PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

EXACT p-DIVISIBILITY OF EXPONENTIAL SUMS VIA THE COVERING METHOD

FRANCIS CASTRO AND IVELISSE M. RUBIO

Abstract. In general, the methods to estimate the p-divisibility of exponential sums or the number of solutions of systems of polynomial equations over finite fields are non-elementary. In this paper we present the covering method, an elementary combinatorial method that can be used to compute the exact p-divisibility of exponential sums over a prime field. The results here allow us to compute the exact p-divisibility of exponential sums of new families of polynomials, to unify and improve previously known results, and to construct families of systems of polynomial equations over finite fields that are solvable.

1. Introduction

The p-divisibility of exponential sums has been used to determine properties in coding theory such as the weight distribution, covering radius and minimum distance; it also can be used to provide families of functions that are balanced and hence are good candidates for applications to cryptography. Moreover, the p-divisibility of exponential sums can be used to answer the fundamental question of whether a system of polynomial equations has solutions over a finite field. If one can compute the exact p-divisibility of an exponential sum associated to a system of polynomial equations over a finite field, one guarantees that the system is solvable.

In general, algebraic methods to estimate the p-divisibility of exponential sums or the number of solutions of systems of polynomial equations over finite fields are non-elementary. In [11], Moreno-Moreno introduced the covering method, providing an elementary way to estimate the 2-divisibility of exponential sums over the binary field. Using this elementary combinatorial method they gave an improvement to Ax's theorem [2] for the binary case. In [10], Moreno-Castro-Mattson used the covering method to give an elementary proof to Moreno-Moreno's result in [9] for finite fields of characteristic 2. Recently, Castro-Randriam-Rubio-Mattson [6] presented a method that unifies and sometimes improves previously known results of Ax-Katz [2, 8], Moreno-Moreno [9], Adolphson-Sperber [1], and Cao-Sun [3]. This method estimates the p-divisibility of exponential sums and generalizes the covering method to any prime field. Even though the method is elementary and is based in the covering method for binary fields, it is algebraic and relies on some technical computations that lose the intuition of the original combinatorial method of selecting certain set of monomials from the terms in the system of polynomials.

The present paper reformulates the definition of the covering for any prime field in a way that resembles the original combinatorial definition for binary fields and provides a more intuitive approach. This approach helps to find sufficient conditions

2010 *Mathematics Subject Classification.* Primary 11L03 ; Secondary 11A07 .

to compute exact p-divisibility of exponential sums and hence extend the results obtained in [5] for Boolean functions to any prime field.

Thus, the paper provides an elementary combinatorial method to compute exact p-divisibility and an intuitive approach to the construction of systems of polynomial equations that are guaranteed to be solvable. The computation of the exact p-divisibility of exponential sums in certain cases improves the results in [6], which only gave bounds for the p-divisibility. We also present a partial extension of a result on the number of solutions of polynomial equations obtained by Cao-Sun [3] to the case of the p-divisibility of exponential sums, and generalize and improve results presented in [7].

2. Preliminaries

Let p be a prime, $\mathbb{F}_p$ be the prime field, $\mathbb{F}_p^n = \{(x_1, \ldots, x_n) \,|\, x_i \in \mathbb{F}_p, i = 1, \ldots, n\}$. Sometimes we use $\mathbf{x}$ instead of $(x_1, \ldots, x_n)$. Let $F(\mathbf{X}) = a_1 X_1^{e_{11}} \cdots X_n^{e_{n1}} + \cdots + a_N X_1^{e_{1N}} X_2^{e_{2N}} \cdots X_n^{e_{nN}}$ 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 variables $X_1, \ldots, X_n$.

The base p expansion of a non-negative integer k is $k = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$, where $0 \leq a_i < p$. The p-weight of k is then defined as $\sigma_p(k) = a_0 + a_1 + \cdots + a_r$. The **exact p-divisibility** of k, $v_p(k)$, is the exponent on the highest power of p dividing k. It is known that

$$v_p(k!) = \frac{k - \sigma_p(k)}{p-1}. \tag{2.1}$$

2.1. **Exponential Sums.** Let ζ be a primitive p-th 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 $\mathbb{F}_q, q = p^f, f \geq 1$, is defined as

$$S(F) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} \zeta^{Tr_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))},$$

where $Tr_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ is the trace map. If $q = p$ one can also use other representations of $\mathbb{F}_p$ to evaluate the sum, as we do after Lemma 3.1.

The next theorem [12, Theorem 7] gives an estimate on the p-divisibility of the exponential sum of a polynomial $F(\mathbf{X})$ over a finite field $\mathbb{F}_q$ of characteristic p:

Theorem 2.1. *Let $F(\mathbf{X}) = \sum_{i=1}^N a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}} \in \mathbb{F}_q^*[\mathbf{X}]$. Then $v_p(S(F)) \geq \frac{L}{p-1}$, where $S(F) = \sum_{\mathbf{x} \in \mathbb{F}_q^n} \zeta^{Tr_{\mathbb{F}_q/\mathbb{F}_p}(F(\mathbf{x}))}$, $L = \min_{(\nu_1, \ldots, \nu_N)} \left\{ \sum_{i=1}^N \sigma_p(\nu_i) \mid 0 \leq \nu_i < q \right\}$, and $(\nu_1, \ldots, \nu_N)$ is a solution to the system*

$$\begin{cases} e_{11}\nu_1 + e_{12}\nu_2 + \cdots + e_{1N}\nu_N & \equiv 0 \bmod q-1 \\ \qquad\qquad \vdots & \qquad\qquad \vdots \\ e_{n1}\nu_1 + e_{n2}\nu_2 + \cdots + e_{nN}\nu_N & \equiv 0 \bmod q-1, \end{cases} \tag{2.2}$$

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

The proof of this result involved the use of non-elementary theorems such as Stickelberger's theorem. The same result, restricted to prime fields $\mathbb{F}_p$ was proven in [6, Theorem 3.1] using only elementary methods. To obtain the estimate on

the p-divisibility of the exponential sum by using these theorems one needs to find minimal solutions to the system of congruences (2.2). Our goal in this paper is to provide a more intuitive combinatorial way to estimate this p-divisibility and to provide sufficient conditions on the polynomial that allow us to compute the exact p-divisibility, $v_p(S(F)) = \frac{L}{p-1}$ (see Corollary 3.8 and Theorem 3.9).

From now on we restrict ourselves to prime fields and only consider polynomials over $\mathbb{F}_p$. Noticing that (2.2) is constructed using the exponents of the monomials in the polynomial $F(\mathbf{X}) = a_1F_1 + \cdots + a_NF_N \in \mathbb{F}_p^*[\mathbf{X}],\ F_i = X_1^{e_{1i}} \cdots X_n^{e_{ni}}$, and rewriting the system as

$$\begin{pmatrix} e_{11} \\ e_{21} \\ \vdots \\ e_{n1} \end{pmatrix} \nu_1 + \cdots + \begin{pmatrix} e_{1N} \\ e_{2N} \\ \vdots \\ e_{nN} \end{pmatrix} \nu_N = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} (p-1), \tag{2.3}$$

one sees that the solutions that we are looking for are exponents ν_i for the monomials F_i in F such that

$$F_1^{\nu_1} F_2^{\nu_2} \cdots F_N^{\nu_N} = X_1^{\lambda_1(p-1)} \cdots X_n^{\lambda_n(p-1)},$$

for $\lambda_1, \ldots, \lambda_n > 0$, and such that $\nu_1 + \cdots + \nu_N$ is as small as possible. This is the motivation for the definition of the minimal m-covering in Definition 2.5, below. Note that the solutions do not depend on the coefficients of the polynomial F.

