Revista [IN]Genios, Vol. 1, Núm. 2, 1-8 (febrero, 2015).
ISSN#: 2324-2747
Universidad de Puerto Rico, Río Piedras

SOLVABILITY OF SYSTEMS OF POLYNOMIAL EQUATIONS OVER FINITE FIELDS

Ramón L. Collazo
Julio J. de la Cruz
Daniel E. Ramírez
Department of Computer Science
College of Natural Sciences

Abstract:
An important problem in mathematics is to determine if a system of polynomial equations has or not solutions over a given set. We study systems of polynomial equations over finite fields $\mathbb{F}_p$, p prime, and look for sufficient conditions that guarantee their solvability over the field. Using the covering method of (Castro & Rubio, n.d.) we get conditions on the degrees of the terms that allow us to construct families of systems that have exact p-divisibility of the number of solutions and therefore guarantee the solvability of the system over the finite field.

Keywords: mathematics, polynomial equations, finite fields, solvability

Resumen:
Un problema importante en las matemáticas es el determinar si un sistema de ecuaciones polinomiales tiene o no soluciones sobre un conjunto dado. Estudiamos sistemas de ecuaciones polinomiales sobre campos finitos $\mathbb{F}_p$, donde p es primo, y buscamos condiciones suficientes para garantizar que el sistema tenga solución sobre el campo. Usando el método de la cubierta de (Castro & Rubio, n.d.) obtenemos condiciones en los grados de los términos de modo que podamos construir familias de sistemas que tengan divisibilidad exacta p del número de soluciones, y por consiguiente garantizar que el sistema tenga solución sobre el campo finito.

Palabras claves: matemáticas, ecuaciones polinomiales, campos finitos, resolución

1 Introduction

The computation of the p-divisibility of an exponential sum is a mathematical tool used for different purposes. In our research, the p-divisibility is used to determine if a system of polynomial equations

$$\begin{aligned} a_{11}\left(X_1^{b_{111}}\cdots X_n^{b_{11n}}\right)^{d_{11}}+\cdots+a_{1r_1}\left(X_1^{b_{1r_11}}\cdots X_n^{b_{1r_1n}}\right)^{d_{1r_1}} &= \alpha_1 \\ \vdots \qquad\qquad\qquad\qquad & \vdots \\ a_{t1}\left(X_1^{b_{t11}}\cdots X_n^{b_{t1n}}\right)^{d_{t1}}+\cdots+a_{tr_t}\left(X_1^{b_{tr_t1}}\cdots X_n^{b_{tr_tn}}\right)^{d_{tr_t}} &= \alpha_t, \end{aligned}$$

where $b_{ijk}\in\{0,1\}$, has solutions or not over a finite field.

The exact p-divisibility of exponential sums was used in (Castro & Rubio, 2010) to determine the solvability of certain systems of polynomial equations. The results in that paper were obtained by solving systems of polynomial congruences. The covering method was used in (Castro & Rubio, n.d.) to prove that if a system of polynomial equations has a certain $(p-1)$-covering the system is solvable. We present sufficient conditions on the degrees of the terms of a system of polynomial equations that guarantee that it produces the type of $(p-1)$-covering in (Castro & Rubio, n.d.) and assure that the system is solvable.

2 Preliminaries

First, we introduce some concepts that will be used in our work. The handbook (Panario & Mullen, 2013) is a complete reference book for all the background and recent results in finite fields.

Definition 1. *A **finite field** $\mathbb{F}_q$ is a field with $q=p^f$ elements, where p is a prime.*

Example 1.

$$\mathbb{F}_7=\mathbb{Z}_7=\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\},$$

with addition and multiplication mod 7 is a field.

Example 2.

$$\mathbb{Z}_6=\{0,\ 1,\ 2,\ 3,\ 4,\ 5\},$$

with addition and multiplication mod 6 is not a field because 3 does not have a multiplicative inverse.

In this work we only deal with prime fields, this is, $q=p$.

