Journal of Pure and Applied Algebra 224 (2020) 106246

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

An improvement of a theorem of Carlitz

Francis N. Castro [a,1], Oscar Moreno [b,2], Ivelisse Rubio [c,*]

[a] *Department of Mathematics, University of Puerto Rico, Río Piedras, 17 Ave Universidad Ste 1701, S.J., PR 00925-2537, United States of America*
[b] *Gauss Research Foundation, PO Box 21613, S.J., PR 00931, United States of America*
[c] *Department of Computer Science, University of Puerto Rico, Río Piedras, 17 Ave Universidad Ste 1701, S.J., PR 00925-2537, United States of America*

ARTICLE INFO

Article history:
Received 10 May 2017
Received in revised form 18 March 2019
Available online 17 October 2019
Communicated by I.M. Duursma

MSC:
11T06

Keywords:
Solvability
Restriction of scalars
p-weight

ABSTRACT

We improve a result of Carlitz about the number of variables needed for a system of polynomial equations with coefficients in $\mathbb{F}_q[X]$ to have non-trivial solutions by considering the p-weight degree of the polynomials. By providing infinite families of polynomials we illustrate that our improvement is significant and, in general, is tight.

1. Introduction

In 1936 Chevalley [1] proved a conjecture of Artin about the existence of non-trivial zeros of a system of polynomials:

If $F_1, \ldots, F_t$ are polynomials in n variables, with coefficients in a finite field $\mathbb{F}_q$, which vanish at $(0, \ldots, 0)$ and $deg(F_1) + \cdots + deg(F_t) < n$, then $F_1, \ldots, F_t$ have a non-trivial zero in $(\mathbb{F}_q)^n$.

Several improvements to this result have been proved [2–7], including a theorem by Katz that gives a bound on the power of q dividing the number of common zeros of the polynomials, and a theorem by Moreno-Moreno in which the degree is replaced by the p-weight degree of the polynomials $F_1, \ldots, F_t$ to improve Katz' result in many cases.

* Corresponding author.
E-mail address: ivelisse.rubio@upr.edu (I. Rubio).
[1] Deceased June 26, 2018.
[2] Deceased July 14, 2015.

https://doi.org/10.1016/j.jpaa.2019.106246

In 1952 Carlitz [8] applied Chevalley's result to provide a sufficient condition on the number of variables $Y_1, \ldots, Y_n$ needed for a system of polynomials with coefficients in $\mathbb{F}_q[X]$ to have non-trivial solutions in $(\mathbb{F}_q[X])^n$. In this work we follow Carlitz's approach together with the methods of [7] to obtain a generalization of Moreno-Moreno's theorem to systems in which the coefficients are polynomials. As a consequence we obtain a significant improvement of Carlitz's result.

2. Preliminaries

Let $\mathbb{F}_q$ be the finite with $q = p^f$ elements, where p is a prime. In [8] Carlitz applied Chevalley's result to prove the following theorem:

Theorem 1 *(Carlitz). Let $F(Y_1, \ldots, Y_n)$ be a polynomial of degree k, coefficients in $\mathbb{F}_q[X]$, and such that $F(0, \ldots, 0) = 0$. Then $F = 0$ has non-trivial solutions in $(\mathbb{F}_q[X])^n$ for $n \geq k^2 + 1$. Moreover, there are equations of this form which have only the trivial solution for $n = k^2$.*

We improve Theorem 1 in Corollary 8, obtaining $n \geq \omega_p(F)k + 1$, where $\omega_p(F)$ is the p-weight degree of F. Since $\omega_p(F) \leq \deg(F)$ our result requires less variables than Carlitz's result to assure that $F = 0$ has non-trivial solutions. The infinite families provided in Example 3 illustrate that the improvement is significant. The proof uses the *method of restriction of scalars* and the *p-weight degree* of the polynomial. These were the methods used by Moreno-Moreno in [7] to give an improvement to the following theorem.

