Journal of Algebra and Its Applications
Vol. 13, No. 6 (2014) 1450013 (15 pages)

DOI: 10.1142/S0219498814500133

World Scientific
www.worldscientific.com

Construction of systems of polynomial equations with exact p-Divisibility via the covering method

Francis N. Castro

Department of Mathematics
University of Puerto Rico, Box 70377
San Juan, PR 00936-8377, USA
franciscastr@gmail.com

Ivelisse M. Rubio

Department of Computer Science
University of Puerto Rico, Box 70377
San Juan, PR 00936-8377, USA
iverubio@gmail.com

Received 16 October 2013
Accepted 25 November 2013
Published 21 March 2014

Communicated by G. Mullen

We present an elementary method to compute the exact p-divisibility of exponential sums of systems of polynomial equations over the prime field. Our results extend results by Carlitz and provide concrete and simple conditions to construct families of polynomial equations that are solvable over the prime field.

Keywords: Solutions; finite fields; covering method; polynomial equations; exponential sums; p-divisibility.

Mathematics Subject Classification: 11T06, 13A05

1. Introduction

It is important to provide elementary methods in mathematics in order to have a broad spectrum of applications and give rise to new results, even within mathematics. An area that has been applied frequently in coding theory and cryptography is the p-divisibility of exponential sums ([3, 4, 11]). Sometimes getting an extra power of p in the p-divisibility can make a difference in the applications. For example, in [4] Canteaut used an improvement of the bound given in Ax–Katz's theorem to obtain information about the covering radius of first-order Reed–Muller codes. The computation of the exact p-divisibility of the exponential sums or the number of

solutions of polynomial equations can be very useful in the applications but is a hard problem in general.

In [8] the authors reformulated the concept of coverings of polynomials introduced in [7] to provide an elementary combinatorial method to compute exact p-divisibility of exponential sums over a prime field and an intuitive approach to the construction of systems of polynomial equations that are guaranteed to be solvable. There, the computation of the exact p-divisibility depended on the existence of a unique minimal $(p-1)$-covering of the polynomials in the system and the results gave sufficient conditions for its existence.

In this paper, we expand the work in [8] by considering systems with several minimal $(p-1)$-coverings. We use $(p-1)$-coverings to extend and improve results of Carlitz that allow us to study families of systems of deformed diagonal equations, compute the p-divisibility of their exponential sums, and determine their solvability by considering the simpler system given by the diagonal part of the equations. Carlitz stated in [6] that the number of solutions of a system of polynomials and a deformation of the same system are congruent modulo p. We extend this result and obtain congruence modulo a power of p for the case of deformed diagonal equations over the prime field. Other results presented here provide general but concrete and simple conditions to construct families of systems that are solvable over the prime field. We also obtain information about the p-divisibility of the number of solutions of systems for which the well-known results of Chevalley–Warning and Katz do not give any information.

2. Preliminaries

Let p be a prime, $\mathbb{F}_p$ be the prime field, $\mathbb{F}_p{}^* = \mathbb{F}_p \backslash 0$ and $\mathbb{F}_p^n = \{(x_1, \ldots, x_n) \,|\, x_i \in \mathbb{F}_p, i = 1, \ldots, n\}$. Sometimes we use $\mathbf{x}$ instead of $(x_1, \ldots, x_n)$. Let $F(\mathbf{X}) = a_1 X_1^{e_{11}} \cdots X_n^{e_{n1}} + \cdots + a_N X_1^{e_{1N}} \cdots X_n^{e_{nN}}$ be a polynomial in n variables over $\mathbb{F}_p$. Without loss of generality, we will assume throughout the rest of the paper that $F(\mathbf{X})$ is not a polynomial in some subset of the variables $X_1, \ldots, X_n$.

Let ζ be a primitive pth root of unity over $\mathbb{Q}$ and set $\theta = 1 - \zeta$. Then the ideal $\langle p \rangle = \langle \theta \rangle^{p-1}$, and this extends the p-adic valuation v_p to the θ-adic valuation $v_\theta(a) = (p-1)v_p(a)$, for all $a \in \mathbb{Q}(\zeta)$. The exponential sum of a polynomial $F(\mathbf{X})$ over $\mathbb{F}_p$, is defined as

$$S(F) = \sum_{\mathbf{x} \in \mathbb{F}_p^n} \zeta^{F(\mathbf{x})}.$$

The exact p-divisibility of $S(F)$, $v_p(S(F))$, is the largest power of p dividing $S(F)$.

The relation between the number of common solutions $\mathcal{N}$ of a system of polynomial equations $G_1(\mathbf{X}) = G_2(\mathbf{X}) = \cdots = G_t(\mathbf{X}) = 0$ and an exponential sum is given by the following lemma ([1, Eq. (2.7)], [2]).

Lemma 2.1. *Let $G_1(\mathbf{X}), \ldots, G_t(\mathbf{X}) \in \mathbb{F}_p[\mathbf{X}]$ and $\mathcal{N}$ be the number of common zeros of $G_1, \ldots, G_t$. Then $\mathcal{N} = p^{-t} \sum_{\mathbf{x} \in \mathbb{F}_p^n, \mathbf{y} \in \mathbb{F}_p^t} \zeta^{(y_1 G_1(\mathbf{x}) + \cdots + y_t G_t(\mathbf{x}))}$.*

It is important to note that if we can compute the exact p-divisibility of the exponential sum $\sum_{\mathbf{x}\in\mathbb{F}_p^n,\mathbf{y}\in\mathbb{F}_p^t}\zeta^{(y_1G_1(\mathbf{x})+\cdots+y_tG_t(\mathbf{x}))}$, we know that $p^{v_p(\mathcal{N})+1}\nmid\mathcal{N}$ and hence $\mathcal{N}\neq 0$.