Definition 2. *A **system of polynomial equations** over $\mathbb{F}_p$ is a set of equations $F_1=0,...,F_n=0$, where F_i are polynomials in n variables $X_1,\ldots,X_n$ and coefficients in $\mathbb{F}_p$.*

We assume that every system of polynomial equations contains all the variables $X_1,\cdots,X_n$, and denote the set of all polynomials in $X_1,\cdots,X_n$ and coefficients in $\mathbb{F}_p$ by $\mathbb{F}_p[\mathbf{X}]$.

2.1 Exponential Sums and Solvability

Definition 3. *The **exponential sum** over $\mathbb{F}_p$ associated with the polynomial $F(\mathbf{X})$ is given by*

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

where ζ is a p-th root of unity.

This number is hard to compute but we are not interested in the exact number, we just look for the greatest power of p that divides the sum.

Definition 4. *The **exact p-divisibility** of a positive integer k, denoted as $\nu_p(k)$, is the exponent of the highest power of p dividing k.*

Example 3.

$$\nu_p(40) = \nu_p(2^3 \cdot 5).$$

Hence,

$$\nu_2(40) = 3,\ \nu_5(40) = 1,\ \textit{and}\ \nu_p(40) = 0\ \textit{for}\ p \neq 2,5.$$

Note that, if $k = 0$, there is no highest power of p that divides k. This is, the exact p-divisibility of 0 is not defined.

To determine if a system is solvable, we need to know if the exponential sum of the system of polynomials has exact p-divisibility. The exponential sum is defined for a single polynomial; we construct a new polynomial from the system of polynomials. This new polynomial is obtained by multiplying a new variable to each polynomial in the system and adding the products. The exponential sum of this new polynomial gives the number of common zeros of the system.

Lemma 1 (Ax (1964))**.** *Let $F_1(\mathbf{X}), \ldots, F_t(\mathbf{X}) \in \mathbb{F}_p[\mathbf{X}]$ and N be the number of common zeros of $F_1, \ldots, F_t$. Then,*

$$N = p^{-t} \cdot S(Y_1 F_1(\mathbf{X}) + \cdots + Y_t F_t(\mathbf{X})).$$

The exact value of this number N is hard to compute because it depends on the exact value of the exponential sum. But we are interested on whether or not the system has solutions and it is enough to know if $N = 0$ or $N \neq 0$.

Note that if $\nu_p(N) = a$, this implies that $p^a | N$ and $p^{a+1} \nmid N$, therefore $N \neq 0$, because 0 is divisible by every number that is not 0. This is, if the exponential sum associated with a system of polynomial equations has exact p-divisibility, we guarantee that the system is solvable.

To determine systems which have exact p-divisibility we use the covering method as it was presented in (Castro & Rubio, n.d.).

2.2 The Covering Method

We now define the $(p-1)$-covering of a polynomial F, which encodes how many monomials of F (including repetitions) are needed to have each variable “represented" a multiple of $p-1$ times.

Definition 5. *Let $F(\mathbf{X}) = a_1F_1 + a_2F_2 + \cdots + a_rF_r$. A set $C = \{F_1{}^{v_1}, \ldots, F_r{}^{v_r}\}$ of powers of the monomials in F is a $(p-1)$-**covering** of F if in the product $F_1{}^{v_1} \cdots F_r{}^{v_r}$ the exponent of each variable is a positive multiple of $p-1$. Note that some of the v_i might be 0. The **size** of the $(p-1)$-covering is $\sum_{i=1}^{r} v_i$.*

Definition 6. *A set $C = \{F_1^{v_1}, \ldots, F_r^{v_r}\}$ is a **minimal** $(p-1)$-**covering** of F if for any other $(p-1)$-covering $C' = \{F_1^{v_1'}, \ldots, F_r^{v_r'}\}$ of F, $\sum_{i=1}^{r} v_i' \geq \sum_{i=1}^{r} v_i$.*

Example 4. *Consider*

$$F(\mathbf{X}) = X_1X_2 + X_3X_4 + X_1X_2X_3X_4 \in \mathbb{F}_2[\mathbf{X}].$$

Then $C_1 = \{(X_1X_2), (X_3X_4)\}$ is a 1-covering of F of size 2 and the minimal 1-covering of F is $C_2 = \{(X_1X_2X_3X_4)\}$ and it has size 1.

