On the number of solutions of systems of certain diagonal equations over finite fields

Mariana Pérez, Melina Privitelli

PII: S0022-314X(21)00270-5
DOI: https://doi.org/10.1016/j.jnt.2021.07.015
Reference: YJNTH 6856

To appear in: *Journal of Number Theory*

Received date: 15 November 2020
Revised date: 13 June 2021
Accepted date: 14 July 2021

ON THE NUMBER OF SOLUTIONS OF SYSTEMS OF CERTAIN DIAGONAL EQUATIONS OVER FINITE FIELDS

MARIANA PÉREZ[1,3] AND MELINA PRIVITELLI[1,2]

ABSTRACT. In this paper we obtain explicit estimates and existence results on the number of $\mathbb{F}_q$-rational solutions of certain systems defined by families of diagonal equations over finite fields. Our approach relies on the study of the geometric properties of the varieties defined by the systems involved. We apply these results to a generalization of Waring's problem and the distribution of solutions of congruences modulo a prime number.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field of q elements. It is a classical problem to determine or to estimate the number N of $\mathbb{F}_q$–rational solutions (i.e. solutions with coordinates in $\mathbb{F}_q$) of systems of polynomial equations over $\mathbb{F}_q$ (see, e.g., [24]). Particularly, the systems of diagonal equations

$$(1.1)\qquad \begin{cases} a_{11}X_1^{d_1} & +a_{12}X_2^{d_2} + \cdots + & a_{1t}X_t^{d_t} = b_1 \\ a_{21}X_1^{d_1} & +a_{22}X_2^{d_2} + \cdots + & a_{2t}X_t^{d_t} = b_2 \\ \vdots & & \vdots \\ a_{n1}X_1^{d_1} & +a_{n2}X_2^{d_2} + \cdots + & a_{nt}X_t^{d_t} = b_n, \end{cases}$$

with $b_1, \ldots, b_n \in \mathbb{F}_q$, have been considered in the literature because the study of its set of $\mathbb{F}_q$–rational solutions has several applications to different areas of mathematics, such as the theory of cyclotomy, Waring's problem and the graph coloring problem (see, e.g. [21] and [24]). Additionally, information on the number N is very useful in different aspects of coding theory such as the weight distribution of some cyclic codes ([36] and [37]) and the covering radius of certain cyclic codes ([16] and [23]).

The case $n = 1$ has been extensively studied. In general, there are no explicit formulas for the number N, except for some very particular diagonal equations satisfying some conditions over the exponents and the coefficients (see, e.g., [24]). For this reason, many articles focus on providing estimates on the number N (see, e.g. [21, 24, 34]). In [25], we obtain existence results and estimates on the number of $\mathbb{F}_q$-rational solutions of some variants of diagonal equations.

In comparison with a (single) diagonal equations, there are much fewer results about the number of $\mathbb{F}_q$–rational solutions of systems of the type (1.1). There are explicit formulas for the number N for some very particular cases (see, e.g., [3] and [35]). A. Tietäväinen provides existence results for some special families of systems of type (1.1) (see [29, 30, 31, 32]). In [27] and [28] K. Spackman, using elementary methods involving character sums, obtains the following estimate which holds under certain conditions on a parameter which measures the extent to which the coefficients' matrix is non–singular over $\mathbb{F}_q$:

$$N = q^{t-n} + \mathcal{O}(q^{(t-1)/2}),$$

2010 *Mathematics Subject Classification.* 11T06, 05E05, 14G05, 14G15, 11G25.

Key words and phrases. Finite fields, systems of diagonal equations, rational solutions, complete intersections, singular locus.

The authors were partially supported by the grants PIP CONICET 11220130100598, PIO CONICET-UNGS 14420140100027, ICI-UNGS 30/1146 and PICTO-UNAHUR-2019-00012.

where the implied constant depends only on $d_1, \ldots, d_t, n$ and t, but it is not explicitly given.

In this article we obtain an explicit estimate on the number N using tools of algebraic geometry. More precisely, for $n, k \leq t$, we consider the following more general system:

$$(1.2) \qquad \begin{cases} a_{11}X_1^{d_1} & +a_{12}X_2^{d_2} + \cdots + & a_{1t}X_t^{d_t} = g_1(X_1, \ldots, X_k) \\ a_{21}X_1^{d_1} & +a_{22}X_2^{d_2} + \cdots + & a_{2t}X_t^{d_t} = g_2(X_1, \ldots, X_k) \\ \quad\vdots & & \quad\vdots \\ a_{n1}X_1^{d_1} & +a_{n2}X_2^{d_2} + \cdots + & a_{nt}X_t^{d_t} = g_n(X_1, \ldots, X_k), \end{cases}$$

where $g_1, \ldots, g_n \in \mathbb{F}_q[X_1, \ldots, X_k]$ are such that $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$ or $0 \leq \deg(g_j) < d_t$ for $1 \leq j \leq n$ and there exists $1 \leq i \leq n$ such that $0 < \deg(g_i)$. Let $V \subset \mathbb{A}^n$ be the $\mathbb{F}_q$–variety defined by the polynomials $f_j := a_{j1}X_1^{d_1} + a_{j2}X_2^{d_2} + \cdots + a_{jt}X_t^{d_t} - g_j(X_1, \ldots, X_k)$, $1 \leq j \leq n$. In order to estimate the number of $\mathbb{F}_q$–rational points of V we consider $\mathrm{pcl}(V)$, the projective closure of V. We provide a suitable bound for the dimension of the singular locus of $\mathrm{pcl}(V)$ which allows us to prove that $\mathrm{pcl}(V)$ is a singular complete intersection whose singular locus has codimension al least 2. Then, applying estimates on the number of $\mathbb{F}_q$–rational points of projective singular complete intersections [13], we provide the main result of this paper.

Theorem 1.1. *Let $d_1 \geq \cdots \geq d_t \geq 2$, and $\mathrm{char}(\mathbb{F}_q)$ does not divide d_i for $1 \leq i \leq t$. Suppose that every $(n \times n)$–submatrix of the coefficients' matrix has rank n. We have the following estimates on N:*

- *If $g_j \in \mathbb{F}_q$ and $n \leq t - 2$, then:*
$$\left|N - q^{t-n}\right| \leq q^{\frac{t-n+1}{2}}(6nd_1)^{t+1}.$$
- *If $0 \leq \deg(g_j) < d_t$ and there exists $1 \leq i \leq n$ such that $\deg(g_i) > 0$, $n \leq t - k - 1$ and $k \leq t - 2$ then:*
$$\left|N - q^{t-n}\right| \leq q^{\frac{t-n+k}{2}}(6nd_1)^{t+1}.$$

We also show that we can replace $X_i^{d_i}$ by $h_i(X_i)$ for $1 \leq i \leq t$ where $h_i \in \mathbb{F}_q[T]$ and $\deg(h_i) = d_i$. In particular, we examine the case where $h_i(X_i)$ is the Dickson's polynomial $D_{d_i}(X_i, a)$ over $\mathbb{F}_q$ of degree d_i with parameter $a \in \mathbb{F}_q$ and we obtain a similar result to Theorem 1.1 for this case.

The paper is organized as follows. In Section 2 we collect the notions of algebraic geometry we use throughout the article. In Section 3 we study the geometric properties of the varieties associated to the system (1.2) and we settle Theorem 1.1. As a consequence, we obtain existence results of $\mathbb{F}_q$–rational solutions of these type of systems. We also study a particular example when $g_i = b_i X_1^{c_{i_1}} \cdots X_n^{c_{i_n}} - a_i$ (the generalized Markoff-Hurwitz-type equations systems). In Section 4 we consider some variants of systems of diagonal equations, such as the Dickson's equations. Finally, in Section 5 we study two applications of our estimates: a generalized Waring's problem over finite fields and the distribution of solutions of systems of congruences module a prime number.

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., [19], [26].

Let $\mathbb{K}$ be any of the fields $\mathbb{F}_q$ or $\overline{\mathbb{F}}_q$, the closure of $\mathbb{F}_q$. 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 $\overline{\mathbb{F}}_q$. 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 $F_1, \dots, F_m \in \mathbb{K}[X_0, \dots, X_r]$. 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 $F_1, \dots, F_m \in \mathbb{K}[X_1, \dots, X_r]$. We think a projective or affine $\mathbb{K}$–variety to be equipped with the induced Zariski topology. We shall denote by $\{F_1 = 0, \dots, F_m = 0\}$ or $V(F_1, \dots, F_m)$ the affine or projective $\mathbb{K}$–variety consisting of the common zeros of $F_1, \dots, F_m$.

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. If W is a subvariety of V, then the number $\dim V - \dim W$ is called the *codimension* of W in V. 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 [17] (see also [11]), 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. We shall use the following *Bézout inequality* (see [11, 17, 33]): if V and W are $\mathbb{K}$–varieties of the same ambient space, then

$$\deg(V \cap W) \leq \deg V \cdot \deg W. \tag{2.1}$$

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* $\mathcal{T}_x V$ to V at x is the kernel of the Jacobian matrix $(\partial F_i / \partial X_j)_{1 \leq i \leq m, 1 \leq j \leq r}(x)$ of $F_1, \dots, F_m$ with respect to $X_1, \dots, X_r$ at x. We have $\dim \mathcal{T}_x V \geq \dim_x V$ (see, e.g., [26, page 94]). The point x is *regular* if $\dim \mathcal{T}_x V = \dim_x V$; 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., [1, Lemma 2.1]):

$$|V(\mathbb{F}_q)| \leq \delta\, q^n. \tag{2.2}$$

On the other hand, if V is a projective variety of dimension n and degree δ, then we have the following bound (see [13, Proposition 12.1] or [2, Proposition 3.1]; see [20] 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 of pure dimension $r - m$, and is called a *set–theoretic complete intersection.* Furthermore, V is called an (ideal–theoretic) *complete intersection* if its ideal $I(V)$ over $\mathbb{K}$ can be generated by m polynomials. We shall frequently use the following criterion to prove that a variety is a complete intersection (see, e.g., [10, Theorem 18.15]).

