Finite Fields and Their Applications 68 (2020) 101728

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Estimates on the number of $\mathbb{F}_q$–rational solutions of variants of diagonal equations over finite fields ☆

Mariana Pérez [a,c], Melina Privitelli [a,b,*]

[a] *Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina*
[b] *Universidad Nacional de General Sarmiento, Instituto de Ciencias, J.M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Buenos Aires, Argentina*
[c] *Universidad Nacional de Hurlingham, Instituto de Tecnología e Ingeniería, Av. Gdor. Vergara 2222 (B1688GEZ) Villa Tesei, Buenos Aires, Argentina*

ARTICLE INFO

Article history:
Received 5 January 2020
Received in revised form 12 July 2020
Accepted 17 July 2020
Available online 28 August 2020
Communicated by Daqing Wan

MSC:
11T06
05E05
14G05
14G15
11G25

Keywords:
Finite fields
Symmetric polynomials
Singular locus
Rational solutions
Diagonal equations

ABSTRACT

In this paper we study the set of $\mathbb{F}_q$-rational solutions of equations defined by polynomials evaluated in power-sum polynomials with coefficients in $\mathbb{F}_q$. This is done by means of applying a methodology which relies on the study of the geometry of the set of common zeros of symmetric polynomials over the algebraic closure of $\mathbb{F}_q$. We provide improved estimates and existence results of $\mathbb{F}_q$-rational solutions to the following equations: *deformed diagonal equations*, *generalized Markoff-Hurwitz-type equations* and *Carlitz's equations*. We extend these techniques to more general variants of diagonal equations over finite fields.

☆ The authors were partially supported by the grants PIP CONICET 11220130100598, PIO CONICET-UNGS 14420140100027 and ICI-UNGS 30/1146.
* Corresponding author.
E-mail addresses: mariana.perez@unahur.edu.ar (M. Pérez), mprivite@ungs.edu.ar (M. Privitelli).

https://doi.org/10.1016/j.ffa.2020.101728
1071-5797/

1. Introduction

Several problems of coding theory, cryptography and combinatorics require the study of the set of rational points of varieties defined over a finite field $\mathbb{F}_q$ on which the symmetric group of permutations of the coordinates acts. In coding theory, deep holes in the standard Reed–Solomon code over $\mathbb{F}_q$ can be expressed in terms of the set of zeros with coefficients in $\mathbb{F}_q$ of certain symmetric polynomials associated to the code (see, e.g., [16] or [8]). In cryptography, the characterization of monomials defining an almost perfect nonlinear polynomial or a differentially uniform mapping can be reduced to estimate the number of $\mathbb{F}_q$–rational zeros of some symmetric polynomials (see, e.g., [36] or [1]). Finally, several applications in combinatorics over finite fields, such as the determination of the average cardinality of the value set and the distribution of factorization patterns of families of univariate polynomials with coefficients in $\mathbb{F}_q$, has also been expressed in terms of the number of common $\mathbb{F}_q$–rational zeros of symmetric polynomials defined over $\mathbb{F}_q$ (see [14] and [15]). In [8], [14], [31], [15] and [33] we have developed a methodology to deal with some of the problems mentioned above. This methodology relies on the study of the geometry of the set of common zeros of the symmetric polynomials under consideration over the algebraic closure of $\mathbb{F}_q$. By means of such study we were able to prove that, in all the cases, the set of common zeros in $\mathbb{F}_q$ of the involved polynomials is a complete intersection whose singular locus has a "controlled" dimension. This allowed us to apply certain explicit estimates on the number of $\mathbb{F}_q$–rational zeros of projective complete intersections defined over $\mathbb{F}_q$ to obtain a conclusion for the problem under consideration (see, e.g., [24], [7], [9] or [32]).

The purpose of this article is twofold. On one hand, we apply our techniques to the problem of estimating the number of $\mathbb{F}_q$–rational solutions of certain variants of diagonal equations. On the other hand, we present a more general framework of the theory by extending the aforementioned methodology to a wider class of varieties defined by polynomials evaluated in symmetric polynomials.

We shall consider three well known classes of polynomial equations over finite fields: *deformed diagonal equations*, *generalized Markoff-Hurwitz-type equations* and *Carlitz's equations*. All previous results on the number of $\mathbb{F}_q$–rational solutions of these types of equations rely on techniques of combinatorial analysis, so our approach to the study these problems is novel.

Deformed diagonal equations. Given $g \in \mathbb{F}_q[X_1, \ldots, X_n]$, a deformed diagonal equation is an equation of the type

$$f := c_1 X_1^m + \cdots + c_n X_n^m + g = 0,$$

where $c_i \in \mathbb{F}_q \setminus \{0\}$ and $\deg(g) < m$. In comparison with diagonal equations, which correspond to the case where g is a constant polynomial, there are much fewer results about the number of $\mathbb{F}_q$-solutions of deformed diagonal equations. In [11], L. Carlitz provides a result which guarantees the existence of an $\mathbb{F}_q$-rational solution of a deformed

diagonal equation when $\mathrm{char}(\mathbb{F}_q)$ divides $m-1$. Later, in 2006, B. Felszeghy [22] extends Carlitz's result by dropping the requirement over $\mathrm{char}(\mathbb{F}_q)$, but which holds only for prime fields. Another generalization was provided by Castro et. al. [13] for the case when the exponents are not necessarily equal by computing the exact p-divisibility of certain exponential sums. On the other hand, A. Adolphson and S. Sperber [3] used Newton polyhedra to prove a result that derives an estimate on the number of $\mathbb{F}_q$–rational solutions of this type of equations. In this article we improve the existence results in the literature imposing no restriction to the characteristic of the field and extending Felszeghy's for several cases. Furthermore, we give an estimate on the number N_g of $\mathbb{F}_q$–rational solutions of these type of equations: we prove that $N_g = q^{n-1} + \mathcal{O}(q^{n/2})$, providing an explicit expression for the constant underlying the $\mathcal{O}$ notation.

Generalized Markoff-Hurwitz-type equations. These are of the form

$$(a_1 X_1^{m_1} + \cdots + a_n X_n^{m_n} + a)^k = bX_1^{k_1} \dots X_n^{k_n},$$

where $n, m_1, \dots, m_n, k_1, \dots, k_n$, k are positive integers, $a, b \in \mathbb{F}_q$ and $a_i \in \mathbb{F}_q \setminus \{0\}$, $1 \leq i \leq n$. Generalized Markoff-Hurwitz-type equations have been well studied in the special case $a = 0$. Moreover, several papers provide explicit formulas of the number of $\mathbb{F}_q$–rational solutions of this type of equations in very particular cases (see, e.g., [4]). In this article, we concentrate in the case $a \neq 0$ and $k = 1$. More precisely, we obtain an estimate on N^*, the number of $\mathbb{F}_q$–rational solutions with the condition that $x_1 \cdots x_n \neq 0$. This estimate improves Mordell's [34] for the case $m := m_1 = \cdots = m_n$ since our result holds without conditions on the characteristic of the field and we require that $m > k_1 + \cdots + k_n$ instead of $k_1 = \cdots = k_n = 1$. Also, our estimate improves Mordell's by determining an extra term in the asymptotic development of N^* in terms of q.

Carlitz's equations. These are of the form

$$h_1(X_1) + \cdots + h_n(X_n) = g,$$

where $h_i = a_{d,i}T^d + \cdots + a_{0,i} \in \mathbb{F}_q[T]$, $\deg(h_i) = d$ for $1 \leq i \leq n$ and $g \in \mathbb{F}_q[X_1, \dots, X_n]$ is such that $\deg(g) < d$. In this case, we provide an explicit estimate on the number N of $\mathbb{F}_q$–solutions of this type of equations which implies that $N = q^{n-1} + \mathcal{O}(q^{n/2})$. We also provide an explicit upper bound for the constant underlying the $\mathcal{O}$ notation in terms of d and n. This result improves Carlitz's estimate $N = q^{n-1} + \mathcal{O}(q^{n-w})$, where $w = \frac{1}{kd}$ and the constant implied by the $\mathcal{O}$ is not explicitly given (see [10]). Moreover, Carlitz's result only holds when g is a constant polynomial. We also obtain an existence result which improves Carlitz's in several aspects. Finally, as a particular case of this type of equations, we study the Dickson's equations.

All the aforementioned results complement those existing in the literature.

Our other main objective is the extension of our geometric methodology to a more general type of equations: those given by polynomials evaluated in power-sum polynomials. More precisely, let $P_{m_j} = X_1^{m_j} + \cdots + X_n^{m_j}$ be the m_j-power sum polynomial

of $\mathbb{F}_q[X_1, \ldots, X_n]$ and $g \in \mathbb{F}_q$ or $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a polynomial with $\deg(g) < c(m_1, \ldots, m_d)$, where $c(m_1, \ldots, m_d)$ is a constant which depends on $m_1, \ldots, m_d$. We consider new indeterminates $Y_1, \ldots, Y_d$ over $\mathbb{F}_q$ and $f \in \mathbb{F}_q[Y_1, \ldots, Y_d]$. Our purpose is to estimate the number of $\mathbb{F}_q$–solutions of the following type of equations:

$$f(P_{m_1}, \ldots, P_{m_d}) + g = 0.$$

We quickly outline our methodology to provide insight on the ideas behind it. Let $\mathsf{wt} : \mathbb{F}_q[Y_1, \ldots, Y_d] \longrightarrow \mathbb{N}$ be the weight defined by setting $\mathsf{wt}(Y_j) := m_j$ for $1 \leq j \leq d$ and let $\mathsf{wt}(f)$ be the *weight* of f. The equation above can be rewritten in the following way:

$$f(P_{m_1}, \ldots, P_{m_d}) + X_1^{\mathsf{wt}(f)} + \cdots + X_n^{\mathsf{wt}(f)} + g_1 = 0,$$

where $g_1 \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $\deg(g_1) < \mathsf{wt}(f)$. We concentrate on the more general problem of estimating the number of $\mathbb{F}_q$–rational solutions of the equation

$$f(P_{m_1}, \ldots, P_{m_d}) + X_1^e + \cdots + X_n^e + g_1 = 0,$$

where $g_1 \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $\deg(g_1) < e$ for *any* positive integer e. Let f^{wt} stand for the component of highest weight of f and let ∇f and ∇f^{wt} be the gradients of f and f^{wt} respectively. Suppose that the following hypotheses hold:

(H_1) $\nabla f \neq 0$ on every point of $\mathbb{A}^d$,
(H_2) $\nabla f^{\mathsf{wt}} \neq 0$ on every point of $\mathbb{A}^d$,

and let R_g be the polynomial $R_g := f(P_{m_1}, \ldots, P_{m_d}) + X_1^e + \cdots + X_n^e + g_1$. We shall study the geometric properties of the affine hypersurfaces $V_g := V(R_g) \subset \mathbb{A}^n$ with similar arguments as those in the papers cited above. In order to estimate the number of $\mathbb{F}_q$-rational points of V_g we consider $\mathrm{pcl}(V_g)$, the projective closure of V_g. We shall provide a suitable bound of the dimension of the singular locus of $\mathrm{pcl}(V_g)$ which allows us to prove that $\mathrm{pcl}(V_g)$ is absolutely irreducible. Then, applying estimates for absolutely irreducible singular projective varieties [24], we can provide the main result of this part.

Theorem 1.1. *Let d, n, e be positive integers such that $1 \leq d \leq n-3$. Let $m_1, \ldots, m_d$ be positive integers with $m_1 < \cdots < m_d$ and $e \neq m_i$ for $1 \leq i \leq d$. Assume that $\mathrm{char}(\mathbb{F}_q)$ does not divide e and m_j for all $1 \leq j \leq d$. Let $V_g = V(R_g) \subset \mathbb{A}^n$ be the variety defined by $R_g = f(P_{m_1}, \ldots, P_{m_d}) + g$ with $f \in \mathbb{F}_q[Y_1, \ldots, Y_d]$ and $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree e defined as $g = X_1^e + \cdots + X_n^e + g_1$. Suppose that $(H_1) - (H_2)$ hold, and let $\delta := \deg(R_g)$. Then we have the following estimates on $|V_g(\mathbb{F}_q)|$, the number of $\mathbb{F}_q$–rational points of V_g:*

- *if $e < \deg(R_g - g)$*

$$\left| |V_g(\mathbb{F}_q)| - q^{n-1} \right| \leq (q^{3/2} + 1) q^{\frac{n+d-4}{2}} ((\delta - 1)^{n-d} q^{1/2} + 6(\delta + 2)^n),$$

- *if* $e = \deg(R_g - g)$

$$\big||V_g(\mathbb{F}_q)| - q^{n-1}\big| \leq (q+1)q^{\frac{n+d-3}{2}}((\delta-1)^{n-d-1}q^{1/2} + 6(\delta+2)^n),$$

- *if* $e > \deg(R_g - g)$

$$\big||V_g(\mathbb{F}_q)| - q^{n-1}\big| \leq q^{\frac{n-2}{2}}\big(((\delta-1)^{n-d-1}q^{1/2} + 6(\delta+2)^n)q^{(d+1)/2} + (\delta-1)^{n-1}\big).$$

On the other hand, if $g \in \mathbb{F}_q$ *we have that*

$$\big||V_g(\mathbb{F}_q)| - q^{n-1}\big| \leq (q+1)q^{\frac{n+d-4}{2}}((\delta-1)^{n-d}q^{1/2} + 6(\delta+2)^n).$$

The paper is organized as follows. In Section 2 we collect the notions of algebraic geometry we use. In Section 3 we study the geometric properties of the *deformed hypersurfaces* V_g and we settle Theorem 1.1. Finally, in Section 4 we apply our methodology to obtain estimates and existence results of deformed diagonal equations, generalized Markoff-Hurwitz-type equations and Carlitz's equations.

