Solvability of systems of polynomial equations over finite fields

Ivelisse Rubio Francis Castro

University of Puerto Rico
Río Piedras

July 9, 2009

Outline

1 Outline

Outline

1. Outline
2. General Problems

Outline

1. Outline
2. General Problems
3. Our Approach

Outline

1. Outline
2. General Problems
3. Our Approach
4. Known Results

Outline

1. Outline
2. General Problems
3. Our Approach
4. Known Results
5. New Results

Outline

1. Outline
2. General Problems
3. Our Approach
4. Known Results
5. New Results
6. Our Method

Outline

1. Outline
2. General Problems
3. Our Approach
4. Known Results
5. New Results
6. Our Method
7. Sketch of Some Proofs

Outline

1. Outline
2. General Problems
3. Our Approach
4. Known Results
5. New Results
6. Our Method
7. Sketch of Some Proofs
8. Conclusion

General Problems

1. Find conditions that guarantee the solvability of systems of polynomial equations (Chevalley)

General Problems

1. Find conditions that guarantee the solvability of systems of polynomial equations (Chevalley)
2. For systems of the form

$$\begin{aligned} a_1X_1^d + \cdots + a_nX_n^d + G_1(X_1, \cdots, X_n) &= 0 \\ b_1X_1^k + \cdots + b_nX_n^k + G_2(X_1, \cdots, X_n) &= 0, \end{aligned} \tag{1}$$

determine the minimum number of variables n such that these systems always have solutions.
(Waring)

Our Approach

Theorem

Let $F(\mathbf{X}) = \sum_{i=1}^{N} a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}}$, $a_i \neq 0$. *If* $S(F) = \sum_{x_1,\cdots,x_n \in \mathbf{F}_q} \phi(F(x_1,\cdots,x_n))$, *then* $v_p(S(F)) \geq \frac{L}{p-1}$, *where* $L = \min_{(j_1,\ldots,j_N)} \left\{ \sum_{i=1}^{N} \sigma_p(j_i) \mid 0 \leq j_i < q \right\}$, *and* $(j_1,\ldots,j_N)$ *is a solution to the system*

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

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

Using this Theorem in our systems we get $v_p(N) \geq 0$.

Our Approach

Compute the exact p-divisibility of exponential sums associated to the systems of polynomials by studying the minimal solutions to

$$\begin{cases} e_{11}j_1 + e_{12}j_2 + \ldots + e_{1N}j_N & \equiv 0 \bmod q-1 \\ \vdots & \vdots \\ e_{n1}j_1 + e_{n2}j_2 + \ldots + e_{nN}j_N & \equiv 0 \bmod q-1, \end{cases} \quad (3)$$

Our Approach: Classify all minimal solutions and count them.

Our Approach

Compute the exact p-divisibility of exponential sums associated to the systems of polynomials by studying the minimal solutions to

$$\begin{cases} e_{11}j_1 + e_{12}j_2 + \ldots + e_{1N}j_N & \equiv 0 \bmod q-1 \\ \vdots & \vdots \\ e_{n1}j_1 + e_{n2}j_2 + \ldots + e_{nN}j_N & \equiv 0 \bmod q-1, \end{cases} \tag{3}$$

Our Approach: Classify all minimal solutions and count them.

- Unique minimal solution (prove this)

Our Approach

Compute the exact p-divisibility of exponential sums associated to the systems of polynomials by studying the minimal solutions to

$$\begin{cases} e_{11}j_1 + e_{12}j_2 + \ldots + e_{1N}j_N & \equiv 0 \bmod q-1 \\ \vdots & \vdots \\ e_{n1}j_1 + e_{n2}j_2 + \ldots + e_{nN}j_N & \equiv 0 \bmod q-1, \end{cases} \tag{3}$$

Our Approach: Classify all minimal solutions and count them.

- Unique minimal solution (prove this)
- All solutions have the same form (prove it and count them)

Our Approach

Compute the exact p-divisibility of exponential sums associated to the systems of polynomials by studying the minimal solutions to

$$\begin{cases} e_{11}j_1 + e_{12}j_2 + \ldots + e_{1N}j_N & \equiv 0 \bmod q-1 \\ \vdots & \vdots \\ e_{n1}j_1 + e_{n2}j_2 + \ldots + e_{nN}j_N & \equiv 0 \bmod q-1, \end{cases} \tag{3}$$

Our Approach: Classify all minimal solutions and count them.