In [8], to compute $v_p(S(F))$, we used the following expansion of the exponential sum of $F(\mathbf{X})=a_1F_1+\cdots+a_NF_N$, where $a_i\neq 0$ and F_i is a monomial:

$$\begin{aligned}S(F)&=\sum_{\mathbf{x}\in\mathbb{F}_p^n}\zeta^{F(\mathbf{x})}=\sum_{\mathbf{x}\in\mathbb{F}_p^n}(1-\theta)^{a_1F_1+\cdots+a_NF_N}\\&=\sum_{\nu_1=0}^{M}\cdots\sum_{\nu_N=0}^{M}\sum_{\mathbf{x}\in\mathbb{F}_p^n}(-\theta)^{|\boldsymbol{\nu}|}\binom{a_1F_1}{\nu_1}\cdots\binom{a_NF_N}{\nu_N},\end{aligned}\tag{2.1}$$

where $\theta=1-\zeta, M=p^{\deg(F)+1}$, $|\boldsymbol{\nu}|=\sum_{i=1}^{N}\nu_i$, and studied the p-divisibility of each term in (2.1). Let $T_{\boldsymbol{\nu}}(F)$ be the term in (2.1) associated with $\boldsymbol{\nu}=(\nu_1,\ldots,\nu_N)$. Then,

$$\begin{aligned}T_{\boldsymbol{\nu}}(F)&=(-\theta)^{|\boldsymbol{\nu}|}\sum_{\mathbf{x}\in\mathbb{F}_p^n}\binom{a_1F_1}{\nu_1}\cdots\binom{a_NF_N}{\nu_N}\\&=\frac{(-\theta)^{|\boldsymbol{\nu}|}a_1^{\nu_1}\cdots a_N^{\nu_N}}{\nu_1!\cdots\nu_N!}\sum_{\mathbf{x}\in\mathbb{F}_p^n}(F_1^{\nu_1}F_2^{\nu_2}\cdots F_N^{\nu_N}+P_{\boldsymbol{\nu}}),\end{aligned}\tag{2.2}$$

where $\deg(P_{\boldsymbol{\nu}})<\deg(F_1^{\nu_1}F_2^{\nu_2}\cdots F_N^{\nu_N})$.

To compute the exact p-divisibility of $S(F)$ one must find the terms $T_{\boldsymbol{\nu}}(F)$ with the smallest p-divisibility $v_p(T_{\boldsymbol{\nu}}(F))$. If there is only one term with minimal p-divisibility, this is, if there exists $T_{\boldsymbol{\nu}}(F)$ such that $v_p(T_{\boldsymbol{\nu}}(F))<v_p(T_{\boldsymbol{\nu}'}(F))$ for all $\boldsymbol{\nu}'\neq\boldsymbol{\nu}$, then $v_p(S(F))=v_p(T_{\boldsymbol{\nu}}(F))$. If there is more than one term with minimal p-divisibility then it is hard to determine the exact p-divisibility of the exponential sum and one also has to consider the relation among $a_1,\ldots,a_N$. This is why many of the well-known results ([2, 10, 12]) only give bounds on the p-divisibility of the exponential sums or the number of solutions of systems of polynomial equations. In this paper, we consider systems where there might be more than one term with minimal p-divisibility.

Terms with minimal p-divisibility are associated with what we call minimal $(p-1)$-coverings. In [8] we found sufficient conditions for the existence of a unique minimal $(p-1)$-covering and constructed systems of polynomial equations with exact p-divisibility of $S(F)$. Here, we consider more general systems and determine conditions that allow us to compute the exact p-divisibility of systems where the minimal $(p-1)$-coverings might not be unique.

2.1. *Coverings*

The concept of an m-covering was introduced in [7] and reformulated in [8]. We recall the definitions related to coverings.

Definition 2.1. Let $F(\mathbf{X}) = a_1F_1 + a_2F_2 + \cdots + a_NF_N$. A set $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ of powers of the monomials in F is an *m-covering of F* if in the product $F_1^{\nu_1} \cdots F_N^{\nu_N}$ the exponent of each variable is a positive multiple of m. We define the *size* of the m-covering $\mathcal{C}$ as the sum $\sum_{i=1}^{N} \nu_i$. The set $\mathcal{C}$ is a *minimal m-covering of F* if for any other m-covering $\mathcal{C}' = \{F_1^{\nu_1'}, \ldots, F_N^{\nu_N'}\}$ of F, $\sum_{i=1}^{N} \nu_i' \geq \sum_{i=1}^{N} \nu_i$. We denote by $\kappa_m(F)$ the size of a minimal m-covering of F.

Definition 2.2. Let $F(\mathbf{X}) = a_1F_1 + a_2F_2 + \cdots + a_NF_N$. A set $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ of powers of the monomials in F is a *partial m-covering of F* if in the product $F_1^{\nu_1} \cdots F_N^{\nu_N}$, the exponent of each variable is a non-negative multiple of m. The set $\mathcal{C}$ is a *minimal partial m-covering of F* if its size $\sum_{i=1}^{N} \nu_i + s(p-1) = \kappa_m(F)$, where s is the number of variables in $F_1^{\nu_1} \cdots F_N^{\nu_N}$ with exponent equal to zero.

To determine the solvability of systems of polynomial equations $G_1(\mathbf{X}) = \cdots = G_t(\mathbf{X}) = 0$ we use Lemma 2.1 to relate the number of solutions of the system to the exponential sum of the polynomial $F = Y_1G_1(\mathbf{X}) + \cdots + Y_tG_t(\mathbf{X})$ and study the exact p-divisibility of $S(F)$ using the $(p-1)$-coverings of F. With this in mind, when we talk about the $(p-1)$-covering of a system of polynomial equations $G_1(\mathbf{X}) = \cdots = G_t(\mathbf{X}) = 0$ we are taking about the $(p-1)$-covering of the polynomial $F = Y_1G_1(\mathbf{X}) + \cdots + Y_tG_t(\mathbf{X})$.

Example 2.1. Consider the system

$$a_1X_1^3 + \cdots + a_4X_4^3 + G = 0,$$
$$b_1X_1 + \cdots + b_4X_4 + \alpha = 0,$$

where $a_i, b_i \in \mathbb{F}_7^*, \alpha \in \mathbb{F}_7, G \in \mathbb{F}_7[X_1, \ldots, X_4]$, and $\deg G < 3$. A 6-covering of this system is a 6-covering of $F = Y_1(X_1^3 + \cdots + X_4^3 + G) + Y_2(X_1 + \cdots + X_4 + \alpha)$. It is easy to see that $\mathcal{C}_1 = \{(Y_1X_4^3)^6\}$, $\mathcal{C}_2 = \{(Y_1X_1^3)^2, (Y_1X_2^3)^2, (Y_1X_3^3)^2, (Y_2X_4)^6\}$ and $\mathcal{C}_3 = \{(Y_1X_1^3), (Y_1X_2^3), (Y_1X_3^3)^2, (Y_1X_4^3)^2, (Y_2X_1)^3, (Y_2X_2)^3\}$ are partial 6-coverings of the system. $\mathcal{C}_2$ and $\mathcal{C}_3$ have size 12 and we will see in Lemma 3.1 that they are minimal. $\mathcal{C}_1$ is not a 6-covering of the system because it has 4 variables missing; its size is $6 + 4(p-1) = 30$.