2.2. **Coverings.** The approach of estimating the p-divisibility of exponential sums of polynomials by finding certain solutions $(\nu_1, \ldots, \nu_N)$ to systems like (2.2), was the one taken in [6] and [12]. The concept of an m-covering was introduced in [6] but in this paper we reformulate the definition by taking the approach of covering sets. We then find sufficient conditions on the $(p-1)$-coverings of a polynomial F that allow us to compute the exact p-divisibility of the exponential sum.

Definition 2.2. Let $F(\mathbf{X}) = a_1F_1 + a_2F_2 + \cdots + a_NF_N$. A set $\mathcal{C} = \left\{F_{i_1}^{\nu_{i_1}}, \ldots, F_{i_r}^{\nu_{i_r}}\right\}$ of powers of monomials in F is an **m-covering of** F if in the product $F_{i_1}^{\nu_{i_1}} \cdots F_{i_r}^{\nu_{i_r}}$ the exponent of each variable is a positive multiple of m. We define the **size** of the covering $\mathcal{C}$ as the sum $\sum_{k=1}^{r} \nu_{i_k}$.

Example 2.3. Let $F(\mathbf{X}) = X_1^2X_2^3 + X_1^2 + X_2^3 \in \mathbb{F}_7[X_1, X_2]$. Then $\mathcal{C}_1 = \left\{\left(X_1^2X_2^3\right)^6\right\}$, $\mathcal{C}_2 = \left\{\left(X_1^2\right)^3, \left(X_2^3\right)^2\right\}, \mathcal{C}_3 = \left\{\left(X_1^2X_2^3\right)^2, \left(X_1^2\right)^1\right\}$ are 6-coverings of F.

Remark 2.4. An m-covering need not use all the F_is. We may use them all if we allow some exponents ν_i to be 0. From now on, all the coverings will be written as $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$, where maybe some $\nu_i = 0$.

In this work we are interested in $(p-1)$-coverings of polynomials in $\mathbb{F}_p[\mathbf{X}]$. If one considers 1-coverings of a polynomial F over $\mathbb{F}_2$, one is looking for sets $\mathcal{C}$ of monomials in F such that every variable X_i appears in at least one monomial in $\mathcal{C}$; this is, one is looking for monomials in F that "cover" all the variables $X_1, \ldots, X_n$.

From the reformulation (2.3) of the system of congruences (2.2) we now see that in order to estimate the p-divisibility of the exponential sum of a polynomial F over $\mathbb{F}_p$ we need to find the minimal $(p-1)$-coverings of F.

Definition 2.5. Let $F(\mathbf{X}) = a_1F_1 + a_2F_2 + \cdots + a_NF_N$. A set $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ is a **minimal m-covering of** F if for any other m-covering $\mathcal{C}' = \left\{F_1^{\nu_1'}, \ldots, F_N^{\nu_N'}\right\}$ 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; that is, $\kappa_m(F) = \sum_{i=1}^N \nu_i$.

Example 2.6. In Example 2.3, $\mathcal{C}_3$ is a minimal 6-covering of F of size 3 and it is unique with the property of having minimal size.

We now restate Theorem 2.1 for $q = p$ (and [6, Theorem 3.1]) using minimal coverings in the following way:

Theorem 2.7. *Let $F(\mathbf{X})$ be a polynomial over $\mathbb{F}_p$ and $\mathcal{C}$ be a minimal $(p-1)$-covering of F of size $\kappa_{p-1}(F)$. Then $v_p(S(F)) \geq \frac{\kappa_{p-1}(F)}{p-1}$.*

In order to simplify the development of our results we introduce the concept of partial m-coverings of a polynomial F and see their relation with the m-coverings of F.

Definition 2.8. 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 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 partial m-coverings $\mathcal{C}$ allow the possibility of having variables in F that do not appear in the monomials in $\mathcal{C}$.

Example 2.9. Consider F as in Example 2.3. Then, $\mathcal{C}_4 = \left\{\left(X_1^2\right)^3\right\}$ is a partial 6-covering of F but not a 6-covering of F.

Remark 2.10. Note that for partial m-coverings we allow the equations in (2.3) to have $\lambda_i \geq 0$. Also note that one can extend a partial m-covering $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ of F to an m-covering $\mathcal{C}' = \left\{F_1^{\nu_1'}, \ldots, F_N^{\nu_N'}\right\}$ of F by letting $\nu_j' = m$ if $\nu_j = 0$ and $\nu_j' = \nu_j$ otherwise.

When we extend the concept of minimality of m-coverings to partial m-coverings, we also consider the number of equations s in (2.3) where $\lambda_i = 0$.

Definition 2.11. Let $F(\mathbf{X}) = a_1F_1 + a_2F_2 + \cdots + a_NF_N$. A set $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ is a **minimal partial m-covering of** F if $\sum_{i=1}^N \nu_i + s(p-1) = \kappa_m(F)$, where s is the number of equations in (2.3) with $\lambda_i = 0$.

It is known [6, Lemma 2.1] that in any partial m-covering of F, $\sum_{i=1}^N \nu_i + s(p-1) \geq \kappa_m(F)$. The next lemma gives a bound for the powers of the monomials in a minimal partial m-covering.

Lemma 2.12. [6, Lemma 2.3] *Let $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ be a minimal partial m-covering of $F(\mathbf{X})$. Then $\nu_i \leq m$ for $i = 1, \ldots, N$.*

3. $(p-1)$-coverings and the exact p-divisibility of exponential sums

In Theorem 2.7 we used the minimal $(p-1)$-coverings of a polynomial F to obtain a bound on the p-divisibility of the exponential sum of F. We now want to find sufficient conditions to compute the exact p-divisibility of the exponential sum. This will extend the results obtained in [5] for Boolean functions to any prime field. We first look at the expansion of the exponential sum of F.

Let $F(\mathbf{X}) = a_1F_1 + \cdots + a_NF_N \in \mathbb{F}_p{}^*[\mathbf{X}]$. Then

$$\begin{aligned} S(F) &= \sum_{\mathbf{x}\in\mathbb{F}_p^n} \zeta^{F(\mathbf{x})} = \sum_{\mathbf{x}\in\mathbb{F}_p^n} (1-\theta)^{a_1F_1+\cdots+a_NF_N} \\ &= \sum_{\mathbf{x}\in\mathbb{F}_p^n} \sum_{\nu_1=0}^{M} \binom{a_1F_1}{\nu_1}(-\theta)^{\nu_1} \times \cdots \times \sum_{\nu_N=0}^{M} \binom{a_NF_N}{\nu_N}(-\theta)^{\nu_N} \\ &= \sum_{\nu_1=0}^{M} \cdots \sum_{\nu_N=0}^{M} \sum_{\mathbf{x}\in\mathbb{F}_p^n} (-\theta)^{|\boldsymbol{\nu}|} \binom{a_1F_1}{\nu_1} \cdots \binom{a_NF_N}{\nu_N}, \end{aligned} \tag{3.1}$$

where $\theta = 1-\zeta$, $M = p^{\deg(F)+1}$, and $|\boldsymbol{\nu}| = \sum_{i=1}^{N} \nu_i$.

The exact p-divisibility of $S(F)$, $v_p(S(F))$, is the largest power of p dividing $S(F)$. To compute $v_p(S(F))$ one can study the p-divisibility of each term in (3.1).

