Divisibility of Exponential Sums and Solvability of Certain Equations Over Finite Fields

Francis N. Castro*
Department of Mathematics
University of Puerto Rico
Box 23355, S.J., PR 00931-3355

Ivelisse Rubio†
Department of Computer Science
University of Puerto Rico
Box 23355, S.J., PR 00931-3355

José M. Vega‡
Department of Mathematics and Physics
University of Puerto Rico
Cayey, PR 00736

March 26, 2008

Abstract

In [3], Carlitz determined conditions under which infinite families of polynomials have solutions in a finite field. In this paper we extend

*franciscastr@gmail.com, Tel: (787)764-0000, X4696, Fax: (787)281-0651. This Researh was partially supported by NSF grant The Puerto Rico Math and Science Partnership 0314557

†iverubio@uprrp.edu, Tel: (787)764-0000 (7245), Fax: (787)773-1717

‡jmanueljmvg@yahoo.com, Tel: 787-738-2161. This Researh was partially supported by NSF grant The Puerto Rico Math and Science Partnership 0314557

some of Carlitz's results by computing the exact p-divisibility of certain exponential sums. As a by-product we obtain an upper bound for the Waring number for polynomials over extensions of finite fields.

1 Introduction

Exponential sums over finite fields have many applications to different areas of mathematics [8]. One of the problems of interest is the estimation of its p-divisibility. By computing the exact p-divisibility of the exponential sum associated to a polynomial one can determine if families of equations have solutions over a finite field.

A common tool for the estimation of this divisibility is the well known theorem of Stickelberger [9]. If the exponential sum is expressed as the sum of Gauss sums, then Stickelberger's theorem gives the exact divisibility of each one of the Gauss sums. Of the many known results on the divisibility of exponential sums we use results presented in [11] that give conditions to obtain exact divisibility.

In [3], Carlitz determined conditions under which infinite families of polynomials have solutions in a finite field. In this paper we compute the exact p-divisibility of certain exponential sums under some natural conditions and extend some of Carlitz's results.

We also apply our results to generalizations of the Waring's Problem over finite fields, where we consider sums of polynomials. These generalizations lead to examples where the degree of the polynomial can be arbitrarily large but its Waring number is small.

2 Preliminaries

Let $q = p^f$, p a prime, $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q{}^* = \mathbb{F}_q \backslash 0$. Given $0 \leq j$, j_i integers such that $0 \leq j_i < p$ and $j = \sum_{i=0}^{r-1} j_i p^i$, we define the p-weight of j by $\sigma_p(j) = \sum_{i=0}^{r-1} j_i$. The p-weight degree of a monomial $X_1^{e_1} \cdots X_n^{e_n}$ is defined by $w_p(X_1^{e_1} \cdots X_n^{e_n}) = \sigma_p(e_1) + \cdots + \sigma_p(e_n)$. Sometimes we use $\mathbf{X}$ to denote the variables $X_1, \cdots, X_n$. The p-weight degree of a polynomial $F(X_1, \ldots, X_n) = \sum_i a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}}$, $a_i \neq 0$ over $\mathbb{F}_{p^f}$ is defined by $w_p(F) = \max_i w_p(X_1^{e_{1i}} \cdots X_n^{e_{ni}})$. The p-weight degree with respect to the variable X_i of the monomial $X_1^{e_1} \cdots X_n^{e_n}$ is denoted by $w_{p,X_i}(X_1^{e_1} \cdots X_n^{e_n}) = \sigma_p(e_i)$. We denote the p-weight degree with respect to the variable X_i of a polynomial F over $\mathbb{F}_q$ by $w_{p,X_i}(F) = \max_i w_{p,X_i}(X_1^{e_{1i}} \cdots X_n^{e_{ni}})$. From now on, we assume that a polynomial $F(X_1, \cdots, X_n)$ contains all the variables $X_1, \cdots, X_n$.

$\mathbb{Q}_p$ is the p-adic field with ring of integers $\mathbb{Z}_p$. Let K be the extension over $\mathbb{Q}_p$ obtained by adjoining a primitive $(p^f - 1)$th root of unity in $\overline{\mathbb{Q}_p}$, the algebraic closure of $\mathbb{Q}_p$. The residue class field is isomorphic to $\mathbb{F}_q$ and let $\mathcal{T}$ denote the Teichmüller representatives of $\mathbb{F}_q$ in K. Let ξ be 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 $\phi : \mathbb{F}_q \to \mathbb{Q}(\xi)$ be a nontrivial additive character. The exponential sum associated to F is defined as follows:

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

Note that, since ϕ is an additive character, if $F = \sum_i a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}} = G(X_1, \cdots, X_n) + \beta$, where $G(0, \cdots, 0) = 0$, then

$$\sum_{x_1, \ldots, x_n \in \mathbb{F}_q} \phi(F) = \sum_{x_1, \ldots, x_n \in \mathbb{F}_q} \phi(G + \beta) = \phi(\beta) \sum_{x_1, \ldots, x_n \in \mathbb{F}_q} \phi(G).$$

Since $\phi(\beta)$ is a unit, the constant term does not affect the p-divisibility of the sum.

The following theorem [11] gives a bound for the valuation of an exponential sum with respect to θ.