From now on $m = p-1$ and we consider $(p-1)$-coverings. As we mentioned before, we can study the exact p-divisibility of $S(F)$ by studying the p-divisibility of the terms (2.2). In [8] we saw that the only terms with minimal p-divisibility are those corresponding to minimal partial $(p-1)$-coverings (with $s \geq 0$). If there is more than one minimal partial $(p-1)$-covering, then the p-divisibility might increase when the corresponding terms in $S(F)$ are added.

The concept of $(p-1)$-covering of a polynomial F is independent of the coefficients of F. However, the exact p-divisibility of the polynomial and its solvability depends on both the minimal $(p-1)$-coverings and the relation among the coefficients. The following lemma gives sufficient conditions to have exact p-divisibility of an exponential sum $S(F)$.

Lemma 2.2. *Let $\mathcal{C}_1, \ldots, \mathcal{C}_r$ be all the minimal $(p-1)$-coverings of a polynomial $F = a_1F_1 + \cdots + a_NF_N$, $\mathcal{C}_i = \{F_1^{\nu_{i1}}, \ldots, F_N^{\nu_{iN}}\}$, and suppose that all minimal partial $(p-1)$-coverings of F have $s = 0$. Then,*

$$v_p(S(F)) \text{ is } \begin{cases} = \dfrac{\kappa_{p-1}(F)}{p-1} & \text{if } \displaystyle\sum_{i=1}^{r} \frac{a_1^{\nu_{i1}} \cdots a_N^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} \not\equiv 0 \pmod{p}, \\ > \dfrac{\kappa_{p-1}(F)}{p-1} & \text{otherwise.} \end{cases}$$

Proof. Let $\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r$ be the exponent vectors corresponding to the minimal $(p-1)$-coverings $\mathcal{C}_1, \ldots, \mathcal{C}_r$. Then,

$$\sum_{i=1}^{r} T_{\boldsymbol{\nu}_i}(F) = (-\theta)^{\kappa_{p-1}(F)} \left[\sum_{i=1}^{r} \left(\frac{a_1^{\nu_{i1}} \cdots a_N^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} \sum_{\mathbf{x} \in \mathbb{F}_p^n} (F_1^{\nu_{i1}} \cdots F_N^{\nu_{iN}} + P_{\boldsymbol{\nu}_i}) \right) \right]$$

and

$$\begin{aligned} &v_p \left(\sum_{i=1}^{r} T_{\boldsymbol{\nu}_i}(F) \right) \\ &\quad = \frac{\kappa_{p-1}(F)}{p-1} + v_p \left[\sum_{i=1}^{r} \left(\frac{a_1^{\nu_{i1}} \cdots a_N^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} \sum_{\mathbf{x} \in \mathbb{F}_p^n} (F_1^{\nu_{i1}} \cdots F_N^{\nu_{iN}} + P_{\boldsymbol{\nu}_i}) \right) \right], \end{aligned}$$

where $\deg(P_{\boldsymbol{\nu}_i}) < \deg(F_1^{\nu_{i1}} \cdots F_N^{\nu_{iN}})$. By [8, Lemma 3.1],

$$\begin{aligned} &\sum_{i=1}^{r} \left(\frac{a_1^{\nu_{i1}} \cdots a_N^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} \sum_{\mathbf{x} \in \mathbb{F}_p^n} (F_1^{\nu_{i1}} \cdots F_N^{\nu_{iN}} + P_{\boldsymbol{\nu}_i}) \right) \\ &\qquad \equiv (p-1)^n \sum_{i=1}^{r} \frac{a_1^{\nu_{i1}} \cdots a_N^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} \pmod{p}. \end{aligned}$$

Terms that do not correspond to the minimal $(p-1)$-coverings will have higher p-divisibility than the terms $T_{\boldsymbol{\nu}_i}$. Therefore, if $\sum_{i=1}^{r} \frac{a_1^{\nu_{i1}} \cdots a_N^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} \not\equiv 0 \pmod{p}$, then $v_p(S(F)) = v_p(\sum_{i=1}^{r} T_{\boldsymbol{\nu}_i}(F)) = \frac{\kappa_{p-1}(F)}{p-1}$. Otherwise $v_p(S(F)) \geq v_p(\sum_{i=1}^{r} T_{\boldsymbol{\nu}_i}(F)) > \frac{\kappa_{p-1}(F)}{p-1}$. □

When applied to the number of solutions of systems of polynomial equations, Lemma 2.2 gives a refinement of Ax–Katz by giving precise conditions for when the bound is achieved or improved. This can make a difference in applications, as it was for example in [4] were an improvement of the bound given by Ax–Katz's theorem was used to obtain information about the covering radius of first-order Reed–Muller codes.

2.2. *Solutions of systems of polynomial equations*

In the theory of polynomial equations over finite fields $\mathbb{F}_q, q = p^f$, a main result is the theorem of Chevalley–Warning: For a polynomial $F(X_1, \ldots, X_n)$ of degree d, over the finite field $\mathbb{F}_q$, if $n > d$, the characteristic p of the field divides the number of solutions of $F = 0$. This theorem has been applied in many areas of mathematics. Ax–Katz improved this result by giving a tight bound on the power of p that divides the number of solutions. None of these results give information about the solvability of the equation $F = 0$ over $\mathbb{F}_q$. For example, $(X_1^d + \cdots + X_n^d)^2 = \alpha$, where α is a quadratic non-residue over $\mathbb{F}_p$, has no solution over $\mathbb{F}_p$ for any n and d.

In 1956, Carlitz ([5]) provided infinite families of polynomials that are solvable.

Theorem 2.1 (Carlitz). *Let d be a divisor of $p-1$, and $a_i \in \mathbb{F}_q^*$ for $i = 1, \ldots, d$. If $G \in \mathbb{F}_q[\mathbf{X}]$ has $\deg(G) < d$, then the equation $a_1 X_1^d + \cdots + a_d X_d^d + G = 0$ has at least one solution over $\mathbb{F}_q$.*

In [9] the authors of the present paper generalized Carlitz's result to generalized diagonal equations by computing the exact p-divisibility of the exponential sum of the polynomial.

Another theorem of Carlitz ([6]) allows us to obtain information about deformed diagonal systems by considering only the diagonal part of the equations.

Theorem 2.2 (Carlitz). *Let $\mathcal{N}$ be the number of solutions of the system*

$$F_i(X_1, \ldots, X_n) + G_i(X_1, \ldots, X_n) = 0, \quad i = 1, \ldots, t,$$

and $\mathcal{N}'$ be the number of solutions of the system

$$F_i(X_1, \ldots, X_n) = 0, \quad i = 1, \ldots, t,$$

where $F_i(X_1, \ldots, X_n)$ are polynomials in $\mathbb{F}_q$ with $\deg(F_i) \leq d_i$, $\sum_i^t d_i = n$ and $G_i(X_1, \ldots, X_n)$ are polynomials in $\mathbb{F}_q$ with $\deg(G_i) < d_i$. Then, $\mathcal{N}' \equiv \mathcal{N} \pmod{p}$.