Let

$$T_{\boldsymbol{\nu}}(F) = (-\theta)^{|\boldsymbol{\nu}|} \sum_{\mathbf{x}\in\mathbb{F}_p^n} \binom{a_1F_1}{\nu_1} \cdots \binom{a_NF_N}{\nu_N} \tag{3.2}$$

be the term in (3.1) associated to $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_N)$. Then

$$\begin{aligned} T_{\boldsymbol{\nu}}(F) &= (-\theta)^{|\boldsymbol{\nu}|} \sum_{\mathbf{x}\in\mathbb{F}_p^n} \frac{a_1F_1\cdots(a_1F_1-\nu_1+1)}{\nu_1!} \cdots \frac{a_NF_N\cdots(a_NF_N-\nu_N+1)}{\nu_N!} \\ &= (-\theta)^{|\boldsymbol{\nu}|} \sum_{\mathbf{x}\in\mathbb{F}_p^n} \frac{a_1^{\nu_1}\cdots a_N^{\nu_N} F_1^{\nu_1}F_2^{\nu_2}\cdots F_N^{\nu_N}}{\nu_1!\cdots\nu_N!} + P_{\boldsymbol{\nu}} \qquad (3.3) \\ &= \frac{(-\theta)^{|\boldsymbol{\nu}|}}{\nu_1!\cdots\nu_N!} a_1^{\nu_1}\cdots a_N^{\nu_N} \sum_{\mathbf{x}\in\mathbb{F}_p^n} \left(F_1^{\nu_1}F_2^{\nu_2}\cdots F_N^{\nu_N} + P_{\boldsymbol{\nu}}\right), \end{aligned}$$

where $\deg(P_{\boldsymbol{\nu}}) < \deg(F_1^{\nu_1}F_2^{\nu_2}\cdots F_N^{\nu_N})$. Now, using that $p \nmid a_i$ and (2.1),

$$v_p(T_{\boldsymbol{\nu}}(F)) = \sum_{i=1}^{N} \frac{\sigma_p(\nu_i)}{p-1} + \nu_p\left(\sum_{\mathbf{x}\in\mathbb{F}_p^n} (F_1^{\nu_1}F_2^{\nu_2}\cdots F_N^{\nu_N} + P_{\boldsymbol{\nu}})\right). \tag{3.4}$$

So, to compute the exact p-divisibility of $S(F)$ one must compute the smallest $v_p(T_{\boldsymbol{\nu}}(F))$. If there exists $\boldsymbol{\nu}$ such that $v_p(T_{\boldsymbol{\nu}}(F)) < v_p(T_{\boldsymbol{\nu}'}(F))$ for all $\boldsymbol{\nu}' \neq \boldsymbol{\nu}$, then $v_p(S(F)) = v_p(T_{\boldsymbol{\nu}}(F))$. The existence of a unique $\boldsymbol{\nu}$ with smallest $|\boldsymbol{\nu}|$ is related to the computation of the exact p-divisibility of $S(F)$.

The next lemma tells us that the terms in $F_1^{\nu_1}\cdots F_N^{\nu_N} + P_{\boldsymbol{\nu}}$ with exponents that are not multiples of $p-1$ produce terms in $\sum_{\mathbf{x}\in\mathbb{F}_p^n}(F_1^{\nu_1}\cdots F_N^{\nu_N} + P_{\boldsymbol{\nu}})$ with high p-divisibility; terms in $F_1^{\nu_1}\cdots F_N^{\nu_N} + P_{\boldsymbol{\nu}}$ with s missing variables (i.e. variables with exponents equal to 0) increase the p-divisibility of the term by s; and terms with exponents that are multiples of $p-1$ give terms in $\sum_{\mathbf{x}\in\mathbb{F}_p^n}(F_1^{\nu_1}\cdots F_N^{\nu_N} + P_{\boldsymbol{\nu}})$ that are not divisible by p. This gives the connection between the $(p-1)$-coverings of F and the p-divisibility of $S(F)$.

Lemma 3.1. *Let $\mathcal{S} = \{0,1\}$ if $p = 2$, and for $p \geq 3$, let g be a generator of the group of units of $\mathbb{Z}/p^m\mathbb{Z}$, and $\mathcal{S} = \{0\} \cup \left\{g^{ip^{m-1}} \mid 0 \leq i \leq p-1\right\}$. Then, the*

elements of $\mathcal{S}$ are a complete residue system modulo p, and for k a non-negative integer,

$$\sum_{x\in\mathcal{S}} x^k \equiv \begin{cases} p \mod p^m & \text{if } k=0 \\ p-1 \mod p^m & \text{if } k \text{ is a nonzero multiple of } p-1 \\ 0 \mod p^m & \text{if } k \text{ is not divisible by } p-1. \end{cases} \tag{3.5}$$

We now can consider the exponential sum of F over the set $\mathcal{S}$,

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

and use (3.5) to compute the p-divisibility of the terms in $S(F)$. We note that a $(p-1)$-covering $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ corresponds to a term $T_{\boldsymbol{\nu}}(F)$ where $F_1^{\nu_1}\cdots F_N^{\nu_N}$ has no missing variables and exponents that are multiples of $p-1$ and therefore $p \nmid \sum_{\mathbf{x}\in S^n} F_1^{\nu_1}\cdots F_N^{\nu_N}$. The next lemma shows that if the covering is also minimal, one can compute the exact p-divisibility of the corresponding term.

Lemma 3.2. *Let $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ be a minimal $(p-1)$-covering of $F(\mathbf{X}) = a_1F_1 + \cdots + a_NF_N$. Then $v_p\left(T_{\boldsymbol{\nu}}(F)\right) = \sum_{i=1}^N \frac{\nu_i}{p-1}$.*

Proof. Note that Lemma 2.12 tells us that $\nu_i \leq p-1$ for $i = 1, \ldots, N$. Hence $\sigma_p(\nu_i) = \nu_i$ and, from (3.4),

$$v_p\left(T_{\boldsymbol{\nu}}(F)\right) = \sum_{i=1}^N \frac{\nu_i}{p-1} + v_p\left(\sum_{\mathbf{x}\in\mathcal{S}^n} (F_1^{\nu_1}\cdots F_N^{\nu_N} + P_{\boldsymbol{\nu}})\right).$$

Since $\mathcal{C}$ is a $(p-1)$-covering, the exponent of each variable in $F_1^{\nu_1}\cdots F_N^{\nu_N}$ is a non-zero multiple of $p-1$. Therefore, by Lemma 3.1, $p \nmid \sum_{\mathbf{x}\in\mathcal{S}^n} F_1^{\nu_1}\cdots F_N^{\nu_N}$. Also, since $\mathcal{C}$ is a minimal covering, there are no terms $F_1^{l_1}\cdots F_N^{l_N}$ in $P_{\boldsymbol{\nu}}$ for which $p-1$ divides all exponents. Therefore all the terms in $\sum_{\mathbf{x}\in\mathcal{S}^n} P_{\boldsymbol{\nu}}$ are divisible by p, and hence $p \nmid \sum_{\mathbf{x}\in\mathcal{S}^n} (F_1^{\nu_1}\cdots F_N^{\nu_N} + P_{\boldsymbol{\nu}})$. This completes the proof. □

We now present lemmas that give conditions under which the terms that do not correspond to minimal coverings will have larger p-divisibility. By studying the expansion of (3.2) given in (3.3), we note that if $F_1^{\nu_1}\cdots F_N^{\nu_N}$ has a variable missing, so does $P_{\boldsymbol{\nu}}$. By Lemma 3.1, each missing variable gives an extra factor of p in $\sum_{\mathbf{x}\in\mathcal{S}^n} \binom{a_1F_1}{\nu_1}\cdots\binom{a_NF_N}{\nu_N}$ and the sum over the other variables is unchanged. This implies the following result [6, Lemma 3.5].