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

$$S(F) = \sum_{x_1, \cdots, x_n \in \mathbb{F}_q} \phi(F(x_1, \cdots, x_n)), \tag{1}$$

then $v_\theta(S(F)) \geq L$, where $L = \min_{(j_1, \ldots, j_N)} \left\{ \sum_{i=1}^{N} \sigma_p(j_i) \mid 0 \leq j_i < q \right\}$, and $(j_1, \ldots, j_N)$ is a solution to the system

$$\begin{cases} e_{11} j_1 + e_{12} j_2 + \ldots + e_{1N} j_N & \equiv 0 \bmod q - 1 \\ \vdots & \vdots \\ e_{n1} j_1 + e_{n2} j_2 + \ldots + e_{nN} j_N & \equiv 0 \bmod q - 1, \end{cases} \tag{2}$$

where $\sum_{i=1}^{N} e_{li} j_i \neq 0$, for $l = 1, \cdots, n$.

To obtain this bound, the authors in [11] use the Teichmüller representatives $a'_i \in \mathcal{T}$ of the coefficients a_i of F to lift and expand the exponential sum $S(F)$:

$$S(F) = \sum_{j_1=0}^{q-1} \cdots \sum_{j_N=0}^{q-1} \left[\prod_{i=1}^{N} c(j_i)\right] \left[\sum_{\mathbf{t}\in\mathcal{T}^n} \mathbf{t}^{j_1\mathbf{e}_1+\cdots+j_N\mathbf{e}_N}\right] \left[\prod_{i=1}^{N} {a'}_i^{j_i}\right]. \qquad (3)$$

For each term $T = \prod_{i=1}^{N} c(j_i) \sum_{\mathbf{t}} \mathbf{t}^{j_1\mathbf{e}_1+\cdots+j_N\mathbf{e}_N} \prod_{i=1}^{N} {a'}_i^{j_i}$ in the sum (3),

$$v_\theta\left(\left[\prod_{i=1}^{N} c(j_i)\right] \left[\sum_{\mathbf{t}} \mathbf{t}^{j_1\mathbf{e}_1+\cdots+j_N\mathbf{e}_N}\right] \left[\prod_{i=1}^{N} {a'}_i^{j_i}\right]\right) \qquad (4)$$

$$= \sum_{i=1}^{N} \sigma_p(j_i) + f(p-1)s,$$

where s is the number of expressions in (2) that are equal to zero for the vector $(j_1, \cdots, j_N)$ associated to the term. Since the polynomial F contains all the variables, we can always find a solution $(j_1, \ldots, j_N)$ such that $\sum_{i=1}^{N} \sigma_p(j_i)$ is minimum and all the expressions in (2) are positive multiples of $q-1$, giving $f(p-1)s = 0$. The triangle inequality is then used to obtain the bound.

Note that 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 give the minimum value and when the associated terms are added they could produce higher powers of θ dividing the exponential sum. In Section 4 we prove that, for many infinite families of polynomials, there is a unique solution $(j_1, \ldots, j_N)$ that gives the minimum. This implies that $v_\theta(S(F)) = L$. To prove that there is a unique minimum solution one has to consider all the possible solutions to the modular system, including those that make some of the equations in (2) equal to zero.

In our computations we will be using the following lemma, which was proved in [11].

Lemma 1. *For any natural number k, $\sigma_p((p^f-1)k) \geq \sigma_p(p^f-1) = f(p-1)$.*

The relation between an exponential sum $S(F) = \sum_{\mathbf{x}\in\mathbb{F}_q{}^n} \phi(F(\mathbf{x}))$ and the number of zeros of a system of polynomials $P_1(\mathbf{X}), \cdots, P_t(\mathbf{X})$ is given by the following lemma that can be found in [1].

Lemma 2. *Let $q = p^f$, $P_1(\mathbf{X}), \cdots, P_t(\mathbf{X}) \in \mathbb{F}_q[\mathbf{X}]$ and N be the number of common zeros of $P_1, \cdots, P_t$. Then,*

$$N = p^{-tf} \sum_{\mathbf{x} \in \mathbb{F}_q{}^n, \mathbf{y} \in \mathbb{F}_q{}^t} \phi(y_1 P_1(\mathbf{x}) + \cdots + y_t P_t(\mathbf{x})).$$

In this paper we use p-divisibility of exponential sums to prove solvability of polynomial equations. Another common method to prove solvability of equations is to estimate the absolute value of the corresponding exponential sum. Usually, for the absolute value method, the solvability only depends on having $q > d^\epsilon$, where d is the degree of the polynomial and q is the size of the field (see [12], [8], [7]). The results presented here cover cases that are not covered by the absolute value method.

3 Carlitz's Results

There are many results on divisibility properties of the number of solutions of systems of polynomial equations over finite fields. Our work generalize the following results of Carlitz ([3]).

Theorem 2. *If $F(X_1, \ldots, X_n)$ is homogeneous of degree n while $G(X_1, \ldots, X_n)$ is of degree less than n, and*

$$\sum_{x_1, \ldots, x_n \in \mathbb{F}_q} F^{q-1}(x_1, \ldots, x_n) \neq 0,$$

then the equation $F(X_1, \ldots, X_n) = G(X_1, \ldots, X_n)$ has at least one solution over $\mathbb{F}_q$.

This is a very general theorem but the condition $\sum_{\mathbf{x} \in \mathbb{F}_q{}^n} F^{q-1}(\mathbf{x}) \neq 0$ could be hard to verify. The following results do not assume this condition.