- Unique minimal solution (prove this)
- All solutions have the same form (prove it and count them)
- More than one form of minimal solutions (need more tools...)

Notation

- $q = p^f$

Notation

- $q = p^f$
- $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_l p^l$ where $0 \leq a_i < p$

Notation

- $q = p^f$
- $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_l p^l$ where $0 \leq a_i < p$
- $\sigma_p(n) = \sum_{i=0}^{l} a_i$.

Notation

- $q = p^f$
- $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_l p^l$ where $0 \leq a_i < p$
- $\sigma_p(n) = \sum_{i=0}^{l} a_i$.
- $w_p(X_1^{e_1} \cdots X_n^{e_n}) = \sigma_p(e_1) + \cdots + \sigma_p(e_n)$.

Notation

- $q = p^f$
- $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_l p^l$ where $0 \leq a_i < p$
- $\sigma_p(n) = \sum_{i=0}^{l} a_i$.
- $w_p(X_1^{e_1} \cdots X_n^{e_n}) = \sigma_p(e_1) + \cdots + \sigma_p(e_n)$.
- $F(X_1, \ldots, X_n) = \sum_i a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}}, \; a_i \neq 0$

Notation

- $q = p^f$
- $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_l p^l$ where $0 \leq a_i < p$
- $\sigma_p(n) = \sum_{i=0}^{l} a_i$.
- $w_p(X_1^{e_1} \cdots X_n^{e_n}) = \sigma_p(e_1) + \cdots + \sigma_p(e_n)$.
- $F(X_1, \ldots, X_n) = \sum_i a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}},\ \ a_i \neq 0$
- $w_p(F) = \max_i w_p(a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}})$.

Chevalley-Warning's Theorem

Theorem

Let $F(X_1, \ldots, X_n)$ be a polynomial of degree d over $\mathbb{F}_q$ with $n > d$. Then p divides the number of solutions of $F = 0$, and, in particular, if $F(0, \ldots, 0) = 0$, then F has a nontrivial solution over $\mathbb{F}_q$.

Carlitz's Theorem

Theorem

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

Felszeghy's Theorem

Theorem

$a_1X_1^d + \cdots + a_nX_n^d + G(X_1, \ldots, X_n) = 0$ *is solvable over* $\mathbb{F}_p$ *for* $n \geq \lfloor \frac{p-1}{\lceil \frac{p-1}{d} \rceil} \rfloor$ *where* $deg(G) < d$.

Previous Results

Theorem

Let $d_i|(p-1)$ and $a_i \in \mathbf{F}_q{}^*$. Suppose that $\sum_{i=1}^{t} \frac{1}{d_i}$ is an integer and consider

$$(X_{i_1} \cdots X_{i_{n_1}})^{d_1}, (X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2}, \ldots, (X_{i_{n_{t-1}+1}} \cdots X_{i_{n_t}})^{d_t} \qquad (4)$$

all with the same degree $d > 1$, disjoint support, and $1 \le i_j \le n = n_t$. If $G(X_1, \ldots, X_n) \in \mathbb{F}_q[\mathbf{X}]$ with $w_p(G) < d$, and

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

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

Previous Results

Theorem

Let $d_i|(p-1)$ and $a_i \in \mathbf{F}_q{}^*$. Suppose that $\sum_{i=1}^{t} \frac{1}{d_i}$ is an integer and consider

$$(X_{i_1} \cdots X_{i_{n_1}})^{d_1}, (X_{i_{n_1+1}} \cdots X_{i_{n_2}})^{d_2}, \ldots, (X_{i_{n_{t-1}+1}} \cdots X_{i_{n_t}})^{d_t} \qquad (4)$$

all with the same degree $d > 1$, disjoint support, and $1 \leq i_j \leq n = n_t$. If $G(X_1, \ldots, X_n) \in \mathbb{F}_q[\mathbf{X}]$ with $w_p(G) < d$, and

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

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

- One minimal solution.

Previous Results

Example

$F = X_1^7 + X_2^7 + \cdots + X_7^7 + \sum_{i<j} a_{i,j} X_i X_j + X_1^{29^i+1} + \cdots + X_7^{29^i+1} \in \mathbb{F}_{29^f}[X_1, \ldots, X_7]$.

Then $F = \beta$ has at least one solution for any $\beta \in \mathbb{F}_{29^f}$.

Previous Results

Example

$F = X_1^7 + X_2^7 + \cdots + X_7^7 + \sum_{i<j} a_{i,j} X_i X_j + X_1^{29^i+1} + \cdots + X_7^{29^i+1} \in \mathbb{F}_{29^f}[X_1, \ldots, X_7]$.