Lemma 3.3. *Let $F(\mathbf{X}) = a_1F_1 + \cdots + a_NF_N$. If $F_1^{\nu_1}\cdots F_N^{\nu_N}$ has $s \geq 1$ variables missing, then $v_p\left(T_{\boldsymbol{\nu}}(F)\right) \geq \sum_{i=1}^N \frac{\nu_i}{p-1} + s > \sum_{i=1}^N \frac{\nu_i}{p-1}$.*

We mentioned before that if there is only one $\boldsymbol{\nu}$ for which the corresponding term $T_{\boldsymbol{\nu}}(F)$ in the exponential sum has smallest p-divisibility, then this gives the exact p-divisibility of the exponential sum. So, one needs to guarantee a unique minimal $(p-1)$-covering $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ and no partial $(p-1)$-covering $\mathcal{C}' = \left\{F_1^{\nu_1'}, \ldots, F_N^{\nu_N'}\right\}$ with $\sum_{j=1}^N \frac{\nu_j'}{p-1} + s = \sum_{j=1}^N \frac{\nu_j}{p-1}$, where s is the number of variables missing in $F_1^{\nu_1'}\cdots F_N^{\nu_N'}$.

Lemma 3.4. *Suppose that* $F(\mathbf{X}) = a_1F_1 + \cdots + a_NF_N$ *has a unique minimal* $(p-1)$*-covering* $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$*, and let* $\mathcal{C}' = \left\{F_1^{\nu_1'}, \ldots, F_N^{\nu_N'}\right\}$ *be any set with* $\sum_{i=1}^N \nu_i' \leq \sum_{i=1}^N \nu_i$ *and* $\mathcal{C}' \not\subseteq \mathcal{C}$*. Then* $v_p\left(T_{\boldsymbol{\nu}'}(F)\right) > \sum_{i=1}^N \frac{\nu_i}{p-1}$.

Proof. Suppose that $\mathcal{C}'$ is not a partial $(p-1)$-covering of F. Then, by Remark 2.10, $(\nu_1', \ldots, \nu_N')$ is not a solution to (2.3) with all $\lambda_i \geq 0$, and Lemma 3.7 in [6] implies the result.

Now suppose that $\mathcal{C}'$ is a partial $(p-1)$-covering of F. Since $\sum_{i=1}^N \nu_i' \leq \sum_{i=1}^N \nu_i$ and $\mathcal{C}$ is the unique minimal $(p-1)$-covering of F, there must be $s > 1$ variables missing in $F_1^{\nu_1'} \cdots F_N^{\nu_N'}$. We can construct another $(p-1)$-covering $\mathcal{C}''$ of F in the following way: for each missing variable, choose a monomial F_i in $\mathcal{C}$ that contains the missing variable and add F_i^{p-1} to the partial $(p-1)$-covering $\mathcal{C}'$. Note that this will still produce a partial $(p-1)$-covering of F and it could happen that the same monomial F_i contains more than one of the missing variables. Continue adding powers of monomials of F to $\mathcal{C}$ until $\mathcal{C}''$ covers all the n variables.

Now, the new covering $\mathcal{C}''$ is such that

$$\sum_{i=1}^N \frac{\nu_i''}{p-1} = \sum_{i=1}^N \frac{\nu_i' + l(p-1)}{p-1} \leq \sum_{i=1}^N \frac{\nu_i'}{p-1} + s,$$

where l is the number of monomials added to the partial $(p-1)$-covering $\mathcal{C}'$. Since $\mathcal{C}$ is the unique minimal $(p-1)$-covering and $\mathcal{C}' \not\subseteq \mathcal{C}$, the new covering $\mathcal{C}''$ must be such that $\sum_{i=1}^N \frac{\nu_i}{p-1} < \sum_{i=1}^N \frac{\nu_i''}{p-1}$ and therefore

$$v_p\left(T_{\boldsymbol{\nu}'}(F)\right) \geq \sum_{i=1}^N \frac{\nu_i'}{p-1} + s \geq \sum_{i=1}^N \frac{\nu_i''}{p-1} > \sum_{i=1}^N \frac{\nu_i}{p-1}.$$

□

The above lemmas guarantee that if F is a polynomial with a unique minimal $(p-1)$-covering $\mathcal{C}$, then almost all the terms in (3.1) that do not correspond to $\mathcal{C}$ have larger p-divisibility. The only terms that were not included in the lemmas are those corresponding to partial $(p-1)$-coverings contained in $\mathcal{C}$. In the next theorem we include as hypothesis a conditional statement where these terms have p-divisibility larger than the terms corresponding to the minimal covering. The theorem provides the conditions needed to compute the exact p-divisibility of new families of polynomial equations, to unify and improve previously known results, and to provide an intuitive way to construct families of systems of polynomial equations over finite fields that are solvable.

Theorem 3.5. *Suppose that* $F(\mathbf{X}) = a_1F_1 + \cdots + a_NF_N$ *has a unique minimal* $(p-1)$*-covering* $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ *such that if* $\mathcal{C}' = \left\{F_1^{\nu_1'}, \ldots, F_N^{\nu_N'}\right\} \subsetneq \mathcal{C}$ *is a partial* $(p-1)$*-covering of* F*, then* $v_p\left(T_{\boldsymbol{\nu}'}(F)\right) > \sum_{i=1}^N \frac{\nu_i}{p-1}$*. Then* $v_p\left(S(F)\right) = \sum_{i=1}^N \frac{\nu_i}{p-1}$.

Proof. Let $\mathcal{C}$ be the unique minimal $(p-1)$-covering of F and $\boldsymbol{\nu}$ the vector associated to $\mathcal{C}$. Lemma 3.2 implies that $v_p\left(T_{\boldsymbol{\nu}}(F)\right) = \sum_{i=1}^N \frac{\nu_i}{p-1}$. If $\sum_{i=1}^N \nu_i' > \sum_{i=1}^N \nu_i$, then, by (3.2), $T_{\boldsymbol{\nu}'}(F) \geq \sum_{i=1}^N \frac{\nu_i'}{p-1} > \sum_{i=1}^N \frac{\nu_i}{p-1}$. Now, let $\boldsymbol{\nu}'$ be such that $\sum_{i=1}^N \boldsymbol{\nu}' \leq$

$\sum_{i=1}^{N} \boldsymbol{\nu}$. If $\mathcal{C}' = \left\{F_1^{\nu_1'}, \ldots, F_N^{\nu_N'}\right\}$ is not a partial $(p-1)$-covering of F, then [6, Lemma 3.7] implies that $v_p\left(T_{\boldsymbol{\nu}'}(F)\right) > \sum_{i=1}^{N} \frac{\nu_i}{p-1}$. If $\mathcal{C}' \not\subset \mathcal{C}$ is a partial $(p-1)$-covering of F, then Lemma 3.4 implies that $v_p\left(T_{\boldsymbol{\nu}'}(F)\right) > \sum_{i=1}^{N} \frac{\nu_i}{p-1}$. If $\mathcal{C}' \subsetneq \mathcal{C}$ is a partial $(p-1)$-covering, then, by hypothesis, $v_p\left(T'_{\boldsymbol{\nu}}(F)\right) > \sum_{i=1}^{N} \frac{\nu_i}{p-1}$. Therefore, $T_{\boldsymbol{\nu}}(F)$ is only term in $S(F)$ with the smallest p-divisibility and $v_p\left(S(F)\right) = v_p\left(T_{\boldsymbol{\nu}}(F)\right) = \sum_{i=1}^{N} \frac{\nu_i}{p-1}$. □

We will prove that, in order to compute the exact p-divisibility of the exponential sum of a polynomial F, it is sufficient to require F to have a unique minimal $(p-1)$-covering where each monomial F_i in $\mathcal{C}$ has at least two variables that are not contained in the other monomials of $\mathcal{C}$. We first prove that the terms associated to the partial $(p-1)$-coverings of F contained in $\mathcal{C}$ have larger p-divisibility.