Theorem 3. *Let d be a divisor of $p-1$, and $a_i \in \mathbb{F}_q{}^*$ for $i = 1, \cdots, d$. If $G(X_1, \ldots, X_d)$ is a polynomial over $\mathbb{F}_q$ with $deg(G) < d$, then the equation $a_1 X_1^d + \cdots + a_d X_d^d + G(X_1, \ldots, X_d) = 0$ has at least one solution over $\mathbb{F}_q$.*

Corollary 4. *Let d be a divisor of $p-1$ and $F_1(X_1), \ldots, F_d(X_d)$ be polynomials over $\mathbb{F}_q$ of degree d. Then the equation $F_1(X_1) + \cdots + F_d(X_d) = 0$ has at least one solution over $\mathbb{F}_q$.*

4 Exact Divisibility of Exponential Sums and Solvability of Equations

In this section we compute the exact divisibility of certain exponential sums and of the number of solutions of the related equations. With this we guarantee that these equations are solvable and obtain generalizations of Carlitz's results.

Theorem 5. *Let d_i be a divisor of $p-1$ and $a_i \in \mathbb{F}_q^*$ for $i = 1, \ldots, t$. Consider the monomials*

$$(X_{i_1} \cdots X_{i_{n_1}})^{d_1}, (X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2}, \ldots, (X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t} \tag{5}$$

all with the same degree $d > 1$, disjoint support, and $1 \leq i_j \leq n = n_t$. If $G(X_1, \ldots, X_n)$ is a polynomial over $\mathbb{F}_q$ with $w_p(G) < d$, and

$$\begin{aligned} F(X_1, \cdots, X_n) = a_1(X_{i_1} \cdots X_{i_{n_1}})^{d_1} + a_2(X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2} + \cdots \\ + a_t(X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t} + G(X_1, \ldots, X_n), \end{aligned}$$

then

$$v_\theta(S(F)) = f(p-1) \sum_{i=1}^{t} \frac{1}{d_i}.$$

Proof. Without of loss of generality, we can assume that the monomials in (5) are of the form

$$(X_1 \cdots X_{n_1})^{d_1}, (X_{n_1+1} \cdots X_{n_2})^{d_2}, \ldots, (X_{n_{t-1}+1} \cdots X_n)^{d_t},$$

and $F(0, \cdots, 0) = 0$. Let $G(X_1, \ldots, X_n) = \sum_{r=1}^{N} b_r X_1^{e_{1r}} \cdots X_n^{e_{nr}}$. As in Theorem 1, we associate a modular system to the polynomial F. The following is the modular system associated to F:

$$1) \left\{ \begin{array}{cc} d_1 h_1 + e_{1,1} s_1 + e_{1,2} s_2 + \cdots + e_{1,N} s_N & \equiv 0 \bmod q-1 \\ \vdots & \vdots \\ d_1 h_1 + e_{n_1,1} s_1 + \cdots + e_{n_1,N} s_N & \equiv 0 \bmod q-1 \end{array} \right. \tag{6}$$

$$2) \left\{ \begin{array}{cc} d_2 h_2 + e_{n_1+1,1} s_1 + \cdots + e_{n_1+1,N} s_N & \equiv 0 \bmod q-1 \\ \vdots & \vdots \\ d_2 h_2 + e_{n_2,1} s_1 + \cdots + e_{n_2,N} s_N & \equiv 0 \bmod q-1 \end{array} \right.$$

$$\vdots$$

$$t)\ \begin{cases} d_t h_t + e_{n_{t-1}+1,1} s_1 + \cdots + e_{n_{t-1}+1,N} s_N & \equiv 0 \bmod q-1 \\ \vdots & \vdots \\ d_t h_t + e_{n,1} s_1 + \cdots + e_{n,N} s_N & \equiv 0 \bmod q-1 \end{cases}$$

Let $(h_1, \cdots, h_t, s_1, \cdots, s_N)$ be any solution to system (6), and T be the term in (3) associated to this solution. Then

$$v_\theta(T) = \sum_{i=1}^{t} \sigma_p(h_i) + \sum_{i=1}^{N} \sigma_p(s_i) + f(p-1)s,$$

where s is the number of equations in (6) that are equal to zero. Let $n_0 = 0$, and, for $i = 1, \cdots, t$, let r_i be the number of equations that are equal to zero in each block i of $n_i - n_{i-1}$ equations in (6). Since $d_i \leq p-1$, $\sigma_p(d_i) = d_i$. Applying σ_p to (6), using Lemma 1, adding the first $n_1 - r_1$ non-zero inequalities, and dividing by $d_1 n_1$, we obtain

$$\sigma_p(h_1) + \tfrac{\sigma_p(e_{1,1})+\cdots+\sigma_p(e_{n_1,1})}{d_1 n_1}\sigma_p(s_1) + \cdots + \tfrac{\sigma_p(e_{1,N})+\cdots+\sigma_p(e_{n_1,N})}{d_1 n_1}\sigma_p(s_N) \geq \tfrac{f(p-1)(n_1-r_1)}{n_1 d_1}.$$

We repeat the same to each block i of modular equations in (6) to obtain:

$$\sigma_p(h_i) + \tfrac{\sigma_p(e_{n_{i-1}+1,1})+\cdots+\sigma_p(e_{n_i,1})}{d_i(n_i-n_{i-1})}\sigma_p(s_1) + \cdots + \tfrac{\sigma_p(e_{n_{i-1}+1,N})+\cdots+\sigma_p(e_{n_i,N})}{d_i(n_i-n_{i-1})}\sigma_p(s_N)$$

$$\geq \tfrac{f(p-1)(n_i-n_{i-1}-r_i)}{(n_i-n_{i-1})d_i} \text{ for } 1 \leq i \leq t.$$