Theorem 2.1. *Let $F_1, \ldots, F_m \in \mathbb{K}[X_1, \ldots, X_r]$ be polynomials which form a regular sequence and let $V := V(F_1, \ldots, F_m) \subset \mathbb{A}^r$. Denote by $(\partial \boldsymbol{F}/\partial \boldsymbol{X})$ the Jacobian matrix of $F_1, \ldots, F_m$ with respect to $\boldsymbol{X} := (X_1, \ldots, X_r)$. If the subvariety of V defined by the set of common zeros of the maximal minors of $(\partial \boldsymbol{F}/\partial \boldsymbol{X})$ has codimension at least one in V, then $F_1, \ldots, F_m$ define a radical ideal. In particular, V is a complete intersection.*

If $V \subset \mathbb{P}^r$ is a complete intersection defined over $\mathbb{K}$ of dimension $r-m$, and $F_1, \ldots, F_m$ is a system of homogeneous generators of $I(V)$, the degrees $d_1, \ldots, d_m$ depend only on V and not on the system of generators. Arranging the d_i in such a way that $d_1 \geq d_2 \geq \cdots \geq d_m$, we call $(d_1, \ldots, d_m)$ the *multidegree* of V. In this case, a stronger version of (2.1) holds, called the *Bézout theorem* (see, e.g., [15, Theorem 18.3]):

$$\deg V = d_1 \cdots d_m. \tag{2.3}$$

A complete intersection V is called *normal* if it is *regular in codimension 1*, that is, the singular locus $\mathrm{Sing}(V)$ of V has codimension at least 2 in V, namely $\dim V - \dim \mathrm{Sing}(V) \geq 2$ (actually, normality is a general notion that agrees on complete intersections with the one we define here). A fundamental result for projective complete intersections is the Hartshorne connectedness theorem (see, e.g., [19, Theorem VI.4.2]): if $V \subset \mathbb{P}^r$ is a complete intersection defined over $\mathbb{K}$ and $W \subset V$ is any $\mathbb{K}$–subvariety of codimension at least 2, then $V \setminus W$ is connected in the Zariski topology of $\mathbb{P}^r$ over $\mathbb{K}$. Applying the Hartshorne connectedness theorem with $W := \mathrm{Sing}(V)$, one deduces the following result.

Theorem 2.2. *If $V \subset \mathbb{P}^r$ is a normal complete intersection, then V is absolutely irreducible.*

3. Systems of diagonal equations

Let $t, n, d_1, \ldots, d_t, k$ be positive integers such that $n, k \leq t$, $d_1 \geq \cdots \geq d_t \geq 2$, and $\mathrm{char}(\mathbb{F}_q)$ does not divide d_i for $1 \leq i \leq t$. Let $X_1, \ldots, X_t$ be indeterminates over $\mathbb{F}_q$ and let $g_1, \ldots, g_n \in \mathbb{F}_q[X_1, \ldots, X_k]$ such that $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$ or $0 \leq \deg(g_j) < d_t$ for $1 \leq j \leq n$ and there exists $1 \leq i \leq n$ such that $0 < \deg(g_i)$.

We consider the following system of n deformed diagonal equations with t unknowns

$$\left\{\begin{array}{llll} a_{11}X_1^{d_1} & +a_{12}X_2^{d_2} + \cdots + & a_{1t}X_t^{d_t} & = g_1(X_1, \ldots, X_k) \\ a_{21}X_1^{d_1} & +a_{22}X_2^{d_2} + \cdots + & a_{2t}X_t^{d_t} & = g_2(X_1, \ldots, X_k) \\ \vdots & & \vdots & \\ a_{n1}X_1^{d_1} & +a_{n2}X_2^{d_2} + \cdots + & a_{nt}X_t^{d_t} & = g_n(X_1, \ldots, X_k). \end{array}\right. \tag{3.1}$$

Let $A = [a_{ij}] \in \mathbb{F}_q^{n \times t}$ be the coefficients' matrix of the above system. Assume that A satisfies the following hypothesis:

(H) Every $(n \times n)$–submatrix of A has rank n.

Let N denote the number of $\mathbb{F}_q$–rational solutions of (3.1). The purpose of this paper is to give an estimate on the number N. To do this, we consider the following polynomials $f_j \in \mathbb{F}_q[X_1, \dots, X_t]$

$$f_j := a_{j1}X_1^{d_1} + a_{j2}X_2^{d_2} + \cdots + a_{jt}X_t^{d_t} - g_j(X_1, \dots, X_k),\ 1 \le j \le n.$$

Without loss of generality and in order to be more clear in the exposition of the proofs, throughout this section we can assume that $\deg(g_j) > 0$, $1 \le j \le n$ or $g_j \in \mathbb{F}_q$, $1 \le j \le n$. Let $V := V(f_1, \dots, f_n) \subset \mathbb{A}^t$ be the $\mathbb{F}_q$–affine variety defined by $f_1, \dots, f_n$. We shall study some facts concerning the geometry of V. From hypothesis (H), the principal minor of A

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix},$$

has rank n. Therefore, there exist an invertible matrix $M \in \mathbb{F}_q^{n\times n}$ and a matrix $B \in \mathbb{F}_q^{n\times t}$ such that $M \cdot A = B$ and

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1n} & \cdots & b_{1t} \\ \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & b_{nn} & \cdots & b_{nt} \end{pmatrix}.$$

Let $\hat{V} \subset \mathbb{A}^t$ be the $\mathbb{F}_q$– affine variety defined by

$$\hat{V} := \left\{ (x_1, \dots, x_t) \in \mathbb{A}^t : B \cdot \begin{pmatrix} x_1^{d_1} \\ \vdots \\ x_t^{d_t} \end{pmatrix} = \begin{pmatrix} \hat{g}_1 \\ \vdots \\ \hat{g}_n \end{pmatrix} \right\},$$

where $\begin{pmatrix} \hat{g}_1 \\ \vdots \\ \hat{g}_n \end{pmatrix} = M \cdot \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix}$, namely $\hat{V} = V(\hat{f}_1, \dots, \hat{f}_n) \subset \mathbb{A}^t$ is the $\mathbb{F}_q$–affine variety defined by $\hat{f}_j := b_{jj}X_j^{d_j} + \cdots + b_{jt}X_t^{d_t} - \hat{g}_j$, for $1 \le j \le n$.

Remark 3.1. It is clear that $V = \hat{V}$ and $(f_1, \dots, f_n) = (\hat{f}_1, \dots, \hat{f}_n)$. Indeed, if $\mathbf{x} \in V$ then

$$A \cdot \begin{pmatrix} x_1^{d_1} \\ \vdots \\ x_t^{d_t} \end{pmatrix} = \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix}.$$

Multiplying both sides of the last equality by M and taking into account that $M \cdot A = B$ and $\begin{pmatrix} \hat{g}_1 \\ \vdots \\ \hat{g}_n \end{pmatrix} = M \cdot \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix}$, we have that $\mathbf{x} \in \hat{V}$. On the other hand, the proof of $\hat{V} \subset V$ is similar. Finally, $(f_1, \dots, f_n) = (\hat{f}_1, \dots, \hat{f}_n)$ follows from that $M \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} \hat{f}_1 \\ \vdots \\ \hat{f}_n \end{pmatrix}$, and M is an invertible matrix.

Theorem 3.2. *V is a set-theoretic complete intersection of pure dimension $t - n$.*

Proof. Observe that $\hat{f}_1, \dots, \hat{f}_n$ form a regular sequence of $\mathbb{F}_q[X_1, \cdots, X_t]$. Indeed, consider the graded lexicographic order of $\mathbb{F}_q[X_1, \cdots, X_t]$ with $X_1 > \cdots > X_t$. With this order we have that $Lt(\hat{f}_j) = b_{jj}X_j^{d_j}$, where $Lt(\hat{f}_j)$ denotes the leading term of the polynomial $\hat{f}_j$. Thus $Lt(\hat{f}_1), \dots, Lt(\hat{f}_n)$ are relatively prime and then they form a Gröbner basis of the ideal J generated by $\hat{f}_j$, $1 \le j \le n$ (see, e.g., [8, §2.9, Proposition 4]). Hence, the initial of the ideal J is generated by $Lt(\hat{f}_1), \dots, Lt(\hat{f}_n)$, which form a regular sequence of $\mathbb{F}_q[X_1, \dots, X_t]$. Therefore, by [10, Proposition 15.15], the polynomials $\hat{f}_1, \dots, \hat{f}_n$ form a regular sequence of $\mathbb{F}_q[X_1, \dots, X_t]$. We conclude that $V(\hat{f}_1, \dots, \hat{f}_n)$ is a set complete intersection of $\mathbb{A}^t$ of pure dimension $t - n$. □

Let C be the following set of $\mathbb{A}^t$:

$$C := \left\{ \mathbf{x} \in V : \ \operatorname{rank} \left(\frac{\partial f}{\partial \mathbf{X}} \right)(\mathbf{x}) < n \right\}, \tag{3.2}$$

where the $(n \times t)$–matrix $\frac{\partial f}{\partial \mathbf{X}}$ is the Jacobian matrix of the polynomials f_j, $1 \leq j \leq n$, with respect to $\boldsymbol{X} := (X_1, \dots, X_t)$. Suppose that $g_j \in \mathbb{F}_q$ or $0 < \deg(g_j) < d_t$, $1 \leq j \leq n$.

Assume that A, the coefficients' matrix of the system (3.1), satisfies the hypothesis (H). Observe that

$$\frac{\partial f}{\partial \mathbf{X}} = \left(\ M_1 \mid M_2 \ \right),$$

where M_1 is a $(n \times k)$–matrix defined by

$$M_1 := \begin{pmatrix} a_{11} d_1 X_1^{d_1 - 1} + \frac{\partial g_1}{\partial X_1} & \cdots & a_{1k} d_k X_k^{d_k - 1} + \frac{\partial g_1}{\partial X_k} \\ \vdots & \vdots & \vdots \\ a_{n1} d_1 X_1^{d_1 - 1} + \frac{\partial g_n}{\partial X_1} & \cdots & a_{nk} d_k X_k^{d_k - 1} + \frac{\partial g_n}{\partial X_k} \end{pmatrix}$$

and M_2 is a $n \times (t - k)$–matrix defined by

$$M_2 := \begin{pmatrix} a_{1k+1} d_{k+1} X_{k+1}^{d_{k+1} - 1} & \cdots & a_{1t} d_t X_t^{d_t - 1} \\ \vdots & \vdots & \vdots \\ a_{nk+1} d_{k+1} X_{k+1}^{d_{k+1} - 1} & \cdots & a_{nt} d_t X_t^{d_t - 1} \end{pmatrix}.$$

Proposition 3.3. *Assume that $n < t - k + 1$. The dimension of C is at most $k - 1$ if $\deg(g_j) > 0$ for $1 \leq j \leq n$ and this dimension is 0 if $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$. In particular, if V is a singular variety, the dimension of the singular locus of V is at most $k - 1$ or it is 0 respectively.*

Proof. Let $\mathbf{x} \in C$. We claim that $\mathbf{x}$ has at least $t - k - n + 1$ coordinates equal to zero among the coordinates $x_{k+1}, \dots, x_t$. Indeed, if $\mathbf{x}$ has at most $t - k - n$ coordinates equal to zero among the coordinates $x_{k+1}, \dots, x_t$ then $\mathbf{x}$ has at least n nonzero coordinates. Suppose that these coordinates are $x_{k+1}, \dots, x_{k+n}$. Then, we consider the following $(n \times n)$–submatrix of $M_2(\mathbf{x})$:

$$M_{2,n}(\mathbf{x}) = \begin{pmatrix} a_{1k+1} d_{k+1} x_{k+1}^{d_{k+1} - 1} & \cdots & a_{1k+n} d_{k+n} x_{k+n}^{d_{k+n} - 1} \\ \vdots & \vdots & \vdots \\ a_{nk+1} d_{k+1} x_{k+1}^{d_{k+1} - 1} & \cdots & a_{nk+n} d_{k+n} x_{k+n}^{d_{k+n} - 1} \end{pmatrix}.$$

We have that $M_{2,n}(\mathbf{x})$ can be written as follows:

$$M_{2,n}(\mathbf{x}) = \begin{pmatrix} a_{1k+1} d_{k+1} & \cdots & a_{1k+n} d_{k+n} \\ \vdots & \vdots & \vdots \\ a_{nk+1} d_{k+1} & \cdots & a_{nk+n} d_{k+n} \end{pmatrix} \cdot \begin{pmatrix} x_{k+1}^{d_{k+1} - 1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & x_{k+n}^{d_{k+n} - 1} \end{pmatrix}. \tag{3.3}$$

From (H) and the fact of $d_i \neq 0$ for all $1 \leq i \leq t$, the determinant of

$$\begin{pmatrix} a_{1k+1} d_{k+1} & \cdots & a_{1k+n} d_{k+n} \\ \vdots & \vdots & \vdots \\ a_{nk+1} d_{k+1} & \cdots & a_{nk+n} d_{k+n} \end{pmatrix}$$

is nonzero. On the other hand, since $x_i \neq 0$ for $k+1 \leq i \leq k+n$ we have that the determinant of the diagonal matrix of the right side of (3.3) is nonzero. Hence $M_2(\mathbf{x})$ has rank n and so $\frac{\partial f}{\partial \mathbf{X}}(\mathbf{x})$ does.

