Solvability of Systems of Polynomial Equations with Some Prescribed Monomials

Ivelisse M. Rubio and Francis N. Castro

Abstract. We prove that, under some natural conditions, given a system of polynomials $F_1, \cdots, F_t$ with monomials of disjoint support, any system $F_1 + G_1, \cdots, F_t + G_t$, where the p-weight degree of the G_i's is smaller than the degree of the monomials in the F_i's, is solvable. This generalizes a result of Carlitz. As byproduct we also compute the exact p-divisibility of the number of solutions of the system.

1. Introduction

Solutions of systems of polynomial equations over finite fields have many applications to different areas of mathematics [**5**]. In general it is difficult to find conditions that guarantee that a system of polynomials has a solution over a given finite field. In this paper we prove that, under some natural conditions, given a system of polynomials $F_1, \cdots, F_t$ with monomials of disjoint support, any system $F_1 + G_1, \cdots, F_t + G_t$, where the p-weight degree of the G_i's is smaller than the degree of the monomials in the F_i's, is solvable. In particular, we generalize a result of Carlitz [**1**] and a result of Castro-Rubio-Vega [**2**] to systems of polynomial equations.

To determine if families of systems of polynomial equations have solutions over a finite field we compute the exact p-divisibility of the exponential sum associated to a system of polynomials. A common tool for the estimation of this divisibility is the well known theorem of Stickelberger [**6**]. If the exponential sum corresponding to the system of polynomials is expressed as the sum of Gauss sums, then Stickelberger's theorem gives the exact divisibility of each one of the Gauss sums. 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 depends on how big is the cardinality of the finite field when compared to the degree of the polynomial (see [**4**], [**5**], [**8**], [**9**]). For example, a diagonal equation $X_1^d + X_2^d = \beta$ is solvable over $\mathbb{F}_q$ if $q > (d-1)^4$ [**8**]. One of the bounds used in the absolute value method is Weil's bound. The results presented here include cases that are not covered by the absolute value method.

1991 *Mathematics Subject Classification.* Primary 11T06 ; Secondary 11T23 .

Key words and phrases. exponential sums, systems of polynomial equations, monomial of disjoint support, p-divisibility.

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 j_i integers such that $0 \leq j_i < p$, $i = 0, \cdots, r-1$ 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 $w_p(X_1^{e_1} \cdots X_n^{e_n}) = \sigma_p(e_1) + \cdots + \sigma_p(e_n)$. 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 $w_p(F) = \max_i w_p(X_1^{e_{1i}} \cdots X_n^{e_{ni}})$. Sometimes we use $\mathbf{X}$ to denote the variables $X_1, \cdots, X_n$.

Let $\mathbb{Q}_p$ be the field of p-adic numbers, ξ be a primitive p-th root of unity in $\overline{\mathbb{Q}}_p$, the algebraic closure of $\mathbb{Q}_p$, and $\phi : \mathbb{F}_q \to \mathbb{Q}(\xi)$ be a nontrivial additive character. The exponential sum associated to F is defined as follows:

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

Let Ω be the completion of $\overline{\mathbb{Q}}_p$ and $\theta = 1 - \xi$. The valuation of $x \in \Omega$, $v_\theta(x)$, is the integer n such that $\theta^n \mid x$ but $\theta^{n+1} \nmid x$. Recall that $v_\theta(p) = p - 1$. The next theorem gives a bound for the valuation of an exponential sum with respect to θ. See Theorem 7 in [**7**] for a proof.

THEOREM 1. *Let $F(\mathbf{X}) = \sum_{i=1}^{N} a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}}$, $a_i \in {\mathbb{F}_q}^*$, and assume that F contains all the variables $X_1, \cdots, X_n$. If $S(F)$ is the exponential sum*

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

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

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

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

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

and s the number of expressions in (1) that are equal to zero.