Recall that $d_i(n_i - n_{i-1}) = d$, and add the above inequalities to get

$$\textstyle\sum_{i=1}^{t} \sigma_p(h_i) + \tfrac{\sigma_p(e_{1,1})+\cdots+\sigma_p(e_{n,1})}{d}\sigma_p(s_1) + \cdots + \tfrac{\sigma_p(e_{1,N})+\cdots+\sigma_p(e_{n,N})}{d}\sigma_p(s_N)$$

$$\geq f(p-1)\textstyle\sum_{i=1}^{t} \tfrac{n_i-n_{i-1}-r_i}{(n_i-n_{i-1})d_i}.$$

Since $\sigma_p(e_{1,k}) + \cdots + \sigma_p(e_{n,k})$ is the p-weight degree of the k^{th} monomial of G, and $w_p(G) < d$, we have that $\frac{\sigma_p(e_{1,k})+\cdots+\sigma_p(e_{n,k})}{d} < 1$. Therefore,

$\sum_{i=1}^{t} \sigma_p(h_i) + \sum_{i=1}^{N} \sigma_p(s_i) \geq$

$\sum_{i=1}^{t} \sigma_p(h_i) + \frac{\sigma_p(e_{1,1})+\cdots+\sigma_p(e_{n,1})}{d}\sigma_p(s_1) + \cdots + \frac{\sigma_p(e_{1,N})+\cdots+\sigma_p(e_{n,N})}{d}\sigma_p(s_N)$

$\geq f(p-1)\sum_{i=1}^{t} \frac{n_i - n_{i-1} - r_i}{(n_i - n_{i-1})d_i}$,

and

$$v_\theta(T) \geq f(p-1)\left[\sum_{i=1}^{t} \frac{n_i - n_{i-1} - r_i}{(n_i - n_{i-1})d_i} + \sum_{i=1}^{t} r_i\right] \tag{7}$$
$$= f(p-1)\left[\sum_{i=1}^{t} \frac{1}{d_i} + \sum_{i=1}^{t} \frac{r_i\left[(n_i - n_{i-1})d_i - 1\right]}{(n_i - n_{i-1})d_i}\right].$$

Note that if $s_i \neq 0$ for some i, we have strict inequality in (7). Also note that since $r_i\left[(n_i - n_{i-1})d_i - 1\right] \geq 0$, any solution with $v_\theta(T) = f(p-1)\sum_{i=1}^{t} \frac{1}{d_i}$ is minimal and has $s_i = 0$ for all $i = 1, \cdots, N$.

Consider
$$\left(\frac{\lambda_1(q-1)}{d_1}, \cdots, \frac{\lambda_t(q-1)}{d_t}, 0, \cdots, 0\right), \tag{8}$$
where $0 \leq \lambda_i \leq d_i$ for all $i = 1, \cdots, t$. This is a solution to (6) with

$$\sum_{i=1}^{t} \sigma_p(h_i) + \sum_{i=1}^{N} \sigma_p(s_i) = \sum_{i=1}^{t} \sigma_p\left(\frac{\lambda_i(q-1)}{d_i}\right)$$
$$= \sum_{i=1}^{t} \sigma_p\left(\frac{\lambda_i(p-1)}{d_i}\sum_{k=1}^{f} p^{f-k}\right) = f(p-1)\sum_{i=1}^{t} \frac{\lambda_i}{d_i},$$

and,

$$v_\theta(T) = f(p-1)\left[\sum_{i=1}^{t} \frac{\lambda_i}{d_i} + s\right],$$

where s is the number of equations in (6) that are equal to zero for this solution.

If $\lambda_i = 1$ for $i = 1, \cdots, t$, then none of the equations in (6) are equal to zero and $v_\theta(T) = f(p-1)\sum_{i=1}^{t} \frac{1}{d_i}$. Therefore, $\left(\frac{q-1}{d_1}, \cdots, \frac{q-1}{d_t}, 0, \cdots, 0\right)$ is a minimal solution. Any other minimal solution must have the form (8) and $\sum_{i=1}^{t} \frac{r_i[(n_i-n_{i-1})d_i-1]}{(n_i-n_{i-1})d_i} = 0$. Since $r_i\left[(n_i-n_{i-1})d_i-1\right] \geq 0$, this sum is zero if and only if $n_i - n_{i-1} = d_i = 1$ or $r_i = 0$ for each $i = 1, \cdots, t$. If $r_i \neq 0$ for some i, then $n_i - n_{i-1} = d_i = 1$ and this implies that the polynomial F has degree 1, which is a contradiction. If $r_i = 0$ for all $i = 1, \cdots, t$, then $\lambda_i \geq 1$ for all i, $v_\theta(T) = f(p-1)\sum_{i=1}^{t} \frac{\lambda_i}{d_i}$, and this is a minimal solution if and only if $\lambda_i = 1$ for all i.

Therefore $\left(\frac{q-1}{d_1}, \cdots, \frac{q-1}{d_t}, 0, \cdots, 0\right)$ is the unique minimal solution and $v_\theta(F) = f(p-1)\sum_{i=1}^{t} \frac{1}{d_i}$.

□

Remark 1. *This result is false if we allow $d = 1$. For example, consider $G(X_1, \cdots, X_n) = c$, a constant, and $F(X_1, \cdots, X_n) = a_1X_1 + \cdots + a_nX_n + c$. Then, $S(F) = 0$ and the formula for $v_\theta(S(F))$ is not correct.*

Even though the above theorem includes the case $p = 2$, because of the importance of Boolean functions, we include this case as a corollary.