Therefore, we observe that

$$C = \bigcup_{\substack{I \subset \{k+1,\dots,t\} \\ |I|>t-k-n}} C(I), \tag{3.4}$$

where $C(I) := \{\mathbf{x} \in C : \ x_i = 0, i \in I\}$. In order to estimate the dimension of C, we first consider $C(I)$ with $|I| = t-n-k+1$. We take $\mathbf{x} \in C(I)$. Without loss of generality, suppose that the null coordinates of $\mathbf{x}$ are $x_{k+1}, \dots, x_{t-n+1}$. Now, we replace $X_{k+1} = \cdots = X_{t-n+1} = 0$ in (3.1) and we obtain a new system of n equations and $k+n-1$ unknowns. From hypothesis (H) and following the arguments of the proof of Theorem 3.2, we deduce that $\mathbf{x}$ belongs to a subvariety of V of dimension $k+n-1-n = k-1$. We conclude that the dimension of $C(I)$ is at most $k-1$. Let $C(I)$ with $|I| > t-n-k+1$, with the same arguments as above we obtain that the dimension of $C(I)$ is at most $k-2$. Finally, since the union (3.4) is finite, we have that the dimension of C is at most $k-1$.

On the other hand, if $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$, with similar arguments, $\mathbf{x}$ has at least $t-n+1$ coordinates equal to zero. From hypothesis (H) and with similar arguments as above we conclude that $\mathbf{x}$ belongs to a subvariety of V of dimension 0. □

From Proposition 3.3 and Theorem 2.1, we have the following result.

Corollary 3.4. *Let k, n, t be positive integers such that $n \leq t$, $k \leq t-2$ and A satisfies the hypothesis (H). If $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$ and $n \leq t-2$ or $\deg(g_j) \geq 0$ for $1 \leq j \leq n$, there exists $1 \leq i \leq n$ such that $0 < \deg(g_i)$ and $n \leq t-k-1$, then the singular locus of V has codimension at least 2 in V and $(f_1, \dots, f_n)$ is a radical ideal.*

Then, we obtain the following result.

Theorem 3.5. *With the same hypotheses as in Corollary 3.4, $V = V(f_1, \dots, f_n) \subset \mathbb{A}^t$ is a complete intersection of degree at most $d_1 \cdots d_n$.*

3.1. **The geometry of the projective closure.** Consider the embedding of $\mathbb{A}^t$ into the projective space $\mathbb{P}^t$ which assigns to any $\boldsymbol{x} := (x_1, \dots, x_t) \in \mathbb{A}^t$ the point $(1 : x_1 : \cdots : x_t) \in \mathbb{P}^t$. Then the closure $\operatorname{pcl}(V) \subset \mathbb{P}^t$ of the image of V under this embedding in the Zariski topology of $\mathbb{P}^t$ is called the projective closure of V. The points of $\operatorname{pcl}(V)$ lying in the hyperplane $\{X_0 = 0\}$ are called the points of $\operatorname{pcl}(V)$ at infinity.

It is well–known that $\operatorname{pcl}(V)$ is the $\mathbb{F}_q$–variety of $\mathbb{P}^t$ defined by the homogenization $F^h \in \mathbb{F}_q[X_0, \dots, X_t]$ of each polynomial F belonging to the ideal $(f_1, \dots, f_n) \subset \mathbb{F}_q[X_1, \dots, X_t]$ (see, e.g., [19, §I.5, Exercise 6]). Denote by $(f_1, \dots, f_t)^h$ the ideal generated by all the polynomials F^h with $F \in (f_1, \dots, f_n)$. Since $(f_1, \dots, f_n)$ is radical it turns out that $(f_1, \dots, f_n)^h$ is also a radical ideal (see, e.g., [19, §I.5, Exercise 6]). Furthermore, $\operatorname{pcl}(V)$ has pure dimension $t-n$ (see, e.g., [19, Propositions I.5.17 and II.4.1]) and degree equal to $\deg V$ (see, e.g., [4, Proposition 1.11]).

Now we discuss the behaviour of $\operatorname{pcl}(V)$ at infinity. Recall that $V = V(\hat{f}_1, , \dots, , \hat{f}_n) \subset \mathbb{A}^t$, where $\hat{f}_j := b_{jj} X_j^{d_j} + \cdots + b_{jt} X_t^{d_t} - \hat{g}_j$ with $\hat{g}_j \in \mathbb{F}_q[X_1, \dots, X_k]$, $k \leq t$ and $0 \leq \deg(\hat{g}_j) < d_t$. Hence, the homogenization of each $\hat{f}_j$ is the following polynomial of $\mathbb{F}_q[X_0, \dots, X_t]$:

$$\hat{f}_j^h := b_{jj} X_j^{d_j} + X_0 \cdot h_j, \ 1 \leq j \leq n,$$

where $h_j \in \mathbb{F}_q[X_0, X_1, \dots, X_t]$, $\deg(h_j) < d_j$, $1 \leq j \leq n$.

In particular, it follows that $\hat{f}_j^h(0, X_1, \dots, X_t) = b_{jj} X_j^{d_j}$ for $1 \leq j \leq n$.

Proposition 3.6. *$V^\infty := \operatorname{pcl}(V) \cap \{X_0 = 0\} \subset \mathbb{P}^{t-1}$ is a non-singular linear complete intersection of pure dimension $t-n-1$ and $V^\infty = V(X_1, \dots, X_n)$.*

Proof. Recall that the projective variety $\mathrm{pcl}(V)$ has pure dimension $t-n$. Hence, each irreducible component of $\mathrm{pcl}(V)\cap\{X_0=0\}$ has dimension at least $t-n-1$. On the other hand, from the definition of $\hat{f}_j^h$, $1\le j\le n$, we deduce that $\mathrm{pcl}(V)\cap\{X_0=0\}\subset V(X_1,\dots,X_n)$. Since $V(X_1,\dots,X_n)$ is a nonsingular irreducible variety of $\mathbb{P}^{t-1}$ of pure dimension $t-n-1$ we obtain that $\mathrm{pcl}(V)\cap\{X_0=0\}=V(X_1,\dots,X_n)$ and therefore, the proposition follows. □

Corollary 3.7. $\mathrm{pcl}(V)$ *has not singular points at infinity.*

Proof. From [13, Lemma 1.1] we have that the set of singular points of $\mathrm{pcl}(V)$ lying in $\{X_0=0\}$ is contained in the set of singular points of the variety $\mathrm{pcl}(V)\cap\{X_0=0\}$. Then, taking into account the above proposition we have that $\mathrm{pcl}(V)$ has not singular points at infinity. □

From Proposition 3.3 and Corollary 3.7, we obtain the following result.

Proposition 3.8. *Let $n\le t-2$ and $g_j\in\mathbb{F}_q$ for $1\le j\le n$. If V is a singular variety then the singular locus of $\mathrm{pcl}(V)\subset\mathbb{P}^t$ has dimension 0. On the other hand, let $k\le t-2$ and $n\le t-k-1$. If $0\le\deg(g_j)$ and there exists g_i such that $\deg(g_i)>0$ for $1\le i\le n$, the singular locus of $\mathrm{pcl}(V)$ has dimension at most $k-1$.*

We conclude this section with a statement that summarizes all the facts we need concerning the geometry of the projective closure $\mathrm{pcl}(V)$.

Theorem 3.9. *With the same hypotheses as above, $\mathrm{pcl}(V)\subset\mathbb{P}^t$ is an absolutely irreducible complete intersection of dimension $t-n$ and degree $d_1\cdots d_n$.*

Proof. Observe that the following inclusions hold:

$$
\begin{aligned}
&V(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})\cap\{X_0\neq 0\}\subset V(\hat{f}_1,\dots,\hat{f}_n),\\
&V(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})\cap\{X_0=0\}\subset V(X_1,\dots,X_n). \qquad (3.5)
\end{aligned}
$$

From Theorem 3.2 and Remark 3.1, we have that $V(\hat{f}_1,\dots,\hat{f}_n)\subset\mathbb{A}^t$ has pure dimension $t-n$. The $\mathbb{F}_q$–variety $V(X_1,\dots,X_n)\subset\mathbb{A}^t$ is an affine cone of pure dimension $t-n$; hence the dimension of $V(X_1,\dots,X_n)\subset\mathbb{P}^{t-1}$ is $t-n-1$. Therefore the dimension of $V(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})\subset\mathbb{P}^t$ is at most $t-n$. On the other hand, since $\mathrm{pcl}(V)\subset V(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})$ is $(t-n)$-dimensional we conclude that $V(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})$ has dimension $t-n$.