To compute the exact p-divisibility of the exponential sum, we study the proof of this theorem and note that, to obtain the bound, the authors use the Teichmüller representatives $a_i' \in \mathcal{T}$ of the coefficients a_i of F to lift and expand the exponential sum $S(F)$:

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

where $c(j_i)$ is defined in [**7**]. Each solution $(j_1, \cdots, j_N)$ to (1) is associated to a term T in the above sum with

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

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

The triangle inequality is then used to obtain the bound.

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 $\sum_{i=1}^{N} \sigma_p(j_i)$ and, for example, when the associated terms are similar some could cancel and produce higher powers of θ dividing the exponential sum. However, there are situations on which one is able to compute the exact p-divisibility $v_\theta(S(F)) = L$. One situation is the one that we present in this paper when there is a unique solution $(j_1, \ldots, j_N)$ that gives the minimum value of $v_\theta(T)$. We call the solutions $(j_1, \ldots, j_N)$ to (1) that give the minimal value L *minimal solutions*.

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 $F_1(\mathbf{X}), \cdots, F_t(\mathbf{X})$ is given by the following lemma.

Lemma 1. *Let $q = p^f$, $F_1(\mathbf{X}), \cdots, F_t(\mathbf{X}) \in \mathbb{F}_q[\mathbf{X}]$ and N be the number of common zeros of $F_1, \cdots, F_t$. Then,*

$$N = p^{-tf} \sum_{\mathbf{x} \in \mathbb{F}_q{}^n, \mathbf{y} \in \mathbb{F}_q{}^t} \phi(y_1 F_1(\mathbf{x}) + \cdots + y_t F_t(\mathbf{x})).$$

The exact p-divisibility of the exponential sum gives exact p-divisibility of N, the number of solutions of the system of equations. Having exact p-divisibility of N implies that there is a power of p that does not divide N and therefore $N \neq 0$. In Section 4 we compute the exact p-divisibility of exponential sums by proving that there is only one minimal solution. With this we determine sufficient conditions that give infinite families of systems of polynomial equations that are solvable.

3. Previous Results

In the theory of polynomial equations over finite fields a main result is the theorem of Chevalley-Warning: Given a polynomial $F(X_1, \ldots, X_n)$ of degree d over the finite field $\mathbb{F}_q$ and $n > d$, the characteristic p of the field divides the number of solutions of $F = 0$. The theorem of Chevalley-Warning has been applied in many areas of mathematics. Note that Chevalley-Warning does not give information about the solvability of the equation $F = 0$ over $\mathbb{F}_q$.

In 1946 Lászlo Rédei formulated the next conjecture about the solvability of polynomial equations over finite fields.

Rédei's Conjecture. Let p be a prime, $\mathbb{F}_p$ be the field with p elements, and $F \in \mathbb{F}_p[X_1, \ldots, X_n]$ be a non constant polynomial with deg $F \leq$ rank F, where rank $F = \dim_{\mathbb{F}_p} V$, and V is the linear subspace spanned by the partial derivatives of F. Then $F(X_1, \ldots, X_n) = 0$ is solvable.

The conjecture turned out to be false in general but, in 1956, Carlitz [**1**] found infinite families of polynomials satisfying Rédei's Conjecture.

Theorem 2 (Carlitz). *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 $\mathbb{F}_q$.*

This result was extended by Felszeghy [**3**] by showing in 2006 that the deformed diagonal equation $a_1X_1^d + \cdots + a_nX_n^d + G(X_1, \ldots, X_n) = 0$ is solvable over $\mathbb{F}_q$ for $n \geq \lfloor \frac{p-1}{\lceil \frac{p-1}{d} \rceil} \rfloor$, where $deg(G) < d$. The condition d divides $p-1$ is not needed for $q = p$ in Felszeghy's result. This family of solvable polynomials also satisfies Rédei's Conjecture.

In 2008, Castro-Rubio-Vega [**2**] extended the result of Carlitz with the following theorem, which also satisfies Rédei's Conjecture.

Theorem 3 (CRV). *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*

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

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

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

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

The technique used in the proof of this theorem was to compute the exact p-divisibility of an exponential sum using the proof of Theorem 1. In this paper we extend the result to systems of polynomial equations.