Theorem 2 *(Katz). Let $F_1, \ldots, F_t$ be polynomials in n variables, coefficients in a finite field $\mathbb{F}_q$, and*

$$\mu = \left\lceil \left(\frac{n - \sum_{i=1}^{t} \deg(F_i)}{max_{1 \leq i \leq t} \{\deg(F_i)\}} \right) \right\rceil. \tag{1}$$

Then, if $\mu \geq 0$, q^μ divides the number of common zeros of $F_1, \ldots, F_t$.

Katz's theorem improves Chevalley's result in [1] and a result by Ax [3]. The theorem can be improved by considering the p-weight degree $\omega_p(F_i)$ of the polynomials F_i instead of their degree. For $d \geq 0$, let $\sigma_p(d)$ denote the sum of the digits in the base p expansion of d. That is, if $d = a_0 + a_1 p + a_2 p^2 + \cdots + a_h p^h$, with $0 \leq a_i < p$, then $\sigma_p(d) = a_0 + a_1 + \cdots + a_h$ and $\sigma_p(d) \leq d$.

Definition 3. The p-weight degree of a monomial $\mathbf{Y}^{\mathbf{d}} = Y_1^{d_1} Y_2^{d_2} \cdots Y_n^{d_n}$ is $\omega_p\left(\mathbf{Y}^{\mathbf{d}}\right) = \sigma_p(d_1) + \cdots + \sigma_p(d_n)$. The **p-weight degree of a polynomial** $F(Y_1, \ldots, Y_n) = \sum_{\mathbf{d}} c_{\mathbf{d}} \mathbf{Y}^{\mathbf{d}}$, $c_{\mathbf{d}} \in {\mathbb{F}_q}^*$, is $\omega_p(F)$, the maximum of the $\omega_p\left(\mathbf{Y}^{\mathbf{d}}\right)$.

The divisibility in Theorem 2 depends on the degree of the polynomials. Note that $\omega_p(F) \leq \deg(F)$ and hence, changing $\deg(F_i)$ to $\omega_p(F_i)$ in (1), gives an improvement of Theorem 2 in many cases.

Theorem 4 *(Moreno-Moreno). Let $F_1, \ldots, F_t$ be polynomials in n variables, coefficients in a finite field $\mathbb{F}_q$, and*

$$\mu = \left\lceil f \left(\frac{n - \sum_{i=1}^{t} \omega_p(F_i)}{max_{1 \leq i \leq t} \{\omega_p(F_i)\}} \right) \right\rceil.$$

Then, if $\mu \geq 0$, p^μ divides the number of common zeros of $F_1, \ldots, F_t$.

Remark 5. Since $p^\mu | 0$, the number of common zeros of the system could be 0. However, if the system has the trivial zero, Theorems 2 and 4 guarantee the existence of non-trivial zeros.

2.1. Method of restriction of scalars

As it was mentioned before, we will use the method of restriction of scalars to refine Carlitz's result. The approach is the same as the one used in [9,7] but, to facilitate the understanding of this paper, we provide the details here.

The method of restriction of scalars essentially changes a polynomial in n variables, taking values in a field $\mathbb{F}_q$, $q = p^f$, to a sum of f polynomials G_j in fn variables, taking values in $\mathbb{F}_p$.

Consider a polynomial $F(Y_1, \ldots, Y_n)$ with coefficients in and taking values in $\mathbb{F}_q$. Since the polynomial is a sum of terms, one only needs to consider a generic term $cY_1^{d_1} \cdots Y_n^{d_n}$ of degree $d = d_1 + \cdots + d_n$. Let $\mu_1, \ldots, \mu_f$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. Then, each variable Y_i can be represented as $Y_i = \sum_{j=1}^{f} Z_j^{(i)} \mu_j$, and, using the base p expansion of each exponent $d_i = a_{i0} + a_{i1}p + \cdots + a_{ih}p^h$, one can write the term