Then $F = \beta$ has at least one solution for any $\beta \in \mathbb{F}_{29^f}$.

- Result generalizes Carlitz's result.

New Result:

$$\sum_r a_{r1}(X_1, \ldots, X_n)^{d_{r,1}} + G_1(X_1, \ldots, X_n) = 0$$

$$\sum_r a_{r2}(X_1, \ldots, X_n)^{d_{r,2}} + G_2(X_1, \ldots, X_n) = 0$$

$$\vdots \qquad\qquad \vdots$$

$$\sum_r a_{rt}(X_1, \ldots, X_n)^{d_{r,t}} + G_t(X_1, \ldots, X_n) = 0.$$

New Result:

Example

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

$$\begin{aligned} X_1^3 + X_2^3 + X_3^3 + X_4^3 + X_5^3 + X_6^3 + G_1(X_1, \ldots, X_{10}) &= 0 \\ X_7^4 + X_8^4 + X_9^4 + X_{10}^4 + G_2(X_1, \ldots, X_{10}) &= 0, \end{aligned}$$

over $\mathbb{F}_{p^f}$, where $w_p(G_i) < 3$.

Then $v_p(N) = p^f$ and the system has solution.

New Result:

Example

Let $6 \mid (p-1)$ and consider

$$X_1^3 + X_2^3 + X_3^6 + X_4^6 + X_1^2 + \cdots + X_{11}^2 = \gamma_1$$
$$(X_5X_6)^2 + (X_7X_8)^2 + \sum_{i<j} X_iX_j = \gamma_2$$
$$X_9^3 + X_{10}^3 + X_{11}^3 + X_1 + \cdots + X_{11} = \gamma_3.$$

over $\mathbb{F}_{p^f}$. The system has solution for every $(\gamma_1, \gamma_2, \gamma_3) \in \mathbb{F}_{p^f}^2$.

New Result:

Theorem

Consider

$$\sum_r a_{r1}(X_1,\ldots,X_n)^{d_{r,1}} + G_1(X_1,\ldots,X_n) = 0$$
$$\sum_r a_{r2}(X_1,\ldots,X_n)^{d_{r,2}} + G_2(X_1,\ldots,X_n) = 0$$
$$\vdots \qquad\qquad \vdots$$
$$\sum_r a_{rt}(X_1,\ldots,X_n)^{d_{r,t}} + G_t(X_1,\ldots,X_n) = 0.$$

where

- *all* $a_{ri}(X_1,\ldots,X_n)^{d_{r,i}}$ *have disjoint support and deg* > 1
- $G_i \in \mathbb{F}_q[\mathbf{X}]$, $w_p(G_i) < \min_i\left\{deg\left(a_{ri}(X_1,\ldots,X_n)^{d_{r,i}}\right)\right\}$
- $d_{r,i}|(p-1)$

Then $v_p(N) = f\sum_{r,i}\frac{1}{d_{r,i}} - tf$, *and the system has solution whenever* $\sum_r \frac{1}{d_{r,i}}$ *is an integer for* $i = 1,\ldots,t$.

New Result:

Theorem

Let $a, b \in \mathbb{F}_p{}^*$, d, k *such that* $\gcd(d, k) = 1$, $dk = p - 1$, d *even and* $n \geq d + k \neq p$.

Let $G_1(X_1, \cdots, X_n)$, $G_2(X_1, \cdots, X_n) \in \mathbb{F}_p[\mathbf{X}]$ *with* $\deg\ G_1 < d, \deg\ G_2 < k$, *and consider*

$$\begin{aligned} aX_1^d + \cdots + aX_n^d + G_1(X_1, \cdots, X_n) &= 0 \\ \pm bX_1^k \pm \cdots \pm bX_n^k + G_2(X_1, \cdots, X_n) &= 0. \end{aligned} \tag{5}$$

Then, the system has solution in $\mathbb{F}_p^n$.

New Result:

Theorem

Let $a, b \in {\mathbb{F}_p}^*$, d, k such that $\gcd(d,k) = 1$, $dk = p - 1$, d even and $n \geq d + k \neq p$.