Lemma 3.6. *Suppose that $F(\mathbf{X}) = a_1F_1 + \cdots + a_NF_N$ has a minimal $(p-1)$-covering $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ where each monomial F_i in $\mathcal{C}$ with $\nu_i \neq 0$ has at least two variables that are not contained in the other monomials of $\mathcal{C}$. Then, if $\mathcal{C}' = \left\{F_1^{\nu_1'}, \ldots, F_N^{\nu_N'}\right\} \subsetneq \mathcal{C}$ is a partial $(p-1)$-covering of F, then $v_p\left(T_{\boldsymbol{\nu}'}(F)\right) > \sum_{i=1}^{N} \frac{\nu_i}{p-1}$.*

Proof. Since $\mathcal{C}' \subsetneq \mathcal{C}$, we can assume without loss of generality that $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_r^{\nu_r}\}$ and $\mathcal{C}' = \{F_1^{\nu_1}, \ldots, F_h^{\nu_h}\}$, where $h < r$. Also, $\mathcal{C}'$ being a partial $(p-1)$-covering implies that there are missing variables in $M = F_1^{\nu_1} \cdots F_h^{\nu_h}$ and, by Lemma 3.3, $v_p\left(T_{\boldsymbol{\nu}'}(F)\right) \geq \sum_{i=1}^{h} \frac{\nu_i}{p-1} + s$, where $s \geq 1$ is the number of variables missing in M. Since each F_i in $\mathcal{C}$ contributes at least two new variables and there are $r - h \geq 1$ monomials in $\mathcal{C}$ that are not included in $\mathcal{C}'$, M is missing at least $2(r-h)$ variables. Hence

$$v_p\left(T_{\boldsymbol{\nu}'}(F)\right) \geq \sum_{i=1}^{h} \frac{\nu_i}{p-1} + 2(r-h) > \sum_{i=1}^{h} \frac{\nu_i}{p-1} + \frac{(r-h)(p-1)}{p-1}$$

$$\geq \sum_{i=1}^{h} \frac{\nu_i}{p-1} + \sum_{i=h+1}^{r} \frac{\nu_i}{p-1} = \sum_{i=1}^{r} \frac{\nu_i}{p-1}.$$

□

The next theorem now follows directly.

Theorem 3.7. *Suppose that $F(\mathbf{X}) = a_1F_1 + \cdots + a_NF_N$ has a unique minimal $(p-1)$-covering $\mathcal{C} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ where each monomial in $\mathcal{C}$ with $\nu_i \neq 0$ has at least two variables that are not contained in the other monomials of $\mathcal{C}$. Then $v_p\left(S(F)\right) = \sum_{i=1}^{N} \frac{\nu_i}{p-1}$.*

One of the advantages of Theorem 3.7 is that it gives simple sufficient conditions on the covering that help us to construct families of polynomials whose exponential sum has exact p-divisibility. The next corollary presents a family of polynomials for which one can easily compute the exact p-divisibility.

Corollary 3.8. Let

$$\begin{aligned} F(\mathbf{X}) &= a_1(X_{i_1}\cdots X_{i_{n_1}})^{d_1} \\ &+ a_2(X_{i_{n_1+1}}\cdots X_{i_{n_2}})^{d_2} + \cdots + a_N(X_{i_{n_{N-1}+1}}\cdots X_{i_{n_N}})^{d_N} \\ &= a_1F_1+\cdots+a_NF_N \in \mathbb{F}_p^*[\mathbf{X}] \end{aligned}$$

be such that each monomial F_i has at least two variables that are not contained in the other monomials of F. Then $v_p(S(F)) = \frac{1}{\gcd(p-1,d_1)} + \cdots + \frac{1}{\gcd(p-1,d_N)}$.

Proof. Just note that $\mathcal{C} = \left\{F_1^{\frac{p-1}{\gcd(p-1,d_1)}}, \ldots, F_N^{\frac{p-1}{\gcd(p-1,d_N)}}\right\}$ is the unique minimal $(p-1)$-covering of F and each monomial contributes at least two new variables to the covering. □

The condition in Lemma 3.6 of having each monomial in the minimal $(p-1)$-covering contributing at least two new variables is sufficient to guarantee that the p-divisibility of the terms associated to certain partial $(p-1)$-coverings have p-divisibility $\sum_{i=1}^N \frac{\nu_i'}{p-1}+s$ larger than the p-divisibility of the minimal $(p-1)$-covering, and hence get exact p-divisibility if the minimal $(p-1)$-covering is unique. But one can get a similar result by imposing other conditions.

In the next theorem, on deformed general diagonal equations, we get another sufficient condition to have a unique minimal $(p-1)$-covering and exact p-divisibility of the exponential sum. In [3, Theorem 2], Cao-Sun presented results for the number of solutions of general diagonal equations. In the following theorem and its corollary we obtain the exact p-divisibility of the exponential sums of deformed general diagonal equations, giving an extension to Cao-Sun's result to exponential sums for the case where, in each term of the diagonal part, the exponent of one of the variables divide all the other exponents in the term and $p-1$. The theorem also generalizes [7, Theorem 5] for the case $q=p$.

Theorem 3.9. *Let* $F(\mathbf{X}) = a_1X_{11}^{d_{11}}\cdots X_{1n_1}^{d_{1n_1}} + \cdots + a_NX_{N1}^{d_{N1}}\cdots X_{Nn_N}^{d_{Nn_N}} + G(\mathbf{X}) = a_1F_1+\cdots+a_NF_N+G \in \mathbb{F}_p^*[\mathbf{X}]$ *be such that the monomials* F_i *have disjoint support. Suppose that for each* $i=1,\ldots,N$, *there is* $1\le j\le n_i$ *such that* $D_i = \gcd(d_{i1}, d_{i2}, \ldots,$
$d_{in_i}, p-1) = d_{ij}$, *and* $\deg G < \min\{D_1,\ldots,D_N\}$. *Then* $v_p(S(F)) = \frac{1}{D_1}+\cdots+\frac{1}{D_N}$.

Proof. We first prove that $\mathcal{C} = \left\{F_1^{\frac{p-1}{D_1}}, \ldots, F_N^{\frac{p-1}{D_N}}\right\} = \{F_1^{\nu_1}, \ldots, F_N^{\nu_N}\}$ is the unique minimal $(p-1)$-covering of F. Suppose that $\mathcal{C}' = \left\{F_1^{\nu_1'}, \ldots, F_N^{\nu_N'}, G_1^{\omega_1}, \ldots, G_M^{\omega_M}\right\}$ is another covering of F, where $G(\mathbf{X}) = G_1+\cdots+G_M$.