If $F(\mathbf{X}) \in \mathbb{F}_5[\mathbf{X}]$, then $C_1 = \{(X_1X_2)^4, (X_3X_4)^4\}$ is a 4-covering of F of size 8, and $C_2 = \{(X_1X_2X_3X_4)^4\}$ is the minimal 4-covering of F of size 4.

The covering method for computing exact 2-divisibility of exponential sums of binary polynomials was introduced in (Castro, Medina, & Rubio, 2011). In (Castro & Rubio, n.d.) the authors presented the following sufficient conditions to obtain polynomials such that their exponential sum has exact p-divisibility.

Theorem 1 ((Castro & Rubio, n.d.), Theorem 3.7)**.** *Suppose that $F = a_1F_1 + \cdots + a_rF_r$ has a unique minimal $(p-1)$-covering $C = \{F_1^{v_1}, \ldots, F_r^{v_r}\}$ where each monomial in C with $v_i \neq 0$ has at least two variables that are not contained in the other monomials of C. Then $\nu_p(S(F)) = \sum_{i=1}^{r} \frac{v_i}{p-1}$.*

3 Conditions for Solvability

The results in (Castro & Rubio, n.d.) gave sufficient conditions to guarantee that the exponential sum of the polynomials has exact p-divisibility. However, these conditions are on the type of $(p-1)$-coverings that the polynomials must have and it might be hard to know if these conditions are satisfied by just looking at the polynomials. Also, for the exact p-divisibility of the number of solutions we have to consider the new variables Y_i as in Lemma 1. Here we present a result similar to Theorem 1 but with conditions in the degrees of the polynomials. We also present a similar theorem for the computation of the exact p-divisibility of the number of solutions of the system of polynomials.

To use Theorem 1 we need the polynomial F to have a unique minimal $(p-1)$-covering. We now prove conditions so that polynomials of the form $F = a_1\left(X_1^{b_{11}} \cdots X_n^{b_{1n}}\right)^{d_1} + \cdots + a_r\left(X_1^{b_{r1}} \cdots X_n^{b_{rn}}\right)^{d_r}$, where $b_{jk} \in \{0,1\}$, have this type of $(p-1)$-covering. Corollary 3.8 in (Castro & Rubio, n.d.) has a similar result but the proof was not provided.

Lemma 2. *If the polynomial $F = a_1\left(X_1^{b_{11}} \cdots X_n^{b_{1n}}\right)^{d_1} + \cdots + a_r\left(X_1^{b_{r1}} \cdots X_n^{b_{rn}}\right)^{d_r}$ $= a_1F_1 + \cdots + a_rF_r \in \mathbb{F}_p[\mathbf{X}]$, where $b_{jk} \in \{0,1\}$, is such that each F_j has at least one variable that is not contained in the other monomials of F, then $C = \{F_1{}^{\frac{p-1}{gcd(p-1,d_1)}}, \ldots, F_r{}^{\frac{p-1}{gcd(p-1,d_r)}}\}$ is the unique minimal $(p-1)$-covering of F.*

Proof. First, in order to prove that C covers all the variables, we have to show that the exponent of each variable in the product $F_1^{\frac{p-1}{gcd(p-1,d_1)}} \cdots F_r^{\frac{p-1}{gcd(p-1,d_r)}}$ is a positive multiple of $(p-1)$. The exponent of X_k has the form $\beta = d_1 \cdot v_1 \cdot b_{1k} + \cdots + d_r \cdot v_r \cdot b_{rk}$, where $v_j = \frac{p-1}{gcd(p-1,d_j)}$. Note that $b_{jk} = 0$ when X_k is not in the monomial F_j and $b_{jk} = 1$ when it is. This is,

$$\begin{aligned}\beta &= d_1 \cdot \frac{p-1}{gcd(p-1,d_1)} \cdot b_{1k} + \cdots + d_r \cdot \frac{p-1}{gcd(p-1,d_r)} \cdot b_{rk} \\ &= lcm(p-1,d_1) \cdot b_{1k} + \cdots + lcm(p-1,d_r) \cdot b_{rk} \\ &= (p-1)l_1 \cdot b_{1k} + \cdots + (p-1)l_r b_{rk},\ l_i \in \mathbb{N} \\ &= (p-1)\left[l_1 \cdot b_{1k} + \cdots + l_r b_{rk}\right],\end{aligned}$$

where $l_i \neq 0$, and, since F contains all the variables, there exist at least one k such that $b_{jk} = 1$. Therefore, $l_1 b_{1k} + \cdots + l_r b_{rk} \in \mathbb{N}$, and the exponent of X_k is a positive multiple of $p-1$. The same reasoning can be used for each of the other variables.