4. Solvability of Systems of Polynomial Equations

In this section we compute the exact divisibility of the exponential sums associated to certain systems of polynomial equations and determine sufficient conditions for the systems to be solvable.

For the next theorem consider terms $a_{r,i}(X_1, \ldots, X_n)$ over $\mathbb{F}_q$ of disjoint support, degree > 1, and where each variable in the term has the same degree $d_{r,i}$.

Theorem 4. *With the above notation consider the system*

$$\sum_{r=1}^{k_1} a_{r,1}(X_1, \ldots, X_n) + G_1(X_1, \ldots, X_n) = 0$$
$$\sum_{r=1}^{k_2} a_{r,2}(X_1, \ldots, X_n) + G_2(X_1, \ldots, X_n) = 0$$
$$\vdots \qquad \vdots$$
$$\sum_{r=1}^{k_t} a_{r,t}(X_1, \ldots, X_n) + G_t(X_1, \ldots, X_n) = 0,$$

where $d_{r,i} | (p-1)$, $\sum_r \frac{1}{d_{r,i}}$ is an integer for $i = 1, \ldots, t$, $D_i = \min_r \{deg\,(a_{r,i}(X_1, \ldots, X_n))\}$, and $G_i \in \mathbb{F}_q[\mathbf{X}]$ is such that $w_p(G_i) < \min_j \{D_j\}$. If N is the number of solutions of the system, then $v_p(N) = f\left(\sum_{r,i} \frac{1}{d_{r,i}} - t\right)$, and the system has at least one solution.

Proof. Note that a change of variables do not change the degree or p-weight degree of a polynomial. Also, each variable on a term $a_{r,i}(X_1,\dots,X_n)$ has the same degree $d_{r,i}$. Hence, without loss of generality, we can make a change of variables to put the variables in ascending order and assume that the monomials are

$$(X_1\cdots X_{n_{1,1}})^{d_{1,1}},(X_{n_{1,1}+1}\cdots X_{n_{2,1}})^{d_{2,1}},\dots,(X_{n_{k_1-1,1}+1}\cdots X_{n_{k_1,1}})^{d_{k_1,1}},$$

$$(X_{n_{k_1,1}+1}\cdots X_{n_{1,2}})^{d_{1,2}},\dots,(X_{n_{k_t-1,t}+1}\cdots X_{n_{k_t,t}})^{d_{k_t,t}}, \tag{2}$$

where $n_{k_t,t}=n$. Let $n_{0,i}=n_{k_{i-1},i-1}$ and $n_{0,1}=1$. Note that $D_i\le(n_{r,i}-n_{r-1,i})d_{r,i}$ for any monomial $(X_{n_{r-1,i}+1}\cdots X_{n_{r,i}})^{d_{r,i}}$.

Let

$$G_i(X_1,\dots,X_n)=\sum_{r=1}^{N_i}b_{r,i}X_1^{e_{1ri}}\cdots X_n^{e_{nri}}.$$

To compute, $v_p(N)$ we apply Lemma 1 and let

$$F=\sum_{i=1}^{t}y_i\left[\sum_r a_{r,i}\left(X_1,\cdots,X_n\right)+G_i\right]. \tag{3}$$

Then,

$$v_p(N)=\frac{1}{p-1}v_\theta\left(S(F)\right)-tf.$$

As in Theoerm 1, consider the following modular system associated to F, where each block corresponds to a monomial in (2):

$$\begin{cases} d_{1,1}h_{1,1}+e_{1,1,1}j_{1,1}+\cdots+e_{1,N_1,1}j_{N_1,1}+e_{1,1,2}j_{1,2}+\cdots+e_{1,N_t,t}j_{N_t,t} & \equiv 0 \bmod q-1\\ \vdots & \vdots\\ d_{1,1}h_{1,1}+e_{n_{1,1},1,1}j_{1,1}+\cdots+e_{n_{1,1},N_1,1}j_{N_1,1}+\cdots+e_{n_{1,1},N_t,t}j_{N_t,t} & \equiv 0 \bmod q-1\end{cases}$$