$$\begin{aligned} cY_1^{d_1} \cdots Y_n^{d_n} &= c \left(\sum_{j=1}^{f} Z_j^{(1)} \mu_j \right)^{d_1} \cdots \left(\sum_{j=1}^{f} Z_j^{(n)} \mu_j \right)^{d_n} \cdots \\ &= c \left(\sum_{j=1}^{f} Z_j^{(1)} \mu_j \right)^{a_{10} + a_{11}p + \cdots + a_{1h}p^h} \\ &\quad \cdots \left(\sum_{j=1}^{f} Z_j^{(n)} \mu_j \right)^{a_{n0} + a_{n1}p + \cdots + a_{nh}p^h} \\ &= c \left(\sum_{j=1}^{f} Z_j^{(1)} \mu_j \right)^{a_{10}} \cdots \left(\sum_{j=1}^{f} Z_j^{(1)} \mu_j^{p^h} \right)^{a_{1h}} \cdots \\ &\quad \cdots \left(\sum_{j=1}^{f} Z_j^{(n)} \mu_j^{p^h} \right)^{a_{nh}}. \end{aligned}$$

The term $cY_1^{d_1} \cdots Y_n^{d_n}$ of degree $d = d_1 + \cdots + d_n$ is now a polynomial in the fn variables $Z_1^{(1)}, \ldots, Z_f^{(1)}$, $\ldots, Z_f^{(n)}$, taking values in $\mathbb{F}_p$, and its degree is $\omega_p\left(Y_1^{d_1} \cdots Y_n^{d_n}\right) = \sigma_p(d_1) + \cdots + \sigma_p(d_n)$.

Doing the same for each term of F, and adding the terms for each basis element, we get

$$F(Y_1, \ldots, Y_n) = \sum_{j=1}^{f} G_j\left(Z_1^{(1)}, \ldots, Z_f^{(n)}\right) \mu_j.$$

Since $\mu_1, \ldots, \mu_f$ forms a basis of $\mathbb{F}_q$, we have $F(Y_1, \ldots, Y_n) = 0$ if and only if $G_j\left(Z_1^{(1)}, \ldots, Z_f^{(n)}\right) = 0$ for each $j = 1, \ldots, f$. Hence, finding the zeros of a polynomial F in n variables, with coefficients in $\mathbb{F}_q$, and of degree d is the same as finding the common zeros of a system of f polynomials $G_1, \ldots, G_f$ in fn variables, with coefficients in $\mathbb{F}_p$, and of degree at most $\omega_p(F)$.

3. p-divisibility and non-trivial solutions

We now follow the approach in Carlitz's paper [8] and consider a single equation of degree k in n variables and coefficients in $\mathbb{F}_q[X]$,

$$F(Y_1, \ldots, Y_n) = \sum A_{i_k} \mathbf{Y}^{i_k} + \sum A_{i_{k-1}} \mathbf{Y}^{i_{k-1}} + \cdots + \sum A_{i_1} \mathbf{Y}^{i_1} = 0, \tag{2}$$

where $\mathbf{Y}^{i_l} = Y_1^{i_{l1}} \cdots Y_n^{i_{ln}}$, $\sum_{h=1}^{n} i_{lh} = l \leq k$ (each sum contains terms of the same degree l), and $A_{i_l} \in \mathbb{F}_q[X]$, $\deg A_{i_l} \leq a$. Note that $F \in \mathbb{F}_q[X]\,[Y_1, \ldots, Y_n]$ and we want solutions $(y_1, \ldots, y_n) \in (\mathbb{F}_q[X])^n$ for $F = 0$.

This is, we need polynomials $y_1, \ldots, y_n \in \mathbb{F}_q[X]$, of degree at most m for some fixed large enough m, such that $F(y_1, \ldots, y_n) = 0$. Let $y_j = a_{jm}X^m + \cdots + a_{j1}X + a_{j0}$. Then F is a polynomial with coefficients in $\mathbb{F}_q[X]$ and $n(m+1)$ variables $a_{10}, \ldots, a_{1m}, a_{n0}, \ldots, a_{nm}$. Using the method of restriction of scalars one represents each variable a_{ji} as a linear combination of the f basis elements of $\mathbb{F}_q$ over $\mathbb{F}_p$, to obtain F as a polynomial in $fn(m+1)$ variables, degree $\omega_p(F)$ and coefficients in $\mathbb{F}_p[X]$. Each of the coefficients is a polynomial in X of degree at most $a + m\deg(f)$ and we need these coefficients to be the zero polynomial. This gives a system of $a + m\deg(F) + 1$ equations in $fn(m+1)$ variables and degree at most $\omega(F)$. For each equation, adding up the terms of the basis, we get another system of f equations. In other words, Equation (2) in $\mathbb{F}_q[X][Y_1, \ldots, Y_n]$ is equivalent to a system of $f(a + m\deg(F) + 1)$ equations of degree at most $\omega(F)$, $fn(m+1)$ variables and coefficients in $\mathbb{F}_p[X]$.