Corollary 6. *Let $p = 2$ and consider the monomials*

$$(X_{i_1} \cdots X_{i_{n_1}}), (X_{i_{n_1+1}} \cdots X_{i_{n_2}}), \ldots, (X_{i_{n_{t-1}+1}} \cdots X_{i_n})$$

all with the same degree $d > 1$, disjoint support, and $1 \leq i_j \leq n = n_t$. If $G(X_1, \ldots, X_n)$ is a polynomial over $\mathbb{F}_q$ with $w_p(G) < d$, and

$$\begin{aligned} F(X_1, \cdots, X_n) = {} & X_{i_1} \cdots X_{i_{n_1}} + X_{i_{n_1+1}} \cdots X_{i_{n_2}} + \cdots \\ & + X_{i_{n_{t-1}+1}} \cdots X_{i_n} + G(X_1, \ldots, X_n), \end{aligned}$$

then

$$v_2(S(F)) = tf.$$

The next corollaries give information about $S(F)$ when $t = 1$.

Corollary 7. *Let d be a divisor of $p-1$, $nd > 1$, and $a \in \mathbb{F}_q^*$. If $G(X_1, \ldots, X_n)$ is a polynomial over $\mathbb{F}_q$ with $w_p(G) < dn$, and*

$$F(X_1, \ldots, X_n) = aX_1^d \cdots X_n^d + G(X_1, \ldots, X_n),$$

then $v_\theta(S(F)) = \frac{f(p-1)}{d}$.

Corollary 8. *Let $d \neq 1$ be a divisor of $p-1$ and $a \in \mathbb{F}_q^*$ If $F(X) = aX^d + b_1X^{d_1} + \cdots + b_rX^{d_r}$ is a polynomial over $\mathbb{F}_q$ where $\sigma_p(d_i) < d$ for every i, then $v_\theta(S(F)) = \frac{f(p-1)}{d}$. Furthermore $S(F) \neq 0$.*

As a consequence of Theorem 5 we can compute the exact divisibility of the number of solutions of families of polynomial equations.

Theorem 9. *Let d_i be a divisor of $p-1$ and $a_i \in \mathbb{F}_q^*$ for $i = 1, \ldots, t$. Suppose that $\sum_{i=1}^t \frac{1}{d_i}$ is an integer and consider the monomials*

$$(X_{i_1} \cdots X_{i_{n_1}})^{d_1}, (X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2}, \ldots, (X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t} \tag{9}$$

all with the same degree $d > 1$, disjoint support, and $1 \leq i_j \leq n = n_t$. If $G(X_1, \ldots, X_n)$ is a polynomial over $\mathbb{F}_q$ with $w_p(G) < d$, and

$$\begin{aligned} F(X_1, \ldots, X_n) = a_1(X_{i_1} \cdots X_{i_{n_1}})^{d_1} + a_2(X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2} + \cdots \\ + a_t(X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t} + G(X_1, \ldots, X_n), \end{aligned}$$

then $p^{f(\sum_{i=}^t \frac{1}{d_i} - 1)}$ is the exact divisibility of the number of solutions of $F = 0$. In particular, F has at least one solution over $\mathbb{F}_q$.

Proof. Consider

$$F' = y\left(a_1(X_{i_1} \cdots X_{i_{n_1}})^{d_1} + \cdots + a_t(X_{i_{n_{t-1}+1}} \cdots X_{i_n})^{d_t} + G(X_1, \ldots, X_n)\right).$$

By Lemma 2, the number of solutions of $F = 0$ is $p^{-f}S(F')$. To compute $S(F')$ we follow the proof of Theorem 5 with F' instead of F. The modular system associated to F' is the same as the one associated to F but with the additional equation

$$h_1 + \cdots + h_t + s_1 + \cdots + s_N \equiv 0 \bmod q-1.$$

If $G(0, \cdots, 0) = 0$, then the proof is almost the same as the one for Theorem 5. If G has a constant term $b_N X_1^{e_{1N}} \cdots X_n^{e_{nN}} \neq 0$, then the term s_N appears in the last new equation of system (6), but $e_{i,N}s_N$ do not appear in the other equations. In any case, we follow the proof of Theorem 5 and note that expression (7) becomes

$$v_\theta(T) \geq f(p-1)\left[\sum_{i=1}^t \frac{1}{d_i} + \sum_{i=1}^t \frac{r_i\left[(n_i - n_{i-1})d_i - 1\right]}{(n_i - n_{i-1})d_i} + \alpha\right],$$

where $\alpha = 1$ if $h_1 + \cdots + h_t + s_1 + \cdots + s_N = 0$ and $\alpha = 0$ otherwise. Again, note that if $s_i \neq 0$ for some i, then we have a strict inequality. Also note that $\sum_{i=1}^t \frac{r_i[(n_i-n_{i-1})d_i-1]}{(n_i-n_{i-1})d_i} + \alpha \geq 0$, and any solution with $v_\theta(T) = f(p-1)\sum_{i=1}^t \frac{1}{d_i}$ is minimal and has $s_i = 0$ for all $i = 1, \cdots, N$.