$$\begin{cases} d_{2,1}h_{2,1}+e_{n_{1,1}+1,1,1}j_{1,1}+\cdots+e_{n_{1,1}+1,N_t,t}j_{N_t,t} & \equiv 0 \bmod q-1\\ \vdots & \vdots\\ d_{2,1}h_{2,1}+e_{n_{2,1},1,1}j_{1,1}+\cdots+e_{n_{2,1},N_1,1}j_{N_1,1}+\cdots+e_{n_{2,1},N_t,t}j_{N_t,t} & \equiv 0 \bmod q-1\end{cases}$$

$$\vdots \qquad\qquad \vdots \tag{4}$$

$$\begin{cases} d_{k_t,t}h_{k_t,t}+e_{n_{k_t-1,t}+1,1,1}j_{1,1}+\cdots+e_{n_{k_t-1,t}+1,N_t,t}j_{N_t,t} & \equiv 0 \bmod q-1\\ \vdots & \vdots\\ d_{k_t,t}h_{k_t,t}+e_{n,1,1}j_{1,1}+\cdots+e_{n,N_1,1}j_{N_1,1}+\cdots+e_{n,N_t,t}j_{N_t,t} & \equiv 0 \bmod q-1\end{cases}$$

$$\begin{cases} h_{1,1}+\cdots+h_{k_1,1}+j_{1,1}+\cdots+j_{N_1,1} & \equiv 0 \bmod q-1\\ \vdots & \vdots\\ h_{1,t}+\cdots+h_{k_t,t}+j_{1,t}+\cdots+j_{N_t,t} & \equiv 0 \bmod q-1.\end{cases}$$

By Theorem 1,

$$v_\theta(S(F)) \geq \min_{(h_{1,1},\cdots,j_{N_t,t})} \left\{ \sum_{i=1}^{t}\sum_{r=1}^{k_i} \sigma_p(h_{r,i}) + \sum_{i=1}^{t}\sum_{r=1}^{N_t} \sigma_p(j_{r,i}) + f(p-1)s \right\}, \tag{5}$$

where s is the number of equations in (4) that are equal to zero, and $0 \leq h_{r,i}, j_{r,i} \leq q-1$. We now prove that there is only one solution

$$(h_{1,1}, \cdots, h_{k_t,t} : j_{1,1}, \cdots, j_{N_t,t})$$

to the system that is minimal in this sense, and hence we have equality in (5).

Let $s_{r,i}$ be the number of congruences that are equal to zero in the block of $n_{r,i} - n_{r-1,i}$ congruences in (4) that correspond to a monomial $a_{r,i}(X_1, \cdots, X_n)$ in (3). Applying σ_p to (4), adding the first $n_{1,1} - s_{1,1}$ non-zero inequalities that are obtained, and then dividing by $(n_{1,1})d_{1,1}$, we get

$$\begin{aligned}
&\sigma_p(h_{1,1}) + \frac{\sigma_p(e_{1,1,1}) + \cdots + \sigma_p(e_{n_{1,1},1,1})}{n_{1,1}d_{1,1}}\sigma_p(j_{1,1}) \\
&+ \cdots + \frac{\sigma_p(e_{1,N_t,t}) + \cdots + \sigma_p(e_{n_{1,1},N_t,t})}{n_{1,1}d_{1,1}}\sigma_p(j_{N_t,t})
\end{aligned}$$

$$\begin{aligned}
= \quad & \frac{\sigma_p(h_{1,1})(n_{1,1} - s_{1,1})d_{1,1}}{(n_{1,1} - s_{1,1})\, d_{1,1}} + \frac{\sigma_p(e_{1,1,1}) + \cdots + \sigma_p(e_{n_{1,1},1,1})}{n_{1,1}d_{1,1}}\sigma_p(j_{1,1}) \\
& + \cdots + \frac{\sigma_p(e_{1,N_t,t}) + \cdots + \sigma_p(e_{n_{1,1},N_t,t})}{n_{1,1}d_{1,1}}\sigma_p(j_{N_t,t})
\end{aligned}$$