2. Basic notions of algebraic geometry

In this section we collect the basic definitions and facts of algebraic geometry that we need in the sequel. We use standard notions and notations which can be found in, e.g., [28], [37].

Let $\mathbb{K}$ be any of the fields $\mathbb{F}_q$ or $\overline{\mathbb{F}}_q$. We denote by $\mathbb{A}^r$ the affine r–dimensional space $\overline{\mathbb{F}}_q^r$ and by $\mathbb{P}^r$ the projective r–dimensional space over $\overline{\mathbb{F}}_q^{r+1}$. Both spaces are endowed with their respective Zariski topologies over $\mathbb{K}$, for which a closed set is the zero locus of a set of polynomials of $\mathbb{K}[X_1, \ldots, X_r]$, or of a set of homogeneous polynomials of $\mathbb{K}[X_0, \ldots, X_r]$.

A subset $V \subset \mathbb{P}^r$ is a *projective variety defined over* $\mathbb{K}$ (or a projective $\mathbb{K}$–variety for short) if it is the set of common zeros in $\mathbb{P}^r$ of homogeneous polynomials $F_1, \ldots, F_m \in \mathbb{K}[X_0, \ldots, X_r]$. Correspondingly, an *affine variety of* $\mathbb{A}^r$ *defined over* $\mathbb{K}$ (or an affine $\mathbb{K}$–variety) is the set of common zeros in $\mathbb{A}^r$ of polynomials $F_1, \ldots, F_m \in \mathbb{K}[X_1, \ldots, X_r]$. We think a projective or affine $\mathbb{K}$–variety to be equipped with the induced Zariski topology. We shall denote by $\{F_1 = 0, \ldots, F_m = 0\}$ or $V(F_1, \ldots, F_m)$ the affine or projective $\mathbb{K}$–variety consisting of the common zeros of $F_1, \ldots, F_m$.

In the remaining part of this section, unless otherwise stated, all results referring to varieties in general should be understood as valid for both projective and affine varieties.

A $\mathbb{K}$–variety V is *irreducible* if it cannot be expressed as a finite union of proper $\mathbb{K}$–subvarieties of V. Further, V is *absolutely irreducible* if it is $\overline{\mathbb{F}}_q$–irreducible as a $\overline{\mathbb{F}}_q$–variety. Any $\mathbb{K}$–variety V can be expressed as an irredundant union $V = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_s$ of irreducible (absolutely irreducible) $\mathbb{K}$–varieties, unique up to reordering, called the *irreducible* (*absolutely irreducible*) $\mathbb{K}$–*components* of V.

For a $\mathbb{K}$–variety V contained in $\mathbb{P}^r$ or $\mathbb{A}^r$, its *defining ideal* $I(V)$ is the set of polynomials of $\mathbb{K}[X_0,\dots,X_r]$, or of $\mathbb{K}[X_1,\dots,X_r]$, vanishing on V. The *coordinate ring* $\mathbb{K}[V]$ of V is the quotient ring $\mathbb{K}[X_0,\dots,X_r]/I(V)$ or $\mathbb{K}[X_1,\dots,X_r]/I(V)$. The *dimension* $\dim V$ of V is the length n of a longest chain $V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n$ of nonempty irreducible $\mathbb{K}$–varieties contained in V. We say that V has *pure dimension* n if every irreducible $\mathbb{K}$–component of V has dimension n. A $\mathbb{K}$–variety of $\mathbb{P}^r$ or $\mathbb{A}^r$ of pure dimension $r-1$ is called a $\mathbb{K}$–*hypersurface*. A $\mathbb{K}$–hypersurface of $\mathbb{P}^r$ (or $\mathbb{A}^r$) can also be described as the set of zeros of a single nonzero polynomial of $\mathbb{K}[X_0,\dots,X_r]$ (or of $\mathbb{K}[X_1,\dots,X_r]$).

The *degree* $\deg V$ of an irreducible $\mathbb{K}$–variety V is the maximum of $|V\cap L|$, considering all the linear spaces L of codimension $\dim V$ such that $|V\cap L|<\infty$. More generally, following [26] (see also [23]), if $V=\mathcal{C}_1\cup\cdots\cup\mathcal{C}_s$ is the decomposition of V into irreducible $\mathbb{K}$–components, we define the degree of V as

$$\deg V := \sum_{i=1}^{s} \deg \mathcal{C}_i.$$

The degree of a $\mathbb{K}$–hypersurface V is the degree of a polynomial of minimal degree defining V.

Let $V\subset\mathbb{A}^r$ be a $\mathbb{K}$–variety, $I(V)\subset\mathbb{K}[X_1,\dots,X_r]$ its defining ideal and x a point of V. The *dimension* $\dim_x V$ *of* V *at* x is the maximum of the dimensions of the irreducible $\mathbb{K}$–components of V containing x. If $I(V)=(F_1,\dots,F_m)$, the *tangent space* $\mathcal{T}_xV$ to V at x is the kernel of the Jacobian matrix $(\partial F_i/\partial X_j)_{1\le i\le m,1\le j\le r}(x)$ of $F_1,\dots,F_m$ with respect to $X_1,\dots,X_r$ at x. We have $\dim \mathcal{T}_xV \ge \dim_x V$ (see, e.g., [37, page 94]). The point x is *regular* if $\dim \mathcal{T}_xV = \dim_x V$; otherwise, x is called *singular*. The set of singular points of V is the *singular locus* of V; it is a closed $\mathbb{K}$–subvariety of V. A variety is called *nonsingular* if its singular locus is empty. For projective varieties, the concepts of tangent space, regular and singular point can be defined by considering an affine neighborhood of the point under consideration.

2.1. Rational points

Let $\mathbb{P}^r(\mathbb{F}_q)$ be the r–dimensional projective space over $\mathbb{F}_q$ and $\mathbb{A}^r(\mathbb{F}_q)$ the r–dimensional $\mathbb{F}_q$–vector space $\mathbb{F}_q^r$. For a projective variety $V\subset\mathbb{P}^r$ or an affine variety $V\subset\mathbb{A}^r$, we denote by $V(\mathbb{F}_q)$ the set of $\mathbb{F}_q$–rational points of V, namely $V(\mathbb{F}_q):=V\cap\mathbb{P}^r(\mathbb{F}_q)$ in the projective case and $V(\mathbb{F}_q):=V\cap\mathbb{A}^r(\mathbb{F}_q)$ in the affine case. For an affine variety V of dimension n and degree δ, we have the following bound (see, e.g., [6, Lemma 2.1]):

$$|V(\mathbb{F}_q)| \le \delta\, q^n.$$

On the other hand, if V is a projective variety of dimension n and degree δ, then we have the following bound (see [24, Proposition 12.1] or [7, Proposition 3.1]; see [29] for more precise upper bounds):

$$|V(\mathbb{F}_q)| \leq \delta\, p_n,$$

where $p_n := q^n + q^{n-1} + \cdots + q + 1 = |\mathbb{P}^n(\mathbb{F}_q)|$.

2.2. Complete intersections

Elements $F_1, \ldots, F_m$ in $\mathbb{K}[X_1, \ldots, X_r]$ or $\mathbb{K}[X_0, \ldots, X_r]$ form a *regular sequence* if F_1 is nonzero and no F_i is zero or a zero divisor in the quotient ring $\mathbb{K}[X_1, \ldots, X_r]/(F_1, \ldots, F_{i-1})$ or $\mathbb{K}[X_0, \ldots, X_r]/(F_1, \ldots, F_{i-1})$ for $2 \leq i \leq m$. In such a case, the (affine or projective) variety $V := V(F_1, \ldots, F_m)$ they define is equidimensional of dimension $r - m$, and is called a *set–theoretic complete intersection*.

For given positive integers $a_1, \ldots, a_r$, we define the weight $\mathsf{wt}(\boldsymbol{X}^{\boldsymbol{\alpha}})$ of a monomial $\boldsymbol{X}^{\boldsymbol{\alpha}} := X_1^{\alpha_1} \cdots X_r^{\alpha_r}$ as $\mathsf{wt}(\boldsymbol{X}^{\boldsymbol{\alpha}}) := \sum_{i=1}^{r} a_i \cdot \alpha_i$. The weight $\mathsf{wt}(f)$ of an arbitrary element $f \in \mathbb{K}[X_1, \ldots, X_r]$ is the highest weight of all the monomials with nonzero coefficients arising in the dense representation of f.

Lemma 2.1. *[33, Lemma 5.4] Let $F_1, \ldots, F_m \in \mathbb{K}[X_1, \ldots, X_r]$. For an assignment of positive integer weights wt to the variables $X_1, \ldots, X_r$, denote by $F_1^{\mathsf{wt}}, \ldots, F_m^{\mathsf{wt}}$ the components of highest weight of $F_1, \ldots, F_m$. If $F_1^{\mathsf{wt}}, \ldots, F_m^{\mathsf{wt}}$ form a regular sequence in $\mathbb{K}[X_1, \ldots, X_r]$, then $F_1, \ldots, F_m$ form a regular sequence in $\mathbb{K}[X_1, \ldots, X_r]$.*

3. Deformed hypersurfaces defined by m_j–power sums

In this section we shall develop the extension of the methodology used in [8], [14], [31], [15] and [33] to the more general case of equations given by polynomials evaluated in power-sum polynomials. Let d, n, e be positive integers such that $1 \leq d \leq n - 3$ and let $m_1, \ldots, m_d$ be positive integers with $m_1 < \cdots < m_d$ and $e \neq m_i$ for $1 \leq i \leq d$. We assume that $\mathrm{char}(\mathbb{F}_q)$ does not divide e and m_j for all $1 \leq j \leq d$. Let $Y_1, \ldots, Y_d$ be indeterminates over $\mathbb{F}_q$ and let $f \in \mathbb{F}_q[Y_1, \ldots, Y_d]$. We consider the weight $\mathsf{wt} : \mathbb{F}_q[Y_1, \ldots, Y_d] \longrightarrow \mathbb{N}$ defined by setting $\mathsf{wt}(Y_j) := m_j$ for $1 \leq j \leq d$ and denote by f^{wt} the component of highest weight of f. Let ∇f and ∇f^{wt} be the gradients of f and f^{wt} respectively. Suppose that the following hypotheses hold:

(H_1) $\nabla f \neq 0$ on every point of $\mathbb{A}^d$.
(H_2) $\nabla f^{\mathsf{wt}} \neq 0$ on every point of $\mathbb{A}^d$.