If one can determine that $p \nmid \mathcal{N}'$, one can conclude that $\mathcal{N} \neq 0$. But, if $\mathcal{N}' \equiv 0 \pmod{p}$, one cannot determine the solvability of the system $F_i(X_1, \ldots, X_n) + G_i(X_1, \ldots, X_n) = 0, i = 1, \ldots, t$, using this theorem. Also, the theorem does not give bounds on the p-divisibility of $\mathcal{N}$ in the case when $p^l \mid \mathcal{N}'$ for $l > 1$.

Motivated by the above results, in this work we use the covering method to find conditions that allow us to obtain information about systems of deformed diagonal equations over $\mathbb{F}_p$ by studying the much simpler systems given by their diagonal part. In particular, in Theorem 4.1, we obtain bounds on the p-divisibility of systems of deformed diagonal equations $\{F_i + G_i = 0\}$ from systems of diagonal equations $\{F_i = 0\}$, generalizing Carlitz's Theorem 2.2 for the case of deformed diagonal equations over prime fields. In Theorem 4.2, we determine the solvability of certain deformed diagonal equations by giving necessary and sufficient conditions on the diagonal part. This provide concrete and simple conditions to construct families of deformed diagonal equations that are solvable as we do in Theorem 4.3.

3. Minimal $(p-1)$-Coverings of Systems of Deformed Diagonal Equations

To compute the p-divisibility of exponential sums of systems of deformed diagonal equations and determine their solvability by just considering the diagonal part of the equations we use information about the minimal $(p-1)$-coverings of the systems. We start by relating the minimal $(p-1)$-coverings of systems of deformed diagonal equations to the minimal $(p-1)$-coverings of systems of diagonal equations. Recall that the size of a minimal partial $(p-1)$-covering $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ is $\sum_{i=1}^{N} \nu_i + s(p-1)$, where s is the number of variables missing in $F_1^{\nu_1} \cdots F_N^{\nu_N}$.

Lemma 3.1. *Consider the systems*

$$\begin{aligned} a_1X_1^d + \cdots + a_nX_n^d + G_1 &= 0, \\ b_1X_1^k + \cdots + b_nX_n^k + G_2 &= 0, \end{aligned} \tag{3.1}$$

$$\begin{aligned} a_1X_1^d + \cdots + a_nX_n^d &= 0, \\ b_1X_1^k + \cdots + b_nX_n^k &= 0, \end{aligned} \tag{3.2}$$

where $a_i, b_i \in \mathbb{F}_p^*$, $G_1, G_2 \in \mathbb{F}_p[\mathbf{X}]$ *and* $\deg G_1 < d, \deg G_2 < k$. *Then*

(a) *any partial* $(p-1)$*-covering of* (3.1) *or* (3.2) *has size* $\geq (\frac{n-k}{d}+1)(p-1)$,
(b) $\mathcal{C}$ *is a minimal partial* $(p-1)$*-covering of* (3.1) *of size* $(\frac{n-k}{d}+1)(p-1)$ *if and only if* $\mathcal{C}$ *is a minimal partial* $(p-1)$*-covering of* (3.2) *of size* $(\frac{n-k}{d}+1)(p-1)$
(c) *all minimal partial* $(p-1)$*-covering of* (3.1) *or* (3.2) *of size* $(\frac{n-k}{d}+1)(p-1)$ *have* $s = 0$.

Proof. Without lost of generality one can assume that $d \geq k$. Let

$$G_1 = \sum_{j=1}^{N} b_j X_1^{e_{1j}} \cdots X_n^{e_{nj}}, \quad G_2 = \sum_{j=1}^{M} c_j X_1^{f_{1j}} \cdots X_n^{f_{nj}}.$$

Then

$$\begin{aligned} \mathcal{C} = \{&(Y_1X_1^d)^{h_1}, \ldots, (Y_1X_n^d)^{h_n}, (Y_1X_1^{e_{11}} \cdots X_n^{e_{n1}})^{t_1}, \ldots, (Y_1X_1^{e_{1N}} \cdots X_n^{e_{nN}})^{t_N}, \\ &(Y_2X_1^k)^{s_1}, \ldots, (Y_2X_n^k)^{s_n}, (Y_2X_1^{f_{11}} \cdots X_n^{f_{n1}})^{l_1}, \ldots, (Y_2X_1^{f_{1M}} \cdots X_n^{f_{nM}})^{l_M}\} \end{aligned}$$

is a partial $(p-1)$-covering of (3.1) if and only if

$$(h_1, \ldots, h_n : t_1, \ldots, t_N : s_1, \ldots, s_n : l_1, \ldots, l_M)$$

is a solution to the system

$$\begin{aligned} dh_i + e_{i1}t_1 + \cdots + e_{iN}t_N + ks_i + f_{i1}l_1 + \cdots + f_{iM}l_M &= \lambda_i(p-1) \quad \text{for } 1 \leq i \leq n, \\ h_1 + \cdots + h_n + t_1 + \cdots + t_N &= \lambda_{n+1}(p-1), \\ s_1 + \cdots + s_n + l_1 + \cdots + l_M &= \lambda_{n+2}(p-1) \end{aligned} \tag{3.3}$$

with $\lambda_i \geq 0$.

The size of this partial $(p-1)$-covering $\mathcal{C}$ is $\sum_{i=1}^{n} h_i + \sum_{j=1}^{N} t_j + \sum_{i=1}^{n} s_i + \sum_{j=1}^{M} l_j + s(p-1)$, where s is the number of equations in (3.3) that are equal to zero.