$$\begin{aligned}
\geq \quad & \frac{\sigma_p(h_{1,1})(n_{1,1} - s_{1,1})d_{1,1}}{n_{1,1}d_{1,1}} + \frac{\sigma_p(e_{1,1,1}) + \cdots + \sigma_p(e_{n_{1,1},1,1})}{n_{1,1}d_{1,1}}\sigma_p(j_{1,1}) \\
& + \cdots + \frac{\sigma_p(e_{1,N_t,t}) + \cdots + \sigma_p(e_{n_{1,1},N_t,t})}{n_{1,1}d_{1,1}}\sigma_p(j_{N_t,t}) \\
\geq \quad & \frac{f(p-1)(n_{1,1} - s_{1,1})}{n_{1,1}d_{1,1}}.
\end{aligned}$$

Note that the first inequality is strict if any equation in (4) is equal to zero. We repeat the same to each of the first $k_1 + k_2 + \cdots + k_t$ blocks of $n_{r,i} - n_{r-1,i}$ modular equations in (4) to obtain:

$$\begin{aligned}
&\sigma_p(h_{r,i}) + \frac{\sigma_p(e_{n_{r-1,i}+1,1,1}) + \cdots + \sigma_p(e_{n_{r,i},1,1})}{(n_{r,i} - n_{r-1,i})d_{r,i}}\sigma_p(j_{1,1}) \\
&+ \cdots + \frac{\sigma_p(e_{n_{r-1,i}+1,N_t,t}) + \cdots + \sigma_p(e_{n_{r,i},N_t,t})}{(n_{r,i} - n_{r-1,i})d_{r,i}}\sigma_p(j_{N_t,t}) \\
\geq \quad & \frac{f(p-1)(n_{r,i} - n_{r-1,i} - s_{r,i})}{(n_{r,i} - n_{r-1,i})d_{r,i}} \quad \text{for} \quad 1 \leq r \leq k_i,\ 1 \leq i \leq t.
\end{aligned}$$

Add the above inequalities to get

$$\sum_{i=1}^{t}\sum_{r=1}^{k_i}\sigma_p(h_{r,i})$$
$$+\left(\frac{\sigma_p(e_{1,1,1})+\cdots+\sigma_p(e_{n_{1,1},1,1})}{n_{1,1}d_{1,1}}+\cdots+\frac{\sigma_p(e_{n_{k_t-1,t}+1,1,1})+\cdots+\sigma_p(e_{n,1,1})}{(n-n_{k_t-1,t-1})d_{k_t,t}}\right)\sigma_p(j_{1,1})$$

$$+\cdots+$$

$$\left(\frac{\sigma_p(e_{1,N_t,t})+\cdots+\sigma_p(e_{n_{1,1},N_t,t})}{n_{1,1}d_{1,1}}+\cdots+\frac{\sigma_p(e_{n_{k_t-1,t}+1,N_t,t})+\cdots+\sigma_p(e_{n,N_t,t})}{(n-n_{k_t-1,t})d_{k_t,t}}\right)\sigma_p(j_{N_t,t})$$
$$\geq f(p-1)\sum_{i=1}^{t}\sum_{r=1}^{k_i}\frac{(n_{r,i}-n_{r-1,i}-s_{r,i})}{(n_{r,i}-n_{r-1,i})d_{r,i}}.$$