Let $X_1, \ldots, X_n$ be new indeterminates over $\mathbb{F}_q$. We consider the m_j-power sum $P_{m_j} = X_1^{m_j} + \cdots + X_n^{m_j}$, $1 \leq j \leq d$. Finally, let $g \in \mathbb{F}_q$ or let $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ be the following polynomial

$$g = X_1^e + \cdots + X_n^e + g_1, \tag{3.1}$$

where $g_1 \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $\deg(g_1) < e$. Our aim is to estimate the number of $\mathbb{F}_q$–rational solutions of the equation

$$f(P_{m_1}, \ldots, P_{m_d}) + g = 0.$$

To do this, we consider $R_g \in \mathbb{F}_q[X_1, \ldots, X_n]$ the polynomial

$$R_g := f(P_{m_1}, \ldots, P_{m_d}) + g. \tag{3.2}$$

Let $V_g := V(R_g) \subset \mathbb{A}^n$ be the $\mathbb{F}_q$-affine hypersurface defined by R_g. We call V_g a *deformed hypersurface* defined by the m_j-powers sum with coefficients in $\mathbb{F}_q$. We shall study some facts concerning the geometry of V_g. For this purpose, we need to obtain an upper bound of the dimension of Σ_g, the singular locus of V_g. Then, for a given $\mathbf{x} \in \mathbb{A}^n$, we shall consider the following $(d \times n)$–matrix $A(\mathbf{x})$:

$$A(\mathbf{x}) := \begin{pmatrix} \frac{\partial P_{m_1}}{\partial X_1}(\mathbf{x}) & \cdots & \frac{\partial P_{m_1}}{\partial X_n}(\mathbf{x}) \\ \vdots & & \vdots \\ \frac{\partial P_{m_d}}{\partial X_1}(\mathbf{x}) & \cdots & \frac{\partial P_{m_d}}{\partial X_n}(\mathbf{x}) \end{pmatrix}. \tag{3.3}$$

By the chain rule, we deduce that the partial derivatives of $f(\mathbf{P})(\mathbf{X})$ satisfy the following equality for $1 \leq j \leq n$:

$$\frac{\partial f(\mathbf{P})}{\partial X_j} = \left(\frac{\partial f}{\partial Y_1} \circ \boldsymbol{P}\right) \cdot \frac{\partial P_{m_1}}{\partial X_j} + \cdots + \left(\frac{\partial f}{\partial Y_d} \circ \boldsymbol{P}\right) \cdot \frac{\partial P_{m_d}}{\partial X_j},$$

where $\boldsymbol{P} = (P_{m_1}, \ldots, P_{m_d})$. Suppose firstly that g is defined as in (3.1). For any $\mathbf{x} \in \Sigma_g$, we have

$$\nabla R_g(\mathbf{x}) = \nabla f(\boldsymbol{P}(\mathbf{x})) \cdot A(\mathbf{x}) + \nabla g(\mathbf{x}) = \mathbf{0}.$$

Then $\mathbf{y} := \nabla f(\boldsymbol{P}(\mathbf{x}))$ is a solution of the system

$$A^t(\mathbf{x}) Y^t = -\nabla g(\mathbf{x})^t. \tag{3.4}$$

Observe that for $\nabla g(\mathbf{x}) = \mathbf{0}$ (H_1) implies that (3.4) has a nonzero solution. Therefore $\operatorname{rank}(A(\mathbf{x})) < d$. On the other hand, if $\nabla g(\mathbf{x}) \neq \mathbf{0}$, either $\operatorname{rank}(A(\mathbf{x})) < d$ or $\operatorname{rank}(A(\mathbf{x})) = \operatorname{rank}(M_A(\mathbf{x})) = d$, where $M_A(\mathbf{x})$ is the augmented matrix of the system (3.4). Hence $\Sigma_g \subset Z_1 \cup Z_2$, where Z_1 and Z_2 are the following sets:

$$Z_1 = \{\mathbf{x} \in \mathbb{A}^n : \operatorname{rank}(A(\mathbf{x})) < d\}$$
$$Z_2 = \{\mathbf{x} \in \mathbb{A}^n : \operatorname{rank}(A(\mathbf{x})) = \operatorname{rank}(M_A(\mathbf{x})) = d\}.$$

Suppose now that $g \in \mathbb{F}_q$ and let $\mathbf{x} \in \Sigma_g$. We have that

$$\nabla R_g(\mathbf{x}) = \nabla f(\boldsymbol{P}(\mathbf{x})) \cdot A(\mathbf{x}) = \mathbf{0}.$$

From (H_1), we have that $\mathbf{y} := \nabla f(\boldsymbol{P}(\mathbf{x}))$ is a nonzero solution of the homogeneous system

$$A^t(\mathbf{x})Y^t = 0.$$

We conclude that $\operatorname{rank}(A(\mathbf{x})) < d$. Therefore $\mathbf{x} \in Z_1$ and $\Sigma_g \subset Z_1$.

We next obtain an upper bound of the dimension of Z_1. In what follows, $VDM(X_1, \ldots, X_t)$ stands for the Vandermonde matrix in the variables $X_1, \ldots, X_t$.

Proposition 3.1. *Z_1 has dimension at most $d-1$.*

Proof. Observe that

$$Z_1 = \bigcup_{j=0}^{d-1} V_j,$$

where $V_j := \{\mathbf{x} \in \mathbb{A}^n : \operatorname{rank}(A(\mathbf{x})) = j\}$. Since $\operatorname{char}(\mathbb{F}_q)$ does not divide m_k for all $1 \leq k \leq d$ then

$$A(\mathbf{X}) := \begin{pmatrix} m_1 X_1^{m_1-1} & \cdots & m_1 X_n^{m_1-1} \\ \vdots & & \vdots \\ m_d X_1^{m_d-1} & \cdots & m_d X_n^{m_d-1} \end{pmatrix}. \tag{3.5}$$

Fix j for $0 \leq j \leq d-1$. We shall prove that the dimension of V_j is at most $d-1$. Let $\mathbf{x} \in V_j$, so $\operatorname{rank}(A(\mathbf{x})) = j$. Thus, there exists a $(j \times j)$–submatrix of $A(\mathbf{x})$ of rank $= j$. Suppose without loss of generality that this submatrix consists of the first j rows and the first j columns of $A(\mathbf{x})$. Let $C_1, \ldots, C_n$ denote the columns of $A(\mathbf{X})$ and let $A(C_1, \ldots, C_j, C_k)$ be the $((j+1) \times (j+1))$–submatrix of $A(\mathbf{X})$ consisting of the entries of the first $j+1$ rows and the columns $C_1, \ldots, C_j, C_k$, $j+1 \leq k \leq n$. By [5, Proposition 5], $\mathbf{x}$ belongs to the set of common zeros of the $(n-j)$ $\mathbb{F}_q$–equations

$$\det A(C_1, \ldots, C_j, C_k) = 0, \ j+1 \leq k \leq n.$$

Now, from [20, Theorem 2.1]:

$$\begin{aligned} &\det A(C_1, \ldots, C_j, C_k)(\mathbf{X}) \\ &\quad = \Pi_{l=1}^{d} m_l \operatorname{VDM}(X_1, \ldots, X_j) \Pi_{l=1}^{j} X_l^{m_1-1} (X_k - X_l) P(X_k), \ j+1 \leq k \leq n, \end{aligned}$$

for some $P \in \mathbb{F}_q[T]$. Since the principal minor of $A(\mathbf{x})$ is nonzero, we deduce that $x_l \neq 0$, $1 \leq l \leq j$, and $x_m \neq x_n$, $1 \leq m < n \leq j$. Therefore $\mathbf{x} \in V(Q_{j+1}, \ldots, Q_n)$, where $Q_k := \Pi_{l=1}^{j}(X_k - X_l)P(X_k)$. We claim that $Q_{j+1}, \ldots, Q_n$ form a regular sequence of $\mathbb{F}_q[X_1, \ldots, X_n]$. Indeed, consider the graded lexicographic order of $\mathbb{F}_q[X_1, \ldots, X_n]$ with $X_n > X_{n-1} > \cdots > X_1$. With this order we have that $Lt(Q_k) = X_k^j \cdot P_k^j$, where $Lt(Q_k)$ denotes the leading terms of the polynomials Q_k and P_k is the leading term of P. Thus $Lt(Q_k)$, $j+1 \leq k \leq n$, are relatively prime and they form a Gröbner basis of the ideal J that they generate (see, e.g., [18, §2.9, Proposition 4]). Hence, the initial of the ideal J is generated by $Lt(Q_{j+1}), \ldots, Lt(Q_n)$, which form a regular sequence of $\mathbb{F}_q[X_1, \ldots, X_n]$. Therefore, by [21, Proposition 15.15], the polynomials $Q_{j+1}, \ldots, Q_n$ form a regular sequence of $\mathbb{F}_q[X_1, \ldots, X_n]$. We conclude that $V(Q_{j+1}, \ldots, Q_n)$ is a set complete intersection of $\mathbb{A}^n$ of dimension j.

Observe finally that, given $\mathbf{x} \in V_j$, there exists a $(d \times n)$-matrix $A'(\mathbf{X})$ obtained by rearranging the columns of $A(\mathbf{X})$ with nonzero principal minor. Therefore, by the same arguments as above, V_j is included in an union of $\mathbb{F}_q$-varieties of dimension j. Thus, Z_1 has dimension at most $d-1$. □

Now, we obtain an upper bound of the dimension of Z_2. First we need the following remark.

Remark 3.2. For all $\mathbf{x} \in Z_2$, $\nabla(g(\mathbf{x})) \neq 0$. Indeed, $\nabla(g(\mathbf{x})) = 0$ implies that the system (3.4) is homogeneous. Since it has a nonzero solution then $\operatorname{rank}(A(\mathbf{x})) < d$, which contradicts $\mathbf{x} \in Z_2$.

Proposition 3.3. *The dimension of Z_2 is at most d.*

Proof. Let $\mathbf{x} \in Z_2$, so $\operatorname{rank}(A(\mathbf{x})) = d$. Thus, there exists a $(d \times d)$–submatrix $B(\mathbf{x})$ of $A(\mathbf{x})$ of rank $= d$. Suppose that this submatrix consists of the first d rows and columns of $A(\mathbf{x})$. Then $\mathbf{x} \in B := \{\mathbf{x} \in \mathbb{A}^n : \det B(\mathbf{x}) \neq 0,\ \operatorname{rank}(M_A(\mathbf{x})) = d\}$. Taking into account that

$$\det B(\mathbf{x}) := \det \begin{pmatrix} m_1 x_1^{m_1-1} & \cdots & m_1 x_d^{m_1-1} \\ \vdots & & \vdots \\ m_d x_1^{m_d-1} & \cdots & m_d x_d^{m_d-1} \end{pmatrix} \neq 0 \tag{3.6}$$

and [5, Proposition 5], we have that $B = V(F_{d+1}, \ldots, F_n)$, where $F_j \in \mathbb{F}_q[X_1, \ldots, X_n]$, $d+1 \leq j \leq n$, are the polynomials:

$$F_j := \det \begin{pmatrix} m_1 X_1^{m_1-1} & \cdots & m_1 X_d^{m_1-1} & m_1 X_j^{m_1-1} \\ \vdots & & \vdots & \vdots \\ m_d X_1^{m_d-1} & \cdots & m_d X_d^{m_d-1} & m_d X_j^{m_d-1} \\ -\frac{\partial g}{\partial X_1} & \cdots & -\frac{\partial g}{\partial X_d} & -\frac{\partial g}{\partial X_j} \end{pmatrix}.$$

By the definition of g, the component $F_j^{\deg(F_j)}$ of highest degree of F_j is the following polynomial:

$$F_j^{\deg(F_j)} := \det \begin{pmatrix} m_1 X_1^{m_1-1} & \cdots & m_1 X_d^{m_1-1} & m_1 X_j^{m_1-1} \\ \vdots & & \vdots & \vdots \\ m_d X_1^{m_d-1} & \cdots & m_d X_d^{m_d-1} & m_d X_j^{m_d-1} \\ -e X_1^{e-1} & \cdots & -e X_d^{e-1} & -e X_j^{e-1} \end{pmatrix}.$$

From [20, Theorem 2.1] we have that

$$F_j^{\deg(F_j)} = e \cdot \Pi_{l=1}^{d} m_l \mathrm{VDM}(X_1, \ldots, X_d) \Pi_{k=1}^{d} X_k^{\min\{m_1, e\}-1} (X_j - X_k) P(X_j)\ , d+1 \leq j \leq n,$$

for some $P \in \mathbb{F}_q[T]$. From (3.6) we deduce that $x_k \neq 0$, $1 \leq k \leq d$, and $x_i \neq x_k$, $1 \leq i < k \leq d$. Therefore $V(F_{d+1}^{\deg F_{d+1}}, \ldots, F_j^{\deg F_j}) = V(Q_{d+1}, \ldots, Q_j)$, where $d+1 \leq j \leq n$ and $Q_j := \Pi_{k=1}^{d}(X_j - X_k)P(X_j)$. The same reasoning as in the proof of Proposition 3.1 shows that $Q_{d+1}, \ldots, Q_n$ form a regular sequence of $\mathbb{F}_q[X_1, \ldots, X_n]$. Hence, $\dim V(F_{d+1}^{\deg F_{d+1}}, \ldots, F_j^{\deg F_j}) = n - j + d$ for $d+1 \leq j \leq n$. Therefore, $F_{d+1}^{\deg F_{d+1}}, \ldots, F_n^{\deg F_n}$ form a regular sequence of $\mathbb{F}_q[X_1, \ldots, X_n]$ and, by Lemma 2.1, $F_{d+1}, \ldots, F_n$ form a regular sequence of $\mathbb{F}_q[X_1, \ldots, X_n]$. This proves B has dimension at most d.

Finally, observe that, given $\mathbf{x} \in Z_2$, there exists a $(d \times n)$-matrix $A'(\mathbf{X})$ obtained from $A(\mathbf{X})$ by reordering its columns, with the condition that the principal minor of $A'(\mathbf{X})$ is nonzero. Therefore, we conclude that Z_2 is included in an union of $\mathbb{F}_q$-varieties of dimension at most d. □

From Proposition 3.1 and Proposition 3.3 we obtain the following result.

Theorem 3.4. *Let $1 \leq d \leq n-3$. Let $f \in \mathbb{F}_q[Y_1, \ldots, Y_d]$ and $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ defined as in (3.1) such that $(H_1) - (H_2)$ hold and R_g is defined as in (3.2). The singular locus Σ_g of V_g has dimension at most d. On the other hand, if $g \in \mathbb{F}_q$, singular locus Σ_g of V_g has dimension at most $d-1$.*

We shall also need information concerning the behavior of V_g at "infinity". For this purpose, we consider the projective closure $\mathrm{pcl}(V_g) \subset \mathbb{P}^n$. It is well known that $\mathrm{pcl}(V_g)$ is the $\mathbb{F}_q$-hypersurface of $\mathbb{P}^n$ defined by the homogenization $R_g^h \in \mathbb{F}_q[X_0, \ldots, X_n]$ of the polynomial R_g (see, e.g., [28, §I.5, Exercise 6]).

