_1-d_2}$. Hence

$$d_1-d_2=j_1+j_2\geq d_1-d_2-\overline{d_1}+\frac{p-1}{d_1-d_2}\leftrightarrow \overline{d_1}\geq\frac{p-1}{d_1-d_2}.$$

This is a contradiction. If $l<0$, then $j_1\leq d_1-d_2-\overline{d_1}-\frac{p-1}{d_1-d_2}$. This a contradiction since $\frac{p-1}{d_1-d_2}>d_1-d_2-\overline{d_1}$. Hence $l=0$.

□

In [**14**], Masuda-Zieve proved the following results about permutation binomials: Let $d_1>d_2$ be positive integers.

- If $F(X)=X^{d_1}+aX^{d_2}$ permutes $\mathbb{F}_p$, then $s>\sqrt{p}-1$, where $s=gcd(d_1-d_2,p-1)$, and $a\in\mathbb{F}_p^*$.
- If $F(X)=X^{d_1}+aX^{d_2}$ permutes $\mathbb{F}_p$, then $p-1\leq(d_1-1)\cdot\max\{d_2,s\}$, where $s=gcd(d_1-d_2,p-1)$, and $a\in\mathbb{F}_p^*$.

EXAMPLE 3.16. Various examples:

- Consider the polynomial $F(X)=X^{29}+aX^9$ over $\mathbb{F}_{61}$. F is a permutation polynomial of $\mathbb{F}_{61}$ for $a\in\{2,3,6,17,19,26,33,36,38,39,41,45\}$.

- Consider the polynomial $F(X) = X^{31} + aX$ over $\mathbb{F}_{2311}$. Masuda-Zieve's result implies that F does not permute $\mathbb{F}_{2311}$ since $30 < \sqrt{2311} - 1$. Theorem 3.15 does not give any information about F since $d_1 - d_2 - \overline{d_1} = -1 < 0$. In this case the minimum is $m = 90$ and it is unique. Hence $\nu_\theta(S(F)) = 90$.
- Consider the polynomial $F(x) = X^{17} + aX^7$ over $\mathbb{F}_{61}$. In this case we have that $6 > 10 - 5 = 5 > 0$. Therefore, Theorem 3.15 implies that F does not permute $\mathbb{F}_{61}$. We have $\nu_\theta(S(F)) = 10$. Masuda-Zeive's results do not give any information since $10 > \sqrt{61} - 1$ and $p - 1 > 16 \times 10 = 160$.
- Consider the polynomial $F(X) = X^{151} + aX^{120}$ over $\mathbb{F}_{683}$. In this case we have that $22 > 31 - 27 = 4 > 0$. Therefore, Theorem 3.15 implies that F does not permute $\mathbb{F}_{683}$. We have $\nu_\theta(S(F)) = 31$. Masuda-Zieve's results do not give any information since $31 > \sqrt{683} - 1$.

REMARK 2. We cannot apply Theorem 3.15 to a polynomial $F(X) = X^{d_1} + aX^{d_2}$, when $d_1 - d_2$ does not divide $p - 1$, but it can be applied to the polynomial $F'(X) = X^{s+d_2 j} + ax^{d_2}$, where $s = gcd(d_1 - d_2, p - 1)$, $js \equiv s \bmod p - 1$ and $gcd(j, p - 1) = 1$. The modular equations associated to F and F' are equivalent. Hence $\nu_\theta(S(F)) = \nu_\theta(S(F'))$.

EXAMPLE 3.17. Consider the polynomial $F(X) = X^{41} + aX^{13}$ over $\mathbb{F}_{127}$. Note that $d_1 - d_2 = 28$ does not divide 126. In this case $F'(X) = X^{79} + aX^{65}$. Note F' satisfies the hypothesis of Theorem 3.15, $9 > 14 - 7 = 7 > 0$. Therefore, Theorem 3.15 implies that $\nu_\theta(S(F)) = 14$ and F does not permute $\mathbb{F}_{127}$.

Now we apply Theorem 3.15 to the Waring Problem.

COROLLARY 3.18. *With the notation and hypotheses of part 2 of Theorem 3.15. Let $F(X) = aX^{d_1} + bX^{d_2}$ be a polynomial over $\mathbb{F}_p$. Then $F(X_1) + \cdots + F(X_s) = a$ is solvable for any $a \in \mathbb{F}_p$ whenever $s \geq \frac{p-1}{d_1 - d_2}$.*

EXAMPLE 3.19. Let $d_1 = 100, d_2 = 9$ and $p = 5279$. Applying Corollary 3.18, the equation $\sum_{i=1}^{s} X_i^{100} + X_i^9 = a$ is solvable for $s \geq 58$, $a \in \mathbb{F}_{5279}$.