One can check that, for $n \geq \omega_p(F)\deg(F) + 1$, if $m \geq \omega_p(F)\,(a + 1 - \deg(F))$, we get

$$n(m+1) > \omega_p(F)\,(a + \deg(F)m + 1)\,.$$

By Theorem 2, the number of solutions is divisible by p^μ, where

$$\mu = \left\lceil f\left(\frac{n(m+1) - \omega_p(F)\,(a + \deg(F)m + 1)}{\omega_p(F)}\right)\right\rceil.$$

3.1. Systems of polynomial equations

The generalization to a system of t equations $F_1 = 0, \ldots, F_t = 0$ is now easy. The equations $F_1 = 0, \ldots, F_t = 0$ are equivalent to a system consisting of t blocks of equations, one block for each F_i. The block corresponding to F_i has $f\,(a + \deg(F_i)m + 1)$ equations in $fn(m+1)$ variables and degree at most $\omega_p(F_i)$.

One can check that, for

$$n \geq \sum_{i=1}^{t} \omega_p(F_i)\deg(F_i) + 1, \quad \text{if} \quad m \geq \sum_{i=1}^{t} \omega_p(F_i)\,(a + 1 - \deg(F_i))\,, \quad \text{one gets}$$

$$n(m+1) > \sum_{i=1}^{t} \omega_p(F_i)\,(a + \deg(F_i)m + 1)\,.$$

Again, by Theorem 2, the number of solutions is divisible by p^μ, where

$$\mu = \left\lceil f\left(\frac{n(m+1) - \sum_{i=1}^{t} \omega_p(F_i)\,(a + \deg(F_i)m + 1)}{max_{1\leq i\leq t}\,\{\omega_p\,(F_i)\}}\right)\right\rceil.$$

This proves the following generalization of Moreno-Moreno's theorem to systems of polynomial equations with coefficients over $\mathbb{F}_q[X]$.

Theorem 6. *Let $F_1, \ldots, F_t$ be polynomials in the variables $Y_1, \ldots, Y_n$, where the coefficients are in $\mathbb{F}_q[X]$, $q = p^f$, and have degree at most a. If $n \geq \sum_{i=1}^{t} \omega_p(F_i)\deg(F_i) + 1$ and $m \geq \sum_{i=1}^{t} \omega_p(F_i)\,(a + 1 - \deg(F_i))$, then the number of n-tuples $(y_1, \ldots, y_n) \in (\mathbb{F}_q[X])^n$ with $\deg(y_i) \leq m$ that are solutions to $F_1 = 0, \ldots, F_t = 0$ is divisible by p^μ, where*

$$\mu = \left\lceil f\left(\frac{n(m+1) - \sum_{i=1}^{t} \omega_p(F_i)\,(a + \deg(F_i)m + 1)}{max_{1\leq i\leq t}\,\{\omega_p\,(F_i)\}}\right)\right\rceil.$$

Note that, as m, the degree of the polynomials considered for the solutions, increases the p-divisibility also increases. Hence, with no restriction on m, if $(0,\dots,0)$ is a solution to the system, the number of solutions is infinite.

The next corollary considers the case where the coefficients of $F_1,\dots,F_t$ are constants.

Corollary 7. *Let $F_1,\dots,F_t$ be polynomials in n variables and coefficients in $\mathbb{F}_q$. If $n \geq \sum_{i=1}^{t} \omega_p(F_i)\deg(F_i)+1$, then the number of n-tuples $(y_1,\dots,y_n) \in (\mathbb{F}_q[X])^n$ with $\deg(y_i) \leq m$ that are solutions to $F_1 = 0,\dots,F_t = 0$ is divisible by p^{μ}, where*

$$\mu = \left\lceil f\left(\frac{n(m+1)-\sum_{i=1}^{t}\omega_p(F_i)\left(\deg(F_i)m+1\right)}{max_{1\leq i\leq t}\left\{\omega_p\left(F_i\right)\right\}}\right)\right\rceil.$$

The next improvement of Carlitz's Theorem 1 is now a consequence of Theorem 6.