The vector

$$\left(\frac{\lambda_1(q-1)}{d_1}, \cdots, \frac{\lambda_t(q-1)}{d_t}, 0, \cdots, 0\right), \tag{10}$$

is a solution to the new modular system if and only if $\sum_{i=1}^t \frac{\lambda_i}{d_i}$ is an integer. By hypothesis, $\sum_{i=1}^t \frac{1}{d_i}$ is an integer, and therefore $\left(\frac{q-1}{d_1}, \cdots, \frac{q-1}{d_t}, 0, \cdots, 0\right)$ is a minimal solution. Any other minimal solution must have the form (10) and $\sum_{i=1}^t \frac{r_i[(n_i-n_{i-1})d_i-1]}{(n_i-n_{i-1})d_i} + \alpha = 0$. This implies that

$$v_\theta(T) = f(p-1)\left[\sum_{i=1}^t \frac{\lambda_i}{d_i}\right],$$

and this is minimal if and only if $\lambda_i = 1$ for all i. Therefore,

$$\left(\frac{q-1}{d_1}, \cdots, \frac{q-1}{d_t}, 0, \cdots, 0\right)$$

is the only minimal solution and the result follows. □

Using the above theorem one can generalize Theorem 3 by substituting the degree by the p-weight degree.

Corollary 10. *Let $d > 1$ be a divisor of $p-1$ and $a_i \in \mathbb{F}_q^*$ for $i = 1, \cdots, d$. If $G(X_1, \ldots, X_d)$ is polynomial over $\mathbb{F}_q$ with $w_p(G) < d$, then the equation $a_1X_1^d + \cdots + a_dX_d^d + G(X_1, \ldots, X_d) = 0$ has at least one solution over $\mathbb{F}_q$.*

Example 1. Let $F(X_1, \ldots, X_7) = X_1^7 + X_2^7 + \cdots + X_7^7 + \sum_{i<j} a_{i,j}X_iX_j + X_1^{29^i+1} + \cdots + X_7^{29^i+1}$ over $\mathbb{F}_{29^f}$. The equation $F = \beta$ has at least one solution for any $\beta \in \mathbb{F}_{29^f}$.

In the following theorem we impose conditions on the partial weight of the monomials to compute the exact divisibility of exponential sums. With the exact divisibility we prove that the related equation is solvable.

Theorem 11. *Let $d_i > 1$ be a divisor of $p-1$ and $a_i \in \mathbb{F}_q^*$ for $i = 1, \ldots, n$. Let $G_1, \cdots, G_N$ be monomials. If $G(X_1, \ldots, X_n) = G_1 + \cdots + G_N$ is polynomial over $\mathbb{F}_q$ with $\sum_{i=1}^n \frac{w_{p,X_i}(G_j)}{d_i} < 1$ for $j = 1, \cdots, N$, and $F = a_1 X_1^{d_1} + \cdots + a_n X_n^{d_n} + G(X_1, \ldots, X_n)$, then*

$$v_\theta(S(F)) = f(p-1) \sum_{i=1}^n \frac{1}{d_i}.$$

Proof. We can assume that

$$G(X_1, \ldots, X_n) = b_1 X_1^{d_{11}} \cdots X_n^{d_{n1}} + \cdots + b_N X_1^{d_{1N}} \cdots X_n^{d_{nN}}$$

and $G(0, \cdots, 0) = 0$.

The following is the system of modular equations associated to F:

$$\begin{aligned} d_1 h_1 + d_{11} s_1 + \cdots + d_{1N} s_N &\equiv 0 \bmod q-1 \\ \vdots \qquad\qquad & \qquad \vdots \\ d_n h_n + d_{n1} s_1 + \cdots + d_{nN} s_N &\equiv 0 \bmod q-1. \end{aligned} \tag{11}$$

Let $(h_1, \cdots, h_n, s_1, \cdots s_N)$ be any solution to system (11). As in Theorem 5, applying σ_p, we obtain:

$$\sigma_p(d_i)\sigma(h_i) + \sigma_p(d_{i1})\sigma_p(s_1) + \cdots + \sigma_p(d_{iN})\sigma_p(s_N) \geq \alpha_i \sigma_p(q-1) = \alpha_i f(p-1),$$

where $\alpha_i = 0$ or $\alpha_i = 1$.

Since $d_i \leq p-1$, $\sigma_p(d_i) = d_i$. Dividing by d_i we obtain

$$\sigma_p(h_i) + \frac{\sigma_p(d_{i1})}{d_i}\sigma_p(s_1) + \cdots + \frac{\sigma_p(d_{iN})}{d_i}\sigma_p(s_N) \geq \frac{\alpha_i f(p-1)}{d_i}, \tag{12}$$

for $i = 1, \cdots, n$.

Note that $\sum_{i=1}^n \sigma_p(d_{ij}) = \sum_{i=1}^n w_{p,X_i}(G_j)$. Adding all the inequalities and using the fact that $\sum_{i=1}^n \frac{w_{p,X_i}(G_j)}{d_i} < 1$, we get

$$\sum_{i=1}^n \sigma_p(h_i) + \sum_{i=1}^N \sigma_p(s_i) \geq$$

$$\sum_{i=1}^n \sigma_p(h_i) + \sum_{i=1}^n \frac{\sigma_p(d_{i1})}{d_i}\sigma_p(s_1) + \cdots + \sum_{i=1}^n \frac{\sigma_p(d_{iN})}{d_i}\sigma_p(s_N) \geq f(p-1)\sum_{i=1}^n \frac{\alpha_i}{d_i}.$$

If T is the term in (3) associated to this solution then

$$\begin{aligned} v_\theta(T) &\geq f(p-1)\left[\sum_{i=1}^n \frac{\alpha_i}{d_i} + \sum_{i=1}^n (1-\alpha_i)\right] \\ &= f(p-1)\left[\sum_{i=1}^n \frac{1}{d_i} + \sum_{i=1}^n \frac{(1-\alpha_i)(d_i-1)}{d_i}\right], \end{aligned}$$

where $\sum_{i=1}^n (1-\alpha_i)$ is the number of equations in (11) that are equal to zero. Note that if $s_i \neq 0$ for some i we have strict inequality and, since $(1-\alpha_i)(d_i-1) \geq 0$, any solution with $v_\theta(T) = f(p-1)\sum_{i=1}^n \frac{1}{d_i}$ is minimal and has $s_i = 0$ for all i.