From Remark 3.1 and Proposition 3.6 the following equalities $\mathrm{pcl}(V)\cap\{X_0\neq 0\}=V(\hat{f}_1,\dots,\hat{f}_n)$ and $\mathrm{pcl}(V)\cap\{X_0=0\}=V(X_1,\dots,X_n)$ hold. Furthermore, from (3.5), $V(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})\cap\{X_0=0\}=V(X_1,\dots,X_n)$. Then, from Corollary 3.4 and taking into account that the variety $V(X_1,\dots,X_n)$ is nonsingular we have that the codimension of the singular locus of $V(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})$ is at least 2. On the other hand, $(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})$ is a radical ideal since $(\hat{f}_1,\dots,\hat{f}_n)=(f_1,\dots,f_n)$ is radical by Corollary 3.4. We conclude that $V(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})$ is a normal complete intersection. Hence, from Theorem 2.2 $V(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})$ is absolutely irreducible and thus $\mathrm{pcl}(V)=V(\hat{f}_1^{\,h},\dots,\hat{f}_n^{\,h})$. Finally, from (2.3) $\mathrm{pcl}(V)$ has degree $d_1\cdots d_n$. □

Remark 3.10. $d_1=\cdots=d_t=d\ge 2$. We consider the following system:

$$
\left\{
\begin{array}{llll}
a_{11}X_1^d & +a_{12}X_2^d+\cdots+ & a_{1t}X_t^d=0\\
a_{21}X_1^d & +a_{22}X_2^d+\cdots+ & a_{2t}X_t^d=0\\
\quad\vdots & & \quad\vdots\\
a_{n1}X_1^d & +a_{n2}X_2^d+\cdots+ & a_{nt}X_t^d=0.
\end{array}
\right. \qquad (3.6)
$$

In this case the system defines a projective variety $V=V(f_1,\dots,f_n)\subset\mathbb{P}^{t-1}$, where $f_i:=a_{i1}X_1^d+a_{i2}X_2^d+\cdots+a_{it}X_t^d$, $1\le i\le n$. Suppose that the coefficients' matrix of the above system satisfies hypothesis (H) and $n \leq t-2$. From Theorem 3.2, $V = V(f_1,\dots,f_n) \subset \mathbb{P}^{t-1}$ is a set theoretic projective complete intersection of dimension $t-n-1$. On the other hand, we consider the set $C \subset \mathbb{A}^t$ defined as in (3.2). From the arguments of Proposition 3.3 when $g_j \in \mathbb{F}_q$, $1 \leq j \leq n$, we have that C is an affine cone of dimension 0. Then, we deduce that $V \subset \mathbb{P}^{t-1}$ is a nonsingular projective variety. From Theorem 2.1 and $n \leq t-2$, we have that $(f_1,\dots,f_n)$ is a radical ideal then V is a complete intersection.

3.2. **Estimates on the number of $\mathbb{F}_q$–rational solutions of systems of diagonal equations.** Let $t, n, d_1, \dots, d_t, k$ be positive integers such that $n, k \leq t$, and $d_1 \geq \cdots \geq d_t \geq 2$. Let $X_1,\dots,X_t$ be indeterminates over $\mathbb{F}_q$ and let $g_1,\dots,g_n \in \mathbb{F}_q[X_1,\dots,X_k]$ such that $0 \leq \deg(g_j) < d_t$ for $1 \leq j \leq n$.

In what follows, we shall use an estimate on the number of $\mathbb{F}_q$–rational points of a projective complete intersection due to S. Ghorpade and G. Lachaud ([13]; see also [14]). In [13, Theorem 6.1], the authors prove that, for an irreducible $\mathbb{F}_q$–complete intersection $V \subset \mathbb{P}^m$ of dimension r, multidegree $\boldsymbol{d} = (d_1,\dots,d_{m-r})$ and singular locus of dimension at most s with $0 \leq s \leq r-1$, the number $|V(\mathbb{F}_q)|$ of $\mathbb{F}_q$–rational points of V satisfies the estimate:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b'_{r-s-1}(m-s-1,\boldsymbol{d})\ q^{\frac{r+s+1}{2}} + C_s(V) q^{\frac{r+s}{2}}, \tag{3.7}$$

where $p_r := q^r + q^{r-1} + \cdots + 1$, $b'_{r-s-1}(m-s-1,\boldsymbol{d})$ is the $(r-s-1)$–th primitive Betti of a nonsingular complete intersection in $\mathbb{P}^m$ of dimension $r-s-1$ and multidegree $\boldsymbol{d}$, and $C_s(V) := \sum_{i=r}^{r+s} b_{i,\ell}(V) + \varepsilon_i$, 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. From [13, Proposition 4.2]

$$b'_{r-s-1}(m-s-1,\boldsymbol{d}) \leq \binom{m-s}{r-s-1} \cdot (d+1)^{m-s-1}, \tag{3.8}$$

where $d := \max\{d_1,\dots,d_{m-r}\}$. On the other hand, from [13, Theorem 6.1], we have that

$$C_s(V) \leq 9 \cdot 2^{m-r} \cdot ((m-r)d+3)^{m+1}.$$

Denote by $\mathrm{pcl}(V)(\mathbb{F}_q)$ the set $\mathbb{F}_q$–rational points of $\mathrm{pcl}(V)$. We start by considering that the system is not of the form (3.6).

From Proposition 3.8 and Theorem 3.9 and the estimate (3.7), we have that, on one hand, if $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$ and $n \leq t-2$ then

$$\big||\mathrm{pcl}(V)(\mathbb{F}_q)| - p_{t-n}\big| \leq b'_{t-n-1}(t-1,\mathbf{d}) q^{(t-n+1)/2} + 9 \cdot 2^n (nd_1+3)^{t+1} q^{(t-n)/2}, \tag{3.9}$$

on the other hand, if $n \leq t-k-1$, $k \leq t-2$, $0 \leq \deg(g_j) < d_t$ for $1 \leq j \leq n$ and there exists $1 \leq i \leq n$ such that $\deg(g_i) > 0$, then

$$\big||\mathrm{pcl}(V)(\mathbb{F}_q)| - p_{t-n}\big| \leq b'_{t-n-k}(t-k,\mathbf{d}) q^{(t-n+k)/2} + 9 \cdot 2^n (nd_1+3)^{t+1} q^{(t-n+k-1)/2}, \tag{3.10}$$

where $\mathbf{d} = (d_1,\dots,d_n)$.

Now we estimate the number of $\mathbb{F}_q$-rational points of $V^\infty = \mathrm{pcl}(V) \cap \{X_0 = 0\} \subset \mathbb{P}^{t-1}$. From Proposition 3.6, we have that V^∞ is a nonsingular complete intersection. We can apply the following result due to P. Deligne (see, e.g., [9]): for a nonsingular complete intersection $V \subset \mathbb{P}^m$ defined over $\mathbb{F}_q$, of dimension r and multidegree $\mathbf{d} = (d_1,\dots,d_{m-r})$, the following estimate holds:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b'_r(m,\mathbf{d}) q^{r/2}, \tag{3.11}$$

where $b'_r(m,\mathbf{d})$ is the rth-primitive Betti number of any nonsingular complete intersection of $\mathbb{P}^m$ of dimension r and multidegree $\mathbf{d}$. Thus, by Proposition 3.6

$$\big||V^\infty(\mathbb{F}_q)| - p_{t-n-1}\big| \leq b'_{t-n-1}(t-1,\boldsymbol{d}) q^{(t-n-1)/2}. \tag{3.12}$$

If $g_j \in \mathbb{F}_q$, $1 \le j \le n$ and $n \le t-2$, from estimates (3.9) and (3.12) and the fact that $\mathrm{pcl}(V)(\mathbb{F}_q) \setminus V^{\infty}(\mathbb{F}_q) = V(\mathbb{F}_q)$, we conclude that

$$\begin{aligned} \big||V(\mathbb{F}_q)| - q^{t-n}\big| \le& \big||\mathrm{pcl}(V)(\mathbb{F}_q)| - p_{t-n}\big| + \big||V^{\infty}(\mathbb{F}_q)| - p_{t-n-1}\big| \\ \le& b'_{t-n-1}(t-1,\mathbf{d})q^{(t-n+1)/2} + 9\cdot 2^n(nd_1+3)^{t+1}q^{(t-n)/2} \\ &+ b'_{t-n-1}(t-1,\boldsymbol{d})q^{(t-n-1)/2}. \end{aligned} \tag{3.13}$$

If $0 \le \deg(g_j) < d_t$, $1 \le j \le n$ and there exists $1 \le i \le n$ such that $\deg(g_i) > 0$, $1 \le j \le n$, $n \le t-k-1$ and $k \le t-2$, from estimates (3.10) and (3.12) and the fact that $\mathrm{pcl}(V)(\mathbb{F}_q) \setminus V^{\infty}(\mathbb{F}_q) = V(\mathbb{F}_q)$, we obtain that

$$\begin{aligned} \big||V(\mathbb{F}_q)| - q^{t-n}\big| \le& \big||\mathrm{pcl}(V)(\mathbb{F}_q)| - p_{t-n}\big| + \big||V^{\infty}(\mathbb{F}_q)| - p_{t-n-1}\big| \\ \le& b'_{t-n-k}(t-k,\mathbf{d})q^{(t-n+k)/2} + 9\cdot 2^n(nd_1+3)^{t+1}q^{(t-n+k-1)/2} \\ &+ b'_{t-n-1}(t-1,\boldsymbol{d})q^{(t-n-1)/2}. \end{aligned} \tag{3.14}$$

We have the following result.

Theorem 3.11. *Let $t, n, d_1, \dots, d_t, k$ be positive integers such that $k, n \le t$, $d_1 \ge \cdots \ge d_t \ge 2$ and the coefficients' matrix of (3.1) satisfies hypothesis (H). Let $g_1, \dots, g_n \in \mathbb{F}_q[X_1, \dots, X_k]$ such that $0 \le \deg(g_j) < d_t$ for $1 \le j \le n$. Let $|V(\mathbb{F}_q)|$ be the number of $\mathbb{F}_q$–rational points of V.*

- *If $g_j \in \mathbb{F}_q$ for $1 \le j \le n$ and $n \le t-2$, then $|V(\mathbb{F}_q)|$ satisfies:*
$$\big||V(\mathbb{F}_q)| - q^{t-n}\big| \le q^{\frac{t-n+1}{2}}(6nd_1)^{t+1}.$$
- *If $0 \le \deg(g_j) < d_t$ for $1 \le j \le n$, there exists $1 \le i \le n$ such that $\deg(g_i) > 0$, $n \le t-k-1$ and $k \le t-2$, then $|V(\mathbb{F}_q)|$ satisfies:*
$$\big||V(\mathbb{F}_q)| - q^{t-n}\big| \le q^{\frac{t-n+k}{2}}(6nd_1)^{t+1}.$$

Proof. Suppose that $g_j \in \mathbb{F}_q$ for $1 \le j \le n$, from (3.13) we need to obtain an upper bound for the number $b'_{t-n-1}(t-1,\mathbf{d})$. From (3.8) we have that $b'_{t-n-1}(t-1,\mathbf{d}) \le \binom{t}{n+1}\cdot(d_1+1)^{t-1}$. On the other hand, taking into account that $\binom{t}{n+1} \le 2^t$ we deduce that

$$b'_{t-n-1}(t-1,\mathbf{d}) \le (d_1+1)^{t-1}2^t.$$

Replacing in (3.13) we obtain that

$$\begin{aligned} \big||V(\mathbb{F}_q)| - q^{t-n}\big| \le& q^{(t-n-1)/2}(nd_1+3)^{t+1}2^t\Big(q + \frac{9}{4}q^{\frac{1}{2}} + 1\Big) \\ \le& 2^{t+2}q^{\frac{t-n+1}{2}}(nd_1+3)^{t+1} \\ \le& q^{\frac{t-n+1}{2}}(6nd_1)^{t+1}. \end{aligned}$$

If $0 \le \deg(g_j) < d_t$ for $1 \le j \le n$ and there exists $1 \le i \le n$ such that $\deg(g_i) > 0$, from (3.14), the estimate can be obtained by using similar arguments as above. □

From Theorem 3.11 we obtain Theorem 1.1, furthermore we can provide the following existence results.