References

[1] Adolphson, A. and Sperber, S., p-adic Estimates for Exponential Sums and the Theorem of Chevalley-Warning, *Ann. Sci. Ecole Norm. Sup.* **20**, 545-556, 1987.

[2] A. Adolphson and S. Sperber, Exponential Sums Nondegenerate Relative to a Lattice, *Algebra & Number Theory* **8**, 881-906, 2009.

[3] T. Cochrane, C. Pinner and J. Rosenhouse, Bounds on Exponential Sums and the Polynomial Waring Problem Mod p, *J. London Math. Soc.* **67**, 319-336, 2003.

[4] T. Cochrane and C. Pinner, Sum-Product Estimates Applied to Waring's Problem Mod p, *INTEGERS: Elec J. Comb. Num. T.* **8**, A46, 2008.

[5] L. Carlitz, D. J. Lewis, W. H. Mills and E. G. Straus, Polynomials over Finite Fields with Minimal Value Sets, *Mathematika* **8**, 121-130, 1961.

[6] Castro, F. N., Rubio, I. and Vega, J., Divisibility of Exponential Sums and Solvability of Certain Equations over Finite Fields, *The Quart. J. Math.* **60**, 169-181, 2008.

[7] F. Castro, L. Medina, and I. Rubio, Exact Divisibility of Exponential Sums over the Binary Field via the Covering Method, *Contemp. Math.* **537**, 129-136, 2011.

[8] D.R. Heath-Brown and S. Koyangin, New Bounds for Gauss Sums Derived from Kth Powers, and for Heilbronn's Exponential Sum, *Quart. J. Math.* **51**, 221-235, 2000.

[9] D. Gomez and A. Winterhof, Waring's Problem in Finite Fields with Dickson Polynomials. Finite fields: Theory and Applications, *Contemp. Math.* **518**, 185-192, 2010.

[10] S. V. Konyagin, Estimates for Gaussian Sums and Waring's Problem Modulo a Prime, *Trudy Mat. Inst.* 198(1992), 111-124 (in Russian); English transl.: Proc. Steklov Inst. Math. **1**, 105-117, 1994.

[11] S. Konyagin and I. Shparlinski, *Character Sums with Exponential Functions and Their Applications* **136**, Cambridge Univ. Press, 1999.
[12] S. Koyangin, Enumerating Permutation Polynomials over Finite Fields by Degree, *Finite Fields and Their Applications* **8**, 548-553, 2002.
[13] R. Lidl, and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, 1997.
[14] A. Masuda and M. Zieve, Permutation Binomials over Finite Fields, *Trans. Amer. Math. Soc.* **361**, 4169-4180, 2009.
[15] O. Moreno and C. J. Moreno, Improvements of the Chevalley-Warning and the Ax-Katz theorems, *Amer. J. Math.* **1**, 241-244, 1995.
[16] O. Moreno, K. Shum , F, N. Castro, and P. V. Kumar, Tight Bounds for Chevalley-Warning-Ax Type Estimates, with Improved Applications, *Proc. of the London Math. Soc.* **88**, 545-564, 2004.
[17] C. J. Moreno, *Algebraic Curves over Finite Fields*, *Cambridge Tracts in Mathematics* **97**, Cambridge University Press, 1994.
[18] A. Ostafe and I. E. Shparlinski, On the Waring Problem with Dickson Polynomials in Finite Fields, *Proc. Amer. Math. Soc.* **139** , 3815-3820, 2011.
[19] I. Rubio and F. N. Castro, Solvability of systems of polynomial equations with some prescribed monomials. Finite fields: Theory and Applications, *Contemp. Math.* **518**, 73-81, 2010.
[20] S. Scholten and H. June Zhu, The First Case of Wan's Conjecture, *Finite Fields and Their Applications* **8**, 414-419, 2002.
[21] S. Sperber, On the p-adic Theory of Exponential Sums, *Amer. J. Math.* **108**, 255-296, 1986.
[22] R. Yang, Newton Polygons of L-functions of polynomials of the form $x^d + \lambda x$, *Finite Fields and Their Applications* **9**, 59-88, 2003.
[23] A. Winterhof, On Waring's Problem in Finite Fields, *Acta Arith.* **LXXXVII.2**, 171-177, 1998.
[24] H. J. Zhu, p-adic Variation of L functions of One Variable Exponential Sums, *J. Reine Angew. Math.* **572**, 219-233, 2004.
[25] H. J. Zhu, Asymptotic Variation of L functions of One Variable Exponential Sums I, *Amer. J. Math.* **125**, 669-690, 2003.

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

E-mail address: junioyjulio@gmail.com

E-mail address: luis.medina17@upr.edu