As in Theorem 5, taking $h_i = (q-1)/d_i$ and $s_1 = \cdots = s_N = 0$, we obtain a solution to the system with $\sum_{i=1}^n \sigma_p(h_i) + \sum_{i=1}^N \sigma_p(s_i) = f(p-1)\sum_{i=1}^n \frac{1}{d_i}$ and therefore is minimal. Any other solution with $s_1 = \cdots = s_N = 0$ has $h_i = \frac{\lambda_i(q-1)}{d_i}$ for $0 \leq \lambda_i \leq d_i$ and $v_\theta(T) = \sum_{i=1}^n \sigma_p(h_i) + \sum_{i=1}^N \sigma_p(s_i) + f(p-1)s = f(p-1)\left[\sum_{i=1}^n \frac{\lambda_i}{d_i} + s\right]$, where s is the number of equations in (11) that are equal to zero for this solution. For this solution to be minimal we must have $\sum_{i=1}^n \frac{(1-\alpha_i)(d_i-1)}{d_i} = 0$. If $1-\alpha_i \neq 0$ for some i, then $d_i = 1$, which is a contradiction. If $1-\alpha_i = 0$ for all i, then $\lambda_i \geq 1$, $v_\theta(T) = f(p-1)\sum_{i=1}^n \frac{\lambda_i}{d_i}$, and this is minimal if and only if $\lambda_i = 1$ for all i.

Therefore, $\left(\frac{q-1}{d_1}, \cdots, \frac{q-1}{d_n}, 0, \cdots, 0\right)$ is the unique minimal solution and $v_\theta(T) = f(p-1)\sum_{i=1}^n \frac{1}{d_i}$. □

Note that in Theorem 3 the polynomial has the same degree on each variable and the degree is equal to the number of variables. Applying Theorem 11 we can get another improvement to Theorem 3 that has less restrictions on the degrees. In Section 5 this improvement will be applied to generalizations of the Waring's problem.

Theorem 12. *Let $d_i > 1$ be a divisor of $p-1$ and $a_i \in \mathbb{F}_q^*$ for $i = 1, \ldots, n$. Suppose that $\sum_{i=1}^n \frac{1}{d_i}$ is an integer, and let $G_1, \cdots, G_N$ be monomials. If $G(X_1, \ldots, X_n) = G_1 + \cdots + G_N$ is a polynomial over $\mathbb{F}_q$ with $\sum_{i=1}^n \frac{w_{p,X_i}(G_j)}{d_i} < 1$ for $j = 1, \cdots, N$, and $F(X_1, \cdots, X_n) = a_1X_1^{d_1} + \cdots + a_nX_n^{d_n} + G(X_1, \ldots, X_n)$, then the exact divisibility of the number of solutions of $F = 0$ is $p^{f(\sum_{i=1}^n \frac{1}{d_i} - 1)}$. In particular, the equation has at least one solution over $\mathbb{F}_q$.*

Proof. Similar to the proof of Theorem 9. □

Example 2. Let $F(X_1,\ldots,X_7) = X_1^{10}+\cdots+X_4^{10}+X_5^5+X_6^5+X_7^5+X_1X_2X_3+X_4X_5X_6X_7$ over $\mathbb{F}_{31}$. Then $F=\beta$ has solution for every $\beta \in \mathbb{F}_{31^f}$.

The following corollary improves Corollary 4.

Corollary 13. *Let $d>1$ be a divisor of $p-1$ and suppose that $\frac{n}{d}$ is an integer. If $F_i(X_i) = a_iX_i^d+G_i(X_i)$ is a polynomial over $\mathbb{F}_q$ with $w_p(G_i) < d$ for every i, then the exact divisibility of the number of solutions $F_1(X_1)+\cdots+F_n(X_n)=0$ is $p^{f(\frac{n}{d}-1)}$. In particular, the equation has at least one solution over $\mathbb{F}_q$.*

Example 3. Let $p>5,\ d=\frac{p-1}{2}$, and consider the polynomial

$$F(X_1,\ldots,X_d) = X_1^d+\cdots+X_d^d+X_1^{p^i+1}+\cdots+X_d^{p^i+1}$$

over $\mathbb{F}_q$. Then $F=\beta$ has at least one solution over $\mathbb{F}_q$ for each $\beta\in\mathbb{F}_q$.

If $q=p^{2i}$, then the equation $X_1^{p^i+1}+\cdots+X_d^{p^i+1}=\beta$ does not have solution for all $\beta\in\mathbb{F}_{p^{2i}}\backslash\mathbb{F}_{p^i}$. The above corollary implies that the extra terms force $X_1^d+\cdots+X_d^d+X_1^{p^i+1}+\cdots+X_d^{p^i+1}=\beta$ to have solutions for all $\beta\in\mathbb{F}_{p^{2i}}$.