Corollary 8. *Let $F_1,\dots,F_t$ be polynomials in the variables $Y_1,\dots,Y_n$, with coefficients in $\mathbb{F}_q[X]$, and such that $F_i(0,\dots,0) = 0$ for $i = 1,\dots,t$. If $n \geq \sum_{i=1}^{t}\omega_p(F_i)\deg(F_i)+1$, then $F_1 = 0,\dots,F_t = 0$ have a non-trivial common solution. Moreover, if $n = \sum_{i=1}^{t}\omega_p(F_i)\deg(F_i)$, there are systems of this form which have only the trivial solution.*

We now provide two examples to show that the bound on n is tight.

Example 1. Let $q = p^f$ be odd. Let v be a non-quadratic residue in $\mathbb{F}_q$ and consider the polynomial

$$\begin{aligned}F(Y_1,\dots,Y_n) = {} & Y_1^{q+1} + vY_2^{q+1} + X^2\left(Y_3^{q+1} + vY_4^{q+1}\right) + X^4\left(Y_5^{q+1} + vY_6^{q+1}\right)\\ & + \cdots + X^{2q}\left(Y_{n-1}^{q+1} + vY_n^{q+1}\right),\end{aligned}$$

with coefficients in $\mathbb{F}_q[X]$.

Note that $n = 2(q+1) = \omega_p(F)\deg(F)$. We will show that $F = 0$ only has the trivial solution. Suppose that $(p_1(X),\dots,p_n(X))$ is a non-trivial solution for $F = 0$, where $\deg(p_1(X))+\cdots+\deg(p_n(X))$ is minimal. Then

$$\begin{aligned}F(p_1(X),\dots,p_n(X)) = {} & p_1(X)^{q+1} + vp_2(X)^{q+1}\\ & + X^2\left(p_3(X)^{q+1} + vp_4(X)^{q+1}\right) + X^4\left(p_5(X)^{q+1} + vp_6(X)^{q+1}\right)\\ & + \cdots + X^{2q}\left(p_{n-1}(X)^{q+1} + vp_n(X)^{q+1}\right) = 0\end{aligned} \tag{3}$$

implies that the constant and linear terms of p_1 and p_2 are zero. Hence $p_1(X) = X^2p_1'(X)$ and $p_2(X) = X^2p_2'(X)$ and Equation (3) is equivalent to

$$\begin{aligned}& X^{2(q+1)}\left(p_1'(X)^{q+1} + vp_2'(X)^{q+1}\right) + X^2\left(p_3(X)^{q+1} + vp_4(X)^{q+1}\right)\\ & \quad + X^4\left(p_5(X)^{q+1} + vp_6(X)^{q+1}\right) + \cdots + X^{2q}\left(p_{n-1}(X)^{q+1} + vp_n(X)^{q+1}\right) = 0,\end{aligned}$$

and this holds if and only if

$$\begin{aligned}& X^{2q}\left(p_1'(X)^{q+1} + vp_2'(X)^{q+1}\right) + \left(p_3(X)^{q+1} + vp_4(X)^{q+1}\right))\\ & \quad + X^2\left(p_5(X)^{q+1} + vp_6(X)^{q+1}\right) + \cdots + X^{2q-2}\left(p_{n-1}(X)^{q+1} + vp_n(X)^{q+1}\right) = 0.\end{aligned}$$

Therefore, $(p_3(X),\dots,p_n(X),p_1'(X),p_2'(X))$ is another solution to $F = 0$, and this contradicts the minimality of $(p_1(X),\dots,p_n(X))$.