Let $R_g^{\deg(R_g)}$ be the component of highest degree of R_g. We shall express $R_g^{\deg(R_g)}$ in terms of the component f^{wt} of highest weight of f. Let $Y_1^{j_1} \cdots Y_d^{j_d}$ be a monomial with nonzero coefficient arising in the dense representation of f. Then its weight

$$\mathsf{wt}(Y_1^{j_1} \cdots Y_d^{j_d}) = m_1 j_1 + \cdots + m_d j_d$$

is equal to the degree of the corresponding monomial $P_{m_1}^{j_1} \cdots P_{m_d}^{j_d}$ of R_g. From these arguments we deduce the following lemma.

Lemma 3.5. *Suppose that g is defined as in (3.1). Then,*

$$R_g^{\deg(R_g)} = \begin{cases} f^{\mathsf{wt}}(P_{m_1}, \ldots, P_{m_d}) & e < \mathsf{wt}(f) \\ f^{\mathsf{wt}}(P_{m_1}, \ldots, P_{m_d}) + X_1^e + \cdots + X_n^e & e = \mathsf{wt}(f) \\ X_1^e + \cdots + X_n^e & e > \mathsf{wt}(f) \end{cases}$$

On the other hand, if $g \in \mathbb{F}_q$, we have that $R_g^{\deg(R_g)} = f^{\mathsf{wt}}(P_{m_1}, \ldots, P_{m_d})$.

Proposition 3.6. *Let $1 \leq d \leq n-3$. Suppose that g is defined as in (3.1).*

- *If $e < \mathsf{wt}(f)$ then $\mathrm{pcl}(V_g)$ has singular locus at infinity of dimension at most $d-2$,*
- *if $e = \mathsf{wt}(f)$ then $\mathrm{pcl}(V_g)$ has singular locus at infinity of dimension at most $d-1$,*
- *if $e > \mathsf{wt}(f)$ then $\mathrm{pcl}(V_g)$ has no singular points at infinity.*

On the other hand, if $g \in \mathbb{F}_q$ then $\mathrm{pcl}(V_g)$ has singular locus at infinity of dimension at most $d-2$.

Proof. Let $\Sigma_g^\infty \subset \mathbb{P}^n$ denote the singular locus of $\mathrm{pcl}(V_g)$ at infinity; namely, the set of singular points of $\mathrm{pcl}(V_g)$ lying in the hyperplane $\{X_0 = 0\}$. We have that $R_g^h(0, X_1, \ldots, X_n) = R_g^{\deg(R_g)}(X_1, \ldots, X_n)$. Suppose first that $e < \mathsf{wt}(f)$. From Lemma 3.5, $R_g^{\deg(R_g)} = f^{\mathsf{wt}}(P_{m_1}, \ldots, P_{m_d})$. Thus, any point $\mathbf{x} = (0 : x_1 : \cdots : x_n) \in \Sigma_g^\infty$ satisfies the equations:

$$f^{\mathsf{wt}}(\mathbf{P}) = 0 \ , \frac{\partial f^{\mathsf{wt}}(\mathbf{P})}{\partial X_j} = 0, \quad 1 \leq j \leq n. \tag{3.7}$$

From (H_2) we have that the homogeneous system $A^t(\mathbf{x})Y^t = \mathbf{0}$, where $A(\mathbf{x})$ is defined as in (3.3), has a nonzero solution $\nabla f^{\mathsf{wt}}(\boldsymbol{P}(\mathbf{x}))$. We conclude that $\mathbf{x} \in Z_1$. Thus, we deduce from Proposition 3.1 that the set of solutions of (3.7) is an affine cone of $\mathbb{A}^n$ of dimension at most $d-1$ and, hence, a projective variety of $\mathbb{P}^{n-1}$ of dimension at most $d-2$. Therefore, the set of singular points of $\mathrm{pcl}(V_g)$ lying in the hyperplane $\{X_0 = 0\}$ has dimension at most $d-2$.

Suppose now that $e = \mathsf{wt}(f)$. From Lemma 3.5 $R_g^{\deg(R_g)} = f^{\mathsf{wt}}(P_{m_1}, \ldots, P_{m_d}) + X_1^e + \cdots + X_n^e$. Then, by (H_2) and the same arguments of the proof of Proposition 3.3, we deduce that the variety defined by the equations:

$$f^{\mathsf{wt}}(\mathbf{P}) + X_1^e + \cdots + X_n^e = 0, \quad \frac{\partial f^{\mathsf{wt}}(\mathbf{P})}{\partial X_j} + eX_j^{e-1} = 0, \quad 1 \leq j \leq n,$$

is an affine cone of A^n of dimension at most d. Therefore, the set of singular points of $\mathrm{pcl}(V_g)$ lying in the hyperplane $\{X_0 = 0\}$ has dimension at most $d-1$.

Finally, if $e > \mathsf{wt}(f)$, observe that $R_g^{\deg(R_g)} = X_1^e + \cdots + X_n^e$, from where it is easy to see that $\mathrm{pcl}(V_g)$ has no singular points at infinity.

Suppose now that $g \in \mathbb{F}_q$. We see that any point $\mathbf{x} = (0 : x_1 : \cdots : x_n) \in \Sigma_g^\infty$ satisfies the equations defined in (3.7). Hence, by (H_2) and the same arguments of the proof of the case $e < \mathsf{wt}(f)$, we deduce that the set of singular points of $\mathrm{pcl}(V_g)$ lying in the hyperplane $\{X_0 = 0\}$ has dimension at most $d-2$. □

From Theorem 3.4 and Proposition 3.6 we obtain the following result.

Theorem 3.7. *Let $1 \leq d \leq n-3$. Let $f \in \mathbb{F}_q[Y_1, \ldots, Y_d]$, $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ defined as in (3.1) such that $(H_1) - (H_2)$ hold and R_g defined as in (3.2). Then $\mathrm{pcl}(V_g)$ has singular locus of dimension at most d. On the other hand, if $g \in \mathbb{F}_q$ then $\mathrm{pcl}(V_g)$ has singular locus of dimension at most $d-1$.*

Corollary 3.8. *The hypersurface V_g is absolutely irreducible, when g is defined as in (3.1) or $g \in \mathbb{F}_q$.*

Proof. Observe that V_g is absolutely irreducible if and only if $\mathrm{pcl}(V_g)$ is absolutely irreducible (see, e.g., [28, Chapter I, Proposition 5.17]). Suppose that $\mathrm{pcl}(V_g)$ is not absolutely irreducible. Then it has a nontrivial decomposition into absolutely irreducible components

$$\mathrm{pcl}(V_g) = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_s,$$

where $\mathcal{C}_1, \ldots, \mathcal{C}_s$ are projective hypersurfaces of $\mathbb{P}^n$. Since $\mathcal{C}_i \cap \mathcal{C}_j \neq \emptyset$ and $\mathcal{C}_i$, $\mathcal{C}_j$ are absolutely irreducible, then $\dim(\mathcal{C}_i \cap \mathcal{C}_j) = n-2$.

Denote by Σ_g^h the singular locus of $\mathrm{pcl}(V_g)$. From Theorem 3.7 we have that $\dim \Sigma_g^h \leq d$. On the other hand, we have $\mathcal{C}_i \cap \mathcal{C}_j \subset \Sigma_g^h$ for any $i \neq j$, which implies $\dim \Sigma_g^h \geq n-2$. This contradicts the assertion $\dim \Sigma_g^h \leq d$, since $d \leq n-3$ by hypothesis. □

3.1. Estimates on the number of $\mathbb{F}_q$–rational points of deformed hypersurfaces

Let d, n, e be positive integers such that $1 \leq d \leq n-3$. In this section we shall estimate the number of $\mathbb{F}_q$-rational points of $V_g := V(R_g) \subset \mathbb{A}^n$, where R_g is defined as in (3.2), thus proving Theorem 1.1.

In what follows, we shall use an estimate on the number of $\mathbb{F}_q$–rational points of a projective hypersurface due to S. Ghorpade and G. Lachaud ([24]; see also [25]). In [24, Theorem 6.1], the authors prove that, for an absolutely irreducible $\mathbb{F}_q$–hypersurface $V \subset \mathbb{P}^{m+1}$ of degree $d \geq 2$ and singular locus of dimension at most $s \geq 0$, the number $|V(\mathbb{F}_q)|$ of $\mathbb{F}_q$–rational points of V satisfies the estimate:

$$\left||V(\mathbb{F}_q)| - p_m\right| \leq b'_{m-s-1,d}\, q^{\frac{m+s+1}{2}} + C_{s,m} q^{\frac{m+s}{2}}, \tag{3.8}$$

where $p_m := q^m + q^{m-1} + \cdots + 1$, $b'_{m,d}$ is the m–th primitive Betti number of any nonsingular hypersurface of $\mathbb{P}^{m+1}$ of degree d and $C_s(V) := \sum_{i=m-1}^{m-1+s} b_{i,\ell}(V) + \varepsilon_i$, where $b_{i,\ell}(V)$ denotes the i–th ℓ–adic Betti number of V for a prime ℓ different from $p := \mathrm{char}(\mathbb{F}_q)$ and $\varepsilon_i := 1$ for even i and $\varepsilon_i := 0$ for odd i. In [8], the authors combine the Katz inequality [27, Theorem 3] with the Adolphson–Sperber bound for hypersurfaces [3, Theorem 5.27] to obtain the following upper bound, which is slightly better than that for an arbitrary complete intersection ([24, Proposition 5.1]):

$$C_{s,m}(V) \leq 6(d+2)^{m+1}. \tag{3.9}$$

On the other hand, according to [24, Theorem 4.1 and Example 4.3], one has the following upper bound:

$$b'_{m,d} \leq \frac{d-1}{d}\left((d-1)^{m+1} - (-1)^{m+1}\right) \leq (d-1)^{m+1}. \tag{3.10}$$

Suppose that g defined as in (3.1). From Theorem 3.7 and Corollary 3.8, we know that $\mathrm{pcl}(V_g)$ is an absolutely irreducible hypersurface of degree $\delta = \deg(R_g)$ and singular locus of dimension at most d. Hence, from (3.8), (3.9) and (3.10) we have that:

$$\left||\mathrm{pcl}(V_g)(\mathbb{F}_q)| - p_{n-1}\right| \leq (\delta-1)^{n-d-1} q^{\frac{n+d}{2}} + 6(\delta+2)^n q^{\frac{n+d-1}{2}}. \tag{3.11}$$

Now, we estimate the number of $\mathbb{F}_q$–rational points of $V_g^\infty = \mathrm{pcl}(V_g) \cap \{X_0 = 0\}$. Note that $V_g^\infty = V(R_g^{\deg R_g})$ is a hypersurface of $\mathbb{P}^{n-1}$. Suppose that $e < \mathsf{wt}(f)$. The same arguments as in the proof of Proposition 3.6 shows that the dimension of the singular locus of V_g^∞ is at most $d-2$. Then, taking into account (3.8), the following estimate holds:

$$\left||V_g^\infty(\mathbb{F}_q)| - p_{n-2}\right| \leq (\delta-1)^{n-d} q^{\frac{n+d-3}{2}} + 6(\delta+2)^{n-1} q^{\frac{n+d-4}{2}}. \tag{3.12}$$

Observe that $|V_g(\mathbb{F}_q)| = |\mathrm{pcl}(V_g)(\mathbb{F}_q)| - |V_g^\infty(\mathbb{F}_q)|$. From (3.11) and (3.12), we have:

$$\begin{aligned}
\left||V_g(\mathbb{F}_q)| - q^{n-1}\right| \leq & \left||\mathrm{pcl}(V_g)(\mathbb{F}_q)| - p_{n-1}\right| + \left||V_g^\infty(\mathbb{F}_q)| - p_{n-2}\right| \\
\leq & (\delta-1)^{n-d-1} q^{\frac{n+d}{2}} + 6(\delta+2)^n q^{\frac{n+d-1}{2}} \\
& + (\delta-1)^{n-d} q^{\frac{n+d-3}{2}} + 6(\delta+2)^{n-1} q^{\frac{n+d-4}{2}} \\
\leq & (q^{3/2}+1) q^{\frac{n+d-4}{2}} \left((\delta-1)^{n-d} q^{1/2} + 6(\delta+2)^n\right).
\end{aligned}$$

Suppose now that $e = \mathsf{wt}(f)$. Also by the same arguments as in the proof of Proposition 3.6 the dimension of the singular locus of V_g^∞ is at most $d-1$. Then, taking into account (3.8), the following estimate holds:

$$\left||V_g^{\infty}(\mathbb{F}_q)| - p_{n-2}\right| \leq (\delta-1)^{n-d-1}q^{\frac{n+d-2}{2}} + 6(\delta+2)^{n-1}q^{\frac{n+d-3}{2}}. \tag{3.13}$$

From (3.11) and (3.13), we obtain that

$$\begin{aligned}\left||V_g(\mathbb{F}_q)| - q^{n-1}\right| \leq& \left||\mathrm{pcl}(V_g)(\mathbb{F}_q)| - p_{n-1}\right| + \left||V_g^{\infty}(\mathbb{F}_q)| - p_{n-2}\right| \\ \leq& (\delta-1)^{n-d-1}q^{\frac{n+d}{2}} + 6(\delta+2)^n q^{\frac{n+d-1}{2}} \\ &+ (\delta-1)^{n-d-1}q^{\frac{n+d-2}{2}} + 6(\delta+2)^{n-1}q^{\frac{n+d-3}{2}} \\ \leq& (q+1)q^{\frac{n+d-3}{2}}((\delta-1)^{n-d-1}q^{1/2} + 6(\delta+2)^n).\end{aligned}$$

Finally, if $e > \mathsf{wt}(f)$, and again from the proof of Proposition 3.6, we have that V_g^{∞} is a nonsingular variety. We can apply the following result due to P. Deligne (see, e.g., [19]): for a nonsingular ideal-theoretic complete intersection $V \subset \mathbb{P}^n$ defined over $\mathbb{F}_q$, of dimension r and multidegree $\mathbf{d} = (d_1, \ldots, d_n)$, the following estimate holds:

$$\left||V(\mathbb{F}_q)| - p_r\right| \leq b'_r(n, \mathbf{d})q^{r/2}, \tag{3.14}$$

where $b'_r(n, \mathbf{d})$ is the rth-primitive Betti number of any nonsingular complete intersection of $\mathbb{P}^n$ of dimension r and multidegree $\mathbf{d}$.

