ON THE VALUE SET OF SMALL FAMILIES OF POLYNOMIALS OVER A FINITE FIELD, I

EDA CESARATTO[1,2], GUILLERMO MATERA[1,2], MARIANA PÉREZ[1], AND MELINA PRIVITELLI[2,3]

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements, let $X_1, \dots, X_r$ be indeterminates over $\mathbb{F}_q$ and let $\mathbb{F}_q[X_1, \dots, X_r]$ denote the ring of r–variate polynomials with coefficients in $\mathbb{F}_q$. Let T be an indeterminate over $\mathbb{F}_q$ and let $f \in \mathbb{F}_q[T]$. We define the value set $\mathcal{V}(f)$ of f as $\mathcal{V}(f) := |\{f(c) : c \in \mathbb{F}_q\}|$ (cf. [**?**]). Birch and Swinnerton–Dyer established the following significant result [**?**]: for fixed $d \geq 1$, if f is a generic polynomial of degree d, then

$$\mathcal{V}(f) = \mu_d\, q + \mathcal{O}(q^{1/2}),$$

where $\mu_d := \sum_{r=1}^{d} (-1)^{r-1}/r!$ and the constant underlying the $\mathcal{O}$–notation depends only on d.

Results on the average value $\mathcal{V}(d, 0)$ of $\mathcal{V}(f)$ when f ranges over all monic polynomials in $\mathbb{F}_q[T]$ of degree d with $f(0) = 0$ were obtained by Uchiyama [**?**] and improved by Cohen [**?**]. More precisely, in [**?**, §2] it is shown that

$$\mathcal{V}(d, 0) = \sum_{r=1}^{d} (-1)^{r-1} \binom{q}{r} q^{1-r} = \mu_d\, q + \mathcal{O}(1).$$

However, if some of the coefficients of f are fixed, the results on the average value of $\mathcal{V}(f)$ are less precise. In fact, Uchiyama [**?**] and Cohen [**?**] obtain the result that we now state. Let be given s with $1 \leq s \leq d-2$ and $\boldsymbol{a} := (a_{d-1}, \dots, a_{d-s}) \in \mathbb{F}_q^s$. For every $\boldsymbol{b} := (b_{d-s-1}, \dots, b_1)$, let

$$f_{\boldsymbol{b}} := f_{\boldsymbol{b}}^{\boldsymbol{a}} := T^d + \sum_{i=1}^{s} a_{d-i} T^{d-i} + \sum_{i=s+1}^{d-1} b_{d-i} T^{d-i}.$$

Then for $p := \mathrm{char}(\mathbb{F}_q) > d$,

$$\mathcal{V}(d, s, \boldsymbol{a}) := \frac{1}{q^{d-s-1}} \sum_{\boldsymbol{b} \in \mathbb{F}_q^{d-s-1}} \mathcal{V}(f_{\boldsymbol{b}}) = \mu_d\, q + \mathcal{O}(q^{1/2}), \tag{1.1}$$

where the constant underlying the $\mathcal{O}$–notation depends only on d and s.

This paper is devoted to obtain an strengthened explicit version of (**??**), which holds without any restriction on p. More precisely, we shall show the following result (see Theorem **??** below).

Date: May 4, 2014.

The authors were partially supported by the grant PIP 11220090100421 CONICET..

Theorem 1.1. *With notations as above, for $1 \leq s \leq \frac{d}{2} - 1$ we have*

$$|\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d\, q| \leq \frac{e^{-1}}{2} + 2\,\frac{(d-2)^5 e^{2\sqrt{d}}}{2^d} + \frac{2(d-s)}{q}.$$

This result strengthens (**??**) in several aspects. The first one is that it holds without any restriction on the characteristic p of $\mathbb{F}_q$, while (**??**) holds for $p > d$. The second aspect is that we show that $\mathcal{V}(d,s,\boldsymbol{a}) = \mu_d\, q + \mathcal{O}(1)$, while (**??**) only asserts that $\mathcal{V}(d,s,\boldsymbol{a}) = \mu_d\, q + \mathcal{O}(q^{1/2})$. Finally, we obtain an explicit expression for the constant underlying the $\mathcal{O}$–notation with a good behavior.

On the other hand, it must be said that our result holds for $s \leq d/2 - 1$, while (**??**) holds for s varying in a larger range of values. This aspect shall be addressed in a forthcoming paper, where we obtain an explicit estimate showing that $\mathcal{V}(d,s,\boldsymbol{a}) = \mu_d\, q + \mathcal{O}(q^{1/2})$ which is valid for $1 \leq s \leq d-3$ and $p > 2$. We shall also exhibit estimates on the average value of the second moment of ****.

In order to obtain our estimate, we express the quantity $\mathcal{V}(d,s,\boldsymbol{a})$ in terms of the number $\chi(\boldsymbol{a}, r)$ of certain "interpolating sets" with $d-s+1 \leq r \leq d$ (see Theorem **??** below). More precisely, for $f_{\boldsymbol{a}} := T^d + a_{d-1}T^{d-1} + \cdots + a_{d-s}T^{d-s}$, we define $\chi(\boldsymbol{a}, r)$ as the number of r–element subsets of $\mathbb{F}_q$ at which $f_{\boldsymbol{a}}$ can be interpolated by a polynomial of degree at most $d-s-1$.

Then we express $\chi(\boldsymbol{a}, r)$ in terms of the number of q–rational solutions with pairwise–distinct coordinates of a polynomial system $\{R^{\boldsymbol{a}}_{d-s} = 0, \ldots, R^{\boldsymbol{a}}_{r-1} = 0\}$, where $R^{\boldsymbol{a}}_{d-s}, \ldots, R^{\boldsymbol{a}}_{r-1}$ are certain polynomials in $\mathbb{F}_q[X_1, \ldots, X_r]$. A critical point for our approach is that $R^{\boldsymbol{a}}_{d-s}, \ldots, R^{\boldsymbol{a}}_{r-1}$ are symmetric polynomials, namely invariant under any permutation of the variables $X_1, \ldots, X_r$. More precisely, we prove that each $R^{\boldsymbol{a}}_j$ can be expressed as a polynomial in the first s elementary symmetric polynomials of $\mathbb{F}_q[X_1, \ldots, X_r]$ (Proposition **??**). This allows us to establish a number of facts concerning the geometry of set $V^{\boldsymbol{a}}_r$ of solutions of such a polynomial system (see, e.g., Corollary **??** and Theorems **??** and **??**). Combining these results with estimates on the number of q–rational points of singular complete intersections of [**?**], we obtain our main result.

We finish this introduction by stressing on the methodological aspects. As mentioned before, a key point is the invariance of the family of sets $V^{\boldsymbol{a}}_r$ under the action of the symmetric group of r elements. In fact, our results on the geometry of $V^{\boldsymbol{a}}_r$ and the estimates on the number of q–rational points can be extended *mutatis mutandis* to any symmetric complete intersection whose projection on the set of primary invariants (using the terminology of invariant theory) defines a nonsingular complete intersection. This might be seen as a further source of interest of our approach, since symmetric polynomials arise frequently in combinatorics, coding theory and cryptography (for example, in the study of deep holes in Reed–Solomon codes, almost perfect nonlinear polynomials or differentially uniform mappings; see, e.g., [**?**], [**?**] or [**?**]).

2. Value sets in terms of interpolating sets

Let notations and assumptions be as in the previous section. In this section we fix s with $1 \leq s \leq d-1$, an s–tuple $\boldsymbol{a} := (a_{d-1}, \ldots, a_{d-s}) \in \mathbb{F}_q^s$ and denote

$$f_{\boldsymbol{a}} := T^d + a_{d-1}T^{d-1} + \cdots + a_{d-s}T^{d-s}.$$

For every $\boldsymbol{b} := (b_{d-s-1}, \ldots, b_1) \in \mathbb{F}_q^{d-s-1}$, we denote by $f_{\boldsymbol{b}} := f_{\boldsymbol{b}}^{\boldsymbol{a}} \in \mathbb{F}_q[T]$ the following polynomial

$$f_{\boldsymbol{b}} := f_{\boldsymbol{a}} + b_{d-s-1}T^{d-s-1} + \cdots + b_1 T.$$

For a given $\boldsymbol{b} \in \mathbb{F}_q^{d-s-1}$, the value set $\mathcal{V}(f_{\boldsymbol{b}})$ of $f_{\boldsymbol{b}}$ equals the number of elements $b_0 \in \mathbb{F}_q$ for which the polynomial $f_{\boldsymbol{b}} + b_0$ has at least one root in $\mathbb{F}_q$. Let $\mathbb{F}_q[T]_d$ denote the set of polynomials of $\mathbb{F}_q[T]$ of degree at most d, let $\mathcal{N} : \mathbb{F}_q[T]_d \to \mathbb{Z}_{\geq 0}$ be the random variable which counts the number of roots in $\mathbb{F}_q$ of a given polynomial and let $\mathbf{1}_{\{\mathcal{N}>0\}} : \mathbb{F}_q[T]_d \to \{0,1\}$ be the characteristic function of the set of elements of $\mathbb{F}_q[T]_d$ having at least one root in $\mathbb{F}_q$. From our previous assertion we deduce the following identity:

$$\sum_{\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}} \mathcal{V}(f_{\boldsymbol{b}}) = \sum_{b_0\in\mathbb{F}_q} \sum_{\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}} \mathbf{1}_{\{\mathcal{N}>0\}}(f_{\boldsymbol{b}} + b_0) = \big|\{g \in \mathbb{F}_q[T]_{d-s-1} : \mathcal{N}(f_{\boldsymbol{a}} + g) > 0\}\big|.$$

For a set $\mathcal{X} \subseteq \mathbb{F}_q$, we define $\mathcal{S}_{\mathcal{X}}^{\boldsymbol{a}}$ as the set $\mathbb{F}_q[T]_{d-s-1}$ of polynomials of $\mathbb{F}_q[T]$ of degree at most $d-s-1$ which interpolate $-f_{\boldsymbol{a}}$ at all the points of $\mathcal{X}$, namely

$$\mathcal{S}_{\mathcal{X}}^{\boldsymbol{a}} := \{g \in \mathbb{F}_q[T]_{d-s-1} : (f_{\boldsymbol{a}} + g)(x) = 0 \textit{ for any } x \in \mathcal{X}\}.$$

Finally, for $r \in \mathbb{N}$ we shall use the symbol $\mathcal{X}_r$ to denote a subset of $\mathbb{F}_q$ of r elements.