Example 2. Let $q = p^f$ be any finite field, v be a element in $\mathbb{F}_q$ that cannot be written as a sum of two (q^2+q+1)-powers, and consider the polynomial

$$\begin{aligned} F(Y_1,\dots,Y_n) &= Y_1^{q^2+q+1} + Y_2^{q^2+q+1} + vY_3^{q^2+q+1} \\ &\quad + X^3\left(Y_4^{q^2+q+1} + Y_5^{q^2+q+1} + vY_6^{q+1}\right) + X^6\left(Y_7^{q^2+q+1} + Y_8^{q^2+q+1} + vY_9^{q^2+q+1}\right) \\ &\quad + \cdots + X^{3(q^2+q)}\left(Y_{n-2}^{q^2+q+1} + Y_{n-1}^{q^2+q+1} + vY_n^{q^2+q+1}\right) \end{aligned}$$

with coefficients in $\mathbb{F}_q[X]$.

Note that $n = 3(q^2+q+1) = \omega_p(F)\deg(F)$. We will show that $F = 0$ only has the trivial solution. Suppose that $(p_1(X),\dots,p_n(X))$ is a non-trivial solution for $F = 0$, where $\deg(p_1(X)) + \cdots + \deg(p_n(X))$ is minimal. Then

$$\begin{aligned} F(p_1(X),\dots,p_n(X)) &= p_1(X)^{q^2+q+1} + p_2(X)^{q^2+q+1} + vp_3(X)^{q^2+q+1} \\ &\quad + X^3\left(p_4(X)^{q^2+q+1} + p_5(X)^{q^2+q+1} + vp_6(X)^{q^2+q+1}\right) \\ &\quad + X^6\left(p_7(X)^{q^2+q+1} + p_8(X)^{q^2+q+1} + vp_9(X)^{q^2+q+1}\right) \\ &\quad + \cdots + X^{3(q^2+q)}(p_{n-2}(X)^{q^2+q+1} + p_{n-1}(X)^{q^2+q+1} + vp_n(X)^{q^2+q+1}) = 0 \end{aligned} \tag{4}$$

implies that the constant, linear and quadratic terms of p_1, p_2, p_3 are zero. Hence $p_1(X) = X^3p_1'(X)$, $p_2(X) = X^3p_2'(X)$ and $p_3(X) = X^3p_3'(X)$, and Equation (4) is equivalent to

$$\begin{aligned} &X^{3(q^2+q+1)}\left(p_1'(X)^{q^2+q+1} + p_2'(X)^{q^2+q+1} + vp_3'(X)^{q^23+q+1}\right) \\ &+ X^3\left(p_4(X)^{q^2+q+1} + p_5(X)^{q^2+q+1} + vp_6(X)^{q^2+q+1}\right) \\ &+ X^6\left(p_7(X)^{q^2+q+1} + p_8(X)^{q^2+q+1} + vp_9(X)^{q^2+q+1}\right) \\ &+ \cdots + X^{3(q^2+q)}\left(p_{n-2}(X)^{q^2+q+1} + p_{n-1}(X)^{q^2+q+1} + vp_n(X)^{q^2+q+1}\right) = 0, \end{aligned}$$

and this holds if and only if

$$\begin{aligned} &X^{3(q^2+q)}\left(p_1'(X)^{q^2+q+1} + p_2'(X)^{q^2+q+1} + vp_3'(X)^{q^2+q+1}\right) \\ &+ (p_4(X)^{q^2+q+1} + p_5(X)^{q^2+q+1} + vp_6(X)^{q^2+q+1}) \\ &+ X^3(p_7(X)^{q^2+q+1} + p_8(X)^{q^2+q+1} + vp_9(X)^{q^2+q+1}) \\ &+ \cdots + X^{3(q^2+q-1)}(p_{n-2}(X)^{q^2+q+1} + p_{n-1}(X)^{q^2+q+1} + vp_n(X)^{q^2+q+1}) = 0. \end{aligned}$$

Therefore, $(p_4(X),\dots,p_n(X),p_1'(X),p_2'(X),p_3'(X))$ is also a solution to $F = 0$, and this contradicts the minimality of $(p_1(X),\dots,p_n(X))$. In particular, we have that

$$\begin{aligned} F(Y_1,\dots,Y_n) &= Y_1^{q^2+q+1} + Y_2^{q^2+q+1} + vY_3^{q^2+q+1} + X^3(Y_4^{q^2+q+1} \\ &\quad + Y_5^{q^2+q+1} + vY_6^{q+1}) + X^6(Y_7^{q^2+q+1} + Y_8^{q^2+q+1} + vY_9^{q^2+q+1}) \\ &\quad + \cdots + X^{3(q^2+q)}(Y_{n-2}^{q^2+q+1} + Y_{n-1}^{q^2+q+1} + vY_n^{q^2+q+1}) \end{aligned}$$

with coefficients in $\mathbb{F}_{q^3}[X]$ has only the trivial solution for any $v \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ since $x^{q^2+q+1} \in \mathbb{F}_q$ for $x \in \mathbb{F}_{q^3}$.