Since $\sigma_p(e_{1,m,i})+\cdots+\sigma_p(e_{n,m,i})$ is the p-weight degree of the mth monomial of G_i, $w_p(G_i)<\min_j D_j$, and $D_i\leq(n_{m,i}-n_{m-1,i})d_{m,i}$, we have that $\frac{\sigma_p(e_{1,m,i})+\cdots+\sigma_p(e_{n,m,i})}{\min_j D_j}<1$, and

$$\begin{aligned}
&\sum_{i=1}^{t}\sum_{r=1}^{k_i}\sigma_p(h_{r,i})+\sum_{i=1}^{t}\sum_{r=1}^{N_t}\sigma_p(j_{r,i})+f(p-1)s\\
\geq\ &\sum_{i=1}^{t}\sum_{r=1}^{k_i}\sigma_p(h_{r,i})+\frac{\sigma_p(e_{1,1,1})+\cdots+\sigma_p(e_{n,1,1})}{\min_j D_j}\sigma_p(j_{1,1})\\
&+\cdots+\frac{\sigma_p(e_{1,N_t,t})+\cdots+\sigma_p(e_{n,N_t,t})}{\min_j D_j}\sigma_p(j_{N_t,t})+f(p-1)s\\
\geq\ &f(p-1)\sum_{i=1}^{t}\sum_{r=1}^{k_i}\frac{(n_{r,i}-n_{r-1,i}-s_{r,i})}{(n_{r,i}-n_{r-1,i})d_{r,i}}+f(p-1)s\\
=\ &f(p-1)\sum_{i=1}^{t}\sum_{r=1}^{k_i}\frac{1}{d_{r,i}}+f(p-1)\left(s-\sum_{i=1}^{t}\sum_{r=1}^{k_i}\frac{s_i}{(n_{r,i}-n_{r-1,i})d_{r,i}}\right).
\end{aligned}$$

The first inequality is strict if $j_{r,i}\neq 0$ for some r,i; the last inequality is strict if any equation in (4) is equal to zero.

Since $\sum_r\frac{1}{d_{r,i}}$ is an integer for $i=1,\ldots,t$, by taking

$$h_{r,i}=\frac{q-1}{d_{r,i}}\ \text{for}\ \ r=1,\ldots,k_i,\ i=1,\ldots,t\ \ \text{and}$$

$$j_{r,i}=0\ \text{for}\ \ r=1,\ldots,N_t,\ i=1,\ldots,t,$$

we obtain a solution to system (4) with

$$\sum_{i=1}^{t}\sum_{r=1}^{k_i}\sigma_p(h_{r,i})+\sum_{i=1}^{t}\sum_{r=1}^{N_t}\sigma_p(j_{r,i})+f(p-1)s=f(p-1)\sum_{r,i}\frac{1}{d_{r,i}},$$

and this is the only minimal solution. Therefore

$$v_\theta(S(F))=f(p-1)\sum_{r,i}\frac{1}{d_{r,i}},\quad v_p(N)=f(\sum_{r,i}\frac{1}{d_{r,i}}-t),$$

and system (2) has a solution.

□

As an immediate consequence, we can obtain a slight generalization of Theorem 3 to non-homogeneous polynomials:

COROLLARY 5. *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*

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

of degree $D_1, \cdots, D_t > 1$, 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 $w_p(G) < min_i \{D_i\}$, 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 p-divisibility of the number of solutions of $F = 0$. In particular, F has at least one solution over $\mathbb{F}_q$.

The following examples illustrate how Theorem 4 is used to determine the solvability of families of systems of polynomial equations and the p-divisibility of the number of solutions.

EXAMPLE 1. Let p be a prime number satisfying that $12 \mid (p-1)$ and consider the following system of two polynomial equations over $\mathbb{F}_{p^f}$:

$$\begin{aligned} a_1(X_1X_2)^2 + a_2X_3^4 + a_3X_4^4 + G_1(X_1, \ldots, X_{10}) = 0 \\ b_1(X_5X_6)^3 + b_2(X_7X_8)^3 + b_3X_9^6 + b_4X_{10}^6 + G_2(X_1, \ldots, X_{10}) = 0, \end{aligned}$$

where $w_p(G_i) < 4$ for $i = 1, 2$, and $a_k, b_j \neq 0$ for $k = 1, \cdots, 3$, $j = 1, \cdots, 4$. Then Theorem 4 gives that $v_p(N) = 0$ and the system has a solution.