Theorem 2.1. *Let be given $s, d \in \mathbb{N}$ with $1 \leq s \leq d-1$. Then we have*

$$\mathcal{V}(d, s, \boldsymbol{a}) = \sum_{r=1}^{d-s} (-1)^{r-1} \binom{q}{r} q^{1-r} + \frac{1}{q^{d-s-1}} \sum_{r=d-s+1}^{d} (-1)^{r-1} \chi(\boldsymbol{a}, r), \tag{2.1}$$

*where $\mathcal{V}(d, s, \boldsymbol{a})$ is defined as in (**??**) and $\chi(\boldsymbol{a}, r)$ is the number of subsets $\mathcal{X}_r$ of $\mathbb{F}_q$ of r elements such that there exists $g \in \mathbb{F}_q[T]_{d-s-1}$ for which $(f_{\boldsymbol{a}} + g)|_{\mathcal{X}_r} \equiv 0$ holds.*

Proof. Given a subset $\mathcal{X}_r := \{x_1, \ldots, x_r\} \subset \mathbb{F}_q$, we consider the corresponding set $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}} \subset \mathbb{F}_q[T]_{d-s-1}$ defined as above. It is easy to see that $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}} = \bigcap_{i=1}^{r} S_{\{x_i\}}^{\boldsymbol{a}}$ and

$$\{g \in \mathbb{F}_q[T]_{d-s-1} : \mathcal{N}(f_{\boldsymbol{a}} + g) > 0\} = \bigcup_{x\in\mathbb{F}_q} \mathcal{S}_{\{x\}}^{\boldsymbol{a}}.$$

Therefore, by the inclusion–exclusion principle we obtain

$$\mathcal{V}(d, s, \boldsymbol{a}) = \frac{1}{q^{d-s-1}} \left| \bigcup_{x\in\mathbb{F}_q} S_{\{x\}}^{\boldsymbol{a}} \right| = \frac{1}{q^{d-s-1}} \sum_{r=1}^{q} (-1)^{r-1} \sum_{\mathcal{X}_r \subseteq \mathbb{F}_q} \left| \mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}} \right|. \tag{2.2}$$

Now we estimate $|\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}|$ for a given set $\mathcal{X}_r := \{x_1, \ldots, x_r\} \subset \mathbb{F}_q$. Let $g := b_{d-s-1}T^{d-s-1} + \ldots + b_1 T + b_0$ be an arbitrary element of $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$. Then we have $f_{\boldsymbol{a}}(x_i) + g(x_i) = 0$ for $1 \leq i \leq r$. These identities can be expressed in matrix form as follows:

$$\mathcal{M}(\mathcal{X}_r) \cdot \widehat{\boldsymbol{b}} + f_{\boldsymbol{a}}(\mathcal{X}_r) = 0$$

where $\mathcal{M}(\mathcal{X}_r) := (m_{i,j}) \in \mathbb{F}_q^{r\times(d-s)}$ is the Vandermonde matrix defined by $m_{i,j} := x_i^{d-s-j}$ for $1 \leq i \leq r$ and $1 \leq j \leq d-s$, $\widehat{\boldsymbol{b}} := (b_{d-s-1}, \ldots, b_0) \in \mathbb{F}_q^{d-s}$ and $f_{\boldsymbol{a}}(\mathcal{X}_r) := (f_{\boldsymbol{a}}(x_1), \ldots, f_{\boldsymbol{a}}(x_r)) \in \mathbb{F}_q^r$.

Since $x_i \neq x_j$ for $i \neq j$, it follows that

$$\operatorname{rank}(\mathcal{M}(\mathcal{X}_r)) = \min\{r, d-s\}. \tag{2.3}$$

We conclude that $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ is an $\mathbb{F}_q$–linear variety and either $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}} = \emptyset$ or

$$\operatorname{rank}(\mathcal{M}(\mathcal{X}_r)) + \dim \mathcal{S}_{\mathcal{X}_r}(f_{\boldsymbol{a}}) = d-s. \tag{2.4}$$

Suppose first that $r \leq d-s$. Then (**??**) implies $\mathrm{rank}(\mathcal{M}(\mathcal{X}_r)) = r$, and hence, $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ is not empty. From (**??**) one obtains $\dim \mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}} = d-s-r$ and then

$$|\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}| = q^{d-s-r}. \tag{2.5}$$

Next we suppose that $r \geq d-s+1$. On one hand, if $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ is nonempty, then (**??**) implies $\dim \mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}} = 0$, and hence $|\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}| = 1$. On the other hand, if $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ is empty, then $|\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}| = 0$.

For $r > d$ we have that, if $g \in \mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$, then $g \in \mathbb{F}_q[T]_{d-s-1}$ and $f_{\boldsymbol{a}}(x_i) + g(x_i) = 0$ holds for $1 \leq i \leq r$. As a consequence, the (nonzero) polynomial $f_{\boldsymbol{a}} + g$ has degree d and r different roots, which contradicts the hypothesis $r > d$. We conclude that $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ is empty, and thus,

$$|\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}| = 0. \tag{2.6}$$

Finally, for $d-s+1 \leq r \leq d$ any of the cases $|\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}| = 0$ or $|\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}| = 1$ can arise.

Now we are able to obtain the expression for $\mathcal{V}(d,s,\boldsymbol{a})$ of the statement of the theorem. Combining (**??**), (**??**) and (**??**) we obtain

$$\mathcal{V}(d,s,\boldsymbol{a}) = \sum_{r=1}^{d-s} (-1)^{r-1} \binom{q}{r} q^{d-s-r} + \sum_{r=d-s+1}^{d} (-1)^{r-1} \sum_{\mathcal{X}_r \subset \mathbb{F}_q} |\mathcal{S}_{\mathcal{X}_r}(f_{\boldsymbol{a}})|.$$

From this identity we immediately deduce the statement of the theorem. □

Remark 2.2. ****Observe that $0 \leq \chi(\boldsymbol{a}, r) \leq \binom{q}{r}$ holds.****

Remark 2.3. ****If $d-s \geq q$, then $\sum_{r=d-s+1}^{d} (-1)^{r-1} \binom{q}{r} \chi(\boldsymbol{a}, r) = 0$.****

2.1. **An algebraic approach to estimate the number of interpolating sets.** According to Theorem **??**, the asymptotic behavior of $\mathcal{V}(d,s,\boldsymbol{a})$ is determined by that of $\chi(\boldsymbol{a}, r)$ for $d-s+1 \leq r \leq d$. In order to find the latter, we follow an approach inspired in [**?**], and further developed in [**?**], which we now describe.

Fix a set $\mathcal{X}_r := \{x_1, \ldots, x_r\} \subset \mathbb{F}_q$ of r elements and $g \in \mathbb{F}_q[T]_{d-s-1}$. Then g belongs to $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ if and only if $(T-x_1)\cdots(T-x_r)$ divides $f_{\boldsymbol{a}} + g$ in $\mathbb{F}_q[T]$. Since $\deg g \leq d-s-1 < r$, we have that the latter is equivalent to the condition that $-g$ is the remainder of the division of $f_{\boldsymbol{a}}$ by $(T-x_1)\cdots(T-x_r)$. In other words, the set $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ is not empty if and only if the remainder of the division of $f_{\boldsymbol{a}}$ by $(T-x_1)\cdots(T-x_r)$ has degree at most $d-s-1$.

Let $X_1, \ldots, X_r$ be indeterminates over $\overline{\mathbb{F}}_q$, let $X := (X_1, \ldots, X_r)$ and let $Q \in \mathbb{F}_q[X][T]$ be the polynomial

$$Q = (T-X_1)\cdots(T-X_r).$$

We have that there exists $R_{\boldsymbol{a}} \in \mathbb{F}_q[X][T]$ with $\deg R_{\boldsymbol{a}} \leq r-1$ such that the following relation holds:

$$f \equiv R_{\boldsymbol{a}} \mod Q. \tag{2.7}$$

Let $R_{\boldsymbol{a}} := R_{r-1}^{\boldsymbol{a}}(X) T^{r-1} + \cdots + R_0^{\boldsymbol{a}}(X)$. Then $R_{\boldsymbol{a}}(x_1, \ldots, x_r, T) \in \mathbb{F}_q[T]$ is the remainder of the division of $f_{\boldsymbol{a}}$ by $(T-x_1)\cdots(T-x_r)$. As a consequence, the set $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ is not empty if and only if the following identities hold:

$$R_j^{\boldsymbol{a}}(x_1, \ldots, x_r) = 0 \quad (d-s \leq j \leq r-1). \tag{2.8}$$

On the other hand, suppose that there exists $\mathbf{x} := (x_1, \ldots, x_r) \in \mathbb{F}_q^r$ with pairwise–distinct coordinates such that (**??**) holds and set $\mathcal{X}_r := \{x_1, \ldots, x_r\}$. Then the remainder of the division of $f_{\boldsymbol{a}}$ by $Q(\mathbf{x},T)=(T-x_1)\cdots(T-x_r)$ is a polynomial $r_{\boldsymbol{a}}:=R_{\boldsymbol{a}}(\mathbf{x},T)$ of degree at most $d-s-1$. This shows that $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ is not empty. We summarize the conclusions of the argumentation above in the following result.