Now, we want to prove that the covering is minimal and unique. Since each F_i has at least one variable that is not contained in F_j, for all $j \neq i$, we can take a variable X_k, that only appears in F_i. Then, in the product $F_1^{\frac{p-1}{gcd(p-1,d_1)}} \cdots F_r^{\frac{p-1}{gcd(p-1,d_r)}}$, X_k has exponent $d_i \cdot \frac{p-1}{gcd(p-1,d_i)} = lcm(p-1,d_i)$ and therefore the exponent of X_k is the smallest multiple of $p-1$ and d_i. This implies that the monomial F_i cannot have a smallest exponent in any other $(p-1)$-covering. The same argument works for all the other monomials in F and the $(p-1)$-covering is minimal and unique with this property. □

Example 5. *Consider the polynomial* $F = 7X_1^4 + 4X_2^5 + 3X_3^9 \in \mathbb{F}_{13}[\mathbf{X}]$. *A* 12*-covering of* F *is*

$$C = \left\{ \left(X_1^4\right)^6, \left(X_2^5\right)^{24}, \left(X_3^9\right)^8 \right\} = \left\{X_1^{24}, X_2^{120}, X_3^{72}\right\},$$

and has size 38*, but the minimal* 12*-covering of* F *is*

$$\begin{aligned}C &= \left\{ \left(X_1^4\right)^{\frac{12}{gcd(12,4)}}, \left(X_2^5\right)^{\frac{12}{gcd(12,5)}}, \left(X_3^9\right)^{\frac{12}{gcd(12,9)}} \right\} \\ &= \left\{ \left(X_1^4\right)^3, \left(X_2^5\right)^{12}, \left(X_3^9\right)^4 \right\} = \left\{X_1^{12}, X_2^{60}, X_3^{36}\right\},\end{aligned}$$

and has size 18.

We now present sufficient conditions on the exponents $d_1, \ldots, d_r$ of the terms in the polynomial F that guarantee that the equation $F = \alpha$ is solvable for any $\alpha \in \mathbb{F}_p$.

Theorem 2. *Suppose that* $F = a_1 \left(X_1^{b_{11}} \cdots X_n^{b_{1n}}\right)^{d_1} + \cdots + a_r \left(X_1^{b_{r1}} \cdots X_n^{b_{rn}}\right)^{d_r}$ $= a_1 F_1 + \cdots + a_r F_r \in \mathbb{F}_p[\mathbf{X}]$*, where* $b_{jk} \in \{0,1\}$*, is such that each monomial* F_i *has at least two variables that are not contained in the other monomials of* F*. If* $gcd(d_i, p-1) = k$ *and* $k|r$*, then* $F(\mathbf{X}) = \alpha$ *is solvable for any* $\alpha \in \mathbb{F}_p$*.*

Proof. By Lemma 1, the number of zeros of $F-\alpha$ is $N = p^{-1}\cdot S(Y(F-\alpha))$, where $S(Y(F-\alpha))$ is the exponential sum of $Y(F-\alpha)$. By Lemma 2, $C = \{F_1^{\frac{p-1}{gcd(p-1,d_1)}},\ldots,F_r^{\frac{p-1}{gcd(p-1,d_r)}}\}$ is the unique minimal $(p-1)$-covering of F. Consider $C' = \{(YF_1)^{\frac{p-1}{gcd(p-1,d_1)}},\ldots,(YF_r)^{\frac{p-1}{gcd(p-1,d_r)}}\}$. Since $gcd(p-1,d_i) = k$ and $k|r$, the variable Y in $(YF_1)^{\frac{p-1}{gcd(p-1,d_1)}}\cdots(YF_r)^{\frac{p-1}{gcd(p-1,d_r)}}$ has exponent $\sum_{i=1}^{r}\frac{p-1}{gcd(p-1,d_i)} = \sum_{i=1}^{r}\frac{p-1}{k} = r(\frac{p-1}{k}) = c(p-1)$, where $c\in\mathbb{N}$, because $k|r$. This implies that Y is $(p-1)$-covered in C'. By the same arguments in the proof of Lemma 2, C' is the unique minimal $(p-1)$-covering of F.