Theorem 3.12. *Let N be the number of $\mathbb{F}_q$–rational solutions of the system (3.1).*

- *Let $g_j \in \mathbb{F}_q$ for $1 \le j \le n$, $n \le t-2$ and $q > (6nd_1)^{\frac{2t+2}{t-n-1}}$, then $N > 0$.*
- *Let $0 \le \deg(g_j) < d_t$ for $1 \le j \le n$ and there exists $1 \le i \le n$ such that $\deg(g_i) > 0$, $n \le t-k-1$, $k \le t-2$ and $q > (6nd_1)^{\frac{2t+2}{t-n-k}}$, then $N > 0$.*

In particular, if t is sufficiently larger than $n+1$ or $n+k$ respectively, then we can guarantee the existence of an $\mathbb{F}_q$–rational solution if $q > (6nd_1)^2$.

We consider now the system (3.6). Let $\overline{N}$ be the number of $\mathbb{F}_q$–rational projective points of V, where V is the projective variety that this system defines. From Remark 3.10 and (3.11) the following estimate holds:

$$\left|\overline{N} - p_{t-n-1}\right| \leq b'_{t-n-1}(t-1,\mathbf{d})q^{\frac{t-n-1}{2}},$$

where $\mathbf{d} = (d_1, \ldots, d_n)$. Since $|V(\mathbb{F}_q)| = \overline{N}(q-1)+1$ we conclude that

$$\left||V(\mathbb{F}_q)| - q^{t-n}\right| \leq (q-1)2^t(d+1)^{t-1}q^{\frac{t-n-1}{2}}. \tag{3.15}$$

In [31, Theorem 4] A. Tietäväinen studies the system (3.6). The author proves that if $c := (d, q-1)$ and $t \geq 2n(n+\log_2(c-1))$ then there exists a nontrivial $\mathbb{F}_q$–rational solution of the system (3.6). From estimate (3.15), we obtain the following result.

Proposition 3.13. *If $q > (4d)^2$ and $t > (n+1)\frac{\log_2(q)}{\log_2(q)-2\log_2(4d)}$ then the system* (3.6) *has at least an $\mathbb{F}_q$–rational solution.*

It is easy to see that $1 < \frac{\log_2(q)}{\log_2(q)-2\log_2(4d)} \leq 256d^4$ for all $q > 16d^2$ while Tietäväinen's result implies that $n+1 \leq n+\log_2(c-1) \leq n+d-1$. Hence, for $n > (4d)^4$ and $q > 16d^2$, our condition over t is less restrictive than Tietäväinen's. We can say that the Tietäväinen's result and ours are complementary.

Remark 3.14. Deformed Diagonal Equations. Let $n = 1$ and $k = 1$, we consider the following deformed diagonal equation:

$$a_{11}X_1^{d_1} + \cdots + a_{1t}X_t^{d_t} = g_1,$$

with $g_1 \in \mathbb{F}_q[X_1]$, $0 < \deg(g_1) < d_t$, $d_1 \geq \cdots \geq d_t \geq 2$ and $\mathrm{char}(\mathbb{F}_q)$ does not divide d_i for $1 \leq i \leq t$. From Theorem 1.1 we have that

$$\left|N - q^{t-1}\right| \leq q^{\frac{t}{2}}(6d_1)^{t+1}.$$

This result complements [25, Theorem 4.1] in the case that g is an univariate polynomial because the exponents $d_1, \ldots, d_t$ are not necessarily the same.

Remark 3.15. In [27] and [28], K. W. Spackman studies the number N of $\mathbb{F}_q$–rational solutions of the system (3.1) when the polynomials $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$. Given μ a positive integer he defines the parameter μ of nonsingularity. Indeed, for a given $(n \times t)$–matrix in $\mathbb{F}_q^{n\times t}$, he says that it is *μ–weakly nonsingular* if and only if for each natural number k satisfying $\mu \cdot (k-1) + 1 \leq \min\{t, \mu \cdot (n-1) + 1\}$, the matrix has the property that among any $\mu \cdot (k-1) + 1$ columns vectors there are at least k $\mathbb{F}_q$–linearly independent ones. If $\mu = 1$, being 1–weakly nonsingular is equivalent to satisfying the hypothesis (H). Furthermore, a 1–weakly nonsingular matrix is also μ–weakly nonsingular for $\mu \geq 2$. In [27, Theorem 1.1] the author proves that if $\mu = 1$, $n \geq 2$ then

$$N = q^{t-n} + \mathcal{O}(q^{\frac{t-1}{2}}),$$

where the implied constant depends only on n, t, $d_1, \ldots, d_t$, but it is not explicitly given. Theorem 1.1 improved this result in several aspects. Indeed, on one hand, we give an explicit estimate on the number N and we obtain that $N = q^{t-n} + \mathcal{O}(q^{\frac{t-1}{2}-\frac{n-2}{2}})$. On the other hand, we also study the case in which each equations can be matched to a non-constant polynomial.

In [28, Theorem 3.2] the author obtains an explicit estimate on N when $\mu \geq 2$ and $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$. More precisely, the following estimate holds

$$|N - q^{t-n}| \leq (d_1 - 1)\cdots(d_t - 1) \cdot (2^t - 1) \cdot q^{\frac{t+(\mu-2)(n-1)}{2}},$$

where n, t and μ are positive integers with $\mu \geq 2$ and $t > \mu \cdot (n-1) \geq 2n-2$. Namely, $N = q^{t-n} + \mathcal{O}(q^{\frac{t+\epsilon}{2}})$, $\epsilon \geq 0$. On the other hand, if hypothesis (H) holds and $t \geq n+2$ we obtain that $N = q^{t-n} + \mathcal{O}(q^{\frac{t-(n-1)}{2}})$. Since the hypothesis (H) implies that the coefficients' matrix is μ–weakly nonsingular for all $\mu \geq 2$, if $n \geq 3$, hypothesis (H) holds and $t \geq 2n-1$, we can apply both estimates but in this case our estimate improves Spackman's.

3.3. **Generalized Markoff-Hurwitz-type systems.** A concrete example of a system of the form (3.1) are the Markoff-Hurwitz systems. These equations have been very well studied (see, e.g., [18, 22, 25]), but there are not results in the literature about this type of systems.

Let $t, n, d_1, \dots, d_t$ be positive integers, $d_1 \geq \cdots \geq d_t \geq 2$ and $\mathrm{char}(\mathbb{F}_q)$ does not divide d_i for $1 \leq i \leq t$. Let c_{ij} be positive integers such that $1 \leq i, j \leq n$ and $c_{j1} + \cdots + c_{jn} < d_t$, $1 \leq j \leq n$. We consider the following system of n generalized Markoff-Hurwitz-type equations with t unknowns over $\mathbb{F}_q$:

$$\left\{\begin{array}{llll} a_{11}X_1^{d_1} & +a_{12}X_2^{d_2} + \cdots + & a_{1t}X_t^{d_t} + a_1 = b_1 X_1^{c_{11}} \cdots X_n^{c_{1n}} \\ a_{21}X_1^{d_1} & +a_{22}X_2^{d_2} + \cdots + & a_{2t}X_t^{d_t} + a_2 = b_2 X_1^{c_{21}} \cdots X_n^{c_{2n}} \\ \quad\vdots & & \quad\vdots \\ a_{n1}X_1^{d_1} & +a_{n2}X_2^{d_2} + \cdots + & a_{nt}X_t^{d_t} + a_n = b_n X_1^{c_{n1}} \cdots X_n^{c_{nn}}, \end{array}\right. \tag{3.16}$$

where $b_1 \cdots b_n \neq 0$ and $a_j \in \mathbb{F}_q$ with $1 \leq j \leq n$. Denote by N the number of $\mathbb{F}_q$–rational solutions of (3.16). Assume that the coefficients' matrix of the above system satisfies the hypothesis (H), $t > 3$ and $n < \frac{t-1}{2}$. Let $g_j := b_j X_1^{c_{j1}} \cdots X_n^{c_{jn}} - a_j$, $1 \leq j \leq n$. Since $\deg(g_j) < d_t$, $1 \leq j \leq n$, from Theorem 1.1 we obtain the following result.

Theorem 3.16. *With the same hypotheses as above, N satisfies the following estimate:*

$$\left|N - q^{t-n}\right| \leq q^{\frac{t}{2}} (6nd_1)^{t+1}.$$

In what follows we obtain sufficient conditions for the existence of an $\mathbb{F}_q$–rational solution with nonzero coordinates namely, with coordinates in $\mathbb{F}_q^*$. Denote by N^* the number of this type of solutions of (3.16). Let $N^=$ be the number of $\mathbb{F}_q$-rational solutions of (3.16) with at least one coordinate equals to zero. Note that $N^* = N - N^=$.

By the inclusion-exclusion principle we obtain that

$$N^= = \sum_{i=1}^{t} (-1)^{i+1} \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} N(I), \tag{3.17}$$

where $N(I)$ denotes the number of $\mathbb{F}_q$–rational solutions of (3.16) satisfying $X_i = 0$ for all $i \in I$.

We shall need the following estimate on the number $N(I)$.

Proposition 3.17. *With the same hypotheses as above, the number $N(I)$ satisfies the following estimate:*

If $1 \leq |I| \leq t - 2n - 1$, then

$$|N(I) - q^{t-|I|-n}| \leq q^{\frac{t-|I|}{2}} (6nd_1)^{t-|I|+1}. \tag{3.18}$$

If $t - 2n \leq |I| \leq t - n$, then

$$N(I) \leq d_1^n q^{t-n-|I|}.$$

If $t - n + 1 \leq |I| \leq t$, then $N(I) \leq d_1^n$.

Proof. Suppose that $|I| = i$ with $1 \leq i \leq t - 2n - 1$. We observe that $N(I)$ is the number of $\mathbb{F}_q$–rational solutions of a system of n deformed diagonal equations with $t - i$ unknowns. The coefficients' matrix of the system satisfies hypothesis (H). Then we deduce (3.18) from Theorem 1.1.

Suppose now $t - 2n \leq i \leq t - n$. In this case, $N(I)$ is the number of $\mathbb{F}_q$–rational solutions of a system of n deformed diagonal equations with $t - i \geq n$ unknowns. We observe that, since the coefficients' matrix of the system satisfies hypothesis (H) we can follow the same arguments presented in the proof of Theorems 3.2 and 3.5, then $V_i \subset \mathbb{A}^{t-i}$, the set of solutions considered, is an $\mathbb{F}_q$–affine complete intersection of dimension $t-i-n$ and $\deg(V_i) \leq d_1^n$. Finally, from (2.2), we have that $N(I) \leq d_1^n \cdot q^{t-i-n}$.