Let $G_1(X_1, \cdots, X_n)$, $G_2(X_1, \cdots, X_n) \in \mathbb{F}_p[\mathbf{X}]$ with $deg\ G_1 < d, deg\ G_2 < k$, and consider

$$\begin{aligned} aX_1^d + \cdots + aX_n^d + G_1(X_1, \cdots, X_n) = 0 \\ \pm bX_1^k \pm \cdots \pm bX_n^k + G_2(X_1, \cdots, X_n) = 0. \end{aligned} \tag{5}$$

Then, the system has solution in $\mathbb{F}_p^n$.

- Minimal solutions of the same form but not unique.

General Coefficients??

Example

Let $q = \mathbb{F}_7$, $deg\ G_1 < 3, deg\ G_2 < 2$, and consider

$$\begin{aligned} X_1^3 + 2X_2^3 + X_3^3 + X_4^3 + X_5^3 + G_1(X_1, \ldots, X_5) &= 0 \\ X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 + G_2(X_1, \ldots, X_5) &= 0. \end{aligned} \quad (6)$$

If all coefficients were equal, our method would give that $7 \not| N$ for any G_1, G_2. But $7|N$

General Coefficients??

Corollary

Let $p \equiv 3 \bmod 4, d = \frac{p-1}{2}, n = d+2, deg\ G_1 < d, deg\ G_2 < 2$ *and consider*

$$\begin{aligned} \pm aX_1^d \pm \cdots \pm aX_n^d + G_1(X_1, \ldots, X_n) = 0 \\ b_1X_1^2 + \cdots + b_nX_n^2 + G_2(X_1, \ldots, X_n) = 0 \end{aligned} \tag{7}$$

Let m *be the number of quadratic nonresidue* mod p *in* $(b_1, \ldots, b_n)$. *Then system is solvable if and only if* $m = 0, 1, \frac{p+1}{2}, n$, *or* $1 < m < \frac{p+1}{2}$ *and* $16m^2 - 24m + 3 \equiv 0 \mod p$. *Otherwise* p *divides* N.

New Result:

Corollary

Let $\beta \in \mathbb{F}_p$ and N be the number of solutions of the system

$$\begin{aligned} aX_1^{p-1} + \cdots + aX_p^{p-1} + G_1(X_1, \cdots, X_p) = 0 \\ \pm bX_1 \pm \cdots \pm bX_p + \beta = 0. \end{aligned} \tag{8}$$

Then, $p|N$.

New Result:

Corollary

Let $\beta \in \mathbb{F}_p$ and N be the number of solutions of the system

$$\begin{aligned} aX_1^{p-1} + \cdots + aX_p^{p-1} + G_1(X_1, \cdots, X_p) = 0 \\ \pm bX_1 \pm \cdots \pm bX_p + \beta = 0. \end{aligned} \tag{8}$$

Then, $p|N$.

- Note that $n = p = \sum d_i$ and this improves Chevalley-Warning's (and Katz's) theorem.

New Result:

Theorem

Let $a \in {\mathbb{F}_p}^*$, $p > 3$, and $d = \frac{p-1}{2}$. Suppose $\deg G < d$ and let N be the number of solutions of the system

$$\begin{aligned} aX_1^d + \cdots + aX_{d+1}^d + G(X_1, \cdots, X_{d+1}) = 0 \\ X_1 + \cdots + X_{d+1} + \beta = 0. \end{aligned} \tag{9}$$

Then $v_p(N) = 0$ and the system has solution in ${\mathbb{F}_p}^n$ for all $\beta \in \mathbb{F}_p$.

New Result:

Theorem

Let $a \in {\mathbb{F}_p}^*$, $p > 3$, and $d = \frac{p-1}{2}$. Suppose deg $G < d$ and let N be the number of solutions of the system

$$\begin{aligned} aX_1^d + \cdots + aX_{d+1}^d + G(X_1, \cdots, X_{d+1}) &= 0 \\ X_1 + \cdots + X_{d+1} + \beta &= 0. \end{aligned} \tag{9}$$

Then $v_p(N) = 0$ and the system has solution in ${\mathbb{F}_p}^n$ for all $\beta \in \mathbb{F}_p$.

- Note that $dk \neq p - 1$.

New Result:

Theorem

Let $a \in \mathbb{F}_p{}^*$, $p > 3$, and $d = \frac{p-1}{2}$. Suppose deg $G < d$ and let N be the number of solutions of the system

$$\begin{aligned} aX_1^d + \cdots + aX_{d+1}^d + G(X_1, \cdots, X_{d+1}) &= 0 \\ X_1 + \cdots + X_{d+1} + \beta &= 0. \end{aligned} \tag{9}$$

Then $v_p(N) = 0$ and the system has solution in $\mathbb{F}_p{}^n$ for all $\beta \in \mathbb{F}_p$.