Thus

$$\left||V_g^{\infty}(\mathbb{F}_q)| - p_{n-2}\right| \leq (\delta-1)^{n-1}q^{(n-2)/2}. \tag{3.15}$$

From (3.11) and (3.15), we conclude that

$$\begin{aligned}\left||V_g(\mathbb{F}_q)| - q^{n-1}\right| \leq& \left||\mathrm{pcl}(V_g)(\mathbb{F}_q)| - p_{n-1}\right| + \left||V_g^{\infty}(\mathbb{F}_q)| - p_{n-2}\right| \\ \leq& (\delta-1)^{n-d-1}q^{\frac{n+d}{2}} + 6(\delta+2)^n q^{\frac{n+d-1}{2}} \\ &+ (\delta-1)^{n-1}q^{(n-2)/2} \\ \leq& q^{\frac{n-2}{2}}\left(((\delta-1)^{n-d-1}q^{1/2} + 6(\delta+2)^n)q^{(d+1)/2} + (\delta-1)^{n-1}\right).\end{aligned}$$

Now, if $g \in \mathbb{F}_q$, observe that $\mathrm{pcl}(V_g) \subset \mathbb{P}^n$ has degree $\delta = \deg(R_g)$ and, from Theorem 3.7, its singular locus has dimension at most $d-1$. Hence, from (3.8), we obtain:

$$\left||\mathrm{pcl}(V_g)(\mathbb{F}_q)| - p_{n-1}\right| \leq (\delta-1)^{n-d}q^{\frac{n+d-1}{2}} + 6(\delta+2)^n q^{\frac{n+d-2}{2}}. \tag{3.16}$$

On the other hand, $V_g^{\infty} = V(R_g^{\deg R_g})$ is a hypersurface of $\mathbb{P}^{n-1}$. As before, the same arguments of Proposition 3.6 give us that the dimension of the singular locus of V_g^{∞} is at most $d-2$. Then taking into account (3.8), the following estimate holds:

$$\left||V_g^{\infty}(\mathbb{F}_q)| - p_{n-2}\right| \leq (\delta-1)^{n-d}q^{\frac{n+d-3}{2}} + 6(\delta+2)^{n-1}q^{\frac{n+d-4}{2}}. \tag{3.17}$$

From (3.16) and (3.17), we conclude that

$$\begin{aligned}\big||V_g(\mathbb{F}_q)| - q^{n-1}\big| \leq & \big||\mathrm{pcl}(V_g)(\mathbb{F}_q)| - p_{n-1}\big| + \big||V_g^{\infty}(\mathbb{F}_q)| - p_{n-2}\big| \\ \leq & (\delta-1)^{n-d} q^{\frac{n+d-1}{2}} + 6(\delta+2)^n q^{\frac{n+d-2}{2}} \\ & + (\delta-1)^{n-d} q^{\frac{n+d-3}{2}} + 6(\delta+2)^{n-1} q^{\frac{n+d-4}{2}} \\ \leq & (q+1) q^{\frac{n+d-4}{2}} ((\delta-1)^{n-d} q^{1/2} + 6(\delta+2)^n).\end{aligned}$$

All this previous discussion settles Theorem 1.1

Remark 3.9. We can provide another estimate for the case when g_1 of the definition (3.1) is identically zero and R_g is an homogeneous polynomial. In this case, $V_g \subset \mathbb{P}^{n-1}$ is also a projective variety with singular locus of dimension at most $d-1$. Indeed, the same arguments as in the proof of Theorem 3.4 imply that the set of $\mathbf{x} \in \mathbb{A}^n$ such that $\nabla R_g(\mathbf{x}) = 0$ defines an affine cone of dimension at most d. Hence, the set of $\mathbf{x} \in \mathbb{P}^{n-1}$ for which $\nabla R_g(\mathbf{x}) = 0$ has dimension at most $d-1$. Thus, from (3.8), we have that

$$\big|\overline{N}_g - p_{n-2}\big| \leq (\delta-1)^{n-d-1} q^{(n+d-2)/2} + 6(\delta+2)^n q^{(n+d-3)/2},$$

where $\overline{N}_g$ denotes the number of $\mathbb{F}_q$–rational projective points of V_g. Since $|V_g(\mathbb{F}_q)| = \overline{N}_g(q-1)+1$ we conclude that

$$\big||V_g(\mathbb{F}_q)| - q^{n-1}\big| \leq (q-1)\Big((\delta-1)^{n-d-1} q^{(n+d-2)/2} + 6(\delta+2)^n q^{(n+d-3)/2}\Big).$$

Note that the order of the error terms in either case $g_1 = 0$ or $g_1 \neq 0$ is the same.

Remark 3.10. It is easy to prove that if $g = 0$ and R_0 is an homogeneous polynomial then the singular locus of $V_0 \subset \mathbb{P}^{n-1}$ has dimension at most $d-2$. Hence we have the following estimate:

$$\big||V_0(\mathbb{F}_q)| - q^{n-1}\big| \leq (q-1)\Big((\delta-1)^{n-d-1} q^{(n+d-3)/2} + 6(\delta+2)^{n-1} q^{(n+d-4)/2}\Big).$$

3.2. f is a linear polynomial

Let $e, n, m_1, \ldots, m_d$ be positive integers with $n \geq 3$, assume that $\mathrm{char}(\mathbb{F}_q)$ does not divide $e, m_1, \ldots, m_d$ and $2 \leq m_1 < \cdots < m_d$. For a linear polynomial f we can obtain better results. Indeed, we can improve Theorem 1.1 by studying the geometric properties of the deformed hypersurfaces in more detail. Let $f = b_1 Y_1 + \cdots + b_d Y_d + a \in \mathbb{F}_q[Y_1, \ldots, Y_d]$ be a nonzero linear polynomial. In the following result we obtain an upper bound of the dimension of Σ_g in this case.

Proposition 3.11. *$V_g \subset \mathbb{A}^n$ is nonsingular or $\dim \Sigma_g = 0$.*

Proof. Suppose first that g is defined as in (3.1) and let $\mathbf{x} \in \Sigma_g$. Then

$$\nabla R_g(\mathbf{x}) = (b_1, \ldots, b_d) \cdot A(\mathbf{x}) + e \cdot (x_1^{e-1}, \ldots, x_n^{e-1}) + \nabla g_1(\mathbf{x}) = \mathbf{0},$$

where $A(\mathbf{x})$ is defined in (3.5). Thus we have the following n equations:

$$Q_j := b_1 m_1 X_j^{m_1-1} + \cdots + b_d m_d X_j^{m_d-1} + eX_j^{e-1} + \frac{\partial g_1}{\partial X_j} = 0,\ 1 \leq j \leq n.$$

Consider the graded lexicographic order of $\mathbb{F}_q[X_1, \ldots, X_n]$ with $X_n > X_{n-1} > \cdots > X_1$. For each $1 \leq j \leq n$, $Lt(Q_j)$ satisfies:

- $Lt(Q_j) = b_i m_i X_j^{m_i-1}$ if $e < m_i$,
- $Lt(Q_j) = b_i m_i X_j^{m_i-1} + eX_j^{e-1}$ if $e = m_i$,
- $Lt(Q_j) = eX_j^{e-1}$ if $e > m_i$,

where $m_i := \max\{m_k, b_k \neq 0, 1 \leq k \leq n\}$. With this monomial order, the leading terms are relatively prime and thus they form a Gröbner basis of the ideal J that they generate. Hence, the initial of the ideal J is generated by $Lt(Q_1), \ldots, Lt(Q_n)$, which form a regular sequence of $\mathbb{F}_q[X_1, \ldots, X_n]$. Therefore, by [21, Proposition 15.15] the polynomials $Q_1, \ldots, Q_n$ form a regular sequence of $\mathbb{F}_q[X_1, \ldots, X_n]$. Thus, we deduce that Σ_g has dimension at most 0.

The case for $g \in \mathbb{F}_q$ follows analogously. □

Corollary 3.12. $\mathrm{pcl}(V_g) \subset \mathbb{P}^n$ *has no singular points at infinity.*

Proof. Suppose that g is defined as in (3.1) and consider $\Sigma_g^\infty \subset \mathbb{P}^n$. From Lemma 3.5, we have that:

- $R_g^h(0, X_1, \ldots, X_n) = f^{\mathsf{wt}}(P_{m_1}, \ldots, P_{m_d})$, if $e < \mathsf{wt}(f)$,
- $R_g^h(0, X_1, \ldots, X_n) = f^{\mathsf{wt}}(P_{m_1}, \ldots, P_{m_d}) + X_1^e + \cdots + X_n^e$, if $e = \mathsf{wt}(f)$,
- $R_g^h(0, X_1, \ldots, X_n) = X_1^e + \cdots + X_n^e$, if $e > \mathsf{wt}(f)$.

On the other hand, if $g \in \mathbb{F}_q$ then $R_g^h(0, X_1, \ldots, X_n) = f^{\mathsf{wt}}(P_{m_1}, \ldots, P_{m_d})$. Observe that $f^{\mathsf{wt}} = b_i Y_i$ where $b_i := \max\{b_k, b_k \neq 0, 1 \leq k \leq n\}$. Following the proof of Proposition 3.11 we deduce that $\Sigma_g^\infty \subset \mathbb{A}^n$ has dimension at most 0. Thus, $\mathrm{pcl}(V_g) \subset \mathbb{P}^n$ has no singular points at infinity. □

From Proposition 3.11 and Corollary 3.12 we conclude the following result.

Theorem 3.13. *Let $n \geq 3$. Let $f \in \mathbb{F}_q[Y_1, \ldots, Y_d]$ be a linear polynomial and $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ defined as in (3.1) or $g \in \mathbb{F}_q$. Then $\mathrm{pcl}(V_g) \subset \mathbb{P}^n$ has singular locus of dimension at most 0.*

From Theorem 3.13 and following the proof of Corollary 3.8, we obtain:

Corollary 3.14. *The hypersurface V_g is absolutely irreducible.*

We arrive at the following result concerning the number of $\mathbb{F}_q$-rational points of the variety V_g for a linear polynomial f.

Theorem 3.15. *Let $n \geq 3$. Let $m_1, \ldots, m_d$ be positive integer with $2 \leq m_1 < \cdots < m_d$. We assume that $\mathrm{char}(\mathbb{F}_q)$ does not divide e and m_j for all $1 \leq j \leq d$. Let $R_g = f(P_{m_1}, \ldots, P_{m_d}) + g$ with $f = b_1Y_1 + \cdots + b_dY_d + a$ and $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree e and g is defined as in (3.1) or $g \in \mathbb{F}_q$. Then,*

$$\big||V_g(\mathbb{F}_q)| - q^{n-1}\big| \leq q^{(n-1)/2}\big(2(m_i-1)^{n-1}q^{1/2} + 6(m_i+2)^n\big),$$

where $m_i := \max\{m_k,\, b_k \neq 0,\, 1 \leq k \leq n\}$.