Let $t-n+1 \leq i \leq t$. In this case n, the number of equations, is greater than the number of unknowns $t-i$. Since the coefficients' matrix of the system (3.1) satisfies hypothesis (H) then, the coefficients' matrix of the system of this case, has rank $t-i$. So, following the arguments of the proof of Theorem 3.2, the set of solutions has dimension zero. Hence, from (2.2), $N(I) \leq d_1^n$. □

Now, we can estimate the number of $\mathbb{F}_q$–rational solutions of (3.16) which satisfy the conditions $x_1 \cdots x_n \neq 0$.

Proposition 3.18. *If $q > 2$, $1 \leq n < \frac{t-1}{2}$, $d_1 \geq \cdots \geq d_t \geq 2$ and $\mathrm{char}(\mathbb{F}_q)$ does not divide d_i for $1 \leq i \leq t$. Then, the number N^* of $\mathbb{F}_q$–rational solutions of (3.16) with nonzero coordinates satisfies the following estimate:*

$$\left| N^* - \left(\frac{(q-1)^t}{q^n} - \sum_{i=t-2n}^{t} (-1)^i \binom{t}{i} q^{t-n-i} \right) \right| \leq (15nd_1)^{t+1} q^{\frac{t}{2}}.$$

Proof. From (3.17) and taking into account that $N^* = N - N^=$, we have that

$$\begin{aligned} N^* &= N + \sum_{i=1}^{t} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} N(I) = N + \sum_{i=1}^{t-2n-1} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} N(I) + \sum_{i=t-2n}^{t} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} N(I) \\ &= N + \sum_{i=1}^{t-2n-1} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} (N(I) - q^{t-n-i}) + \sum_{i=1}^{t-2n-1} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} q^{t-n-i} + \sum_{i=t-2n}^{t} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} N(I) \\ &= N + \sum_{i=1}^{t-2n-1} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} (N(I) - q^{t-n-i}) + \sum_{i=1}^{t-2n-1} (-1)^i \binom{t}{i} q^{t-n-i} + \sum_{i=t-2n}^{t} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} N(I) \\ &= N - q^{t-n} + \sum_{i=1}^{t-2n-1} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} (N(I) - q^{t-n-i}) + \sum_{i=0}^{t-2n-1} (-1)^i \binom{t}{i} q^{t-n-i} + \sum_{i=t-2n}^{t} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} N(I). \end{aligned}$$

Thus, we deduce that

$$N^* - \sum_{i=0}^{t-2n-1} (-1)^i \binom{t}{i} q^{t-n-i} = (N - q^{t-n}) + \sum_{i=1}^{t-2n-1} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} (N(I) - q^{t-n-i}) + \sum_{i=t-2n}^{t} (-1)^i \sum_{\substack{I \subset \{1,\dots,t\} \\ |I|=i}} N(I).$$

Therefore, from Theorem 3.16 and Proposition 3.17:

$$\begin{aligned}
\left|N^*-\sum_{i=0}^{t-2n-1}(-1)^i\binom{t}{i}q^{t-n-i}\right| &\leq |N-q^{t-n}|+\sum_{i=1}^{t-2n-1}\binom{t}{i}(6nd_1)^{t-i+1}q^{(t-i)/2}+\sum_{i=t-2n}^{t}\sum_{\substack{I\subset\{1,\dots,t\}\\ |I|=i}}N(I)\\
&\leq (6nd_1)^{t+1}\Big(q^{\frac{t}{2}}+\sum_{i=1}^{t-2n-1}\binom{t}{i}q^{\frac{t-i}{2}}\Big)+\sum_{i=t-2n}^{t-n}\binom{t}{i}d_1^n q^{t-n-i}+\sum_{i=t-n+1}^{t}\binom{t}{i}d_1^n\\
&\leq (6nd_1)^{t+1}\left(q^{\frac{t}{2}}+2^t q^{\frac{t-1}{2}}\right)+2^t d_1^n(q^n+1)\\
&\leq (6nd_1)^{t+1}q^{\frac{t-1}{2}}(2^t+q^{\frac{1}{2}})+2^{t+1}d_1^n q^{\frac{t-3}{2}}\\
&\leq 2^{t+2}(6nd_1)^{t+1}q^{\frac{t}{2}}\\
&\leq (15nd_1)^{t+1}q^{\frac{t}{2}}.
\end{aligned}$$

□

In [25] we study the following Markoff-Hurwitz's equation:

$$a_1X_1^{d_1}+a_2X_2^{d_1}+\cdots+a_tX_t^{d_1}+a=bX_1^{c_1}\dots X_t^{c_t},$$

where $a_i\in\mathbb{F}_q$, $1\leq i\leq t$ and $a,b\in\mathbb{F}_q\setminus\{0\}$. More precisely, in [25, Proposition 4.7], we have that, if $q>2$, then

$$\left|N^*-\frac{(q-1)^t-(-1)^t}{q}\right|\leq 7(2d_1)^t q^{\frac{t}{2}}.$$

In particular, Proposition 3.18 provides an estimate in the case $n=1$, $c_{n+1}=\cdots=c_t=0$ and $c_1<d_t$. The error term of both estimates is of order $\mathcal{O}(q^{t/2})$ but $7(2d_1)^t<(15d_1)^{t+1}$. However, in Proposition 3.18 we obtain two new terms in the asymptotic development of N^* in terms of q. Indeed, we have that $N^*=\frac{(q-1)^t-(-1)^t}{q}+(-1)^t t+(-1)^{t-1}\frac{t(t-1)}{2}q+\mathcal{O}(q^{t/2})$.

In what follows, we provide an existence result for $\mathbb{F}_q$–rational solutions with nonzero coordinates.

Proposition 3.19. *If $q>(30nd_1)^{\frac{2t+2}{t-2n}}$ and $n<\frac{t-1}{2}$ then the system (3.16) has at least one solution in $(\mathbb{F}_q^*)^t$. In particular, if t is sufficiently larger than $2n$, then we can guarantee the existence of an $\mathbb{F}_q$–rational solution if $q>(30nd_1)^2$.*

Proof. Suppose that $q>2$. From the above proposition we deduce that

$$N^*\geq\frac{(q-1)^t}{q^n}-\sum_{i=t-2n}^{t}(-1)^i\binom{t}{i}q^{t-n-i}-(15nd_1)^{t+1}q^{\frac{t}{2}}. \tag{3.19}$$

We observe that

$$\begin{aligned}
\sum_{i=t-2n}^{t}(-1)^i\binom{t}{i}q^{t-n-i} &= (-1)^t\sum_{j=0}^{2n}(-1)^j\binom{t}{2n-j}q^{n-j}\\
&= (-1)^t\left(q^{-n}+\sum_{\substack{l\text{ odd}\\ l\in\{1,\dots,2n\}}}q^{n-l}A_l\right),
\end{aligned} \tag{3.20}$$

where $A_l:=\binom{t}{2n-l+1}q-\binom{t}{2n-l}$.

Let l be an odd integer such that $l\in\{1,\cdots,2n\}$. We affirm that if $q\geq\frac{2n}{t-2n+1}$, then $A_l\geq 0$. Indeed, it is easy to see that $A_l\geq 0$ if and only if $q\geq\frac{2n-l+1}{t-2n+l}$. We consider the function $f(l) := \frac{2n-l+1}{t-2n+l}$. Since $f(l)$ is a decreasing function in l, we have that $A_l \geq 0$ if $q \geq \frac{2n}{t-2n+1}$.

Suppose that t is an odd number and $q \geq \frac{2n}{t-2n+1}$. From (3.20) and since $A_l \geq 0$, we deduce that

$$\sum_{i=t-2n}^{t} (-1)^i \binom{t}{i} q^{t-n-i} \leq 0.$$

Thus, from (3.19) we conclude that

$$N^* \geq \frac{(q-1)^t}{q^n} - (15nd_1)^{t+1} q^{\frac{t}{2}} \tag{3.21}$$

Now, suppose that t is an even number and $q \geq \frac{2n}{t-2n+1}$. From (3.20) and taking into account that $A_l \geq 0$, we have that

$$\sum_{i=t-2n}^{t} (-1)^i \binom{t}{i} q^{t-n-i} \geq 0.$$

On the other hand, since $n < \frac{t-1}{2}$ we deduce that

$$\begin{aligned}\sum_{i=t-2n}^{t} (-1)^i \binom{t}{i} q^{t-n-i} &= \sum_{j=0}^{2n} (-1)^j \binom{t}{2n-j} q^{n-j} \leq q^n \sum_{j=0}^{2n} \binom{t}{2n-j} \\ &\leq 2^t q^n \leq (15nd_1)^{t+1} q^{t/2}.\end{aligned}$$

Thus, from (3.19) we conclude that

$$N^* \geq \frac{(q-1)^t}{q^n} - 2(15nd_1)^{t+1} q^{\frac{t}{2}} \tag{3.22}$$

From (3.21) and (3.22), we have that if $q \geq \frac{2n}{t-2n+1}$, then

$$\begin{aligned}N^* &\geq \frac{(q-1)^t}{q^n} - 2(15nd_1)^{t+1} q^{\frac{t}{2}} \\ &\geq \frac{q^{t-n}}{2^t} - 2(15nd_1)^{t+1} q^{\frac{t}{2}} \\ &\geq q^{\frac{t}{2}} \Big(\frac{q^{\frac{t-2n}{2}}}{2^t} - 2(15nd_1)^{t+1} \Big).\end{aligned}$$

Therefore, (3.16) has at least one solution in $\mathbb{F}_q^t$ with nonzero coordinates if

$$\frac{q^{\frac{t-2n}{2}}}{2^t} - 2(15nd_1)^{t+1} > 0,$$

namely $q^{\frac{t-2n}{2}} > (30nd_1)^{t+1}$, this concludes the proof of the proposition. □

4. Generalization: variants of systems of diagonal equations

Let $t, n, d_1, \ldots, d_t, k$ be positive integers such that $k, n \leq t$, $d_1 \geq \cdots \geq d_t \geq 2$, and $\mathrm{char}(\mathbb{F}_q)$ does not divide d_i for $1 \leq i \leq t$. Let $h_1, \ldots, h_t \in \mathbb{F}_q[T]$ with $\deg(h_i) = d_i$ and $h_i^{'} \neq 0$ for $1 \leq i \leq t$. Let $X_1, \ldots, X_t$ be indeterminates over $\mathbb{F}_q$ and let $g_1, \ldots, g_n \in \mathbb{F}_q[X_1, \ldots, X_k]$ such that $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$ or $0 \leq \deg(g_j) < d_t$ for $1 \leq j \leq n$ and there exists i such that $\deg(g_i) > 0$.

We consider the following system of n variants of Carlitz's equations and t unknowns

$$(4.1)\qquad \begin{cases} a_{11}h_1(X_1) & +a_{12}h_2(X_2)+\cdots+ & a_{1t}h_t(X_t)=g_1(X_1,\dots,X_k) \\ a_{21}h_1(X_1) & +a_{22}h_2(X_2)+\cdots+ & a_{2t}h_t(X_t)=g_2(X_1,\dots,X_k) \\ \quad\vdots & & \quad\vdots \\ a_{n1}h_1(X_1) & +a_{n2}h_2(X_2)+\cdots+ & a_{nt}h_t(X_t)=g_n(X_1,\dots,X_k). \end{cases}$$

Assume that the coefficients' matrix of the above system satisfies hypothesis (H). Carlitz's equations has been defined in [5]. In this article the author provides a non-explicit estimate for the case $n=1$ and $g_1 \in \mathbb{F}_q$. In [25] we improve his results in several aspects.