Lemma 2.4. *Let $s,d\in\mathbb{N}$ with $1\le s\le d-1$, let $R_j^{\boldsymbol{a}}$ $(d-s\le j\le r-1)$ be the polynomials of (??) and let $\mathcal{X}_r:=\{x_1,\dots,x_r\}\subset\mathbb{F}_q$ be a set with r elements. Then $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ is not empty if and only if (??) holds.*

It follows that the number $\chi(\boldsymbol{a},r)$ of sets $\mathcal{X}_r\subset\mathbb{F}_q$ of r elements such that $S_{\mathcal{X}_r}^{\boldsymbol{a}}$ is not empty equals the number of points $\mathbf{x}:=(x_1,\dots,x_r)\in\mathbb{F}_q^r$ with pairwise–distinct coordinates satisfying (**??**), up to permutations of coordinates, namely $1/r!$ times the number of solutions $\mathbf{x}\in\mathbb{F}_q^r$ of the following system of equalities and non-equalities:

$$R_j^{\boldsymbol{a}}(X_1,\dots,X_r)=0\quad(d-s\le j\le r-1),\ \prod_{1\le i<j\le r}(X_i-X_j)\ne 0. \tag{2.9}$$

2.2. $R_{\boldsymbol{a}}$ **in terms of the elementary symmetric polynomials.** Fix r with $d-s+1\le r\le d$. Assume that $2(s+1)\le d$ holds and consider the elementary symmetric polynomials $\Pi_1,\dots,\Pi_r$ of $\mathbb{F}_q[X_1,\dots,X_r]$. For convenience of notation, we shall denote $\Pi_0:=1$. In Section **??** we obtain polynomials $R_j^{\boldsymbol{a}}\in\mathbb{F}_q[X_1,\dots,X_r]$ $(d-s\le j\le r-1)$ with the following property: for a given set $\mathcal{X}_r:=\{x_1,\dots,x_r\}\subset\mathbb{F}_q$ of r elements, the set $\mathcal{S}_{\mathcal{X}_r}^{\boldsymbol{a}}$ is not empty if and only if $(x_1,\dots,x_r)$ is a common zero of $R_{d-s}^{\boldsymbol{a}},\dots,R_{r-1}^{\boldsymbol{a}}$.

The main purpose of this section is to show how the polynomials $R_j^{\boldsymbol{a}}$ can be expressed in terms of the elementary symmetric polynomials $\Pi_1,\dots,\Pi_{s-2}$. In order to do this, we first obtain a recursive expression for the remainder of the division of T^j by $Q:=(T-X_1)\cdots(T-X_r)$ for $r\le j\le d$.

Lemma 2.5. *For $r\le j\le d$, the following congruence relation holds:*

$$T^j\equiv H_{r-1,j}T^{r-1}+H_{r-2,j}T^{r-2}+\cdots+H_{0,j}\mod Q, \tag{2.10}$$

where each $H_{i,j}$ is equal to zero or an homogeneous element of $\mathbb{F}_q[X_1,\dots,X_r]$ of degree $j-i$. Furthermore, for $j-i\le r$, the polynomial $H_{i,j}$ is a monic element of $\mathbb{F}_q[\Pi_1,\dots,\Pi_{j-i-1}][\Pi_{j-i}]$, up to a nonzero constant of $\mathbb{F}_q$.

Proof. We argue by induction on $j\ge r$. Taking into account that

$$T^r\equiv\Pi_1T^{r-1}-\Pi_2T^{r-2}+\cdots+(-1)^{r-1}\Pi_r\mod Q, \tag{2.11}$$

we immediately deduce (**??**) for $j=r$.

Next assume that (**??**) holds for a given j with $r\le j$. Multiplying both sides of (**??**) by T and combining with (**??**) we obtain:

$$\begin{aligned}T^{j+1}&\equiv H_{r-1,j}T^r+H_{r-2,j}T^{r-1}+\cdots+H_{0,j}T\\&\equiv(\Pi_1H_{r-1,j}+H_{r-2,j})T^{r-1}+\cdots+((-1)^{r-2}\Pi_{r-1}H_{r-1,j}+H_{0,j})T\\&\quad+(-1)^{r-1}\Pi_rH_{r-1,j},\end{aligned}$$

where both congruences are taken modulo Q.

Define

$$\begin{aligned}H_{k,j+1}&:=(-1)^{r-1-k}\Pi_{r-k}H_{r-1,j}+H_{k-1,j}\ \textit{for}\ 1\le k\le r-1,\\H_{0,j+1}&:=(-1)^{r-1}\Pi_rH_{r-1,j}.\end{aligned}$$

Then we have

$$T^{j+1} \equiv H_{r-1,j+1}T^{r-1} + H_{r-2,j+1}T^{r-2} + \cdots + H_{0,j+1} \mod Q.$$

There remains to prove that the polynomials $H_{k,j+1}$ have the form asserted.

Fix k with $1 \le k \le r-1$. Then $H_{k,j+1} = (-1)^{r-1-k}\Pi_{r-k}H_{r-1,j} + H_{k-1,j}$. By the inductive hypothesis we have that $H_{r-1,j}$ and $H_{k-1,j}$ are equal to zero or homogeneous polynomials of degree $j-r+1$ and $j-k+1$ respectively. We easily conclude that $H_{k,j+1}$ is equal to zero or homogeneous of degree $j-k+1$. Further, for $j+1-k \le r$, since $\max\{r-k, j-r+1\} \le j-k < r$ we see that $\Pi_{r-k}H_{r-1,j}$ is an element of the polynomial ring $\mathbb{F}_q[\Pi_1,\dots,\Pi_{j-k}]$. On the other hand, $H_{k-1,j}$ is a monic element of $\mathbb{F}_q[\Pi_1,\dots,\Pi_{j-k}][\Pi_{j-k+1}]$, up to a nonzero constant of $\mathbb{F}_q$, which implies that so is $H_{k,j+1}$.

Finally, for $k=0$ we have $H_{0,j+1} := (-1)^{r-1}\Pi_r H_{r-1,j}$, which shows that $H_{0,j+1}$ is equal to zero or an homogeneous polynomials of $\mathbb{F}_q[X_1,\dots,X_r]$ of degree $r+j-r+1 = j+1$. This finishes the proof of the lemma. □

We observe that an explicit expression of the polynomials $H_{i,j}$ can be obtained following the approach of [**?**, Proposition 2.2]. As we do not need such an explicit expression we shall not pursue this point any further.

Finally we obtain an expression of the polynomials $R_j^{\boldsymbol{a}} \in \mathbb{F}_q[X_1,\dots,X_r]$ $(d-s \le j \le r-1)$ in terms of the polynomials $H_{i,j}$.

Proposition 2.6. *Let $s,d \in \mathbb{N}$ with $1 \le s \le d-1$ and $2(s+1) \le d$. For $d-s \le j \le r-1$, the following identity holds:*

$$R_j^{\boldsymbol{a}} = a_j + \sum_{i=r}^{d} a_i H_{j,i}, \tag{2.12}$$

where the polynomials $H_{j,i}$ are defined in Lemma **??**. *In particular, $R_j^{\boldsymbol{a}}$ is a monic element of $\mathbb{F}_q[\Pi_1,\dots,\Pi_{d-1-j}][\Pi_{d-j}]$ of degree $d-j \le s$ for $d-s \le j \le r-1$.*

Proof. By Lemma **??** we have the following congruence relation for $r \le j \le d$:

$$T^j \equiv H_{r-1,j}T^{r-1} + H_{r-2,j}T^{r-2} + \cdots + H_{0,j} \mod Q.$$

Hence we obtain

$$\begin{aligned}
\sum_{j=d-s}^{d} a_j T^j &= \sum_{j=d-s}^{r-1} a_j T^j + \sum_{j=r}^{d} a_j T^j \\
&\equiv \sum_{j=d-s}^{r-1} a_j T^j + \sum_{j=r}^{d} a_j \sum_{i=d-s}^{r-1} H_{i,j}T^i + \mathcal{O}(T^{d-s-1}) \mod Q \\
&\equiv \sum_{j=d-s}^{r-1} \Big(a_j + \sum_{i=r}^{d} a_i H_{j,i}\Big) T^j + \mathcal{O}(T^{d-s-1}) \mod Q,
\end{aligned}$$

where $\mathcal{O}(T^{d-s-1})$ represents a sum of terms of $\mathbb{F}_q[X_1,\dots,X_r][T]$ of degree at most $d-s-1$ in T. This shows that the polynomials $R_j^{\boldsymbol{a}}$ have the form asserted in (**??**). Furthermore, we observe that, for each $H_{j,i}$ occurring in (**??**), we have $i-j \le s \le d-s-2 \le r$. This implies that each $H_{j,i}$ is a monic element of $\mathbb{F}_q[\Pi_1,\dots,\Pi_{i-j-1}][\Pi_{i-j}]$ of degree $i-j$. As a consequence, we see that $R_j^{\boldsymbol{a}}$ is a monic element of $\mathbb{F}_q[\Pi_1,\dots,\Pi_{d-1-j}][\Pi_{d-j}]$ of degree $d-j$ for $d-s \le j \le r-1$. This finishes the proof. □

3. The geometry of the set of zeros of $R^{\boldsymbol{a}}_{d-s},\dots,R^{\boldsymbol{a}}_{r-1}$

For positive integers s, d with $1\le s\le d-1$ and $2(s+1)\le d$, we fix as in the previous section an s–tuple $\boldsymbol{a}:=(a_{d-1},\dots,a_{d-s})\in\mathbb{F}_q^s$ and consider the polynomial $f_{\boldsymbol{a}}:=T^d+a_{d-1}T^{d-1}+\cdots+a_{d-s}T^{d-s}$. For fixed r with $d-s+1\le r\le d$, in Section **??** we associate to $f_{\boldsymbol{a}}$ polynomials $R^{\boldsymbol{a}}_j\in\mathbb{F}_q[X_1,\dots,X_r]$ $(d-s\le j\le r-1)$, whose sets of common q–rational zeros are relevant for our purposes.