The next example shows that Corollary 8 provides a substantial improvement to Carlitz's Theorem 1.

Example 3. Let $q = p^f$ and consider the polynomial

$$F(Y_1, \ldots, Y_n) = A_1(X)Y_1^{p^i+p^j} + \cdots + A_n(X)Y_n^{p^i+p^j}$$

with coefficients in $\mathbb{F}_q[X]$. Carlitz's Theorem 1 guarantees a non-trivial solution to $F = 0$ if F has at least $p^{2i} + p^{2j} + 2p^{i+j} + 1$ variables. Using our result, we get that $2(p^i + p^j) + 1$ variables are enough to guarantee a non-trivial solution.

Remark 9. The above results can also be extended to polynomials with coefficients in a quotient field $\mathbb{F}_q(X)$. Carlitz also considered polynomial equations in which the coefficients are polynomials in more than one variable. His result on these polynomials can also be improved by considering the p-weight degree instead of the degree of the polynomial, but, in order to keep the notation of the paper simple, we chose not include this case.

Acknowledgements

The late Oscar Moreno noticed some years ago that the method of restriction of scalars and the p-weight degree techniques could be used to obtain improvements to Carlitz's results in [8]. It turned out that, obtaining the improvement of Carlitz's result, we also obtained a generalization of the work which Oscar felt most proud about, the paper "Improvements of the Chevalley-Warning and Ax-Katz theorems" co-authored with Carlos Moreno [7]. Co-author Francis Castro passed away before this paper was accepted for publication. This paper is a humble tribute to Oscar and is dedicated to the memory of Francis.

References

[1] C. Chevalley, Démonstration d'une hypothèse de M. Artin, Abh. Math. Semin. Univ. Hamb. 11 (1) (1935) 73–75, https://doi.org/10.1007/BF02940714. URL https://doi.org/10.1007/BF02940714.
[2] A. Adolphson, S. Sperber, p-adic estimates for exponential sums and the theorem of Chevalley-Warning, Ann. Sci. Éc. Norm. Supér. (4) 20 (4) (1987) 545–556. URL http://www.numdam.org/item?id=ASENS_1987_4_20_4_545_0.
[3] J. Ax, Zeros of polynomials over finite fields, Am. J. Math. 86 (1964) 255–261.
[4] H. Chevalley, E. Warning, Bemerkung zur vorstehenden Arbeit, Abh. Math. Semin. Univ. Hamb. 11 (1) (1935) 76–83, https://doi.org/10.1007/BF02940715. URL https://doi.org/10.1007/BF02940715.
[5] D.R. Heath-Brown, On Chevalley-Warning theorems, Usp. Mat. Nauk 66 (2(398)) (2011) 223–232, https://doi.org/10.1070/RM2011v066n02ABEH004744. URL https://doi.org/10.1070/RM2011v066n02ABEH004744.
[6] N.M. Katz, On a theorem of Ax, Am. J. Math. 93 (1971) 485–499.
[7] O. Moreno, C.J. Moreno, Improvements of the Chevalley-Warning and the Ax-Katz theorems, Am. J. Math. 117 (1) (1995) 241–244, https://doi.org/10.2307/2375042. URL https://doi.org/10.2307/2375042.
[8] L. Carlitz, Some applications of a theorem of Chevalley, Duke Math. J. 18 (1951) 811–819.
[9] O. Moreno, C.J. Moreno, The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes, IEEE Trans. Inf. Theory 40 (6) (1994) 1894–1907, https://doi.org/10.1109/18.340464. URL https://doi.org/10.1109/18.340464.