Let $V := V(f_1,\dots,f_n) \subset \mathbb{A}^t$ be the $\mathbb{F}_q$–affine variety defined by $f_i := a_{i1}h_1(X_1) + a_{i2}h_2(X_2)+\cdots+a_{it}h_t(X_t) - g_i(X_1,\dots,X_k)$, for $1 \le i \le n$. With the same arguments of Theorem 3.2, we obtain that $V \subset \mathbb{A}^t$ is a set-theoretic complete intersection of dimension $t-n$. We consider the set C as in (3.2).

Observe that

$$\frac{\partial f}{\partial \mathbf{X}} = \left(\begin{array}{c|c} M_1 & M_2 \end{array} \right),$$

where M_1 is a $(n \times k)$–matrix defined by

$$M_1 := \begin{pmatrix} a_{11}h_1'(X_1)+\frac{\partial g_1}{\partial X_1} & \cdots & a_{1k}h_k'(X_k)+\frac{\partial g_1}{\partial X_k} \\ \vdots & \vdots & \vdots \\ a_{n1}h_1'(X_1)+\frac{\partial g_n}{\partial X_1} & \cdots & a_{nk}h_k'(X_k)+\frac{\partial g_n}{\partial X_k} \end{pmatrix}$$

and M_2 is a $n \times (t-k)$–matrix defined by

$$M_2 := \begin{pmatrix} a_{1k+1}h_{k+1}'(X_{k+1}) & \cdots & a_{1t}d_th_t'(X_t) \\ \vdots & \vdots & \vdots \\ a_{nk+1}h_{k+1}'(X_{k+1}) & \cdots & a_{nt}h_t'(X_t) \end{pmatrix}.$$

Proposition 4.1. *Assume that $n < t-k+1$. The dimension of C is at most $k-1$ if $\deg(g_j) \ge 0$ for $1 \le j \le n$ and there exists i such that $\deg g_i > 0$. On the other hand, this dimension is 0 if $g_i \in \mathbb{F}_q$ for $1 \le i \le n$. In particular, the dimension of the singular locus of V is at most $k-1$ or 0 respectively.*

Proof. Let $\mathbf{x} \in C$. We observe that M_2 satisfies

$$M_2 := \begin{pmatrix} a_{1k+1} & \cdots & a_{1t} \\ \vdots & \vdots & \vdots \\ a_{nk+1} & \cdots & a_{nt} \end{pmatrix} \cdot \begin{pmatrix} h_{k+1}'(X_{k+1}) & \cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \cdots & h_t'(X_t) \end{pmatrix}.$$

From hypothesis (H) we have that the diagonal matrix of right side can not have n nonzero columns. Then, we deduce that the number of zero columns is at least $t-n-k+1$. Suppose that $\mathbf{x} \in C$ is such that $h_{k+1}'(x_{k+1}) = 0, \dots, h_{t-n+1}'(x_{t-n+1}) = 0$. Then, we obtain that the coordinates $X_{k+1},\dots,X_{t-n+1}$ of $\mathbf{x}$ take finite values in $\overline{\mathbb{F}}_q$ because the derivate $h_i^{'}$ is not identically null for all $1 \le i \le t$. Then, we deduce that C is contained in a finite union of $\overline{\mathbb{F}}_q$–linear varieties of dimension $n+k-1$. From hypothesis (H), the intersection of each of these linear varieties with V is a subvariety of V of dimension $k-1$, if $\deg(g_j) > 0$ for $1 \le j \le n$, and the dimension is 0, if $g_j \in \mathbb{F}_q$ for $1 \le j \le n$.

□

Corollary 4.2. *Let k, n, t be positive integers such that $n, k \le t$ and A satisfies the hypothesis (H). If $g_j \in \mathbb{F}_q$ for $1 \le j \le n$ and $n \le t-2$ or $\deg(g_j) \ge 0$ for $1 \le j \le n$, there exists $1 \le i \le n$ such that $0 < \deg(g_i)$ and $n \le t-k-1$, $k \le t-2$ then the singular locus of V has codimension at least 2 in V and $(f_1,\dots,f_n)$ is a radical ideal.*

With the same arguments of the Section 3.1 we have that $\mathrm{pcl}(V) \subset \mathbb{P}^t$ is an absolutely irreducible complete intersection of dimension $t-n$ and degree $d_1 \cdots d_n$ and its singular locus has dimension at most $k-1$ if $\deg(g_j) \geq 0$ for $1 \leq j \leq n$ and there exists $1 \leq i \leq n$ such that $0 < \deg(g_i)$ or its dimension is 0 if $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$. From Theorem 1.1 if N denotes the number of $\mathbb{F}_q$–rational solutions of the system defined in (4.1), we deduce the following result.

Theorem 4.3. *With the same hypothesis as in the above theorem, N satisfies:*

- *If $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$ and $n \leq t-2$ then N satisfies:*
$$\left|N - q^{t-n}\right| \leq q^{\frac{t-n+1}{2}}(6nd_1)^{t+1}.$$
- *If $0 \leq \deg(g_j) < d_t$ for $1 \leq j \leq n$ and there exists i such that $\deg(g_i) > 0$, $k \leq t-2$ and $n \leq t-k-1$ then N satisfies:*
$$\left|N - q^{t-n}\right| \leq q^{\frac{t-n+k}{2}}(6nd_1)^{t+1}.$$

Corollary 4.4. *Theorem 3.12 holds for system* (4.1). *In particular, if t is sufficiently larger than $n+1$ or $n+k$ respectively, then we can guarantee the existence of an $\mathbb{F}_q$–rational solution if $q > (6nd_1)^2$.*

Remark 4.5. In [25] we study Carlitz's equations. Let d, t be positive integers with $d \geq 2$ and $t \geq 3$. Let $h_i = a_{d,i}T^d + \cdots + a_{0,i} \in \mathbb{F}_q[T]$, with $\deg(h_i) = d$, $1 \leq i \leq t$. Let $g \in \mathbb{F}_q[X_1, \ldots, X_t]$ such that $\deg(g) < d$. Suppose that $\mathrm{char}(\mathbb{F}_q)$ does not divide d. We consider the following Carlitz's equation:
$$h_1(X_1) + \cdots + h_t(X_t) = g.$$
We obtain an explicit estimate on the number N of $\mathbb{F}_q$–rational solutions of Carlitz's equations. Indeed, we have that
$$\left|N - q^{t-1}\right| \leq q^{(t-1)/2}\big(2(d-1)^{t-1}q^{1/2} + 6(d+2)^t\big). \tag{4.2}$$
The result of Theorem 4.3 complements the estimate (4.2) when g is an univariate polynomial and the degrees of the polynomials h_i are not necessarily the same.

4.1. **Systems of Dickson's equations.** These systems are a particular case of systems of the form (4.1). Let $d \in \mathbb{N}$ and $a \in \mathbb{F}_q$. The Dickson's polynomial over $\mathbb{F}_q$ of degree d with parameter a is the following:
$$D_d(X, a) = \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i}\binom{d-i}{i}(-a)^i X^{d-2i}.$$
Dickson's polynomials have been extensively studied because they play very important roles in both theoretical work as well as in various applications (see, [24, Chapter 7]). The set of $\mathbb{F}_q$–rational solution of Dickson's equations has been very well studied in the literature (see [25] and [7]). However, there are few results concerning the set of solutions of systems of equations given by Dickson's polynomials.

Let $t, n, d_1, \ldots, d_t, k$ be positive integers such that $n \leq t-k-1$, $k \leq t-2$, $d_1 \geq \cdots \geq d_t \geq 2$, and $\mathrm{char}(\mathbb{F}_q)$ does not divide d_i for $1 \leq i \leq t$. Let $D_{d_1}(T, a_1), \ldots, D_{d_t}(T, a_t) \in \mathbb{F}_q[T]$ with $a_1, \ldots, a_t \in \mathbb{F}_q$. Let $X_1, \ldots, X_t$ be indeterminates over $\mathbb{F}_q$ and let $g_1, \ldots, g_n \in \mathbb{F}_q[X_1, \ldots, X_k]$ such that $g_j \in \mathbb{F}_q$ for $1 \leq j \leq n$ or $0 \leq \deg(g_j) < d_t$ for $1 \leq j \leq n$ and there exists i such that $\deg(g_i) > 0$.

We consider the following system of n Dickson's equations with t unknowns
$$\begin{cases} a_{11}D_{d_1}(X_1, a_1) & +a_{12}D_{d_2}(X_2, a_2) + \cdots + & a_{1t}D_{d_t}(X_t, a_t) = g_1(X_1, \ldots, X_k) \\ a_{21}D_{d_1}(X_1, a_1) & +a_{22}D_{d_2}(X_2, a_2) + \cdots + & a_{2t}D_{d_t}(X_t, a_t) = g_2(X_1, \ldots, X_k) \\ \quad\vdots & & \quad\vdots \\ a_{n1}D_{d_1}(X_1, a_1) & +a_{n2}D_{d_2}(X_2, a_2) + \cdots + & a_{nt}D_{d_t}(X_t, a_t) = g_n(X_1, \ldots, X_k). \end{cases}$$

Let $A = [a_{ij}] \in \mathbb{F}_q^{n\times t}$ be the coefficients' matrix of the above system. Assume that A satisfies hypothesis (H). From Theorem 4.3 we obtain an estimate on the number of $\mathbb{F}_q$–solutions of this type of systems.

5. Applications

5.1. **Generalized Waring's problems over finite fields.** One of the most important questions in number theory is to find properties on a system of equations that guarantee solutions over a field, for example, the so called generalized Waring's problem (see, e.g. [3, 6, 30]). Let $\mathcal{S}$ be the following system over $\mathbb{F}_q$ with n equations and t unknowns

$$\left\{\begin{array}{llll} a_{11}X_1^{d_1} & +a_{12}X_2^{d_2}+\cdots+ & a_{1t}X_t^{d_t} & = b_1 \\ a_{21}X_1^{d_1} & +a_{22}X_2^{d_2}+\cdots+ & a_{2t}X_t^{d_t} & = b_2 \\ \quad\vdots & & \quad\vdots & \\ a_{n1}X_1^{d_1} & +a_{n2}X_2^{d_2}+\cdots+ & a_{nt}X_t^{d_t} & = b_n, \end{array}\right. \tag{5.1}$$

where the coefficients' matrix of the system satisfies the hypothesis (H), $d_1 \geq \cdots \geq d_t \geq 2$ and $\mathrm{char}(\mathbb{F}_q)$ does not divide d_i for $1 \leq i \leq t$.