We now look for a lower bound for the size of the covering $\mathcal{C}$. Since

$$\begin{aligned}&\frac{\sum_{j=1}^{N} e_{1j}t_j}{d} + \cdots + \frac{\sum_{j=1}^{N} e_{nj}t_j}{d}\\ &\quad = t_1\left(\frac{e_{11}+e_{21}+\cdots+e_{n1}}{d}\right) + \cdots + t_N\left(\frac{e_{1N}+e_{2N}+\cdots+e_{nN}}{d}\right),\end{aligned}$$

and $\deg G_1 < d, \deg G_2 < k$, one has $\sum_{j=1}^{N} t_j \geq \sum_{j=1}^{N}\sum_{i=1}^{n} \frac{e_{ij}t_j}{d}$ and $\sum_{j=1}^{M} l_j \geq \sum_{j=1}^{M}\sum_{i=1}^{n} \frac{f_{ij}l_j}{k}$. Therefore,

$$\begin{aligned}&d\left(\sum_{i=1}^{n} h_i + \sum_{j=1}^{N} t_j + \sum_{i=1}^{n} s_i + \sum_{j=1}^{M} l_j\right)\\ &\quad = d\left(\sum_{i=1}^{n} h_i + \sum_{j=1}^{N} t_j\right) + k\left(\sum_{i=1}^{n} s_i + \sum_{j=1}^{M} l_j\right) + (d-k)\left(\sum_{i=1}^{n} s_i + \sum_{j=1}^{M} l_j\right)\\ &\quad \geq d\left(\sum_{i=1}^{n} h_i + \sum_{i=1}^{n}\sum_{j=1}^{N} \frac{e_{ij}t_j}{d}\right) + k\left(\sum_{i=1}^{n} s_i + \sum_{i=1}^{n}\sum_{j=1}^{M} \frac{f_{ij}l_j}{k}\right)\\ &\qquad + (d-k)\left(\sum_{i=1}^{n} s_i + \sum_{j=1}^{M} l_j\right)\\ &\quad = \sum_{i=1}^{n}\left(dh_i + \sum_{j=1}^{N} e_{ij}t_j + ks_i + \sum_{j=1}^{M} f_{ij}l_j\right) + (d-k)\left(\sum_{i=1}^{n} s_i + \sum_{j=1}^{M} l_j\right)\\ &\quad = \left(\sum_{i=1}^{n} \lambda_i\right)(p-1) + (d-k)\lambda_{n+2}(p-1)\\ &\quad \geq (n-s')(p-1) + (d-k)\lambda_{n+2}(p-1),\end{aligned}$$

where s' is the number of $\lambda_i = 0, i = 1, \ldots, n$.

If $\lambda_{n+2} \neq 0$, then the size of $\mathcal{C}$ is

$$\begin{aligned}&\geq \frac{n-s'}{d}(p-1) + \frac{d-k}{d}(p-1) + s(p-1), \quad \text{where } s \geq s'\\ &\quad = \left(\frac{n-k}{d} + 1\right)(p-1) + \left(s - \frac{s'}{d}\right)(p-1).\end{aligned}$$

If $\lambda_{n+2} = 0$, then the size of $\mathcal{C}$ is

$$\geq \frac{n-s'}{d}(p-1) + s(p-1) = \left(\frac{n}{d} + s - \frac{s'}{d}\right)(p-1), \quad \text{where } s \geq s'+1$$

$$\geq \left(\frac{n}{d}+1\right)(p-1) + \left(s' - \frac{s'}{d}\right)(p-1).$$

In any case, the size of a partial $(p-1)$-covering of (3.1) is $\geq (\frac{n-k}{d}+1)(p-1)$.

Note that a solution $(h_1, \ldots, h_n : 0, \ldots, 0 : s_1, \ldots, s_n : 0, \ldots, 0)$ to system (3.3) corresponds to a solution $(h_1, \ldots, h_n : s_1, \ldots, s_n)$ to

$$\begin{aligned} dh_i + ks_i &= \lambda_i(p-1), \quad 1 \leq i \leq n, \\ \sum_{i=1}^{n} h_i &= \lambda_{n+1}(p-1), \\ \sum_{i=1}^{n} s_i &= \lambda_{n+2}(p-1), \end{aligned} \tag{3.4}$$

which is the system associated with a partial $(p-1)$-covering $\mathcal{C}'$ of (3.2) with size $\geq (\frac{n-k}{d}+1)(p-1)$. This proves part (a).

Note that if $\mathcal{C}$ is a minimal partial $(p-1)$-covering of (3.1) with size $(\frac{n-k}{d}+1)(p-1)$, then $s = 0, l_i = t_j = 0$, for all $i = 1, \ldots, M, j = 1, \ldots, N, \lambda_i = 1$ for $i = 1, \ldots, n, n+2$, and $\lambda_{n+1} \geq 1$. This implies that $\mathcal{C}$ is also a minimal partial $(p-1)$-covering of (3.2). Similarly, a minimal partial $(p-1)$-covering of (3.2) with size $(\frac{n-k}{d}+1)(p-1)$ has $s = 0$ and is also a minimal partial $(p-1)$-covering of (3.1). This completes the proof. □

Remark 3.1. One can obtain a similar result for a single deformed diagonal equation or systems of more than two deformed diagonal equations, $a_1X_1^d + \cdots + a_nX_n^d + G_1 = b_{11}X_1^{k_1} + \cdots + b_{1n}X_n^{k_1} + G_1' = \cdots = b_{r1}X_1^{k_r} + \cdots + b_{rn}X_n^{k_r} + G_r' = 0$. In this case the bound for the size of the coverings is $(\frac{n-\sum_{i=1}^{r} k_i}{d} + r)(p-1)$, where $r+1$ is the number of polynomials in the system.

We now give sufficient conditions so that systems of deformed diagonal equations with associated polynomial F have minimal $(p-1)$-coverings with $\kappa_{p-1}(F) = (\frac{n-k}{d}+1)(p-1)$.

Lemma 3.2. *Let F be the polynomial associated with the system*

$$\begin{aligned} a_1X_1^d + \cdots + a_nX_n^d + G_1 &= 0, \\ b_1X_1^k + \cdots + b_nX_n^k + G_2 &= 0, \end{aligned} \tag{3.5}$$

where $a_i, b_i \in \mathbb{F}_p^*, \gcd(d,k) = 1, dk = p-1, n = dl + k, G_1, G_2 \in \mathbb{F}_p[\mathbf{X}]$ and $\deg G_1 < d, \deg\ G_2 < k$. Then all the minimal $(p-1)$-coverings of (3.5) have the

form

$$\{(Y_1X_{i_1}^d)^k,\ldots,(Y_1X_{i_{dl}}^d)^k,(Y_2X_{i_{dl+1}}^k)^d,\ldots,(Y_2X_n^k)^d\},\tag{3.6}$$

and $\kappa_{p-1}(F)=(l+1)(p-1)$.

Proof. It is easy to see that the size of these $(p-1)$-coverings is $(\frac{n-k}{d}+1)(p-1)=(l+1)(p-1)$, and by Lemma 3.1 it is minimal. Hence, $\kappa_{p-1}(F)=(l+1)(p-1)$.

We now prove that these are all the minimal $(p-1)$-coverings of the system. From the proof of Lemma 3.1, we know that the exponents in any minimal $(p-1)$-covering of F satisfy $dh_i+ks_i=p-1$ and $\lambda_{n+2}=1$. This implies that

$$dh_i=dk-ks_i=k(d-s_i)$$

and hence k divides dh_i. Since $\gcd(d,k)=1, h_i=kx$ for some $x\geq 0$. This implies that

$$dkx+ks_i=p-1,$$

$$0\leq ks_i=(p-1)(1-x)$$

and therefore $x=0,1$. This means that any minimal $(p-1)$-covering of F has $h_i=k$ and $s_i=0$ or $h_i=0$ and $s_i=d$.