According to Proposition **??**, we may express each $R^{\boldsymbol{a}}_j$ as a polynomial in the first s elementary symmetric polynomials $\Pi_1,\dots,\Pi_s$ of $\mathbb{F}_q[X_1,\dots,X_r]$. More precisely, let $Y_1,\dots,Y_s$ be new indeterminates over $\overline{\mathbb{F}}_q$. Then we have that

$$R^{\boldsymbol{a}}_j=S^{\boldsymbol{a}}_j(\Pi_1,\dots,\Pi_{d-j})\quad(d-s\le j\le r-1),$$

where each $S^{\boldsymbol{a}}_j\in\mathbb{F}_q[Y_1,\dots,Y_{d-j}]$ is a monic element of $\mathbb{F}_q[Y_1,\dots,Y_{d-1-j}][Y_{d-j}]$ of degree 1 in Y_{d-j}.

In this section we obtain critical information on the geometry of the set of common zeros of the polynomials $R^{\boldsymbol{a}}_j$ that will allow us to establish estimates on the number of common q–rational zeros of $R^{\boldsymbol{a}}_{d-s},\dots,R^{\boldsymbol{a}}_{r-1}$.

3.1. **Notions of algebraic geometry.**

Since our approach relies on tools of algebraic geometry, we briefly collect the basic definitions and facts that we need in the sequel. We use standard notions and notations of algebraic geometry, which can be found in, e.g., [**?**], [**?**].

We denote by $\mathbb{A}^n$ the affine n–dimensional space $\overline{\mathbb{F}}_q^n$ and by $\mathbb{P}^n$ the projective n–dimensional space over $\overline{\mathbb{F}}_q^{n+1}$. Both spaces are endowed with their respective Zariski topologies, for which a closed set is the zero locus of polynomials of $\overline{\mathbb{F}}_q[X_1,\dots,X_n]$ or of homogeneous polynomials of $\overline{\mathbb{F}}_q[X_0,\dots,X_n]$. For $\mathbb{K}:=\mathbb{F}_q$ or $\mathbb{K}:=\overline{\mathbb{F}}_q$, we say that a subset $V\subset\mathbb{A}^n$ is an affine $\mathbb{K}$–variety if it is the set of common zeros in $\mathbb{A}^n$ of polynomials $F_1,\dots,F_m\in\mathbb{K}[X_1,\dots,X_n]$. Correspondingly, a projective $\mathbb{K}$–variety is the set of common zeros in $\mathbb{P}^n$ of a family of homogeneous polynomials $F_1,\dots,F_m\in\mathbb{K}[X_0,\dots,X_n]$. We shall frequently denote by $V(F_1,\dots,F_m)$ the affine or projective $\mathbb{K}$–variety consisting of the common zeros of polynomials $F_1,\dots,F_m$. The set $V(\mathbb{F}_q):=V\cap\mathbb{F}_q^n$ is the set of q–rational points of V.

A $\mathbb{K}$–variety V is $\mathbb{K}$–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 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, which are called the irreducible (absolutely irreducible) $\mathbb{K}$–components of V.

For a $\mathbb{K}$-variety V contained in $\mathbb{A}^n$ or $\mathbb{P}^n$, we denote by $I(V)$ its defining ideal, namely the set of polynomials of $\mathbb{K}[X_1,\dots,X_n]$, or of $\mathbb{K}[X_0,\dots,X_n]$, vanishing on V. The coordinate ring $\mathbb{K}[V]$ of V is the quotient ring $\mathbb{K}[X_1,\dots,X_n]/I(V)$ or $\mathbb{K}[X_0,\dots,X_n]/I(V)$. The dimension $\dim V$ of a $\mathbb{K}$-variety V is the length r of the longest chain $V_0\subsetneq V_1\subsetneq\cdots\subsetneq V_r$ of nonempty irreducible $\mathbb{K}$-varieties contained in V. A $\mathbb{K}$–variety is called equidimensional if all its irreducible $\mathbb{K}$–components are of the same dimension.

The degree $\deg V$ of an irreducible $\mathbb{K}$-variety V is the maximum number of points lying in the intersection of V with a generic linear space L of codimension $\dim V$, for which $V\cap L$ is a finite set. More generally, following [**?**] (see also [**?**]), 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

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

An important tool for our estimates is the following *Bézout inequality* (see [**?**], [**?**], [**?**]): if V and W are $\mathbb{K}$–varieties, then the following inequality holds:

$$\deg(V \cap W) \leq \deg V \cdot \deg W. \tag{3.1}$$

We shall also make use of the following well–known identities relating the degree of an affine $\mathbb{K}$–variety $V \subset \mathbb{A}^n$, the degree of its projective closure (with respect to the projective Zariski $\mathbb{K}$–topology) $\overline{V} \subset \mathbb{P}^n$ and the degree of the affine cone $\widetilde{V}$ of $\overline{V}$ (see, e.g., [**?**, Proposition 1.11]):

$$\deg V = \deg \overline{V} = \deg \tilde{V}.$$

Elements $F_1, \ldots, F_{n-r}$ in $\mathbb{K}[X_1, \ldots, X_n]$ or in $\mathbb{K}[X_0, \ldots, X_n]$ form a regular sequence if F_1 is nonzero and each F_i is not a zero divisor in the quotient ring $\mathbb{K}[X_1, \ldots, X_n]/(F_1, \ldots, F_{i-1})$ or $\mathbb{K}[X_0, \ldots, X_n]/(F_1, \ldots, F_{i-1})$ for $2 \leq i \leq n-r$. In such a case, the (affine or projective) $\mathbb{K}$–variety $V := V(F_1, \ldots, F_{n-r})$ they define is equidimensional of dimension r, and is called a set–theoretic complete intersection. If the ideal $(F_1, \ldots, F_{n-r})$ generated by $F_1, \ldots, F_{n-r}$ is radical, then we say that V is an ideal–theoretic complete intersection. If $V \subset \mathbb{P}^n$ is an ideal–theoretic complete intersection defined over $\mathbb{K}$, of dimension r and degree δ, and $F_1, \ldots, F_{n-r}$ is a system of generators of $I(V)$, the degrees $d_1, \ldots, d_{n-r}$ depend only on V and not on the system of generators. Arranging the d_i in such a way that $d_1 \geq d_2 \geq \cdots \geq d_{n-r}$, we call $\boldsymbol{d} := (d_1, \ldots, d_{n-r})$ the multidegree of V. In particular, it follows that $\delta = \prod_{i=1}^{n-r} d_i$ holds.

Let V be a variety contained in $\mathbb{A}^n$ and let $I(V) \subset \overline{\mathbb{F}}_q[X_1, \ldots, X_n]$ be the defining ideal of V. Let $\mathbf{x}$ be a point of V. The dimension $\dim_{\mathbf{x}} V$ of V at $\mathbf{x}$ is the maximum of the dimensions of the irreducible components of V that contain $\mathbf{x}$. If $I(V) = (F_1, \ldots, F_m)$, the tangent space $\mathcal{T}_{\mathbf{x}} V$ to V at $\mathbf{x}$ is the kernel of the Jacobian matrix $(\partial F_i / \partial X_j)_{1 \leq i \leq m, 1 \leq j \leq n}(\mathbf{x})$ of the polynomials $F_1, \ldots, F_m$ with respect to $X_1, \ldots, X_n$ at $\mathbf{x}$. The point $\mathbf{x}$ is regular if $\dim \mathcal{T}_{\mathbf{x}} V = \dim_{\mathbf{x}} V$ holds. Otherwise, the point $\mathbf{x}$ is called singular. The set of singular points of V is the singular locus $\mathrm{Sing}(V)$ of V. A variety is called nonsingular if its singular locus is empty. For a projective variety, the concepts of tangent space, regular and singular point can be defined by considering an affine neighborhood of the point under consideration.

Let V and W be irreducibles $\mathbb{K}$–varieties of the same dimension and let $f : V \to W$ be a regular map for which $\overline{f(V)} = W$ holds, where $\overline{f(V)}$ denotes the closure of $f(V)$ with respect to the Zariski topology of W. Then f induces a ring extension $\mathbb{K}[W] \hookrightarrow \mathbb{K}[V]$ by composition with f. We say that f is a finite morphism if this extension is integral, namely if each element $\eta \in \mathbb{K}[V]$ satisfies a monic equation with coefficients in $\mathbb{K}[W]$. A basic fact is that a finite morphism is necessarily closed. Another fact concerning finite morphisms we shall use in the sequel is that the preimage $f^{-1}(S)$ of an irreducible closed subset $S \subset W$ is equidimensional of dimension $\dim S$.

3.2. **The singular locus of symmetric complete intersections.** With the notations and assumptions of the beginning of Section **??**, let $V_r^{\boldsymbol{a}} \subset \mathbb{A}^r$ be the affine

$\mathbb{F}_q$–variety defined by the polynomials $R^{\boldsymbol{a}}_{d-s},\dots,R^{\boldsymbol{a}}_{r-1}\in\mathbb{F}_q[X_1,\dots,X_r]$. In this section we shall establish several facts concerning the geometry of $V_r^{\boldsymbol{a}}$. For this purpose, we consider the somewhat more general framework that we now introduce. This will allow us to make more transparent the facts concerning the algebraic structure of the family of polynomials $R^{\boldsymbol{a}}_{d-s},\dots,R^{\boldsymbol{a}}_{r-1}$ which are important at this point.