Let k_{ihj} be the exponent of the variable X_{ih} in the term G_j of G. Consider the variable X_{i1}. Then k_{i1j} is the exponent of X_{i1} in the term G_j of G, and, since the monomials $F_1,\ldots,F_N$ have disjoint support, X_{i1} is contained only in F_i and G. Then, the exponent of the variable X_{i1} in $F_1^{\nu_1'}F_N^{\nu_N'}G_1^{\omega_1}G_M^{\omega_M}$ is

$$\nu_i'D_i + \omega_1k_{i11} + \cdots + \omega_Mk_{i1M} = \lambda_i(p-1)$$

for some $\lambda_i \in \mathbb{N}$. Also, $\sum_{i=1}^N k_{i1j} \le \sum_{i=1}^N\sum_{h=1}^{n_N} k_{ihj} = \deg G_j \le \deg G < \min\{D_1,\ldots,D_N\}$, and this implies

$$\sum_{i=1}^{N}\nu_i'+\sum_{i=1}^{M}\omega_i>\sum_{i=1}^{N}\nu_i'\frac{D_i}{D_i}+\omega_1\left(\sum_{i=1}^{N}\frac{k_{i11}}{D_i}\right)+\cdots+\omega_M\left(\sum_{i=1}^{N}\frac{k_{i1M}}{D_i}\right)$$
$$\geq\sum_{i=1}^{N}\frac{1}{D_i}\left[\nu_i'D_i+\omega_1k_{i11}+\cdots+\omega_Mk_{i1M}\right]=\sum_{i=1}^{N}\frac{\lambda_i(p-1)}{D_i}\geq\sum_{i=1}^{N}\frac{p-1}{D_i}.$$

This implies that $\mathcal{C}'$ is not minimal and therefore $\mathcal{C}$ is the unique minimal $(p-1)$-covering of F.

We now prove that if $\mathcal{C}'=\left\{F_1^{\nu_1'},\ldots,F_N^{\nu_N'}\right\}\subsetneq\mathcal{C}$ is a partial $(p-1)$-covering, then $v_p\left(T_{\boldsymbol{\nu}'}(F)\right)>\frac{1}{D_1}+\cdots+\frac{1}{D_N}$.

Note that $F_1,\ldots,F_N$ with disjoint support and $\mathcal{C}'$ a partial $(p-1)$-covering imply that $\nu_i'=\frac{p-1}{D_i}$ or $\nu_i'=0$. Without loss of generality, suppose that $\nu_i'=\frac{p-1}{D_i}$ for $i=1,\ldots,r$ and $\nu_i'=0$ for $r+1,\ldots,N$. Then, there are at least $N-r$ variables that do not appear in the product $F_1^{\nu_1'}\cdots F_N^{\nu_N'}$ and therefore

$$v_p\left(T_{\boldsymbol{\nu}'}(f)\right)\geq\sum_{i=1}^{r}\frac{\nu_i}{p-1}+N-r=\sum_{i=1}^{r}\frac{\nu_i}{p-1}+\sum_{i=r+1}^{N}\frac{p-1}{p-1}$$
$$>\sum_{i=1}^{N}\frac{\nu_i}{p-1}=\frac{1}{D_1}+\cdots+\frac{1}{D_N}.$$

The result now follows from Theorem 3.5. □

Corollary 3.10. The exact p-divisibility of the exponential sum of the deformed diagonal equation $a_1X_{11}^{d_{11}}\cdots X_{1n_1}^{d_{1n_1}}+\cdots+a_NX_{N1}^{d_{N1}}\cdots X_{Nn_N}^{d_{Nn_N}}+G(\mathbf{X})$ is equal to the exact p-divisibility of the exponential sum of $a_1(X_{11}\cdots X_{1n_1})^{D_1}+\cdots+a_N(X_{N1}\cdots X_{Nn_N})^{D_N}+G(\mathbf{X})$, where the monomials have disjoint support, $D_i=\gcd(d_{i1},d_{i2},\ldots,d_{in_i},p-1)=d_{ij}$ for some $1\leq j\leq n_i$ and $\deg G<\min\{D_1,\ldots,D_N\}$.

The next corollary presents families of polynomials that, if $q=p$, are more general than the ones presented in [7, 4]. Also, the proof there was less intuitive than the one presented here, but the methods in [7, 4] are still useful since they work for polynomials over any field; so far, the covering method only works for polynomials over prime fields.

Corollary 3.11. Let $F(\mathbf{X})=a_1(X_{11}\cdots X_{1n_1})^{d_1}+\cdots+a_N(X_{N1}\cdots X_{Nn_N})^{d_N}+G\in\mathbb{F}_p^*[\mathbf{X}]$ have monomials with disjoint support and $\deg G<\min_i\{\gcd(d_i,p-1)\}$. Then $v_p\left(S(F)\right)=\frac{1}{\gcd(d_1,p-1)}+\cdots+\frac{1}{\gcd(d_N,p-1)}$.

4. Solvability of polynomial equations over finite fields

One can use results on the p-divisibility of an exponential sum of a polynomial F to obtain information on the number of solutions of $F(\mathbf{X})=0$. The relation between the number of common solutions $\mathcal{N}$ of a system of polynomial equations $G_1(\mathbf{X})=G_2(\mathbf{X})=\ldots=G_t(\mathbf{X})=0$ and an exponential sum is given by the following lemma ([1, Equation 2.7], [2]).

Lemma 4.1. *Let $q=p^f$, $G_1(\mathbf{X}),\ldots,G_t(\mathbf{X})\in\mathbb{F}_q[\mathbf{X}]$ and $\mathcal{N}$ be the number of common zeros of $G_1,\ldots,G_t$. Then $\mathcal{N}=p^{-tf}\sum_{\mathbf{x}\in\mathbb{F}_q^n,\mathbf{y}\in\mathbb{F}_q^t}\zeta^{Tr_{\mathbb{F}_q/\mathbb{F}_p}(y_1G_1(\mathbf{x})+\cdots+y_tG_t(\mathbf{x}))}$.*

Note that if we can compute the exact p-divisibility of the exponential sum $\sum_{\mathbf{x}\in\mathbb{F}_q^n,\mathbf{y}\in\mathbb{F}_q^t}\zeta^{Tr_{\mathbb{F}_q/\mathbb{F}_p}(y_1G_1(\mathbf{x})+\cdots+y_tG_t(\mathbf{x}))}$, we know that $p^{v_p(\mathcal{N})+1}\nmid\mathcal{N}$ and hence $\mathcal{N}\neq 0$. Therefore the results in the previous section can be used to construct families of systems of polynomial equations that are solvable.

We will first show that if a polynomial $F(\mathbf{X})=a_1F_1+a_2F_2+\cdots+a_NF_N$ has a unique minimal $(p-1)$-covering $\{F_1^{\nu_1},\ldots,F_N^{\nu_N}\}$ with certain properties, and $\sum_{i=1}^N\frac{v_i}{p-1}$ is an integer, then $yF(\mathbf{X})$ has a unique minimal $(p-1)$-covering $\{(yF_1)^{\nu_1},\ldots,(yF_N)^{\nu_N}\}$ with the same properties and one gets the exact p-divisibility of $\mathcal{N}$ and hence the solvability of $F=0$. We recall that in this paper we only consider polynomials over $\mathbb{F}_p$.

The next proposition corresponds to Theorem 3.5 in the previous section.