Suppose that there are m of the s_i's equal to d. Then

$$md=\sum_{i=1}^{n}s_i=\lambda_{n+2}(p-1)=p-1.$$

This implies that $m=k$, and any minimal $(p-1)$-coverings of F has k of the s_i's equal to d and the corresponding h_i equal to 0. The other dl s_i's are equal to 0 and the corresponding h_i's are equal to k, the form of the exponents in (3.6). Therefore, all the minimal $(p-1)$-coverings of F have the form (3.6) and the result follows. □

4. Exact *p*-Divisibility of the Number of Solutions and Solvability

The p-divisibility of the exponential sum of a system of deformed diagonal equations is related to the p-divisibility of the exponential sum of the much simpler system given by its diagonal part. Using Lemma 3.1, we can improve Carlitz Theorem 2.2 for the case of deformed diagonal equations over the prime field where the degrees divide $p-1$. The result extends to more than two equations but, for simplicity of the notation, we only state it for the case of two equations.

Theorem 4.1. *Let* $\mathcal{N}$ *be the number of solutions of*

$$\begin{aligned}a_1X_1^d+\cdots+a_nX_n^d+G_1&=0,\\ b_1X_1^k+\cdots+b_nX_n^k+G_2&=0\end{aligned}\tag{4.1}$$

and $\mathcal{N}'$ be the number of solutions of

$$\begin{aligned} a_1X_1^d + \cdots + a_nX_n^d &= 0, \\ b_1X_1^k + \cdots + b_nX_n^k &= 0, \end{aligned} \tag{4.2}$$

where $a_i, b_i \in \mathbb{F}_p^*, d, k \mid (p-1), n = dl + k, G_1, G_2 \in \mathbb{F}_p[\mathbf{X}]$ and $\deg G_1 < d, \deg G_2 < k$. Then $\mathcal{N} \equiv \mathcal{N}' \pmod{p^{l-1}}$.

Proof. Note that

$$\mathcal{C} = \{(Y_1X_1^d)^{\frac{p-1}{d}}, \ldots, (Y_1X_{dl}^d)^{\frac{p-1}{d}}, (Y_2X_{dl+1}^k)^{\frac{p-1}{k}}, \ldots, (Y_2X_n^k)^{\frac{p-1}{k}}\}$$

is a $(p-1)$-covering of (4.2) of size $(l+1)(p-1) = (\frac{n-k}{d}+1)(p-1)$. By Lemma 3.1 this $(p-1)$-covering is minimal and corresponds to a minimal $(p-1)$-covering of (4.1). The result now follows from Lemma 2.2. □

Next we prove that if the number of solutions of a system of diagonal equations has certain exact p-divisibility, the number of solutions of a deformed system will have the same exact p-divisibility, providing a way to study p-divisibility using simpler systems. The result also gives a way to construct systems of solvable deformed diagonal equations starting from simpler solvable systems.

Lemma 4.1. *Let $\mathcal{N}$ be the number of solutions of*

$$\begin{aligned} a_1X_1^d + \cdots + a_nX_n^d + G_1 &= 0, \\ b_1X_1^k + \cdots + b_nX_n^k + G_2 &= 0 \end{aligned} \tag{4.3}$$

and $\mathcal{N}'$ be the number of solutions of

$$\begin{aligned} a_1X_1^d + \cdots + a_nX_n^d &= 0, \\ b_1X_1^k + \cdots + b_nX_n^k &= 0, \end{aligned} \tag{4.4}$$

where $a_i, b_i \in \mathbb{F}_p^*, G_1, G_2 \in \mathbb{F}_p[\mathbf{X}]$ and $\deg G_1 < d, \deg G_2 < k$. Then $v_p(\mathcal{N}) = \frac{n-k}{d} - 1$ if and only if $v_p(\mathcal{N}') = \frac{n-k}{d} - 1$.

Proof. By Lemma 3.1, there is a minimal $(p-1)$-covering of (4.3) of size $(\frac{n-k}{d} + 1)(p-1)$ if and only if there is a minimal $(p-1)$-covering of (4.4) of size $(\frac{n-k}{d} + 1)(p-1)$. Therefore, by Lemmas 2.1 and 2.2, $v_p(\mathcal{N}) = \frac{n-k}{d} - 1$ if and only if $v_p(\mathcal{N}') = \frac{n-k}{d} - 1$. □

Remark 4.1. The above lemma does not guarantee that $v_p(\mathcal{N}) = \frac{n-k}{d} - 1$.

The next example illustrates that, even when there are minimal $(p-1)$-coverings with $\kappa_{p-1}(F) = (\frac{n-k}{d}+1)(p-1)$ this information might not enough to obtain exact p-divisibility of the number of solutions. In particular, $v_p(\mathcal{N}) \neq \frac{n-k}{d} - 1$.

Example 4.1. Consider the following system over $\mathbb{F}_7$

$$\begin{aligned} X_1^3 + 2X_2^3 + X_3^3 + X_4^3 + X_5^3 + G_1 = 0, \\ X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 + G_2 = 0, \end{aligned} \tag{4.5}$$

where $G_1, G_2 \in \mathbb{F}_7[X_1, \ldots, X_5]$ and $\deg G_1 < 3, \deg G_2 < 2$. Note that $\{(Y_1X_{i_1}^3)^2, (Y_1X_{i_2}^3)^2, (Y_1X_{i_3}^3)^2, (Y_2X_{i_4}^2)^3, (Y_2X_{i_5}^2)^3\}$, where $1 \leq i_j \neq i_k \leq 5$, are 6-coverings of size 12 and by Lemma 3.1 are minimal, $\kappa_{p-1}(F) = (\frac{n-k}{d} + 1)(p-1)$. However, the exact p-divisibility of the number of solutions of the system is not $\frac{n-k}{d} - 1 = 0$. In fact, the p-divisibility changes if one changes the deformation polynomials G_1 and G_2 as it is illustrated in the next table.

(α, β)	$\mathcal{N}$
$(0,0)$	$5 \times 7 \times 11$
$(1,0)$	$2 \times 3 \times 7^2$
$(1,1)$	7×41
$(3,4)$	7^3

In Theorem 4.2, we will see that we also need to consider the relation among the coefficients to obtain exact p-divisibility.