Theorem 1 implies that

$$\nu_p(S(Y(F-\alpha))) = \sum_{i=1}^{r}\frac{v_i}{(p-1)} = \sum_{i=1}^{r}\frac{(p-1)}{gcd(p-1,d_i)}\cdot\frac{1}{(p-1)} = \sum_{i=1}^{r}\frac{1}{k} = r\cdot\frac{1}{k} = c.$$

Now we have that

$$\nu_p(N) = \nu_p\left(p^{-1}S(Y(F-\alpha))\right) = \nu_p\left(p^{-1}\right) + \nu_p\left(S\left(Y\left(F-\alpha\right)\right)\right) = -1+c,$$

$c\in\mathbb{N}$. Since $\nu_p\left(S\left(N\right)\right) = c-1$, we have that $p^c \nmid N$ and therefore $N\neq 0$.

□

Example 6. *Consider the polynomial* $F = (X_1X_2)^8 + (X_3X_4)^{10}\in\mathbb{F}_{19}[\mathbf{X}]$. *The number of zeros of* $F-\alpha$, $\alpha\in F_{19}$ *is* $N = p^{-1}\cdot S\left(Y\left(F-\alpha\right)\right)$. *By Lemma 2, the unique minimal* 18*-covering of* $Y(F-\alpha)$ *is*

$$\begin{aligned} C &= \left\{\left(Y\left(X_1X_2\right)^8\right)^{\frac{18}{gcd(18,8)}},\left(Y\left(X_3X_4\right)^{10}\right)^{\frac{18}{gcd(18,10)}}\right\} \\ &= \left\{\left(Y\left(X_1X_2\right)^8\right)^{9},\left(Y\left(X_3X_4\right)^{10}\right)^{9}\right\} = \left\{Y^9\left(X_1X_2\right)^{72},Y^9\left(X_3X_4\right)^{90}\right\}. \end{aligned}$$

Using Theorem 1,

$$\nu_p\left(S\left(Y(F-\alpha)\right)\right) = \sum_{i=1}^{2}\frac{v_i}{(p-1)} = \frac{18}{gcd(18,8)}\cdot\frac{1}{18} + \frac{18}{gcd(18,10)}\cdot\frac{1}{18} = 1.$$

By Lemma 1, this implies that $\nu_p(N) = 1-1 = 0$, *where N is the number of solutions of* $F-\alpha = 0$. *Therefore, the equation* $F=\alpha$ *is solvable for any* $\alpha\in F_{19}$.

We can extend this theorem to systems with several equations. To simplify the notation, we only state the result for 2 equations.

Theorem 3. *Consider a system of two polynomials equations over* $\mathbb{F}_p$

$$\begin{aligned} F_1 &= a_{11}\left(X_1^{b_{111}}\cdots X_n^{b_{11n}}\right)^{d_{11}} + \cdots + a_{1r_1}\left(X_1^{b_{1r_11}}\cdots X_n^{b_{1r_1n}}\right)^{d_{1r_1}} \\ F_2 &= a_{21}\left(X_1^{b_{211}}\cdots X_n^{b_{21n}}\right)^{d_{21}} + \cdots + a_{2r_2}\left(X_1^{b_{2r_21}}\cdots X_n^{b_{2r_2n}}\right)^{d_{2r_2}}, \end{aligned}$$

where $b_{jk} \in \{0,1\}$*, and* $F_1 = a_{11}F_{11} + \cdots + a_{1r_1}F_{1r_1}, F_2 = a_{21}F_{21} + \cdots + a_{2r_2}F_{2r_2}$ *are such that each monomial* F_{ji} *has at least two variables that are not contained in the other monomials of* $F_1 + F_2$*. If* $gcd(p-1, d_{1i}) = k_1$*, where* $k_1 | r_1$*, and* $gcd(p-1, d_{2i}) = k_2$*, where* $k_2 | r_2$*, then the system* $F_1 = \alpha_1, F_2 = \alpha_2$ *is solvable for any* $\alpha_1, \alpha_2 \in F_p$*.*