Let $Y_1,\dots,Y_s$ be new indeterminates over $\overline{\mathbb{F}}_q$ and let be given polynomials $S_j\in\mathbb{F}_q[Y_1,\dots,Y_s]$ for $d-s\le j\le r-1$. Let $(\partial S/\partial Y):=(\partial S_j/\partial Y_k)_{d-s\le j\le r-1,1\le k\le s}$ be the Jacobian matrix of $S_{d-s},\dots,S_{r-1}$ with respect to $Y_1,\dots,Y_s$. Our assumptions on s, d and r imply $r-d+s\le s$ and thus, $(\partial S/\partial Y)$ has full rank if and only if $\mathrm{rank}(\partial S/\partial Y)=r-d+s$ holds. Assume that $S_{d-s},\dots,S_{r-1}$ satisfy the following conditions:

(H1) $S_{d-s},\dots,S_{r-1}$ form a regular sequence of $\mathbb{F}_q[Y_1,\dots,Y_s]$;
(H2) $(\partial S/\partial Y)(\mathbf{y})$ has full rank $r-d+s$ for every $\mathbf{y}\in\mathbb{A}^s$.

From (H1) and (H2) we immediately conclude that the affine variety $W_r\subset\mathbb{A}^s$ defined by $S_{d-s},\dots,S_{r-1}$ is a nonsingular set–theoretic complete intersection of dimension $d-r$. Furthermore, as a consequence of [**?**, Theorem 18.15] we conclude that $S_{d-s},\dots,S_{r-1}$ define a radical ideal, and hence W_r is an ideal–theoretic complete intersection.

Let $\Pi_1,\dots,\Pi_s$ be the first s elementary symmetric polynomials of $\mathbb{F}_q[X_1,\dots,X_r]$ and let $R_j:=S_j(\Pi_1,\dots,\Pi_s)$ for $d-s\le j\le r-1$. We denote by $V_r\subset\mathbb{A}^r$ the affine variety defined by $R_{d-s},\dots,R_{r-1}$. In what follows we shall establish several facts concerning the geometry of V_r.

For this purpose, we consider the following surjective morphism of $\mathbb{F}_q$–varieties:

$$\begin{array}{rcl}\Pi^{\boldsymbol{r}}:\mathbb{A}^r & \to & \mathbb{A}^r\\ \mathbf{x} & \mapsto & (\Pi_1(\mathbf{x}),\dots,\Pi_r(\mathbf{x})).\end{array}$$

It is easy to see that $\Pi^{\boldsymbol{r}}$ is finite morphism (see, e.g., [**?**, §5.3, Example 1]). In particular, the preimage $(\Pi^{\boldsymbol{r}})^{-1}(Z)$ of an irreducible affine variety $Z\subset\mathbb{A}^r$ of dimension m is equidimensional and of dimension m (see, e.g., [**?**, §4.2, Proposition]).

We now consider $S_{d-s},\dots,S_{r-1}$ as elements of $\mathbb{F}_q[Y_1,\dots,Y_r]$. Since they form a regular sequence, the affine variety $W_j^{\boldsymbol{r}}=V(S_{d-s},\dots,S_j)\subset\mathbb{A}^r$ is equidimensional of dimension $r-j+d-s-1$. This implies that the affine variety $V_j^{\boldsymbol{r}}=(\Pi^{\boldsymbol{r}})^{-1}(W_j^{\boldsymbol{r}})$ defined by $R_{d-s},\dots,R_j$ is equidimensional of dimension $r-j+d-s-1$. We conclude that the polynomials $R_{d-s},\dots,R_{r-1}$ form a regular sequence of $\mathbb{F}_q[X_1,\dots,X_r]$ and deduce the following result.

Lemma 3.1. *Let $V_r\subset\mathbb{A}^r$ be the $\mathbb{F}_q$–variety defined by $R_{d-s},\dots,R_{r-1}$. Then V_r is a set–theoretic complete intersection of dimension $d-s$.*

Next we discuss the dimension of the singular locus of V_r. For this purpose, we consider the following surjective morphism of $\mathbb{F}_q$–varieties:

$$\begin{array}{rcl}\Pi:V_r & \to & W_r\\ \mathbf{x} & \mapsto & (\Pi_1(\mathbf{x}),\dots,\Pi_s(\mathbf{x})).\end{array}$$

For $\mathbf{x}\in V_r$ and $\mathbf{y}:=\Pi(\mathbf{x})$, we denote by $\mathcal{T}_{\mathbf{x}}V_r$ and $\mathcal{T}_{\mathbf{y}}W_r$ the tangent spaces to V_r at $\mathbf{x}$ and to W_r at $\mathbf{y}$. We also consider the differential map of Π at $\mathbf{x}$, namely

$$\begin{array}{rcl}\mathrm{d}_{\mathbf{x}}\Pi:\mathcal{T}_{\mathbf{x}}V_r & \to & \mathcal{T}_{\mathbf{y}}W_r\\ \mathbf{v} & \mapsto & A(\mathbf{x})\cdot\mathbf{v},\end{array}$$

where $A(\mathbf{x})$ stands for the $(s \times r)$–matrix

$$A(\mathbf{x}) := \begin{pmatrix} \frac{\partial \Pi_1}{\partial X_1}(\mathbf{x}) & \cdots & \frac{\partial \Pi_1}{\partial X_r}(\mathbf{x}) \\ \vdots & & \vdots \\ \frac{\partial \Pi_s}{\partial X_1}(\mathbf{x}) & \cdots & \frac{\partial \Pi_s}{\partial X_r}(\mathbf{x}) \end{pmatrix}. \tag{3.2}$$

In order to prove our result about the singular locus of V_r, we first make a few remarks concerning the Jacobian matrix of the elementary symmetric polynomials that will be useful in the sequel.

It is well known that the first partial derivatives of the elementary symmetric polynomials Π_i satisfy the following equalities (see, e.g., [**?**]) for $1 \le i, j \le r$:

$$\frac{\partial \Pi_i}{\partial X_j} = \Pi_{i-1} - X_j \Pi_{i-2} + X_j^2 \Pi_{i-3} + \cdots + (-1)^{i-1} X_j^{i-1}. \tag{3.3}$$

As a consequence, denoting by A_r the $(r \times r)$–Vandermonde matrix

$$A_r := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_r \\ \vdots & \vdots & & \vdots \\ X_1^{r-1} & X_2^{r-1} & \cdots & X_r^{r-1}, \end{pmatrix}, \tag{3.4}$$

we deduce that the Jacobian matrix of $\Pi_1, \ldots, \Pi_r$ with respect to $X_1, \ldots, X_r$ can be factored as follows:

$$\left(\frac{\partial \Pi_i}{\partial X_j}\right)_{1 \le i,j \le r} := B_r \cdot A_r := \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ \Pi_1 & -1 & 0 & & \\ \Pi_2 & -\Pi_1 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ \Pi_{r-1} & -\Pi_{r-2} & \Pi_{r-3} & \cdots & (-1)^{r-1} \end{pmatrix} \cdot A_r. \tag{3.5}$$

We observe that the left factor B_r is a square, lower–triangular matrix whose determinant is equal to $(-1)^{(r-1)r/2}$. This implies that the determinant of the matrix $(\partial \Pi_i / \partial X_j)_{1 \le i,j \le r}$ is equal, up to a sign, to the determinant of A_r, i.e.,

$$\det \left(\frac{\partial \Pi_i}{\partial X_j}\right)_{1 \le i,j \le r} = (-1)^{(r-1)r/2} \prod_{1 \le i < j \le r} (X_i - X_j).$$

Let $(\partial R / \partial X) := (\partial R_j / \partial X_k)_{d-s \le j \le r-1, 1 \le k \le r}$ be the Jacobian matrix of the polynomials $R_{d-s}, \ldots, R_{r-1}$ with respect to $X_1, \ldots, X_r$.

Theorem 3.2. *The set of points $\mathbf{x} \in \mathbb{A}^r$ for which $(\partial R / \partial X)(\mathbf{x})$ has not full rank has dimension at most $s-1$. In particular, the singular locus Σ_r of V_r has dimension at most $s-1$.*

Proof. By the chain rule we deduce that the partial derivatives of R_j satisfy the following equality for $1 \le k \le r$:

$$\frac{\partial R_j}{\partial X_k} = \left(\frac{\partial S_j}{\partial Y_1} \circ \Pi\right) \cdot \frac{\partial \Pi_1}{\partial X_k} + \cdots + \left(\frac{\partial S_j}{\partial Y_s} \circ \Pi\right) \cdot \frac{\partial \Pi_{s-2}}{\partial X_k}$$

Therefore we obtain

$$\left(\frac{\partial R}{\partial X}\right) = \left(\frac{\partial S}{\partial Y} \circ \Pi\right) \cdot \left(\frac{\partial \Pi}{\partial X}\right).$$

Fix an arbitrary point $\mathbf{x}$ for which $(\partial R/\partial X)(\mathbf{x})$ has not full rank. Let $\mathbf{v} \in \mathbb{A}^{r-d+s}$ a nonzero vector in the left kernel of $(\partial R/\partial X)(\mathbf{x})$. Then

$$\mathbf{0} = \mathbf{v} \cdot \left(\frac{\partial R}{\partial X}\right)(\mathbf{x}) = \mathbf{v} \cdot \left(\frac{\partial S}{\partial Y}\right)\big(\Pi(\mathbf{x})\big) \cdot A(\mathbf{x}),$$

where $A(\mathbf{x})$ is the matrix defined in (**??**). Since by (H2) the Jacobian matrix $(\partial S/\partial Y)\big(\Pi(\mathbf{x})\big)$ has full rank, $\mathbf{w} := \mathbf{v} \cdot (\partial S/\partial Y)\big(\Pi(\mathbf{x})\big) \in \mathbb{A}^s$ is nonzero and

$$\mathbf{w} \cdot A(\mathbf{x}) = \mathbf{0}.$$

Hence, all the maximal minors of $A(\mathbf{x})$ must be zero.