Proof. From Theorem 3.13, Corollary 3.14 and the estimate (3.8), we have

$$\big||\mathrm{pcl}(V_g)(\mathbb{F}_q))| - p_{n-1}\big| \leq (m_i-1)^{n-1}q^{n/2} + 6(m_i+2)^n q^{(n-1)/2}. \tag{3.18}$$

Now, we estimate the number of $\mathbb{F}_q$-rational points of $V_g^\infty := \mathrm{pcl}(V_g) \cap \{X_0 = 0\} \subset \mathbb{P}^{n-1}$. Note that $V_g^\infty = V(R_g^{\deg R_g})$ is a hypersurface of $\mathbb{P}^{n-1}$ of dimension $n-2$. Following the proof of Corollary 3.12 we deduce that V_g^∞ is nonsingular variety of degree $\deg(R_g) = m_i$. Then, from (3.14):

$$||V_g^\infty(\mathbb{F}_q)| - p_{n-2}| \leq (m_i-1)^{n-1}q^{(n-2)/2}. \tag{3.19}$$

From (3.18) and (3.19), we conclude that

$$\begin{aligned}\big||V_g(\mathbb{F}_q)| - q^{n-1}\big| \leq& \big||\mathrm{pcl}(V_g)(\mathbb{F}_q)| - p_{n-1}\big| + \big||V_g^\infty(\mathbb{F}_q)| - p_{n-2}\big| \\ \leq& (m_i-1)^{n-1}q^{n/2} + 6(m_i+2)^n q^{(n-1)/2} + (m_i-1)^{n-1}q^{(n-2)/2} \\ \leq& q^{(n-1)/2}\big(2(m_i-1)^{n-1}q^{1/2} + 6(m_i+2)^n\big). \quad \square\end{aligned}$$

Remark 3.16. Note that Theorem 3.15 improves Theorem 1.1 when f is a nonzero linear polynomial. Indeed, the estimate of Theorem 3.15 does not depend on d, the number of m_j-power sum polynomials in which f is evaluated. Concretely, from Theorem 1.1 we have that $|V_g(\mathbb{F}_q)| = q^{n-1} + \mathcal{O}(q^{(n+d)/2})$, while Theorem 3.15 implies $|V_g(\mathbb{F}_q)| = q^{n-1} + \mathcal{O}(q^{n/2})$.

Remark 3.17. Suppose that the polynomial g_1 of the definition (3.1) is identically zero and R_g is an homogeneous polynomial. Then $R_g = c(X_1^e + \cdots + X_n^e)$ for some $c \in \mathbb{F}_q$ and $V_g \subset \mathbb{P}^{n-1}$. It is easy to see that the set of $\{\mathbf{x} \in \mathbb{A}^n :\ \nabla R_g(\mathbf{x}) = 0\} = \{\mathbf{0}\}$, from where V_g is a nonsingular variety. Thus, from (3.14):

$$\big|\overline{N}_g - p_{n-2}\big| \leq (e-1)^{n-1}q^{(n-2)/2},$$

where $\overline{N}_g$ is the number of $\mathbb{F}_q$–rational projective points of V_g. As in Remark 3.9, we conclude that

$$\left||V_g(\mathbb{F}_q)| - q^{n-1}\right| \leq (e-1)^{n-1}q^{(n-2)/2}(q-1).$$

Remark 3.18. Suppose that $g = 0$ and R_0 is an homogeneous polynomial. Then $R_0 = c(X_1^m + \cdots + X_n^m)$ with $c \in \mathbb{F}_q$. Following the arguments of the above remark, it can be shown that

$$\left||V_0(\mathbb{F}_q)| - q^{n-1}\right| \leq (m-1)^{n-1}q^{(n-2)/2}(q-1).$$

4. Special deformed hypersurfaces

In this section we follow the same methodology to obtain estimates of $\mathbb{F}_q$–solutions of some well known equations over finite fields. These results are not obtained directly from applying Theorem 1.1 since we can take advantage of the properties of the polynomial f under consideration for these particular cases.

4.1. Deformed diagonal equations over a finite field

Let m, n be positive integers such that $n \geq 3$ and $m \geq 2$ is not divisible by $\mathrm{char}(\mathbb{F}_q)$ and let $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ with $\deg(g) < m$. Consider the equation:

$$c_1X_1^m + \cdots + c_nX_n^m + g(X_1, \ldots, X_n) = 0, \tag{4.1}$$

where $c_i \in \mathbb{F}_q \setminus \{0\}$, $1 \leq i \leq n$. We denote by N_g the number of $\mathbb{F}_q$–rational solutions of (4.1). Let $R_g := c_1X_1^m + \cdots + c_nX_n^m + g(X_1, \ldots, X_n)$ and let $V_g \subset \mathbb{A}^n$ be defined by $V_g = V(R_g)$. In this case, $\mathbf{x} \in \Sigma_g$ satisfies

$$R_g = 0, \quad c_jmX_j^{m-1} + \frac{\partial g}{\partial X_j} = 0, \quad 1 \leq j \leq n.$$

Following the same arguments used to prove Proposition 3.11, Corollaries 3.12 and 3.14 and Theorems 3.13 and 3.15 we can deduce the following result.

Theorem 4.1. *With the hypotheses as above, we have that*

$$|N_g - q^{n-1}| \leq q^{(n-1)/2}\big(2(m-1)^{n-1}q^{1/2} + 6(m+2)^n\big). \tag{4.2}$$

Observe that in [2] the authors use the Newton polyhedra to prove a result that allows one to obtain an estimate on the number of $\mathbb{F}_q$-solution of a deformed diagonal equation. This result holds under some hypotheses for g, which are not present in Theorem 4.1.

Theorem 4.2. *Let $q > (m+2)^{\frac{2n}{n-2}}$ and $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree less than m. Assume that* $\mathrm{char}(\mathbb{F}_q)$ *does not divide m. Then, the equation $c_1X_1^m + \cdots + c_nX_n^m + g(X_1, \ldots, X_n) = 0$, has at least one solution in $\mathbb{F}_q^n$.*

Proof. Observe that if $q > 144$ then $6(m+2)^n < 1/2(m+2)^n q^{1/2}$. On the other hand, we have that $2(m-1)^{n-1} < 1/2(m+2)^n$. Then, from (4.2) we deduce that

$$|N_g - q^{n-1}| \leq q^{n/2}(m+2)^n,$$

from where

$$N_g \geq q^{n-1} - q^{n/2}(m+2)^n. \tag{4.3}$$

Therefore, the equation $R_g = c_1X_1^m + \cdots + c_nX_n^m + g(X_1, \cdots, X_n) = 0$ has at least one solution in $\mathbb{F}_q^n$ if the right-hand side of (4.3) is a positive number. The result follows. □

Remark 4.3. Note that if $q > (m+2)^2$ then $n > \frac{2\log(q)}{\log(\frac{q}{(m+2)^2})}$. Observe that $E(q) = \frac{2\log(q)}{\log(\frac{q}{(m+2)^2})}$ is a decreasing function and $\lim_{q\to\infty} E(q) = 2$. Hence, for q sufficiently large, the equation (4.1) has at least one solution in $\mathbb{F}_q^n$, $n > 2$.

Carlitz [11] showed that if $m = n$, m divides $\mathrm{char}(\mathbb{F}_q) - 1$ and $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ is of degree less than m, then $R_g = 0$ has at least one solution in $\mathbb{F}_q^n$. This result was extended by Felszeghy [22], who proved that $R_g = 0$ has at least one solution in $\mathbb{F}_q^n$ if $q = p := \mathrm{char}(\mathbb{F}_q)$ and

$$n \geq \left\lceil \frac{p-1}{\lfloor \frac{p-1}{m} \rfloor} \right\rceil. \tag{4.4}$$

He also shows that if m divides $p-1$ and $n \geq m$, then $R_g = 0$ is solvable in $\mathbb{F}_q^n$.

Theorem 4.2 improves (4.4) in several aspects. Indeed, on one hand, our result holds for any q such that $\mathrm{char}(\mathbb{F}_q)$ does not divide m while (4.4) holds if $q = p$. On the other hand, we prove that if $q > (m+2)^2$ then (4.1) has at least a $\mathbb{F}_q$-rational solution for $n \geq 3$ while Felszeghy's result requires $p \geq m+1$ and $n \geq m+1$. In particular, if $p > (m+2)^2$ we can guarantee the existence of at least one $\mathbb{F}_p$-rational solution for any $n \geq 3$ instead of $n \geq m+1$.

Remark 4.4. For $b \in \mathbb{F}_q$ consider the following diagonal equation:

$$c_1X_1^m + \cdots + c_nX_n^m = b.$$

If $b = 0$ then Theorem 3.15 gives us

$$\left|N_0(\mathbb{F}_q) - q^{n-1}\right| \leq (m-1)^{n-1}q^{(n-2)/2}(q-1),$$

which is of similar order to the results in the literature (see, e.g., [30, Chapter 6, §3]). Suppose then $b \neq 0$. From (4.2), we have that $N_b = q^{n-1} + \mathcal{O}(q^{n/2})$, but this estimate can be improved. Indeed, it can be shown that the singular locus Σ_b of the affine variety $V(R_b)$ defined by $R_b = c_1X_1^m + \cdots + c_nX_n^m - b$ is $\Sigma_b = \{0\}$. Hence, the projective variety $\mathrm{pcl}(V(R_b))$ is nonsingular and, from (3.14), we have

$$|N_b - q^{n-1}| \leq (m-1)^n q^{(n-2)/2}(1 + q^{1/2}).$$

Observe that this result is Weil's estimate for diagonal equations (see, e.g., [30, Chapter 6, §3]).

4.2. Generalized Markoff-Hurwitz-type equations

Let $m, n, k_1, \ldots, k_n$ be positive integers, $n \geq 3$ and $m \geq 2$, $a, b \in \mathbb{F}_q$ and $a_i \in \mathbb{F}_q \setminus \{0\}$, $1 \leq i \leq n$. Consider the equation

$$a_1X_1^m + \cdots + a_nX_n^m + a = bX_1^{k_1} \ldots X_n^{k_n}. \tag{4.5}$$

Observe that this is an special case of deformed diagonal equations. Denote by N the number of $\mathbb{F}_q$–rational solutions of (4.5). Suppose that $\mathrm{char}(\mathbb{F}_q)$ does not divide m. Let $R_g := a_1X_1^m + \cdots + a_nX_n^m + g$, where $g = a - bX_1^{k_1} \cdots X_n^{k_n}$ and $k_1 + \cdots + k_n < m$. From Theorem 4.1 we obtain the following result.

Theorem 4.5. *With the same hypotheses as above, N satisfies the following estimate:*

$$\left|N - q^{n-1}\right| \leq q^{(n-1)/2}\left(2(m-1)^{n-1}q^{1/2} + 6(m+2)^n\right).$$

In what follows we obtain sufficient conditions for the existence of a $\mathbb{F}_q$–rational solution with nonzero coordinates. We shall need the following estimate on the number of $\mathbb{F}_q$–rational solutions of (4.5) with i coordinates equal to zero. We denote this number by N_i.

Proposition 4.6. *With the same hypotheses as above, the number N_i satisfies the following estimate:*

If $a = 0$ and $i = 1, \ldots, n-2$, then

$$|N_i - q^{n-i-1}| \leq (m-1)^{n-i-1}q^{(n-i-2)/2}(q-1). \tag{4.6}$$

If $a \neq 0$ and $i = 1, \ldots, n-1$, then

$$|N_i - q^{n-i-1}| \leq (m-1)^{n-i}q^{(n-i-2)/2}(1 + q^{1/2}) \tag{4.7}$$

Proof. Follows from (4.5) and Remark 4.4. □

Let N^* be the number of $\mathbb{F}_q$-rational solutions of (4.5) with nonzero coordinates and let $N^=$ be the number of $\mathbb{F}_q$-rational solutions of (4.5) with at least one coordinate equal to zero. Note that $N^* = N - N^=$. By the inclusion-exclusion principle we obtain

$$N^= = \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} N_i. \tag{4.8}$$

Suppose that $a \neq 0$. From (4.8) and since $N_n = 0$, we have

$$\begin{aligned} N^* - \frac{(q-1)^n}{q} &= N - N^= - \sum_{i=0}^{n} (-1)^i \binom{n}{i} q^{n-i-1} \\ &= N - \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} N_i - \sum_{i=0}^{n} (-1)^i \binom{n}{i} q^{n-i-1} \\ &= N - q^{n-1} + \sum_{i=1}^{n-1} (-1)^i \binom{n}{i} (N_i - q^{n-i-1}) + (-1)^n (N_n - q^{-1}) \\ &= (N - q^{n-1}) + \sum_{i=1}^{n-1} (-1)^i \binom{n}{i} (N_i - q^{n-i-1}) - (-1)^n \frac{1}{q}. \end{aligned}$$

Thus, we deduce that

$$N^* - \frac{(q-1)^n - (-1)^n}{q} = (N - q^{n-1}) + \sum_{i=1}^{n-1} (-1)^i \binom{n}{i} (N_i - q^{n-i-1}).$$

Therefore, from Theorem 4.5 and (4.7):

$$\begin{aligned} \left| N^* - \frac{(q-1)^n - (-1)^n}{q} \right| &\leq |N - q^{n-1}| + \sum_{i=1}^{n-1} \binom{n}{i} |N_i - q^{n-i-1}| \\ &\leq 6(2m)^n q^{n/2} + 2m^{n-1} \sum_{i=1}^{n-1} \binom{n}{i} q^{(n-i-1)/2} \\ &\leq 6(2m)^n q^{n/2} + 2m^{n-1} \frac{(\sqrt{q}+1)^n - \sqrt{q}^n - 1}{\sqrt{q}} \\ &\leq 6(2m)^n q^{n/2} + \frac{2}{m} (2m)^n q^{\frac{n-1}{2}} \\ &\leq 6(2m)^n q^{n/2} + (2m)^n q^{n/2} \\ &\leq 7(2m)^n q^{n/2}. \end{aligned}$$

We have proved the following result.