4.1. *Solvability*

We now find conditions on the coefficients and the $(p-1)$-coverings of the diagonal systems to guarantee that systems of deformed diagonal equations are solvable.

Theorem 4.2. *Let $\mathcal{N}$ be the number of solutions of the system*

$$\begin{aligned} a_1X_1^d + \cdots + a_nX_n^d + G_1 = 0, \\ b_1X_1^k + \cdots + b_nX_n^k + G_2 = 0, \end{aligned} \tag{4.6}$$

where $a_i, b_i \in \mathbb{F}_p^*, G_1, G_2 \in \mathbb{F}_p[\mathbf{X}]$ and $\deg G_1 < d, \deg G_2 < k$. Let F be the polynomial associated with (4.6), $\boldsymbol{\nu}_i$ the exponent vector of a minimal $(p-1)$-covering of F, and suppose that there are r minimal $(p-1)$-coverings of the system. The system has solutions in $\mathbb{F}_p^n$ and $v_p(\mathcal{N}) = \frac{n-k}{d} - 1$ if and only if $\kappa_{p-1}(F) = (\frac{n-k}{d} + 1)(p-1)$ and $\sum_{i=1}^{r} \frac{a_1^{\nu_{i1}} \cdots b_n^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} \not\equiv 0 \pmod{p}$.

Proof. By Lemma 4.1 we only have to prove that $v_p(\mathcal{N}') = \frac{n-k}{d} - 1$, where $\mathcal{N}'$ is the number of solutions of system (4.6) with $G_1 = G_2 = 0$. By Lemma 2.1 $v_p(\mathcal{N}') = \frac{n-k}{d} - 1$ if and only if $v_p(S(F)) = \frac{n-k}{d} + 1$. Lemma 3.1 implies that all partial $(p-1)$-coverings of F of size $(\frac{n-k}{d} + 1)(p-1)$ have $s = 0$. The result now follows from Lemma 2.2. □

In Example 4.1, we saw that having $\kappa_{p-1}(F) = (\frac{n-k}{d} + 1)(p-1)$ was not enough to obtain exact p-divisibility. There, the system had 10 minimal 6-coverings of the same form and the next lemma shows that these are all the minimal 6-coverings for

the system. Since $\sum_{i=1}^{r} \frac{a_1^{\nu_{i1}} \cdots b_n^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} \equiv 0 \pmod 7$, Theorem 4.2 tells us that $v_7(\mathcal{N}) > 0$ for any G_1, G_2 with $\deg G_1 < 3, \deg G_2 < 2$. The table in the example shows that, the p-divisibility of the system might increase by more than one. This occurs because, in some cases, when the terms associated with the minimal $(p-1)$-coverings are added the p-divisibility of the sum is larger than $\frac{\kappa_{p-1}(F)}{p-1}$ and some terms associated with non-minimal $(p-1)$-coverings might also affect the p-divisibility of the exponential sum. In these cases it is hard to determine the exact p-divisibility of the sum, but we can improve some of the known bounds.

With the previous theorem and Lemma 3.2 we get necessary and sufficient conditions to obtain systems of deformed diagonal equations that are solvable. This gives very simple and concrete conditions to construct general systems of polynomial equations that are solvable.

Theorem 4.3. *Let $\mathcal{N}$ be the number of solutions of the system*

$$\begin{aligned} a_1 X_1^d + \cdots + a_n X_n^d + G_1 &= 0, \\ b_1 X_1^k + \cdots + b_n X_n^k + G_2 &= 0, \end{aligned} \tag{4.7}$$

where $\gcd(d,k) = 1, dk = p-1, n = dl + k, a_i, b_i \in \mathbb{F}_p^*, G_1, G_2 \in \mathbb{F}_p[\mathbf{X}]$ *and* $\deg G_1 < d, \deg G_2 < k$. *The system has solutions in* $\mathbb{F}_p^n$ *and* $v_p(\mathcal{N}) = l - 1$ *if and only if* $\sum_{i=1}^{r} \frac{a_1^{\nu_{i1}} \cdots b_n^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} \not\equiv 0 \pmod p$.

The next corollary gives families of systems of deformed diagonal equations that are solvable.

Corollary 4.1. *Let $\mathcal{N}$ be the number of solutions of the system*

$$\begin{aligned} a_1 X_1^d + \cdots + a_n X_n^d + G_1 &= 0, \\ b_1 X_1^k + \cdots + b_n X_n^k + G_2 &= 0, \end{aligned} \tag{4.8}$$

where $\gcd(d,k) = 1, dk = p-1, n = dl + k < p, a_i, b_i \in \mathbb{F}_p^*, a_i^k = 1, b_i^d = 1, G_1, G_2 \in \mathbb{F}_p[\mathbf{X}]$ *and* $\deg G_1 < d, \deg G_2 < k$. *Then,* $v_p(\mathcal{N}) = l-1$ *and the system has solutions in* $\mathbb{F}_p^n$.

Proof. Note that all the minimal $(p-1)$-coverings have the form

$$\{(Y_1 X_{i_1}^d)^k, \ldots, (Y_1 X_{i_{dl}}^d)^k, (Y_2 X_{i_{dl+1}}^k)^d, \ldots, (Y_2 X_n^k)^d\}$$

and there are $r = \binom{n}{dl}$ of them. Since $n < p$, we have that $p \nmid \binom{n}{dl}$, and $\sum_{i=1}^{r} \frac{a_1^{\nu_{i1}} \cdots b_n^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} = \binom{n}{dl} \frac{1}{(k!)^{dl} (d!)^k} \not\equiv 0 \pmod p$. The result follows from Theorem 4.3. □

One of the advantages of our results is that they give a simple way to construct systems that are solvable and where we know the exact p-divisibility of the number of solutions, even for cases for which previous results do not give information about

p-divisibility. The following example covers the case $n = p$ which is not covered by Chevalley–Warning or Ax–Katz's theorems, where the number of variables must be greater than the sum of the degrees of the equations.

Example 4.2. Let $\mathcal{N}$ be the number of solutions of the system

$$\begin{aligned} aX_1^{p-1} + \cdots + aX_p^{p-1} + G_1 = 0, \\ b_1X_1 + \cdots + b_pX_p + \alpha = 0, \end{aligned} \tag{4.9}$$

where $a, b_i \in \mathbb{F}_p^*, \alpha \in \mathbb{F}_p, G_1 \in \mathbb{F}_p[\mathbf{X}]$ and $\deg G_1 < p-1$. Here $\sum_{i=1}^{r} \frac{a_1^{\nu_{i1}} \cdots b_n^{\nu_{iN}}}{\nu_{i1}! \cdots \nu_{iN}!} = \frac{p}{(p-1)!}$. This implies that $v_p(\mathcal{N}) > 0$.