5 Applications to generalizations of the Waring's Problem

The original Waring's problem is to find the minimum number of variables such that the equation $X_1^d+\cdots+X_n^d=\beta$ has solutions for any natural number β. This minimum number is called the *Waring number* associated to d. The Waring's problem has also been considered for equations over finite fields and there are many bounds for their Waring numbers ([8], [13], [7]). Many of these bounds are consequences of good estimates of the absolute value of Gauss sums ([8], [6]).

In this section we consider a generalization of the Waring's problem: Given a polynomial $F(X)$ over $\mathbb{F}_q$, find the minimum number of variables such that

$$F(X_1)+\cdots+F(X_n)=\beta \tag{13}$$

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

$$\beta = F_1(x_1) + \cdots + F_n(x_n), \tag{14}$$

where $x_1, \dots, x_n \in \mathbb{F}_q$. This problem was considered by Carlitz et. al. [4] and Cochrane et. al. [5] for the prime field. Carlitz et. al. proved that given $F_1(X_1), \dots, F_n(X_n)$ polynomials over $\mathbb{F}_p$ of degree $d_1, \dots, d_n$, every element $\beta \in \mathbb{F}_p$ can be written as $\beta = F_1(x_1) + \cdots + F_n(x_n)$, 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 $\alpha(X_i - \beta)^{\frac{1}{2}(p-1)} + \lambda$. If $F = F_1 = \cdots = F_d$, the above result implies that $\gamma(F, p) \le d$, where d is the degree of F and $d \ne p-1, \frac{p-1}{2}$ (see [5]). In [5], Cochrane et. al. use estimates for exponential sums to prove that (13) has at least one solution for every $\beta \in \mathbb{F}_p$, whenever $r_1 + \cdots + r_{\gamma(F,p)} \ge \log p$, 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 $\mathbb{F}_p$.

We now apply Theorem 12 and obtain some natural conditions so that the elements $\beta \in \mathbb{F}_q$ can be written as $\beta = F_1(x_1) + \ldots + F_n(x_n)$. This gives an upper bound on $\gamma(F, q)$ for polynomials F that satisfy certain natural conditions.

Our results apply to extension fields while the above results only apply for polynomials over $\mathbb{F}_p$.

Theorem 14. *Let $d_i > 1$ be a divisor of $p-1$, $a_i \in \mathbb{F}_q^*$ and $F_i(X) = a_i X_i^{d_i} + G_i(X_i)$ be polynomials over $\mathbb{F}_q$ for $i = 1, \dots, n$. Suppose that $\sum_{i=1}^{n} \frac{1}{d_i}$ is an integer. If $w_p(G_i) < d_i$, then every $\beta \in \mathbb{F}_q$ can be written as*

$$\beta = F_1(x_1) + \cdots + F_n(x_n),$$

for some $x_1, \cdots, x_n \in \mathbb{F}_q$.

Example 4. Let $F_1(X_1) = X_1^6 + X_1^{18}$, $F_2(X_2) = X_2^3 + X_2^{14}$, $F_3(X_3) = X_3^2 + X_3$ over $\mathbb{F}_{13^f}$. Then every $\beta \in \mathbb{F}_{13^f}$ can be written as $\beta = x_1^6 + x_1^{18} + x_2^3 + x_2^{14} + x_3^2 + x_3$.

Corollary 15. *Let $F(X) = aX^d + G(X)$ be a polynomial over $\mathbb{F}_q$, where $d \neq 1$ divides $p-1$. If $w_p(G) < d$, then $\gamma(F,q) \leq d$.*

Example 5. Let $F(X) = X^3 + aX^{p^i+1}$ over $\mathbb{F}_q$, where 3 divides $p-1$. Then $\gamma(F,q) \leq 3$. Using Maple, we obtain that $\gamma(x^3 + x^8, 49) = 2$ and $\gamma(x^3 + x^{14}, 169) = 2$. Note that $\gamma(x^8, 49)$ and $\gamma(x^{14}, 169)$ do not exist.

Example 6. Let $F(X) = X^4 + a_1X^{p^{i_1}+p^{j_1}+1} + a_2X^{p^{i_2}+p^{j_2}+1} + \cdots + a_nX^{p^{i_n}+p^{j_n}+1}$ over $\mathbb{F}_{29^f}$, then $\gamma(F, 29^f) \leq 4$.

Acknowledgements

The authors want to acknowledge that the example presented in Remark 1 was provided by one of the reviewers as a counterexample to a theorem in the original version of the paper. They appreciate the careful review and comments that helped to correct and improve the present version.

References

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

[2] J. Ax, Zeros of Polynomials over Finite Fields, *Am. J. of Math.*, **86**, (1964), pp 255–261.

[3] L. Carlitz, Solvability of Certain Equations in a Finite Field, *Quart. J. Math*, Oxford(**7**) (1956), 3-4.

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

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

[6] 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** (2000), 221-235.

[7] 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**) (1994), 105-117.

[8] S. Konyagin and I. Shparlinski, *Character Sums with Exponential Functions and Their Applications*, (**136**), Cambridge Univ. Press, 1999.

[9] C. J. Moreno, *Algebraic Curves Over Finite Fields*, Cambridge University Press, 1991.

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

[11] 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 Mathematical Society*, **(3) 88** (2004), 545-564.

[12] C. Small, Sums of Powers in Large Fields, *Proc. Amer. Math. Soc.* **65** (1977), 35-36.

[13] A. Winterhof, On Waring's Problem in Finite Fields, *Acta Arithmetica* **LXXXVII.2** (1998), 171-177.