Proposition 4.7. *With the hypotheses as above, the number N^* of $\mathbb{F}_q$–rational solutions of (4.5) with nonzero coordinates satisfies the following estimate:*

$$\left|N^* - \frac{(q-1)^n - (-1)^n}{q}\right| \leq 7(2m)^n q^{n/2}.$$

In [34] Mordell studies the following equation:

$$(a_1 X_1^{m_1} + \cdots + a_n X_n^{m_n} + a)^k = b X_1^{k_1} \cdots X_n^{k_n},$$

where $a_1, \ldots, a_n, a$ are nonzero elements of $\mathbb{F}_q$, $k, m_1, \ldots, m_n \in \mathbb{N}$, $k_1, \ldots, k_n$ are non-negative integers and $n \geq 2$. The author shows that if $k_1 = \cdots = k_n = 1$ and $q = p$ then

$$\left|N^* - \frac{(q-1)^n}{q}\right| \leq d_1 \cdots d_n q^{n/2}, \tag{4.9}$$

where $d_i = \gcd(m_i, q-1)$. Observe that Proposition 4.7 improves (4.9) when $k = 1$ and $m = m_1 = \cdots = m_n$. Indeed, our result holds for all q with $\mathrm{char}(\mathbb{F}_q)$ not dividing m and $m > k_1 + \cdots + k_n$. Moreover, we determine one more term in the asymptotic development in terms of q. Namely, we prove $N^* = \frac{(q-1)^n - (-1)^n}{q} + \mathcal{O}(q^{n/2})$ instead of $N^* = \frac{(q-1)^n}{q} + \mathcal{O}(q^{n/2})$. Observe that this term appears in the asymptotic development of N^* when $a = 0$ (see, e.g., [4, Theorem 3.1]). Now, we provide an existence result for $\mathbb{F}_q$–rational solutions with nonzero coordinates. From Proposition 4.7 we deduce that

$$\begin{aligned}
N^* &\geq \frac{(q-1)^n - (-1)^n}{q} - 7(2m)^n q^{n/2} \\
&\geq \frac{(q-1)^n}{2q} - 7(2m)^n q^{n/2} \\
&\geq q^{(n-2)/2}(2m)^n \Big(\frac{(q-1)^n}{2(2m)^n q^{n/2}} - 7q \Big) \\
&\geq q^{(n-2)/2}(2m)^n \Big(\frac{1}{2(2m)^n} \big(\frac{(q-1)^2}{q} \big)^{n/2} - 7q \Big) \\
&\geq q^{(n-2)/2}(2m)^n \Big(\frac{(q-2)^{n/2}}{2(4m^2)^{n/2}} - 7q \Big)
\end{aligned}$$

From Bernoulli's inequality we obtain

$$N^* \geq q^{(n-2)/2}(2m)^n \Big(\frac{n}{4} \Big(\frac{q-2-4m^2}{4m^2} \Big) - 7q \Big)$$

Therefore, (4.5) has at least one solution in $\mathbb{F}_q^n$ with nonzero coordinates if

$$\frac{n}{4} \Big(\frac{q-2-4m^2}{4m^2} \Big) - 7q > 0.$$

That is,

$$n(q-2-4m^2)-112m^2q>0,$$

which is equivalent to

$$(q-2-4m^2)(n-112m^2)-112m^2(2+4m^2)>0.$$

We conclude that if $n>112m^2$ the equation (4.5) has at least a solution in $(\mathbb{F}_q^*)^n$ for

$$q>\frac{112m^2(2+4m^2)}{n-112m^2}+2+4m^2.$$

We have proved:

Proposition 4.8. *If* $q>\frac{112m^2(2+4m^2)}{n-112m^2}+2+4m^2$, $\mathrm{char}(\mathbb{F}_q)$ *does not divide* m *and* $n>112m^2$ *then the equation* (4.5) *has at least one solution in* $(\mathbb{F}_q^*)^n$ *for the case* $a\neq 0$.

Remark 4.9. It can be shown that if $q>(2m)^{\frac{2n}{n-4}}$, $m\geq 3$ and $n\geq 5$, then the equation (4.5) has at least one solution in $(\mathbb{F}_q^*)^n$. This existence result holds for far more values of n although it requires larger values of q.

Remark 4.10. Suppose that $a=0$. With the same hypotheses and arguments of Theorem 4.5 and taking into account (4.6), we deduce that the number N^* of $\mathbb{F}_q$–rational solutions of (4.5) with nonzero coordinates satisfies the following estimate:

$$\left|N^*-\frac{(q-1)^n}{q}-(-1)^n(n+1-\frac{1}{q})\right|\leq 7(2m)^nq^{n/2}. \tag{4.10}$$

For $a=0$, $k_1=\cdots=k_n=1$, $n\geq 2$ and $1\leq m\leq q-1$, Baoulina [4] shows that

$$\left|N^*-\frac{(q-1)^n-(-1)^n}{q}\right|\leq (d_0d_1^{n-1}-1)q^{(n-1)/2}+(d-d_0)d_1^{n-1}q^{(n-2)/2}, \tag{4.11}$$

where $d_1=\gcd(m,q-1)$, $d=\gcd(n-km,\frac{q-1}{d_1})$ and $d_0=\gcd(d,k)$. Although (4.11) is better than (4.10) when $k_1=\cdots=k_n=1$, our estimate extends (4.11) for the case $k_1+\cdots+k_n<m$. Moreover, we determine one more term in the asymptotic development of N^* in terms of q, namely $N^*=\frac{(q-1)^n-(-1)^n}{q}+(-1)^n(n+1)+\mathcal{O}(q^{n/2})$.

4.3. Carlitz's equations

Let d,n be positive integers with $d\geq 2$ and $n\geq 3$. Let $h_i=a_{d,i}T^d+\cdots+a_{0,i}\in\mathbb{F}_q[T]$, with $\deg(h_i)=d$, $1\leq i\leq n$. Let $g\in\mathbb{F}_q[X_1,\ldots,X_n]$ such that $\deg(g)<d$. Suppose that $\mathrm{char}(\mathbb{F}_q)$ does not divide d. Carlitz's equations are:

$$h_1(X_1) + \cdots + h_n(X_n) = g. \tag{4.12}$$

Denote by N the number of $\mathbb{F}_q$-rational solutions of (4.12). Let R_g, V_g and Σ_g be defined as usual. A given $\mathbf{x} \in \Sigma_g$ satisfies the following equations:

$$Q_j := h_j'(X_j) - \frac{\partial g}{\partial X_j} = 0, \ \ 1 \leq j \leq n.$$

By the same arguments as before we can show that Q_j, $1 \leq j \leq n$, form a regular sequence of $\mathbb{F}_q[X_1, \ldots, X_n]$ and $\mathrm{pcl}(V_g)$ has no singular points at infinity. Thus, we obtain the following result.

Theorem 4.11. *Let $n \geq 3$ and $d \geq 2$ not divisible by $\mathrm{char}(\mathbb{F}_q)$. Then the singular locus of $\mathrm{pcl}(V_g)$ has dimension at most 0 and V_g is absolutely irreducible.*

Following the same reasoning as in the proof of Theorem 3.15 we conclude:

Theorem 4.12. *Let $n \geq 3$ and $d \geq 2$ not divisible by $\mathrm{char}(\mathbb{F}_q)$. Then*

$$\left|N - q^{n-1}\right| \leq q^{(n-1)/2}\left(2(d-1)^{n-1}q^{1/2} + 6(d+2)^n\right).$$

Remark 4.13. Observe that for $h_1 = \cdots = h_n = h$ then the equation (4.12) can be written as

$$a_1 P_1 + \cdots + a_d P_d + n a_0 = g.$$

Thus, (4.12) can be expressed as $f(P_1, \ldots, P_d) + n a_0 = g$, where $f \in \mathbb{F}_q[Y_1, \ldots, Y_d]$ is the linear polynomial $f := a_1 Y_1 + \cdots + a_d Y_d$. We can then apply Theorem 3.15 to obtain a similar result as the one in the previous theorem.

Carlitz [10] studies the number of $\mathbb{F}_q$–rational solutions of the equation

$$h_1(X_1) + \cdots + h_n(X_n) = \alpha,$$

where $h_i \in \mathbb{F}_q[T]$ with $2 < \deg(h_i) = k_i < \mathrm{char}(\mathbb{F}_q)$ and $\alpha \in \mathbb{F}_q$. More precisely, he proves that the number N of $\mathbb{F}_q$-rational solutions of this equation is given by

$$N = q^{n-1} + \mathcal{O}(q^{n-w}), \tag{4.13}$$

where $w = \frac{1}{k_1} + \cdots + \frac{1}{k_n}$ and the constant implied by the $\mathcal{O}$ is not explicitly given. Theorem 4.12 improves (4.13) in several aspects if $\deg(h_i) = d$, $1 \leq i \leq n$. On one hand, Theorem 4.12 gives an explicit estimate on the number N. On the other hand,

the equation can be matched to a non-necessarily constant polynomial. Finally, our result implies $N = q^{n-1} + \mathcal{O}(q^{n/2})$ while (4.13) implies that $N = q^{n-1} + \mathcal{O}(q^{n-w}) = q^{n-1} + \mathcal{O}(q^{n/2+\epsilon})$, where $\epsilon = n(\frac{1}{2} - \frac{1}{d}) > 0$ if $d > 2$ and $w = \frac{n}{d}$.

Regarding existence results, Carlitz [11] shows that if $\deg(h_i) = n$, $1 \leq i \leq n$ and n divides $\mathrm{char}(\mathbb{F}_q) - 1$, then (4.12) has at least one solution in $\mathbb{F}_q^n$. From Theorem 4.12 we can find conditions which imply that (4.12) has at least one solution in $\mathbb{F}_q^n$ when $d \geq 2$ and $n \geq 3$.

Theorem 4.14. *Let $q > (d+2)^{\frac{2n}{(n-2)}}$, $d \geq 2$ not divisible by $\mathrm{char}(\mathbb{F}_q)$ and $n \geq 3$. Let $h_i \in \mathbb{F}_q[T]$ be defined by $h_i = a_{d,i}T^d + \cdots + a_{0,i}$, $1 \leq i \leq n$, with $\deg(h_i) = d$ and $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ with $\deg(g) < d$. Then the equation $h_1(X_1) + \cdots + h_n(X_n) = g$ has at least one solution in $\mathbb{F}_q^n$.*

Remark 4.15. Theorem 4.12 provides an upper bound of Waring's number for univariate polynomials over $\mathbb{F}_q$. Waring's problem consists in finding the minimum number of variables such that the equation $X_1^d + \cdots + X_n^d = \beta$ has solutions for any natural number β. This minimum number is called the *Waring's number associated to d*. The Waring's problem has also been considered for equations over finite fields and there are many bounds for their Waring number (see, e. g., [35, Chapter 13]).

Consider the following generalization of Waring's problem: given a polynomial $h \in \mathbb{F}_q[T]$ of degree d, find the minimum number of variables such that

$$h(X_1) + \cdots + h(X_n) = \beta \tag{4.14}$$

has a solution in $\mathbb{F}_q^n$ for any $\beta \in \mathbb{F}_q$. We denote this number by $\gamma(h, q)$. Carlitz [12] proves that if q is a prime number then $\gamma(h, q) \leq d$ whenever $d \neq p-1, \frac{p-1}{2}$. On the other hand, Castro et. al. [13] obtain an upper bound on $\gamma(h, q)$ for polynomials of the form $h = aT^d + g \in \mathbb{F}_q[T]$, where $d \neq 1$ divides $p-1$ and g satisfies certain hypothesis related to p-weight degree of g.

Let N be the number of $\mathbb{F}_q$–rational solutions of equation (4.14). Suppose that $d \geq 2$ and $n \geq 3$. From Theorem 4.12 we have that

$$\left|N - q^{n-1}\right| \leq q^{(n-1)/2}\left(2(d-1)^{n-1}q^{1/2} + 6(d+2)^n\right).$$

On one hand, $q > 144$ implies that $6(d+2)^n < 1/2(d+2)^n q^{1/2}$. On the other hand, $2(d-1)^{n-1} < 1/2(d+2)^n$ holds. Thus, $N > 0$ provided that $q^{n/2}\left(q^{(n-2)/2} - (d+2)^n\right) > 0$; that is $q^{(n-2)/2} > (d+2)^n$. Now, if $q > (d+2)^2$ the condition $q^{(n-2)/2} > (d+2)^n$ is equivalent to

$$n > \frac{log(q^2)}{log(\frac{q}{(d+2)^2})}.$$

We conclude that if $n > \frac{log(q^2)}{log(\frac{q}{(d+2)^2})}$ then $\gamma(h,q) \leq \left\lceil \frac{log(q^2)}{log(\frac{q}{(d+2)^2})} \right\rceil$. On the other hand, if $q > (d+2)^{2(d-1)/(d-3)}$, then we obtain that $\left\lceil \frac{log(q^2)}{log(\frac{q}{(d+2)^2})} \right\rceil \leq d$. Thus, we have the following result.