Waring's problem consists in finding $\gamma(\mathcal{S})$ the least number of variables t such that (5.1) has solution in $\mathbb{F}_q^t$ for every n-tuple $(b_1, \dots, b_n) \in \mathbb{F}_q^n$. From Theorem 1.1 we have that N, the number of $\mathbb{F}_q$–rational solutions of (5.1), satisfies that

$$N \geq q^{\frac{t-n+1}{2}}\left(q^{\frac{t-n-1}{2}} - (6nd_1)^{t+1}\right).$$

Then $N > 0$ provided that $q^{\frac{t-n-1}{2}} - (6nd_1)^{t+1} > 0$, namely $q^{\frac{t-n-1}{2}} > \big(6nd_1\big)^{t+1}$. Now if $q > (6nd_1)^2$ then, the last condition is equivalent to

$$t > \frac{\log(6nd_1 \cdot q^{\frac{n+1}{2}})}{\log(\frac{q^{1/2}}{6nd_1})}.$$

Then, if $q > (6nd_1)^2$ we obtain that

$$\gamma(\mathcal{S}) \leq \left\lceil \frac{\log(6nd_1 \cdot q^{\frac{n+1}{2}})}{\log(\frac{q^{1/2}}{6nd_1})} \right\rceil.$$

We observe that $h(q) := \frac{\log(6nd_1 \cdot q^{\frac{n+1}{2}})}{\log(\frac{q^{1/2}}{6nd_1})}$ is a decreasing function and $\lim_{q\to\infty} h(q) = n+1$. Therefore $h(q) > n+1$ if $q > (6nd_1)^2$. Then we deduce that if q sufficiently large, $\gamma(\mathcal{S}) \leq n+2$. In particular if $q \geq (6nd_1)^3$ then $\gamma(\mathcal{S}) \leq 3n+5$.

5.2. **Distribution of solutions to systems of congruences equations modulo a prime number.** In this section we apply our estimates to obtain asymptotic formulas for the distribution of simultaneous solutions to congruences modulo p, a prime number. This is a well studied problem, see, for example [28] and [32].

Let $t, n, d_1, \dots, d_t$ be positive integers such that $n \leq t-2$, $d_1 \geq \cdots \geq d_t \geq 2$, and p does not divide d_i for $1 \leq i \leq t$. We consider the following systems of congruences equations

$$\left\{\begin{array}{lllll} a_{11}X_1^{d_1} & +a_{12}X_2^{d_2}+\cdots+ & a_{1t}X_t^{d_t} & \equiv 0 & \pmod{p} \\ a_{21}X_1^{d_1} & +a_{22}X_2^{d_2}+\cdots+ & a_{2t}X_t^{d_t} & \equiv 0 & \pmod{p} \\ \quad\vdots & & \quad\vdots & & \\ a_{n1}X_1^{d_1} & +a_{n2}X_2^{d_2}+\cdots+ & a_{nt}X_t^{d_t} & \equiv 0 & \pmod{p}. \end{array}\right.$$

Assume that the coefficients' matrix satisfies the hypothesis (H). From Theorem 1.1 we have an estimate on N_p, the number of solutions in $[0, p-1]^t$. Indeed, the following estimate holds:

$$\left|N_p - p^{t-n}\right| \leq p^{\frac{t-n+1}{2}} (6nd_1)^{t+1}. \tag{5.2}$$

Let $m << p^{1-\delta}$ and suppose that $\delta < \frac{t-n-1}{2}$. Our purpose is to obtain an estimate on N_m, the number of solution in $[0, p-m-1]^t$. Let S_1 and S_2 the following intervals in $\mathbb{Z}$: $S_1 = [0, p-m-1]$ and $S_2 = [p-m, p-1]$. From the well known Zippel–Schwartz Lemma (see, e.g., [12]) we have that

$$|V \cap S_2^t| \leq d_1^t m^{t-n},$$

where $V \subset \mathbb{A}^t$ is the $\mathbb{F}_p$–variety defined by the polynomials $f_j := a_{j1}X_1^{d_1} + a_{j2}X_2^{d_2} + \cdots + a_{jt}X_t^{d_t} \in \mathbb{Z}[X_1, \ldots, X_t]$, $1 \leq j \leq n$. Then from (5.2)

$$\begin{aligned} \left||V \cap S_1^t| - (p-m)^{t-n}\right| &\leq \left||V \cap \mathbb{F}_p^t| - p^{t-n}\right| + |V \cap S_2^t| + (p^{t-n} - (p-m)^{t-n}) \\ &\leq p^{\frac{t-n+1}{2}} (6nd_1)^{t+1} + d_1^t m^{t-n} + m(t-n)p^{t-n-1} \\ &\leq 2p^{t-n-\delta}(6nd_1)^{t+1}(t-n), \end{aligned}$$

for $\delta > 0$. Finally the number of solutions in the t–cube $[0, p-m-1]^t$ satisfies $N_m = (p-m)^{t-n} + \mathcal{O}(p^{t-n-\delta})$ with $m << p^{1-\delta}$ and $\delta < \frac{t-n-1}{2}$.

Acknowledgements. The authors gratefully acknowledge the comments by the anonymous referees, which helped to significantly improve the presentation of the results of this paper.

References

[1] A. Cafure and G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. 12 (2006), no. 2, 155–185.

[2] A. Cafure and G. Matera, *An effective Bertini theorem and the number of rational points of a normal complete intersection over a finite field*, Acta Arith. 130 (2007), no. 1, 19–35.

[3] X. Cao, W-S. Chou and J. Gu, *On the number of solutions of certain diagonal equations over finite fields*, Finite Fields Appl. 42 (2016), 225–252.

[4] L. Caniglia, A. Galligo, and J. Heintz, *Equations for the projective closure and effective Nullstellensatz*, Discrete Appl. Math. 33 (1991), 11–23.

[5] L. Carlitz, *Some special equations in a finite field*, Pacific J. Math. 3 (1953), 13–24.

[6] F. N. Castro, I. Rubio, P. Guan and R. Figueroa, *On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p*, Finite Fields Appl. 14 (2008), no. 3, 648–657

[7] W.-S. Chou, G. L. Mullen and B. Wassermann, *On the number of solutions of equations of Dickson polynomials over finite fields*, Taiwanese J. Math.12 (2008), 917–931.

[8] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: an introduction to computational algebraic geometry and commutative algebra*. Undergrad. Texts Math. Springer, New York, 1992.

[9] P. Deligne, *La conjecture de Weil. I*, Inst. Hautes Etudes Sci. Publ. Math. (1974), no. 43, 273–307.

[10] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Grad. Texts in Math., vol. 150, Springer, New York, 1995.

[11] W. Fulton, *Intersection theory*, Springer, Berlin Heidelberg New York, 1984.

[12] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge Univ. Press, Cambridge, 1999.

[13] S. Ghorpade and G. Lachaud, *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields*, Mosc. Math. J. 2 (2002), no. 3, 589–631.

[14] S. Ghorpade and G. Lachaud, *Number of solutions of equations over finite fields and a conjecture of Lang and Weil*, Number Theory and Discrete Mathematics (Chandigarh, 2000) (New Delhi) (A.K. Agarwal et al., ed.), Hindustan Book Agency, (2002), 269–291.

[15] J. Harris, *Algebraic geometry: a first course*, Grad. Texts in Math., vol. 133, Springer, New York Berlin Heidelberg, 1992.

[16] T. Helleseth, *On the covering radius of cyclic linear codes and arithmetic codes*, Discrete Appl. Math. 11 (1985), no. 2, 157–173.

[17] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci. 24 (1983), no. 3, 239–277.

[18] K. Jiang, W. Gao, W. Cao, *Counting solutions to generalized Markoff-Hurwitz-type equations in finite fields*, Finite Fields Appl. 62 (2020).

[19] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser, Boston, 1985.

[20] G. Lachaud and R. Rolland, *On the number of points of algebraic sets over finite fields*, J. Pure Appl. Algebra 219 (2015), no. 11, 5117–5136.

[21] R. Lidl and H. Niederreiter, *Finite fields*, Addison–Wesley, Reading, Massachusetts, 1983.

[22] L. J. Mordell, *On a special polynomial congruence and exponential sums*, 1963 Calcutta Math. Soc. Golden Jubilee Commemoration Vol, 29–32 Calcutta Math. Soc., Calcutta.

[23] O. Moreno and F. N. Castro, *Divisibility properties for covering radius of certain cyclic codes*, IEEE Trans. Inform. Theory 49 (2003), no. 12, 3299–3303.

[24] Gary L. Mullen and Daniel Panario, *Handbook of Finite Fields (1st ed.)*, Chapman and Hall/CRC, 2013.

[25] M. Pérez and M. Privitelli, *Estimates on the number of rational solutions of variants of diagonal equations over finite fields*, Finite Fields and Appl. 68 (2020), Article ID 101728, 30 p.

[26] I.R. Shafarevich, *Basic algebraic geometry: Varieties in projective space*, Springer, Berlin Heidelberg New York, 1994.

[27] K. W. Spackman, *Simultaneous solutions to diagonal equations over finite fields*, J. Number Theory **11** (1979), no. 1, 100–115.

[28] K. W. Spackman, *On the number and distribution of simultaneous solutions to diagonal congruences*, Canadian J. Math. 33 (1981), no. 2, 421–436. .

[29] A. Tietäväinen, *On the non-trivial solvability of some systems of equations in finite fields*, Ann. Univ. Turku. Ser. A I 71 (1964), 1-5.

[30] A. Tietäväinen, *On systems of linear and quadratic equations in finite fields*, Ann. Acad. Sci. Fenn. Ser. A I no. 382 (1965), 1-5.

[31] A. Tietäväinen, *On the non-trivial solvability of some equations and systems of equations in finite fields*, Ann. Acad. Sci. Fenn. Ser. A I no. 360 (1965), 1-38.

[32] A. Tietäväinen, *On the solvability of equations in incomplete finite fields*, Ann. Univ. Turku. Ser. A I 102 (1967), 1-13.

[33] W. Vogel, *Results on Bézout's theorem*, Tata Inst. Fundam. Res. Lect. Math., vol. 74, Tata Inst. Fund. Res., Bombay, 1984.

[34] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), 497–508.

[35] J. Wolfmann, *Some systems of diagonal equations over finite fields*, Finite Fields Appl. 4 (1998), no. 1, 29–37.

[36] X. Zeng L. Hu, W. Jiang, Q. Yue and X. Cao, *The weight distribution of a class of p-ary cyclic codes*, Finite Fields Appl. 16 (2010), no. 1, 56–73.

[37] D. Zheng, X. Wang, X. Zeng and L. Hu, *The weight distribution of a family of p-ary cyclic codes*, Des. Codes Cryptogr. 75 (2015), no. 2, 263–275.

[1] Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina

[2] Universidad Nacional de General Sarmiento, Instituto de Ciencias, J.M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Buenos Aires, Argentina
Email address: mprivite@campus.ungs.edu.ar

[3] Universidad Nacional de Hurlingham, Instituto de Tecnología e Ingeniería, Av. Gdor. Vergara 2222 (B1688GEZ) Villa Tesei, Buenos Aires, Argentina
Email address: mariana.perez@unahur.edu.ar