The matrix $A(\mathbf{x})$ is the $(s \times r)$–submatrix of $(\partial \Pi_i/\partial X_j)_{1 \le i,j \le r}(\mathbf{x})$ consisting of the first s rows of the latter. Therefore, from (**??**) we conclude that

$$A(\mathbf{x}) = B_{s,r}(\mathbf{x}) \cdot A_r(\mathbf{x}),$$

where $B_{s,r}(\mathbf{x})$ is the $(s \times r)$–submatrix of $B_r(\mathbf{x})$ consisting of the first s rows of $B_r(\mathbf{x})$. Since the last $r-s$ columns of $B_{s,r}(\mathbf{x})$ are zero, we may rewrite this identity in the following way:

$$A(\mathbf{x}) = B_s(\mathbf{x}) \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_r \\ \vdots & \vdots & & \vdots \\ x_1^{s-1} & x_2^{s-1} & \dots & x_r^{s-1}, \end{pmatrix}, \tag{3.6}$$

where $B_s(\mathbf{x})$ is the $(s \times s)$–submatrix of $B_r(\mathbf{x})$ consisting on the first s rows and the first s columns of $B_r(\mathbf{x})$.

Fix $1 \le l_1 < \cdots < l_s \le r$, set $I := (l_1, \ldots, l_s)$ and consider the $(s \times s)$–submatrix $M_I(\mathbf{x})$ of $A(\mathbf{x})$ consisting of the columns $l_1, \ldots, l_s$ of $A(\mathbf{x})$, namely $M_I(\mathbf{x}) := (\partial \Pi_i/\partial X_{l_j})_{1 \le i,j \le s}(\mathbf{x})$.

From (**??**) and (**??**) we easily see that $M_I(\mathbf{x}) = B_s(\mathbf{x}) \cdot A_{s,I}(\mathbf{x})$, where $A_{s,I}(\mathbf{x})$ is the Vandermonde matrix $A_{s,I}(\mathbf{x}) := (x_{l_j}^{i-1})_{1 \le i,j \le s}$. Therefore, we obtain

$$\det\big(M_I(\mathbf{x})\big) = (-1)^{\frac{(s-1)s}{2}} \det A_{s,I}(\mathbf{x}) = (-1)^{\frac{(s-1)s}{2}} \prod_{1 \le m < n \le s} (x_{l_m} - x_{l_n}) = 0. \tag{3.7}$$

Since (**??**) holds for every $I := (l_1, \ldots, l_s)$ as above, we conclude that $\mathbf{x}$ has at most $s-1$ pairwise–distinct coordinates. In particular, the set of points $\mathbf{x}$ for which $\mathrm{rank}(\partial R/\partial X)(\mathbf{x}) < r - d + s$ is contained in a finite union of linear varieties of $\mathbb{A}^r$ of dimension $s-1$, and thus is an affine variety of dimension at most $s-1$.

Now let $\mathbf{x}$ be an arbitrary point Σ_r. By Lemma **??** we have $\dim \mathcal{T}_{\mathbf{x}} V_r > d - s$. This implies that $\mathrm{rank}\,(\partial R/\partial X)\,(\mathbf{x}) < r - d + s$, for otherwise we would have $\dim \mathcal{T}_{\mathbf{x}} V_r \le d - s$, contradicting thus the fact that $\mathbf{x}$ is a singular point of V_r. This finishes the proof of the theorem. $\square$

From Lemma **??** and Theorem **??** we obtain further algebraic and geometric consequences concerning the polynomials R_j and the variety V_r. By Theorem **??** we have that the set of points $\mathbf{x} \in \mathbb{A}^r$ for which the Jacobian matrix $(\partial R/\partial X)(\mathbf{x})$ has not full rank has dimension at most $s-1$. Since $R_{d-s}, \ldots, R_{r-1}$ form a regular sequence and $s - 1 < d - s$ holds, from [**?**, Theorem 18.15] we conclude that $R_{d-s}, \ldots, R_{r-1}$ define a radical ideal of $\mathbb{F}_q[X_1, \ldots, X_r]$. This in turn implies that $\deg V_r = \prod_{j=d-s}^{r-1} \deg R_j$ (see, e.g., [**?**, Theorem 18.3]). In other words, we have the following statement.

Corollary 3.3. *The polynomials $R_{d-s},\dots,R_{r-1}$ define a radical ideal and the variety V_r has degree* $\deg V_r=\prod_{j=d-s}^{r-1}\deg R_j$.

3.3. **The geometry of $V_r^{\boldsymbol{a}}$.** Now we consider the affine $\mathbb{F}_q$–variety $V_r^{\boldsymbol{a}}\subset\mathbb{A}^r$ defined by the polynomials $R_{d-s}^{\boldsymbol{a}},\dots,R_{r-1}^{\boldsymbol{a}}\in\mathbb{F}_q[X_1,\dots X_r]$ associated to the s–tuple $\boldsymbol{a}:=(a_{d-1},\dots,a_{d-s})\in\mathbb{F}_q^s$ and the polynomial $f_{\boldsymbol{a}}:=T^d+a_{d-1}T^{d-1}+\cdots+a_{d-s}T^{d-s}$. According to Proposition **??**, we may express each $R_j^{\boldsymbol{a}}$ in the form $R_j^{\boldsymbol{a}}=S_j^{\boldsymbol{a}}(\Pi_1,\dots,\Pi_{d-j})$, where $S_j^{\boldsymbol{a}}\in\mathbb{F}_q[Y_1,\dots,Y_{d-j}]$ is a monic polynomial in Y_{d-j}, up to a nonzero constant, of degree 1 in Y_{d-j}. In particular, by a recursive argument it is easy to see that

$$\overline{\mathbb{F}}_q[Y_1,\dots,Y_s]/(S_{d-s}^{\boldsymbol{a}},\dots,S_j^{\boldsymbol{a}})\simeq\overline{\mathbb{F}}_q[Y_1,\dots,Y_{d-j-1}]$$

for $d-s\le j\le r-1$. We conclude that $S_{d-s}^{\boldsymbol{a}},\dots,S_{r-1}^{\boldsymbol{a}}$ form a regular sequence of $\mathbb{F}_q[Y_1,\dots,Y_s]$, namely they satisfy (H1). Furthermore, we observe that

$$\left(\frac{\partial S^{\boldsymbol{a}}}{\partial Y}\right)(\mathbf{y})=\begin{pmatrix}\dfrac{\partial S_{d-s}^{\boldsymbol{a}}}{\partial Y_1}(\mathbf{y}) & \cdots & \dfrac{\partial S_{d-s}^{\boldsymbol{a}}}{\partial Y_{d-r}}(\mathbf{y}) & & \cdots & & c_{d-s}\\ \dfrac{\partial S_{d-s+1}^{\boldsymbol{a}}}{\partial Y_1}(\mathbf{y}) & \cdots & \dfrac{\partial S_{d-s+1}^{\boldsymbol{a}}}{\partial Y_{d-r}}(\mathbf{y}) & & \cdots & c_{d-s+1} & \\ \vdots & & \vdots & & \iddots & & \\ \dfrac{\partial S_{r-1}^{\boldsymbol{a}}}{\partial Y_1}(\mathbf{y}) & \cdots & \dfrac{\partial S_{r-1}^{\boldsymbol{a}}}{\partial Y_{d-r}}(\mathbf{y}) & c_{r-1} & & & \end{pmatrix}$$

holds for every $\mathbf{y}\in\mathbb{A}^s$, where $c_{d-s},\dots,c_{r-1}$ are certain nonzero elements of $\mathbb{F}_q$. As a consequence, we have that $(\partial S^{\boldsymbol{a}}/\partial Y)(\mathbf{y})$ has full rank for every $\mathbf{y}\in\mathbb{A}^s$, that is, $S_{d-s}^{\boldsymbol{a}},\dots,S_{r-1}^{\boldsymbol{a}}$ satisfy (H2). Then the results of Section **??** can be applied to $V_r^{\boldsymbol{a}}$. In particular, we have the following immediate consequence of Lemma **??**, Theorem **??** and Corollary **??**.

Corollary 3.4. *Let $V_r^{\boldsymbol{a}}\subset\mathbb{A}^r$ be the $\mathbb{F}_q$–variety defined by $R_{d-s}^{\boldsymbol{a}},\dots,R_{r-1}^{\boldsymbol{a}}$. Then $V_r^{\boldsymbol{a}}$ is an ideal–theoretic complete intersection of dimension $d-s$, degree $s!/(d-r)!$ and singular locus $\Sigma_r^{\boldsymbol{a}}$ of dimension at most $s-1$.*

3.3.1. *The projective closure of $V_r^{\boldsymbol{a}}$.* In order to obtain estimates on the number of q–rational points of $V_r^{\boldsymbol{a}}$ we also need information concerning the behavior of $V_r^{\boldsymbol{a}}$ "at infinity". For this purpose, we consider the projective closure $\mathrm{pcl}(V_r^{\boldsymbol{a}})\subset\mathbb{P}^r$ of $V_r^{\boldsymbol{a}}$, whose definition we now recall. Consider the embedding of $\mathbb{A}^r$ into the projective space $\mathbb{P}^r$ which assigns to any $\mathbf{x}:=(x_1,\dots,x_r)\in\mathbb{A}^r$ the point $(1:x_1:\cdots:x_r)\in\mathbb{P}^r$. The closure $\mathrm{pcl}(V_r^{\boldsymbol{a}})\subset\mathbb{P}^r$ of the image of $V_r^{\boldsymbol{a}}$ under this embedding in the Zariski topology of $\mathbb{P}^r$ is called the projective closure of $V_r^{\boldsymbol{a}}$. The points of $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ lying in the hyperplane $\{X_0=0\}$ are called the points of $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ at infinity.