Proof. Let $F = Y_1(F_1 - \alpha_1) + Y_2(F_2 - \alpha_2)$. By Lemma 1, the number of common solutions of the system is

$$N = p^{-2} \cdot S(F),$$

where $S(F)$ is the exponential sum associated with the system. By Lemma 2, the unique minimal $(p-1)$-covering of $F_1 + F_2$ is $C = \left\{ F_{11}^{\frac{p-1}{gcd(p-1,d_{11})}}, \ldots, F_{1r_1}^{\frac{p-1}{gcd\left(p-1,d_{1r_1}\right)}}, (F_{21})^{\frac{p-1}{gcd(p-1,d_{21})}}, \ldots, (F_{2r_2})^{\frac{p-1}{gcd\left(p-1,d_{2r_2}\right)}} \right\}$. Consider $C' = \left\{ (Y_1F_{11})^{\frac{p-1}{gcd(p-1,d_{11})}}, \ldots, (Y_2F_{2r_2})^{\frac{p-1}{gcd\left(p-1,d_{2r_2}\right)}} \right\}$. Since $gcd\,(p-1, d_{1_i}) = k_1$ and $gcd\,(p-1, d_{2_i}) = k_2$, the exponents of Y_1 in $(Y_1F_{11})^{\frac{p-1}{gcd(p-1,d_{11})}} \cdots (Y_1F_{1r_1})^{\frac{p-1}{gcd\left(p-1,d_{1r_1}\right)}}$ and Y_2 in $(Y_2F_{21})^{\frac{p-1}{gcd(p-1,d_{21})}} \cdots (Y_2F_{2r2})^{\frac{p-1}{gcd\left(p-1,d_{2r_2}\right)}}$ are $\sum_{i=1}^{r_1} \frac{p-1}{gcd(p-1,d_{1i})} = \sum_{i=1}^{r_1} \frac{p-1}{k_1} = r_1\frac{p-1}{k_1} = (p-1)c_1$ and $\sum_{i=1}^{r_2} \frac{p-1}{gcd(p-1,d_{2i})} = \sum_{i=1}^{r_2} \frac{p-1}{k_2} = r_2\frac{p-1}{k_2} = (p-1)c_2$, respectively, where $c_1, c_2 \in \mathbb{N}$. Therefore Y_1 and Y_2 are $(p-1)$-covered in C'. By the same arguments in the proof of Lemma 2, C' is the unique minimal $(p-1)$-covering of F.

Theorem 1 implies that

$$\nu_p\left(S(F)\right) = \sum_{i=1}^{r_1} \frac{v_{1i}}{(p-1)} + \sum_{i=1}^{r_2} \frac{v_{2i}}{(p-1)}$$

$$= \sum_{i=1}^{r_1} \frac{(p-1)}{gcd(p-1,d_{1i})} \cdot \frac{1}{(p-1)} + \sum_{i=1}^{r_2} \frac{(p-1)}{gcd(p-1,d_{2i})} \cdot \frac{1}{(p-1)}$$

$$= \sum_{i=1}^{r_1} \frac{1}{k_1} + \sum_{i=1}^{r_2} \frac{1}{k_2} = r_1 \cdot \frac{1}{k_1} + r_2 \cdot \frac{1}{k_2} = c_1 + c_2.$$

Now we have that

$$\begin{aligned} \nu_p(N) &= \nu_p\left(p^{-2} \cdot S(F)\right) \\ &= \nu_p\left(p^{-2}\right) + \nu_p\left(S(F)\right) = -2 + c_1 + c_2, \end{aligned}$$

$c_1, c_2 \in \mathbb{N}$. Since $\nu_p(N) = c_1 + c_2 - 2$, we have that $p^{c_1+c_2-1} \nmid N$ and therefore $N \neq 0$.