Proposition 4.2. Suppose that $F(\mathbf{X})=a_1F_1+a_2F_2+\cdots+a_NF_N$ has unique minimal $(p-1)$-covering $\mathcal{C}=\{F_1^{\nu_1},\ldots,F_N^{\nu_N}\}$ such that if $\mathcal{C}'=\left\{F_1^{\nu_1'},\ldots,F_N^{\nu_N'}\right\}\subsetneq\mathcal{C}$ is a partial $(p-1)$-covering of F, then $v_p\left(T_{\boldsymbol{\nu}'}(F)\right)>\sum_{i=1}^N\frac{\nu_i}{p-1}$. If $\sum_{i=1}^N\frac{\nu_i}{p-1}$ is an integer, then $v_p(\mathcal{N})=\left(\sum_{i=1}^N\frac{\nu_i}{p-1}\right)-1$ and $F(\mathbf{X})=0$ is solvable.

Proof. By Lemma 4.1, the number of solutions of $F(\mathbf{X})=0$ is

$$\mathcal{N}=p^{-1}\sum_{\mathbf{x}\in\mathbb{F}_p^n,y\in\mathbb{F}_p}\zeta^{yF(\mathbf{x})}.$$

Let $\mathcal{C}=\{F_1^{\nu_1},\ldots,F_N^{\nu_N}\}$ be a $(p-1)$-covering of F that satisfies the hypothesis and assume that $\sum_{i=1}^N\frac{\nu_i}{p-1}$ is an integer. Then, as in Theorem 3.5, $\mathcal{C}_y=\{(yF_1)^{\nu_1},\ldots,(yF_N)^{\nu_N}\}$ is the unique minimal $(p-1)$-covering of yF and, if $\mathcal{C}_y'=\left\{(yF_1)^{\nu_1'},\ldots,(yF_N)^{\nu_N'}\right\}\subsetneq\mathcal{C}_y$ is a partial $(p-1)$-covering of yF, then $v_p\left(T_{\boldsymbol{\nu}'}(F)\right)>\sum_{i=1}^N\frac{\nu_i}{p-1}$. Therefore, using Lemma 4.1, we find that $v_p(\mathcal{N})=\left(\sum_{i=1}^N\frac{\nu_i}{p-1}\right)-1$ and $F(\mathbf{X})=0$ is solvable. □

The next results correspond to results in the previous section. Their proofs are similar to the proof of Proposition 4.2 above.

Theorem 4.3. *Suppose that $F(\mathbf{X})=a_1F_1+\cdots+a_NF_N$ has a unique minimal $(p-1)$-covering $\mathcal{C}=\{F_1^{\nu_1},\ldots,F_N^{\nu_N}\}$ where each monomial in $\mathcal{C}$ has at least two variables that are not contained in the other monomials of $\mathcal{C}$. If $\sum_{i=1}^N\frac{\nu_i}{p-1}$ is an integer, then $v_p(\mathcal{N})=\left(\sum_{i=1}^N\frac{\nu_i}{p-1}\right)-1$ and $F(\mathbf{X})=0$ is solvable.*

We now can construct specific families of solvable equations illustrating the utility of the covering method for this application.

Corollary 4.4. Let $F(\mathbf{X})=a_1(X_{i_1}\cdots X_{i_{n_1}})^{d_1}+\cdots+a_N(X_{i_{n_{N-1}+1}}\cdots X_{i_{n_N}})^{d_N}=a_1F_1+\cdots+a_NF_N\ \in\mathbb{F}_p^*[\mathbf{X}]$ be such that each monomial F_i has at least two variables that are not contained in the other monomials of F, and let $\mathcal{N}$ be the number of solutions of $F(\mathbf{X})=0$. If $\frac{1}{\gcd(p-1,d_1)}+\cdots+\frac{1}{\gcd(p-1,d_N)}$ is an integer, then $v_p(\mathcal{N})=\left(\sum_{i=1}^N\frac{1}{\gcd(p-1,d_i)}\right)-1$ and $F(\mathbf{X})=0$ is solvable.

Theorem 4.5. *Let $F(\mathbf{X})=a_1X_{11}^{d_{11}}\cdots X_{1n_1}^{d_{1n_1}}+\cdots+a_NX_{N1}^{d_{N1}}\cdots X_{Nn_N}^{d_{Nn_N}}+G=a_1F_1+\cdots+a_NF_N+G\ \in\mathbb{F}_p^*[\mathbf{X}]$ be such that the monomials F_i have disjoint*

support. Suppose that for each $i = 1, \ldots, N$*, there is* $1 \leq j \leq n_i$ *such that* $D_i = \gcd(d_{i1}, d_{i2}, \ldots,$
$d_{in_i}, p-1) = d_{ij}$*, and* $\deg G < \min\{D_1, \ldots, D_N\}$*. If* $\frac{1}{D_1} + \cdots + \frac{1}{D_N}$ *is an integer, then* $v_p(\mathcal{N}) = \left(\sum_{i=1}^{N} \frac{1}{D_i}\right) - 1$ *and* $F(\mathbf{X}) = 0$ *is solvable.*

Corollary 4.6. Let $F(\mathbf{X}) = a_1(X_{11} \cdots X_{1n_1})^{d_1} + \cdots + a_N(X_{N1} \cdots X_{Nn_N})^{d_N} + G(\mathbf{X}) \in \mathbb{F}_p^*[\mathbf{X}]$ have monomials of disjoint support and $\deg G < \min_i\{\gcd(d_i, p-1)\}$. If $\frac{1}{\gcd(d_1,p-1)} + \cdots + \frac{1}{\gcd(d_N,p-1)}$ is an integer, then $v_p(\mathcal{N}) = \left(\sum_{i-1}^{N} \frac{1}{\gcd(d_i,p-1)}\right) - 1$ and $F(\mathbf{X}) = 0$ is solvable.

In [3, Theorem 2], Cao-Sun proved that the number of solutions of a general diagonal equation of the form $a_1 X_{11}^{d_{11}} \cdots X_{1n_1}^{d_{1n_1}} + \cdots + a_N X_{N1}^{d_{N1}} \cdots X_{Nn_N}^{d_{Nn_N}} + G(y_1, \ldots, y_m) = 0$ is equal to the number of solutions of $a_1(X_{11} \cdots X_{1n_1})^{D_1} + \cdots + a_N(X_{N1} \cdots X_{Nn_N})^{D_N} + G(y_1, \ldots, y_m) = 0$, where the polynomials are over $\mathbb{F}_q$, the terms have disjoint support, $y_k \neq X_{ij}$ and $D_i = \gcd(d_{i1}, d_{i2}, \ldots, d_{in_i}, p-1)$. With this theorem they improved Chevalley-Warning's theorem for this class of polynomials [3, Theorem 3]. The next result gives the exact p-divisibility of the number of solutions of a more general polynomial, where the polynomial G can have the same variables as the diagonal part of F, but the polynomial is defined over $\mathbb{F}_p$, and we have the additional condition that D_i is equal to one of the exponents d_{ij} in the term $a_i X_{i1}^{d_{i1}} \cdots X_{in_i}^{d_{in_i}}$.