It is well–known that $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ is the $\mathbb{F}_q$–variety of $\mathbb{P}^r$ defined by the homogenization $F^h\in\mathbb{F}_q[X_0,\dots,X_r]$ of each polynomial F in the ideal $(R_{d-s}^{\boldsymbol{a}},\dots,R_{r-1}^{\boldsymbol{a}})\subset\mathbb{F}_q[X_1,\dots,X_r]$ (see, e.g., [**?**, §I.5, Exercise 6]). Denote by $(R_{d-s}^{\boldsymbol{a}},\dots,R_{r-1}^{\boldsymbol{a}})^h$ the ideal generated by all the polynomials F^h with $F\in(R_{d-s}^{\boldsymbol{a}},\dots,R_{r-1}^{\boldsymbol{a}})$. Since $(R_{d-s}^{\boldsymbol{a}},\dots,R_{r-1}^{\boldsymbol{a}})$ is radical it turns out that $(R_{d-s}^{\boldsymbol{a}},\dots,R_{r-1}^{\boldsymbol{a}})^h$ is also a radical ideal (see, e.g., [**?**, §I.5, Exercise 6]). Furthermore, $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ is an equidimensional variety of dimension $d-s$ (see, e.g., [**?**, Propositions I.5.17 and II.4.1]) and degree $s!/(d-r)!$ (see, e.g., [**?**, Proposition 1.11]).

Now we discuss the behavior of $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ at infinity. By Proposition **??**, for $d-s \le j \le r-1$ we have

$$R_j^{\boldsymbol{a}} = a_j + \sum_{i=r}^{d} a_i H_{j,i},$$

where the polynomials $H_{j,i}$ are homogeneous of degree $i-j$. Hence, the homogenization of each $R_j^{\boldsymbol{a}}$ is the following polynomial of $\mathbb{F}_q[X_0,\ldots,X_r]$:

$$R_j^{\boldsymbol{a},h} = a_j X_0^{d-j} + \sum_{i=r}^{d} a_i H_{j,i} X_0^{d-i}. \tag{3.8}$$

In particular, it follows that $R_j^{\boldsymbol{a},h}(0,X_1,\ldots,X_r) = H_{j,d}$ $(d-s \le j \le r-1)$ are the polynomials associated to the polynomial $T^d \in \mathbb{F}_q[T]$ in the sense of Lemma **??**.

Lemma 3.5. $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ *has singular locus at infinity of dimension at most* $s-2$.

Proof. Let $\Sigma_{r,\infty}^{\boldsymbol{a}} \subset \mathbb{P}^r$ denote the singular locus of $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ at infinity, namely the set of singular points of $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ lying in the hyperplane $\{X_0=0\}$, and let $\mathbf{x} := (0 : x_1 : \cdots : x_r)$ be an arbitrary point of $\Sigma_{r,\infty}^{\boldsymbol{a}}$. Since the polynomials $R_j^{\boldsymbol{a},h}$ vanish identically in $\mathrm{pcl}(V_r^{\boldsymbol{a}})$, we have $R_j^{\boldsymbol{a},h}(\mathbf{x}) = H_{j,d}(x_1,\ldots,x_r) = 0$ for $d-s \le j \le r-1$. Let $(\partial H_d/\partial X)$ be the Jacobian matrix of $\{H_{j,d} : d-s \le j \le r-1\}$ with respect to $X_1,\ldots,X_r$. We have

$$\mathrm{rank}\left(\frac{\partial H_d}{\partial X}\right)(\mathbf{x}) < r-d+s, \tag{3.9}$$

for if not, we would have that $\dim \mathcal{T}_{\mathbf{x}}(\mathrm{pcl}(V_r^f)) \le d-s$, which implies that $\mathbf{x}$ is a nonsingular point of $\mathrm{pcl}(V_r^{\boldsymbol{a}})$, contradicting thus the hypothesis on $\mathbf{x}$.

From Proposition **??** it follows that the polynomials $H_{j,d}$ $(d-s \le j \le r-1)$ satisfy the hypotheses of Theorem **??**. Then Theorem **??** shows that the set of points satisfying (**??**) is an affine equidimensional cone of dimension at most $s-1$. We conclude that the projective variety $\Sigma_{r,\infty}^{\boldsymbol{a}}$ has dimension at most $s-2$. $\square$

Theorem 3.6. $\mathrm{pcl}(V_r^{\boldsymbol{a}}) \cap \{X_0=0\} \subset \mathbb{P}^{r-1}$ *is an absolutely irreducible ideal–theoretic complete intersection of dimension* $d-s-1$*, degree* $s!/(d-r)!$*, and singular locus of dimension at most* $s-2$.

Proof. From (**??**) it is easy to see that the polynomials $H_{j,d}$ vanish identically in $\mathrm{pcl}(V_r^{\boldsymbol{a}}) \cap \{X_0=0\}$ for $d-s \le j \le r-1$. Lemma **??** shows that $\{H_{j,d} : d-s \le j \le r-1\}$ satisfy the conditions (H1) and (H2). Then Corollary **??** shows that the variety of $\mathbb{A}^r$ defined by $H_{j,d}$ $(d-s \le j \le r-1)$ is an affine equidimensional cone of dimension $d-s$, degree $s!/(d-r)!$ and singular locus of dimension at most $s-1$. It follows that the projective variety of $\mathbb{P}^{r-1}$ defined by these polynomials is equidimensional of dimension $d-s-1$, degree $s!/(d-r)!$ and singular locus of dimension at most $s-2$.

Observe that $V(H_{j,d} : d-s \le j \le r-1) \subset \mathbb{P}^{r-1}$ is a set–theoretic complete intersection, whose singular locus has codimension at least $d-s-1-(s-2) \ge 3$. Therefore, the Hartshorne connectedness theorem (see, e.g., [**?**, Theorem 4.2]) shows that $V(H_{j,d} : d-s \le j \le r-1)$ is absolutely irreducible.

On the other hand, since $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ is equidimensional of dimension $d-s$ we have that each irreducible component of $\mathrm{pcl}(V_r^{\boldsymbol{a}}) \cap \{X_0=0\}$ has dimension at least $d-s-1$. Furthermore, $\mathrm{pcl}(V_r^{\boldsymbol{a}}) \cap \{X_0=0\}$ is contained in the projective variety

$V(H_{j,d} : d-s \leq j \leq r-1)$, which is absolutely irreducible of dimension $d-s-1$. We conclude that $\mathrm{pcl}(V_r^{\boldsymbol{a}}) \cap \{X_0 = 0\}$ is also absolutely irreducible of dimension $d-s-1$, and hence

$$\mathrm{pcl}(V_r^{\boldsymbol{a}}) \cap \{X_0 = 0\} = V(H_{j,d} : d-s \leq j \leq r-1).$$

This finishes the proof of the theorem. □

We conclude this section with a statement that summarizes all the facts we shall need concerning the projective closure $\mathrm{pcl}(V_r^{\boldsymbol{a}})$.

Theorem 3.7. *The projective variety* $\mathrm{pcl}(V_r^{\boldsymbol{a}}) \subset \mathbb{P}^r$ *is an absolutely irreducible ideal–theoretic complete intersection of dimension* $d-s$*, degree* $s!/(d-r)!$ *and singular locus of dimension at most* $s-1$*.*

Proof. We have already shown that $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ is an equidimensional variety of dimension $d-s$ and degree $s!/(d-r)!$. According to Corollary **??**, the singular locus of $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ lying in the open set $\{X_0 \neq 0\}$ has dimension at most $s-1$, while Lemma **??** shows that the singular locus at infinity has dimension at most $s-2$. This shows that the singular locus of $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ has dimension at most $s-1$.

Next we observe that $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ is contained in the projective variety $V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1)$. We have the inclusions

$$V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1) \cap \{X_0 \neq 0\} \subset V(R_j^{\boldsymbol{a}} : d-s \leq j \leq r-1)$$
$$V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1) \cap \{X_0 = 0\} \subset V(H_{d,j} : d-s \leq j \leq r-1).$$

Both $\{R_j^{\boldsymbol{a}} : d-s \leq j \leq r-1\}$ and $\{H_{j,d} : d-s \leq j \leq r-1\}$ satisfy the conditions (H1) and (H2). Then Corollary **??** shows that $V(R_j^{\boldsymbol{a}} : d-s \leq j \leq r-1) \subset \mathbb{A}^r$ is equidimensional of dimension $d-s$ and $V(H_{d,j} : d-s \leq j \leq r-1) \subset \mathbb{P}^{r-1}$ is equidimensional of dimension $d-s-1$. We conclude that $V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1)$ has dimension at most $d-s$. Taking into account that it is defined by $r-d+s$ polynomials, we deduce that it is a set–theoretic complete intersection of dimension $r-(r-d+s) = d-s$. Finally, since its singular locus has dimension at most $s-1$ and $d-s-(s-1) \geq 3$, the Hartshorne connectedness theorem (see, e.g., [**?**, Theorem 4.2]) proves that $V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1)$ is absolutely irreducible

Summarizing, we have that $\mathrm{pcl}(V_r^{\boldsymbol{a}})$ and $V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1)$ are projective equidimensional varieties of dimension $d-s$ with $\mathrm{pcl}(V_r^{\boldsymbol{a}}) \subset V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1)$ and $V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1)$ absolutely irreducible. Therefore, we deduce that

$$\mathrm{pcl}(V_r^{\boldsymbol{a}}) = V(R_j^{\boldsymbol{a},h} : d-s \leq j \leq r-1).$$

From this identity the proof of the theorem easily follows. □

4. The number of q–rational points of $V_r^{\boldsymbol{a}}$

As before, let be given integers d and s with $1 \leq s \leq d-1$ and $2(s+1) \leq d$. Let also be given $\boldsymbol{a} := (a_{d-1}, \ldots, a_{d-s})$ and set $f_{\boldsymbol{a}} := T^d + a_{d-1}T^{d-1} + \cdots + a_{d-s}T^{d-s} \in \mathbb{F}_q[T]$. As asserted before, our objective is to determine the asymptotic behavior of the average value set $\mathcal{V}(d, s, \boldsymbol{a})$ of (**??**).