□

Example 7. *Consider the polynomials* $F_1 = (X_1X_2)^3 + (X_3X_4X_5)^9 + (X_6X_7X_8)^{21}$ *and* $F_2 = (X_8X_9X_{10})^2 + (X_{11}X_{12})^{14}$ *over* $\mathbb{F}_{31}$*. The number of common zeros is* $N = p^{-2} \cdot S(Y_1F_1 + Y_2F_2)$*. The unique minimal* 30*-covering of* $F = Y_1F_1 + Y_2F_2$ *is*

$$C = \left\{ \left(Y_1 \left(X_1 X_2 \right)^3 \right)^{\frac{30}{gcd(30,3)}}, \left(Y_1 \left(X_3 X_4 X_5 \right)^9 \right)^{\frac{30}{gcd(30,9)}}, \left(Y_1 \left(X_6 X_7 X_8 \right)^{21} \right)^{\frac{30}{gcd(30,21)}}, \right.$$
$$\left. \left(Y_2 \left(X_8 X_9 X_{10} \right)^2 \right)^{\frac{30}{gcd(30,2)}}, \left(Y_2 \left(X_{11} X_{12} \right)^{14} \right)^{\frac{30}{gcd(30,14)}} \right\}$$
$$= \left\{ Y_1^{10} \left(X_1 X_2 \right)^{30}, Y_1^{10} \left(X_3 X_4 X_5 \right)^{90}, Y_1^{10} \left(X_6 X_7 X_8 \right)^{210}, Y_2^{15} \left(X_8 X_9 X_{10} \right)^{30}, \right.$$
$$\left. Y_2^{15} \left(X_{11} X_{12} \right)^{210} \right\}.$$

Using Theorem 1,

$$\nu_p \left(S(F) \right) = \sum_{i=1}^{3} \frac{v_{1i}}{(p-1)} + \sum_{i=1}^{2} \frac{v_{2i}}{(p-1)}$$
$$= \sum_{i=1}^{3} \frac{1}{gcd(30, d_{1i})} + \sum_{i=2}^{2} \frac{1}{gcd(30, d_{2i})} = \frac{1}{3} + \frac{1}{3} + \frac{1}{3} + \frac{1}{2} + \frac{1}{2} = 2.$$

This implies that $\nu_p(N) = 0$ *and* $F_1 = \alpha_1$, $F_2 = \alpha_2$ *is solvable.*

4 Acknowledgements

This research has been supported by a grant from the Center of Undergraduate Research in Mathematics (CURM) from Brigham Young University, NSF grant #DMS-1148695, and was conducted under the direction of Prof. Ivelisse Rubio, Department of Computer Science, and Prof. Francis Castro, Department of Mathematics, University of Puerto Rico, Rio Piedras.

References

Ax, J. (1964). Zeroes of polynomials over finite fields. *Amer. J. Math.*, *86*, 255–261.

Castro, F. N., Medina, L. A., & Rubio, I. M. (2011). Exact divisibility of exponential sums over the binary field via the covering method. In *Groups, algebras and applications* (Vol. 537, pp. 129–136). Amer. Math. Soc., Providence, RI. doi: 10.1090/conm/537/10570

Castro, F. N., & Rubio, I. (n.d.). Exact p-divisibility of exponential sums via the covering method. *accepted in Proc. Amer. Math. Soc.*.

Castro, F. N., & Rubio, I. M. (2010). Solvability of systems of polynomial equations with some prescribed monomials. In *Finite fields: theory and applications* (Vol. 518, pp. 73–81). Amer. Math. Soc., Providence, RI. doi: 10.1090/conm/518/10197

Castro, F. N., & Rubio, I. M. (2014). Construction of systems of polynomial equations with exact p-divisibility via the covering method. *Journal of Algebra and Its Applications*, *13*(06), 1450013, 15.

Panario, D., & Mullen, G. L. (2013). *Handbook of finite fields*. CRC Press.