- Note that $dk \neq p - 1$.
- Two different forms of solutions.

p-divisibility and Number of Solutions

Theorem

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

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

To determine solvability:

- **Exact p-divisibility:** If $v_p(N) = a$, then $N \neq 0$

Bound on p-divisibility:

Theorem

Let $F(\mathbf{X}) = \sum_{i=1}^{N} a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}}$, $a_i \neq 0$. *If* $S(F) = \sum_{x_1,\cdots,x_n \in \mathbf{F}_q} \phi(F(x_1,\cdots,x_n))$, *then* $v_p(S(F)) \geq \frac{L}{p-1}$, *where* $L = \min_{(j_1,\ldots,j_N)} \left\{ \sum_{i=1}^{N} \sigma_p(j_i) \mid 0 \leq j_i < q \right\}$, *and* $(j_1,\ldots,j_N)$ *is a solution to the system*

$$\begin{cases} e_{11}j_1 + e_{12}j_2 + \ldots + e_{1N}j_N & \equiv 0 \bmod q-1 \\ \vdots & \vdots \\ e_{n1}j_1 + e_{n2}j_2 + \ldots + e_{nN}j_N & \equiv 0 \bmod q-1, \end{cases} \tag{10}$$

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

Using this Theorem in our systems we get $v_p(N) \geq 0$.

Our approach

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

$$v_p(T) = v_p\left(\left[\prod_{i=1}^{N} c(j_i)\right] \left[\sum_{\mathbf{t}} \mathbf{t}^{j_1\mathbf{e}_1+\cdots+j_N\mathbf{e}_N}\right] \left[\prod_{i=1}^{N} a_i'^{j_i}\right]\right) \qquad (11)$$

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

Problem: There can be many $(j_1, \ldots, j_N)$ that produce solutions with minimal p-divisibility.
Our solution: To classify all minimal solutions and count them.

Goal:

To compute exact divisibility of the exponential sum by:

- Finding all minimal solutions
- Determining if they give similar terms in the sum
- Counting the number of similar terms in each group
- Computing the exact value of the terms

Case $\gcd(d,k)=1,\ dk=p-1$ and $n=d+k$:

Theorem

Let $a, b \in {\mathbb{F}_p}^*$, d, k *such that* $\gcd(d,k)=1,\ dk=p-1,\ d$ *even and* $n \geq d+k \neq p$.

Let $G_1(X_1,\cdots,X_n),\ G_2(X_1,\cdots,X_n) \in \mathbb{F}_p[\mathbf{X}]$ *with* $\deg\ G_1 < d, \deg\ G_2 < k$, *and consider*

$$\begin{aligned} aX_1^d + \cdots + aX_n^d + G_1(X_1,\cdots,X_n) &= 0 \\ \pm bX_1^k \pm \cdots \pm bX_n^k + G_2(X_1,\cdots,X_n) &= 0. \end{aligned} \tag{12}$$

Then, the system has solution in $\mathbb{F}_p^n$.

Case $\gcd(d,k)=1,\ dk=p-1$ and $n=d+k$:

$$X_1^d+\cdots+X_n^d=\alpha$$
$$X_1^k+\cdots+X_n^k=\beta.$$

Associated system of modular equations:

$$\begin{aligned}
dh_1+ks_1 &\equiv 0 \bmod p-1\\
\vdots \qquad & \qquad \vdots\\
dh_n+ks_n &\equiv 0 \bmod p-1\\
h_1+\cdots+h_n+h_{n+1} &\equiv 0 \bmod p-1\\
s_1+\cdots+s_n+s_{n+1} &\equiv 0 \bmod p-1.
\end{aligned}$$

$$(h_1,\cdots,h_n : s_1,\cdots,s_n : h_{n+1},s_{n+1})$$

Case $\gcd(d,k)=1$, $dk=p-1$ and $n=d+k$:

All solutions with minimal p-divisibility have the form:

$$\left(\overbrace{k,\cdots,k}^{d},\overbrace{0,\cdots,0}^{k}:\overbrace{0,\cdots,0}^{d},\overbrace{d,\cdots,d}^{k}:0,0\right)$$

They produce $\binom{n}{d}$ similar terms T with $v_p(T)=2$.

$$N=p^{-2}\binom{n}{d}p^2N', \quad p\not|N'.$$

If $n=d+k\neq p$, then $p\not|\binom{n}{d}$ and $v_p(N)=0$.