In contrast to Theorem 4.3 in which $dk = p-1$ is a precondition, the next result presents solvable systems for which $dk \neq p-1$. In this case there is more than one type of minimal $(p-1)$-coverings.

Proposition 4.1. *Let $\mathcal{N}$ be the number of solutions of the system*

$$\begin{aligned} aX_1^d + \cdots + aX_{d+1}^d + G = 0, \\ X_1 + \cdots + X_{d+1} + \alpha = 0, \end{aligned} \tag{4.10}$$

where $a \in \mathbb{F}_p^*, p > 3, d = \frac{p-1}{2}, G \in \mathbb{F}_p[\mathbf{X}]$ and $\deg G < d$. Then $v_p(\mathcal{N}) = 0$ and the system has a solution in $\mathbb{F}_p{}^n$ for all $\alpha \in \mathbb{F}_p$.

Proof. Note that

$$\{(Y_1X_{i_1}^d)^2, \ldots, (Y_1X_{i_d}^d)^2, (Y_2X_{i_{d+1}})^{p-1}\}, \tag{4.11}$$

$1 \leq i_k \neq i_j \leq d+1$ for $k \neq j$, are $(p-1)$-coverings of the polynomial F associated with system (4.10). These $(p-1)$-coverings have size $2(p-1) = (\frac{n-1}{d} + 1)(p-1) = \kappa_{p-1}(F)$ and hence are minimal. There are $d+1$ minimal $(p-1)$-coverings of this form. Also,

$$\{(Y_1X_{i_1}^d), (Y_1X_{i_2}^d), (Y_1X_{i_3}^d)^2, \ldots, (Y_1X_{i_{d+1}}^d)^2, (Y_2X_{i_1})^d, (Y_2X_{i_2})^d\}, \tag{4.12}$$

are minimal $(p-1)$-coverings of the system. There are $\binom{d+1}{2}$ minimal $(p-1)$-coverings of this form. We now prove that all the minimal $(p-1)$-coverings are of the form (4.11) or (4.12).

Let $(h_1, \ldots, h_n : s_1, \ldots, s_n)$ be the exponent vector of a minimal $(p-1)$-covering of (4.10) with $G = \alpha = 0$. In the proof of Lemma 3.1 we saw that $\lambda_i = 1$ for $i = 1, \ldots, n, n+2$, and $dh_i + s_i = p-1$, and this implies that $s_i = 2d - dh_i = d(2-h_i)$ for all i. Note that, since $s_i, h_i \geq 0$, from $s_i = d(2-h_i)$ we get that $h_i = 0$, $h_i = 1$, or $h_i = 2$ and $s_i = 2d = p-1$, $s_i = d$, or $s_i = 0$, respectively. If a minimal $(p-1)$-covering has one $s_i = p-1$ then $s_j = 0$ for all $j \neq i$ because otherwise $\sum_{i=0}^{n} s_i > p-1$. So, any exponent vector of a minimal $(p-1)$-covering with an $s_i = p-1$ has the form of (4.11). Suppose now that a minimal $(p-1)$-covering has r of the s_i's equal to d and the other equal to zero. Then, since $p-1 = \sum_{i=0}^{n} s_i = dr$,

we must have that $r = 2$ and the exponent vector of the $(p-1)$-covering has the form of (4.12).

Therefore,

$$\begin{aligned}\sum_{i=1}^{r} \frac{a^{\nu_{i1}} \cdots a^{\nu_{in}}}{\nu_{i1}! \cdots \nu_{iN}!} &= (d+1)\frac{a^{2d}}{2^d(p-1)!} + \binom{d+1}{2}\frac{a^{2d}}{2^{d-1}(d!)^2} \\ &= \frac{(d+1)a^{2d}}{2^d}\left(\frac{1}{(p-1)!} + \frac{d}{(d!)^2}\right) \\ &\equiv \frac{(d+1)a^{2d}}{2^d}\left(-1 + \frac{1}{d[(d-1)!]^2}\right) \pmod{p}.\end{aligned}$$

It can be easily proved that $\frac{1}{d[(d-1)!]^2} \not\equiv 1 \pmod{p}$ and hence $\sum_{i=1}^{r} \frac{a^{\nu_{i1}} \cdots a^{\nu_{in}}}{\nu_{i1}! \cdots \nu_{iN}!} \not\equiv 0 \pmod{p}$. The result now follows from Theorem 4.2. □

Acknowledgments

The authors appreciate the corrections and helpful suggestions to the original version of this paper made by Dr. Arne Winterhof and also the changes suggested by the referee.

References

[1] A. Adolphson and S. Sperber, p-adic estimates for exponential sums and the theorem of Chevalley-Warning, *Ann. Sci. École Norm. Sup.* (4) **20**(4) (1987) 545–556.
[2] J. Ax, Zeroes of polynomials over finite fields, *Amer. J. Math.* **86** (1964) 255–261.
[3] A. Canteaut, Cryptographic functions and design criteria for block ciphers, in *Progress in Cryptology — INDOCRYPT 2001* (*Chennai*), Lecture Notes in Computer Science, Vol. 2247 (Springer, Berlin, 2001), pp. 1–16.
[4] A. Canteaut, On the weight distributions of optimal cosets of the first-order Reed — Muller codes, *IEEE Trans. Inform. Theory* **47**(1) (2001) 407–413.
[5] L. Carlitz, Solvability of certain equations in a finite field, *Q. J. Math. Oxford Ser.* (2) **7** (1956) 3–4.
[6] L. Carlitz, Solvability of certain equations in a finite field, *Acta Arith.* **7** (1961/1962) 389–397.
[7] F. N. Castro, H. Randriam, I. Rubio and H. F. Mattson, Jr., Divisibility of exponential sums via elementary methods, *J. Number Theory* **130**(7) (2010) 1520–1536.
[8] F. N. Castro and I. Rubio, Exact p-divisibility of exponential sums via the covering method, *Proc. Amer. Math. Soc.* (in press).
[9] F. N. Castro and I. Rubio and J. M. Vega, Divisibility of exponential sums and solvability of certain equations over finite fields, *Q. J. Math.* **60**(2) (2009) 169–181.
[10] N. M. Katz. On a theorem of Ax, *Amer. J. Math.* **93** (1971) 485–499.
[11] O. Moreno and F. N. Castro, Divisibility properties for covering radius of certain cyclic codes, *IEEE Trans. Inform. Theory* **49**(12) (2003) 3299–3303.
[12] O. Moreno and C. J. Moreno, Improvements of the Chevalley-Warning and the Ax–Katz theorems, *Amer. J. Math.* **117**(1) (1995) 241–244.