Corollary 4.7. If $\frac{1}{D_1} + \cdots + \frac{1}{D_N}$ is an integer, then the exact p-divisibility of the number of solutions of $a_1 X_{11}^{d_{11}} \cdots X_{1n_1}^{d_{1n_1}} + \cdots + a_N X_{N1}^{d_{N1}} \cdots X_{Nn_N}^{d_{Nn_N}} + G(\mathbf{X}) = 0$ is equal to the exact p-divisibility of the number of solutions of $a_1(X_{11} \cdots X_{1n_1})^{D_1} + \cdots + a_N(X_{N1} \cdots X_{Nn_N})^{D_N} + G = 0$, where the monomials have disjoint support, $D_i = \gcd(d_{i1}, d_{i2}, \ldots, d_{in_i}, p-1) = d_{ij}$ for some $1 \leq j \leq n_i$ and $\deg G < \min\{D_1, \ldots, D_N\}$.

4.1. **Extension to systems of polynomial equations.** As we mentioned above, we can use Lemma 4.1 together with the results in Section 3 to construct families of systems of polynomial equations that are solvable. One needs to guarantee that the polynomials $G_1(\mathbf{X}), G_2(\mathbf{X}), \ldots, G_t(\mathbf{X})$ are such that the polynomial $F(\mathbf{X}) = G_1 + \cdots + G_t$ has a unique minimal $(p-1)$-covering $\mathcal{C} = \left\{G_{11}^{\nu_{11}}, \ldots, G_{1N_1}^{\nu_{1N_1}}, \ldots, G_{tN_t}^{\nu_{tN_t}}\right\}$, where $\sum_{j=1}^{N_j} \frac{\nu_{ij}}{p-1}$ is an integer for each $i = 1, \ldots, t$, and that the covering satisfies one of the conditions in the results above (terms with disjoint support, contributing two new variables, etc.). In this situation, the exact p-divisibility of $\mathcal{N}$ is $v_p(\mathcal{N}) = \left(\sum_{i=1}^{t} \sum_{j=1}^{N_j} \frac{\nu_{ij}}{p-1}\right) - t$.

Example 4.8. Consider

$$\begin{aligned}(X_1X_2X_3X_4)^2 + (X_1X_5X_6)^2 &= \alpha\\ X_3X_7X_8 + X_1X_9X_{10} &= \beta\end{aligned}$$

over $\mathbb{F}_5$. The polynomial associated to this system has the form of the polynomial in Theorem 4.3. It is easy to see that

$$\mathcal{C} = \left\{\left[(X_1X_2X_3X_4)^2\right]^2, \left[(X_1X_5X_6)^2\right]^2, \left[X_3X_7X_8\right]^4, \left[X_1X_9X_{10}\right]^4\right\}$$

is the unique minimal covering of $F = (X_1X_2X_3X_4)^2 + (X_1X_5X_6)^2 + X_3X_7X_8 + X_1X_9X_{10}$, where $\nu_{11} = \nu_{12} = 2 = \frac{p-1}{\gcd(2,p-1)}, \nu_{21} = \nu_{22} = 4 = \frac{p-1}{\gcd(1,p-1)}$ and $\frac{\nu_{11}+\nu_{12}}{p-1}, \frac{\nu_{21}+\nu_{22}}{p-1}$ are integers. Therefore, $v_5(\mathcal{N}) = \frac{1}{2}+\frac{1}{2}+\frac{1}{1}+\frac{1}{1}-2 = 1$ and 5 divides the number of solutions of the system for any $\alpha, \beta \in \mathbb{F}_5$. One can verify that, for $(\alpha, \beta) = (4, 1)$, $\mathcal{N} = 2^7 \times 5 \times 557$, and for $(\alpha, \beta) = (0, 0)$, $\mathcal{N} = 109,367 \times 3 \times 5$.

Example 4.9. Consider

$$X_1^2X_2^4 + X_3^6X_4^2 + X_1 + X_2 + X_6 + X_7 = \alpha$$
$$X_5^2X_6^2 + X_7^6X_8^2 + X_3 + X_5 + X_8 = \beta$$

over $\mathbb{F}_p$. The polynomial associated to this system has the form of the polynomial in Theorem 4.5. Note that for p odd, $\deg(X_1+X_2+X_6+X_7) < 2 = \min\{\gcd(2,4,p-1), \gcd(6,2,p-1)\}$ and $\deg(X_3+X_5+X_8) < 2 = \min\{\gcd(2,2,p-1), \gcd(6,2,p-1)\}$. It is easy to see that the unique minimal covering for the system is

$$\mathcal{C} = \left\{ \left[X_1^2X_2^4\right]^{\frac{p-1}{2}}, \left[X_3^6X_4^2\right]^{\frac{p-1}{2}}, \left[X_5^2X_6^4\right]^{\frac{p-1}{2}}, \left[X_7^6X_8^2\right]^{\frac{p-1}{2}} \right\}$$

and $v_p(\mathcal{N}) = \left(\frac{p-1}{2}\right) 4/(p-1) - 2 = 0$. Hence the number of solutions of the system is not divisible by p and the system is solvable for any $\alpha, \beta \in \mathbb{F}_p$.

Acknowledgements

The authors appreciate the careful review, comments and corrections made by the referee and H.F. Mattson Jr. which helped to correct and improve the paper.

References

[1] Alan Adolphson and Steven Sperber. p-adic estimates for exponential sums and the theorem of Chevalley-Warning. *Ann. Sci. École Norm. Sup. (4)*, 20(4):545–556, 1987.

[2] James Ax. Zeroes of polynomials over finite fields. *Amer. J. Math.*, 86:255–261, 1964.

[3] Wei Cao and Qi Sun. Improvements upon the Chevalley-Warning-Ax-Katz-type estimates. *J. Number Theory*, 122(1):135–141, 2007.

[4] F. Castro and F. N. Castro-Velez. Improvement to Moreno-Moreno's theorems. *Finite Fields Appl.*, 18(6):1207–1216, 2012.

[5] Francis N. Castro, Luis A. Medina, and Ivelisse M. Rubio. Exact divisibility of exponential sums over the binary field via the covering method. In *Groups, algebras and applications*, volume 537 of *Contemp. Math.*, pages 129–136. Amer. Math. Soc., Providence, RI, 2011.

[6] Francis N. Castro, Hugues Randriam, Ivelisse Rubio, and H. F. Mattson, Jr. Divisibility of exponential sums via elementary methods. *J. Number Theory*, 130(7):1520–1536, 2010.

[7] Francis N. Castro, Ivelisse Rubio, and José M. Vega. Divisibility of exponential sums and solvability of certain equations over finite fields. *Q. J. Math.*, 60(2):169–181, 2009.

[8] Nicholas M. Katz. On a theorem of Ax. *Amer. J. Math.*, 93:485–499, 1971.

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

[10] Oscar Moreno, Francis N. Castro, and H. F. Mattson, Jr. Correction to: "Divisibility properties for covering radius of certain cyclic codes" [IEEE Trans. Inform. Theory **49** (2003), no. 12, 3299–3303; mr2045808] by Moreno and Castro. *IEEE Trans. Inform. Theory*, 52(4):1798–1799, 2006.

[11] Oscar Moreno and Carlos J. Moreno. The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes. *IEEE Trans. Inform. Theory*, 40(6):1894–1907, 1994.

[12] Oscar Moreno, Kenneth W. Shum, Francis N. Castro, and P. Vijay Kumar. Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications. *Proc. London Math. Soc. (3)*, 88(3):545–564, 2004.

(Francis Castro) Department of Mathematics, University of Puerto Rico, Río Piedras, PO Box 70377, San Juan, Puerto Rico 00936
E-mail address: franciscastr@gmail.com

(Ivelisse Rubio) Department of Computer Science, University of Puerto Rico, Río Piedras, PO Box 70377, San Juan, Puerto Rico 00936
E-mail address: iverubio@gmail.com