Case $d = \frac{p-1}{2}$:

$$\begin{aligned} aX_1^d + \cdots + aX_{d+1}^d + G(X_1, \cdots, X_{d+1}) &= 0 \\ X_1 + \cdots + X_{d+1} + \beta &= 0. \end{aligned} \tag{13}$$

Associated system of modular equations:

$$\begin{aligned} dh_1 + e_{11}t_1 + \cdots + e_{1N}t_N + s_1 &\equiv 0 \bmod p-1 \\ &\vdots \qquad\qquad \vdots \\ dh_{d+1} + e_{d+11}t_1 + \cdots + e_{d+1N}t_N + s_{d+1} &\equiv 0 \bmod p-1 \\ h_1 + \cdots + h_{d+1} + t_1 + \cdots + t_N &\equiv 0 \bmod p-1 \\ s_1 + \cdots + s_{d+1} + l &\equiv 0 \bmod p-1. \end{aligned} \tag{14}$$

$$(h_1, \cdots, h_{d+1} : s_1, \cdots, s_{d+1} : t_1, \cdots, t_N : l)$$

Case $d = \frac{p-1}{2}$:

Minimal solutions have two forms:

$$(0, 2, \cdots, 2 : p-1, 0, \cdots, 0 : 0, \cdots, 0 : 0)$$

$$(1, 1, 2, \cdots, 2 : d, d, 0, \cdots, 0 : 0, \cdots, 0 : 0)$$

They produce $d+1$ similar terms T_1 and $\binom{d+1}{2}$ similar terms T_2 with $v_p(T_i) = 2$.

Problems!!!!

Case $d = \frac{p-1}{2}$:

To prove that $v_p(N) = 0$, we need to compute the values of :

$$c(0)^{2d+3+N} c(2)^d c(p-1)(p-1)^{d+3}(a')^{2d}$$
$$= c(2)^d c(p-1)(p-1)^{d+3}(a')^{2d},$$

$$c(0)^{d-1+N} c(1)^2 c(2)^{d-1} c(d)^2 (p-1)^{d+3}(a')^{2d}$$
$$= c(1)^2 c(2)^{d-1} c(d)^2 (p-1)^{d+3}(a')^{2d}$$

and

$$v_\theta(F) = v_\theta\Big((d+1)c(2)^d c(p-1)(p-1)^{d+3}(a')^{2d}$$
$$+\binom{d+1}{2} c(1)^2 c(2)^{d-1} c(d)^2 (p-1)^{d+3}(a')^{2d}\Big).$$

Case $d = \frac{p-1}{2}$:

We prove that $v_p(N) = 0$ by proving that

$$\frac{(d+1)c(2)^d c(p-1)(p-1)^{d+3}}{\theta^{2(p-1)}} + \frac{\binom{d+1}{2} c(1)^2 c(2)^{d-1} c(d)^2 (p-1)^{d+3}}{\theta^{2(p-1)}} \not\equiv 0 \bmod \theta.$$

Case $d = \frac{p-1}{2}$:

Lemma

There is a unique polynomial $C(X) = \sum_{j=0}^{q-1} c(j)X^j \in K(\xi)[X]$ *of degree* $q-1$ *such that*

$$C(t) = \xi^{\mathrm{Tr}_{K/\mathbb{Q}_p}(t)}, \quad \text{for all } t \in \mathcal{T}.$$

Moreover, the coefficients of $C(X)$ *satisfy*

$$\begin{aligned} c(0) &= 1 \\ (q-1)c(q-1) &= -q \\ (q-1)c(j) &= g(j) \quad \text{for } 0 < j < q-1, \end{aligned}$$

where $g(j)$ *is the Gauss sum,*

$$g(j) = \sum_{t \in \mathcal{T}^*} t^{-j} \xi^{\mathrm{Tr}_{K/\mathbb{Q}_p}(t)}.$$

Case $d = \frac{p-1}{2}$:

Theorem (Stickelberger)

For $0 \leq j < q-1$,

$$\frac{g(j)\rho_p(j)}{\theta^{\sigma_p(j)}} \equiv -1 \mod \theta.$$

Conclusion

We computed exact divisibility of exponential sums to determine that very general families of systems of polynomial equations always have solutions over finite fields. The solvability of these type of systems could not be determined before by other methods. Our results extend and generalize well know theorems such as Chevalley's and Carlitz's theorems.