Theorem 4.16. *Let $n \geq 3$ and $d \geq 4$. Assume that $\mathrm{char}(\mathbb{F}_q)$ does not divide d. For any $q > (d+2)^{2(d-1)/(d-3)}$ and any $h \in \mathbb{F}_q[T]$ of degree d, we have that*

$$\gamma(h,q) \leq \left\lceil \frac{log(q^2)}{log(\frac{q}{(d+2)^2})} \right\rceil$$

Note in particular that solutions with small number of variables require large values of q.

4.4. Equations in Dickson polynomials

Let $d \in \mathbb{N}$ and $a \in \mathbb{F}_q$. The Dickson polynomials over $\mathbb{F}_q$ of degree d with parameter a are:

$$D_d(X,a) = \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-a)^i X^{d-2i}.$$

Dickson polynomials have been extensively studied because they play very important roles in both theoretical work as well as in various applications (see, [35, Chapter 7]).

Let d, n be positive integers with $d \geq 2$ and $n \geq 3$ and assume that $\mathrm{char}(\mathbb{F}_q)$ does not divide d. Let $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ be such that $\deg(g) < d$. Consider the following polynomial equation

$$c_1 D_d(X_1, a_1) + \cdots + c_n D_d(X_n, a_n) = g, \tag{4.15}$$

where $a_1, \ldots, a_n \in \mathbb{F}_q$ and $c_1, \ldots, c_n \in \mathbb{F}_q \setminus \{0\}$. Observe that for $a_i = 0$ for $1 \leq i \leq n$, this is a deformed diagonal equation. Equation (4.15) is a particular case of Carlitz's equations defined in (4.12) for $h_i := c_i D_d(X_i, a_i)$. From Theorem 4.12 we have:

Theorem 4.17. *Let $n \geq 3$ and $d \geq 2$ not divisible by $\mathrm{char}(\mathbb{F}_q)$. Then*

$$\left| N - q^{n-1} \right| \leq q^{(n-1)/2} \left(2(d-1)^{n-1} q^{1/2} + 6(d+2)^n \right), \tag{4.16}$$

where N denotes the number of $\mathbb{F}_q$–rational solutions of (4.15).

Remark 4.18. Observe that if $a_1 = \cdots = a_n = a$ and $c_1 = \cdots = c_n = c$, then the equation (4.15) can be written as follows

$$\sum_{i=0}^{\lfloor d/2 \rfloor} b_i P_{d-2i} = g,$$

where $b_i = \frac{d}{d-i}\binom{d-i}{d}(-a)^i$ and $P_{d-2i} = X_1^{d-2i} + \cdots + X_n^{d-2i}$ for $0 \leq i \leq \lfloor d/2 \rfloor$. Thus, equation (4.15) can be expressed as

$$f(P_{d-2\lfloor d/2 \rfloor}, \ldots, P_d) = g,$$

where $f \in \mathbb{F}_q[Y_{d-2\lfloor d/2 \rfloor}, \ldots, Y_d]$ is the linear polynomial $f := \sum_{i=0}^{\lfloor d/2 \rfloor} b_i Y_{d-2i}$. Hence, applying Theorem 3.15 we obtain a similar result as the one in the previous theorem.

In [17] the authors study the number of $\mathbb{F}_q$–rational solutions of the equation

$$c_1 D_{d_1}(X_1, a_1) + \cdots + c_n D_{d_n}(X_n, a_n) = c,$$

where $d_1, \ldots, d_n$ are positive integers, $c_1, \ldots, c_n \in \mathbb{F}_q \setminus \{0\}$ and $c, a_1, \ldots, a_n \in \mathbb{F}_q$. More precisely, they prove that if $n, d_1, \ldots, d_n \geq 2$ and there exists $0 \leq t \leq n$ such that $a_1 = \cdots = a_t = 0$ and $a_j \neq 0$ for all $t < j \leq n$, then the number N of $\mathbb{F}_q$-rational solutions of these equations satisfies:

$$|N - q^{n-1}| \leq q^{(n-2)/2}(q-1)\prod_{j=1}^{t}(m_j - 1)\prod_{j=t+1}^{n}(m_j + l_j), \tag{4.17}$$

where $m_j = \gcd(d_j, q-1)$ and $l_j = \gcd(d_j, q+1)$ for $1 \leq j \leq n$. If $d_1 = \cdots = d_n = d$ then Theorem 4.17 extends the estimation in (4.17) in the sense that it holds for $c \in \mathbb{F}_q[X_1, \ldots, X_n]$ with $0 < \deg(c) < d$.

Finally, from Theorem 4.17 we derive conditions about the solvability of (4.15) in $\mathbb{F}_q^n$.

Theorem 4.19. *Let $q > \frac{4}{9}(d+2)^{\frac{2n}{(n-2)}}$, $d \geq 2$ not divisible by $\mathrm{char}(\mathbb{F}_q)$ and $n \geq 3$. Let $g \in [X_1, \ldots, X_n]$, $\deg(g) < d$. Then the equation*

$$c_1 D_d(X_1, a_1) + \cdots + c_n D_d(X_n, a_n) = g$$

has at least one solution in $\mathbb{F}_q^n$.

Proof. From (4.16), we have that

$$\left|N - q^{n-1}\right| \leq q^{(n-1)/2}\left(2(d-1)^{n-1}q^{1/2} + 6(d+2)^n\right).$$

Observe that if $q > 36^2$ then $6(d+2)^n < 1/6(d+2)^n q^{1/2}$. On the other hand, $2(d-1)^{n-1} < 1/2(d+2)^n$. Under this condition we have that

$$\left|N - q^{n-1}\right| \leq \frac{2}{3}q^{n/2}(d+2)^n.$$

Thus, N satisfies the following inequality:

$$N \geq q^{n-1} - \frac{2}{3}q^{n/2}(d+2)^n = q^{n/2}(q^{(n-2)/2} - \frac{2}{3}(d+2)^n). \tag{4.18}$$

We conclude that (4.15) has at least one solution in $\mathbb{F}_q^n$ if $q^{(n-2)/2} > \frac{2}{3}(d+2)^n$. □

Remark 4.20. Suppose that $d_1 = \cdots = d_n = d$. Observe that, when g is a constant, Theorem 4.19 gives similar conditions on q, d and n than [17, Theorem 11], under which there exists at least one $\mathbb{F}_q$–rational solution of (4.15). Theorem 4.19 extends [17] since it holds for a polynomial g of positive degree at most d.

Acknowledgments

The authors are pleased to thank Guillermo Matera for several valuable comments and suggestions.

References

[1] Y. Aubry, F. Rodier, Differentially 4-uniform functions, in: Arithmetic, Geometry, Cryptography and Coding Theory 2009, in: Contemp. Math., vol. 521, Amer. Math. Soc., Providence, RI, 2010, pp. 1–8.
[2] A. Adolphson, S. Sperber, Exponential sums and Newton polyhedra, Bull. Am. Math. Soc. (N.S.) 16 (2) (1987) 282–286.
[3] A. Adolphson, S. Sperber, On the degree of the L-function associated with an exponential sum, Compos. Math. 68 (2) (1988) 125–159.
[4] I. Baoulina, On the solvability of certain equations over finite fields, in: Topics in Finite Fields, in: Contemp. Math., vol. 632, Amer. Math. Soc., Providence, RI, 2015, pp. 19–27.
[5] B. Bank, M. Giusti, J. Heintz, G. Mbakop, Polar varieties and efficient real equation solving: the hypersurface case, J. Complex. 13 (1) (1997) 5–27.
[6] A. Cafure, G. Matera, Improved explicit estimates on the number of solutions of equations over a finite field, Finite Fields Appl. 12 (2) (2006) 155–185.
[7] A. Cafure, G. Matera, An effective Bertini theorem and the number of rational points of a normal complete intersection over a finite field, Acta Arith. 130 (1) (2007) 19–35.
[8] A. Cafure, G. Matera, M. Privitelli, Singularities of symmetric hypersurfaces and Reed-Solomon codes, Adv. Math. Commun. 6 (1) (2012) 69–94.
[9] A. Cafure, G. Matera, M. Privitelli, Polar varieties, Bertini's theorems and number of points of singular complete intersections over a finite field, Finite Fields Appl. 31 (2015) 42–83.
[10] L. Carlitz, Some special equations in a finite field, Pac. J. Math. 3 (1953) 13–24.
[11] L. Carlitz, Solvability of certain equations in a finite field, Q. J. Math. Oxf. Ser. (2) 7 (1956) 3–4.
[12] L. Carlitz, D.J. Lewis, W.H. Mills, E.G. Straus, Polynomials over finite fields with minimal value sets, Mathematika 8 (1961) 121–130.
[13] N. Castro, Ivelisse Rubio, José M. Vega, Divisibility of exponential sums and solvability of certain equations over finite fields, Q. J. Math. 60 (2) (2009) 169–181.
[14] E. Cesaratto, G. Matera, M. Pérez, M. Privitelli, On the value set of small families of polynomials over a finite field. I, J. Comb. Theory, Ser. A 124 (2014) 203–227.
[15] E. Cesaratto, G. Matera, M. Pérez, The distribution of factorization patterns on linear families of polynomials over a finite field, Combinatorica 37 (5) (2017) 805–836.
[16] Q. Cheng, E. Murray, On deciding deep holes of Reed-Solomon codes, in: Theory and Applications of Models of Computation, in: Lecture Notes in Comput. Sci., vol. 4484, Springer, Berlin, 2007, pp. 296–305.
[17] W.-S. Chou, G.L. Mullen, B. Wassermann, On the number of solutions of equations of Dickson polynomials over finite fields, Taiwan. J. Math. 12 (2008) 917–931.

[18] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Undergrad. Texts Math., Springer, New York, 1992.
[19] P. Deligne, La conjecture de Weil. I, Publ. Math. Inst. Hautes Études Sci. 43 (1974) 273–307.
[20] S. De Marchi, Polynomials arising in factoring generalized Vandermonde determinants II: a condition for monicity, Appl. Math. Lett. 15 (5) (2002) 627–632.
[21] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Grad. Texts in Math., vol. 150, Springer, New York, 1995.
[22] B. Felszeghy, On the solvability of some special equations over finite fields, Publ. Math. (Debr.) 68 (1–2) (2006) 15–23.
[23] W. Fulton, Intersection Theory, Springer, Berlin Heidelberg New York, 1984.
[24] S. Ghorpade, G. Lachaud, Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields, Mosc. Math. J. 2 (3) (2002) 589–631.
[25] S. Ghorpade, G. Lachaud, Number of solutions of equations over finite fields and a conjecture of Lang and Weil, in: A.K. Agarwal, et al. (Eds.), Number Theory and Discrete Mathematics, Chandigarh, 2000, New Delhi, Hindustan Book Agency, 2002, pp. 269–291.
[26] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theor. Comput. Sci. 24 (3) (1983) 239–277.
[27] N. Katz, Sums of Betti numbers in arbitrary characteristic, Finite Fields Appl. 7 (2001) 29–44.
[28] E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser, Boston, 1985.
[29] G. Lachaud, R. Rolland, On the number of points of algebraic sets over finite fields, J. Pure Appl. Algebra 219 (11) (2015) 5117–5136.
[30] R. Lidl, H. Niederreiter, Finite Fields, Addison–Wesley, Reading, Massachusetts, 1983.
[31] G. Matera, M. Pérez, M. Privitelli, On the value set of small families of polynomials over a finite field, II, Acta Arith. 165 (2) (2014) 141–179.
[32] G. Matera, M. Pérez, M. Privitelli, Explicit estimates for the number of rational points of singular complete intersections over a finite field, J. Number Theory 158 (2) (2016) 54–72.
[33] G. Matera, M. Pérez, M. Privitelli, Factorization patterns on nonlinear families of univariate polynomials over a finite field, J. Algebraic Comb. 51 (1) (2020) 103–153.
[34] L.J. Mordell, On a special polynomial congruence and exponential sums, in: Calcutta Math. Soc. Golden Jubilee Commemoration Vol., Calcutta Math. Soc., Calcutta, 1963, pp. 29–32.
[35] Gary L. Mullen, Daniel Panario, Handbook of Finite Fields, 1st ed., Chapman and Hall/CRC, 2013.
[36] F. Rodier, Borne sur le degré des polynômes presque parfaitement non-linéaires, in: Arithmetic, Geometry, Cryptography and Coding Theory, in: Contemp. Math., vol. 487, Amer. Math. Soc., Providence, RI, 2009, pp. 169–181.
[37] I.R. Shafarevich, Basic Algebraic Geometry: Varieties in Projective Space, Springer, Berlin Heidelberg New York, 1994.