EXAMPLE 2. Let $12 \mid (p-1)$ and consider

$$\begin{aligned} a_1X_1^3 + a_2X_2^3 + a_3X_3^3 + a_4X_4^3 + a_5X_5^3 + a_6X_6^3 + G_1(X_1, \ldots, X_{10}) = 0 \\ b_1X_7^4 + b_2X_8^4 + b_3X_9^4 + b_4X_{10}^4 + G_2(X_1, \ldots, X_{10}) = 0, \end{aligned}$$

over $\mathbb{F}_{p^f}$, where $w_p(G_i) < 3$ for $i = 1, 2$, and $a_k, b_j \neq 0$ for $k = 1, \cdots, 6$, $j = 1, \cdots, 4$. Then $v_p(N) = f$ and the system has a solution.

EXAMPLE 3. Let p be a prime number satisfying that $6 \mid (p-1)$ and consider the following system of three polynomial equations over $\mathbb{F}_{p^f}$:

$$\begin{aligned} a_1X_1^3 + a_2X_2^3 + a_3X_3^6 + a_4X_4^6 + a_5X_1^2 + \cdots + a_{15}X_{11}^2 = \gamma_1 \\ b_1(X_5X_6)^2 + b_2(X_7X_8)^2 + \sum_{i<j} b_{i,j}X_iX_j = \gamma_2 \\ c_1X_9^3 + c_2X_{10}^3 + c_3X_{11}^3 + c_4X_1 + \cdots + c_{14}X_{11} = \gamma_3, \end{aligned}$$

where $a_k, b_1, b_2, c_j \neq 0$ for $k = 1, \cdots, 4$, $j = 1, \cdots, 3$. Then, Theorem 4 gives that $v_p(N) = 0$ and the system has at least one solution for every $(\gamma_1, \gamma_2, \gamma_3) \in \mathbb{F}_{p^f}^3$.

The next examples show that some of the conditions in the theorem are necessary.

EXAMPLE 4. Let d be a divisor of $q-1$. The following system of polynomial equations is not solvable whenever γ_i is not a d-th power, for some i:

$$\begin{aligned} X_1^d &= \gamma_1 \\ X_2^d &= \gamma_2 \\ \vdots \quad & \quad \vdots \\ X_n^d &= \gamma_n. \end{aligned}$$

Note that this system does not satisfy the condition that requires the sum of the reciprocal of the exponents on each equation to be an integer.

EXAMPLE 5. Let $\alpha \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$. Then the equation

$$X_1^{p+1} + \cdots + X_n^{p+1} = \alpha$$

does not have a solution because $\gamma \in \mathbb{F}_{p^2}$ implies that $\left(\gamma^{p+1}\right)^{p-1} = 1$ and therefore $\gamma^{p+1} \in \mathbb{F}_p$. This example shows that it is necessary that the exponents of the variables divide $p-1$.

EXAMPLE 6. Let $p = 5$. Then the equation

$$X_1X_2X_3X_4 + X_1^4 + X_2^4 + X_3^4 + X_4^4 = 4$$

does not have a solution. Note that the monomials do not have disjoint support and $deg\ \left(X_1^4 + X_2^4 + X_3^4 + X_4^4\right) = deg\ (X_1X_2X_3X_4)$.

References

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

[2] F. N. Castro, I. Rubio, and J. Vega, Divisibility of Exponential Sums and Solvability of Certain Equations over Finite Fields, *The Quart. J. Math.*, doi: 10.1093/qmath/han013, 2008.

[3] B. Felszeghy, On the Solvability of some Special Equations over Finite Fields, *Publ. Math. Debrece*, **68**, 15-23, 2006.

[4] 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.

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

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

[7] 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.

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

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

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF PUERTO RICO, RÍO PIEDRAS, BOX 23328, SAN JUAN, PR 00931

E-mail address: iverubio@uprrp.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PUERTO RICO, RÍO PIEDRAS, BOX 23355, SAN JUAN, PR 00931

E-mail address: franciscastr@gmail.com