For this purpose, according to Theorem **??**, we have to determine for $d-s+1 \leq r \leq d$ the number $\chi(\boldsymbol{a}, r)$ of subsets $\mathcal{X}_r$ of r elements of $\mathbb{F}_q$ such that there exists $g \in \mathbb{F}_q[T]$ of degree at most $d-s-1$ interpolating $-f_{\boldsymbol{a}}$ at all the elements of

$\mathcal{X}_r$. In Section **??** we associate to $\boldsymbol{a}$ certain polynomials $R_j^{\boldsymbol{a}} \in \mathbb{F}_q[X_1,\dots,X_r]$ $(d-s \le j \le r-1)$ with the property that the number of common q–rational zeros of $R_{d-s}^{\boldsymbol{a}},\dots,R_{r-1}^{\boldsymbol{a}}$ with pairwise distinct coordinates equals $r!\chi(\boldsymbol{a},r)$, namely

$$\chi(\boldsymbol{a},r)=\frac{1}{r!}\left|\left\{\mathbf{x}\in\mathbb{F}_q^r : R_j^{\boldsymbol{a}}(\mathbf{x})=0\ (d-s\le j\le r-1), x_k\neq x_l\ (1\le k<l\le r)\right\}\right|.$$

The results of Section **??** are fundamental for establishing the asymptotic behavior of $\chi(\boldsymbol{a},r)$. Fix r with $d-s+1\le r\le d$, let $V_r^{\boldsymbol{a}}\subset\mathbb{A}^r$ be the affine variety defined by $R_{d-s}^{\boldsymbol{a}},\dots,R_{r-1}^{\boldsymbol{a}}\in\mathbb{F}_q[X_1,\dots X_r]$ and denote by $\mathrm{pcl}(V_r^{\boldsymbol{a}})\subset\mathbb{P}^r$ the projective closure of $V_r^{\boldsymbol{a}}$. According to Theorems **??** and **??**, both $\mathrm{pcl}(V_r^{\boldsymbol{a}})\subset\mathbb{P}^r$ and $\mathrm{pcl}(V_r^{\boldsymbol{a}})\cap\{X_0=0\}\subset\mathbb{P}^{r-1}$ are projective, absolutely irreducible, ideal–theoretic complete intersections defined over $\mathbb{F}_q$, of dimension $d-s$ and $d-s-1$ respectively, both of degree $s!/(d-r)!$, having a singular locus of dimension at most $s-1$ and $s-2$ respectively.

4.1. **Estimates on the number of q–rational points of complete intersections.** In what follows, we shall use an estimate on the number of q–rational points of a projective complete intersection defined over $\mathbb{F}_q$ due to [**?**] (see [**?**], [**?**] for further explicit estimates of this type). In [**?**, Corollary 8.4] the authors prove that, for an absolutely irreducible ideal–theoretic complete intersection $V\subset\mathbb{P}^m$ of dimension $n:=m-r$, degree $\delta\ge 2$, which is defined over $\mathbb{F}_q$ by polynomials of degree $d_1\ge\cdots\ge d_r\ge 2$, and having singular locus of dimension at most $s\le n-3$, the number $|V(\mathbb{F}_q)|$ of q–rational points of V satisfies the estimate

$$\big||V(\mathbb{F}_q)|-p_n\big|\le 14D^3\delta^2q^{n-1}, \tag{4.1}$$

where $p_n:=q^n+q^{n-1}+\cdots+q+1$ is the cardinality of $\mathbb{P}^n(\mathbb{F}_q)$ and $D:=\sum_{i=1}^r(d_i-1)$.

From (**??**) we obtain the following result.

Theorem 4.1. *With notations and assumptions as above, for $d-s+1\le r\le d$ we have*

$$\left|\chi(\boldsymbol{a},r)-\frac{q^{d-s}}{r!}\right|\le\frac{r(r-1)}{2r!}\delta(d,s,r)q^{d-s-1}+\frac{14}{r!}D(s,d,r)^3\delta(s,d,r)^2(q+1)q^{d-s-2},$$

where $D(s,d,r):=\sum_{j=d-r+1}^{s}(j-1)$ and $\delta(s,d,r):=\prod_{j=d-r+1}^{s}j$.

Proof. First we obtain an estimate on the number of q–rational points of $V_r^{\boldsymbol{a}}$. Let $V_{r,\infty}^{\boldsymbol{a}}:=\mathrm{pcl}(V_r^{\boldsymbol{a}})\cap\{X_0=0\}$. Combining Theorems **??** and **??** with (**??**) we obtain

$$\begin{aligned}\big||\mathrm{pcl}(V_r^{\boldsymbol{a}})(\mathbb{F}_q)|-p_{d-s}\big| &\le 14D(s,d,r)^3\delta(s,d,r)^2q^{d-s-1},\\ \big||V_{r,\infty}^{\boldsymbol{a}}(\mathbb{F}_q)|-p_{d-s-1}\big| &\le 14D(s,d,r)^3\delta(s,d,r)^2q^{d-s-2}.\end{aligned}$$

As a consequence,

$$\begin{aligned}\big||V_r^{\boldsymbol{a}}(\mathbb{F}_q)|-q^{d-s}\big| &= \big||\mathrm{pcl}(V_r^{\boldsymbol{a}})(\mathbb{F}_q)|-|V_{r,\infty}^{\boldsymbol{a}}(\mathbb{F}_q)|-p_{d-s}+p_{d-s-1}\big|\\ &\le \big||\mathrm{pcl}(V_r^{\boldsymbol{a}})(\mathbb{F}_q)|-p_{d-s}\big|+\big||V_{r,\infty}^{\boldsymbol{a}}(\mathbb{F}_q)|-p_{d-s-1}\big|\\ &\le 14D(s,d,r)^3\delta(s,d,r)^2(q+1)q^{d-s-2}. \end{aligned} \tag{4.2}$$

Next we obtain an upper bound on the number of q–rational points of $V_r^{\boldsymbol{a}}$ which are not useful for our purposes, namely those with at least two distinct coordinates taking the same value.

Let $V_{r,=}^{\boldsymbol{a}}(\mathbb{F}_q)$ be the subset of $V_r^{\boldsymbol{a}}(\mathbb{F}_q)$ consisting of all such points, namely

$$V_{r,=}^{\boldsymbol{a}}(\mathbb{F}_q) := \bigcup_{1\le i<j\le r} V_r^{\boldsymbol{a}}(\mathbb{F}_q)\cap\{X_i = X_j\},$$

and set $V_{r,\neq}^{\boldsymbol{a}}(\mathbb{F}_q) := V_r^{\boldsymbol{a}}(\mathbb{F}_q)\setminus V_{r,=}^{\boldsymbol{a}}(\mathbb{F}_q)$. Let $\mathbf{x} := (x_1,\dots,x_r)\in V_{r,=}^{\boldsymbol{a}}(\mathbb{F}_q)$. Without loss of generality we may assume that $x_{r-1} = x_r$ holds. Then $\mathbf{x}$ is a q–rational point of the affine variety $W_{r-1,r}\subset\{X_{r-1} = X_r\}$ defined by the polynomials $S_{d-s}^{\boldsymbol{a}}(\Pi_1^*,\dots,\Pi_s^*),\dots,S_{r-1}^{\boldsymbol{a}}(\Pi_1^*,\dots,\Pi_s^*)\in\mathbb{F}_q[X_1,\dots X_{r-1}]$, where $\Pi_i^* := \Pi_i(X_1,\dots,X_{r-1},X_{r-1})$ is the polynomial of $\mathbb{F}_q[X_1,\dots,X_{r-1}]$ obtained by substituting X_{r-1} for X_r in the ith elementary symmetric polynomial of $\mathbb{F}_q[X_1,\dots,X_r]$. Taking into account that $\Pi_1^*,\dots,\Pi_s^*$ are algebraically independent elements of $\overline{\mathbb{F}}_q[X_1,\dots,X_{r-1}]$, we conclude that $S_{d-s}^{\boldsymbol{a}}(\Pi_1^*,\dots,\Pi_s^*),\dots,S_{r-1}^{\boldsymbol{a}}(\Pi_1^*,\dots,\Pi_s^*)$ form a regular sequence of $\mathbb{F}_q[X_1,\dots X_{r-1}]$. This implies that $W_{r-1,r}$ is of dimension $d-s-1$, and hence, [**?**, Proposition 12.1] or [**?**, Proposition 3.1] show that

$$|W_{r-1,r}(\mathbb{F}_q)|\le\deg W_{r-1,r}q^{d-s-1}\le\deg V_r^{\boldsymbol{a}}q^{d-s-1}.$$

As a consequence, we obtain

$$|V_{r,=}^{\boldsymbol{a}}(\mathbb{F}_q)|\le\frac{r(r-1)}{2}\delta(d,s,r)q^{d-s-1}.$$

Combining (**??**) with this upper bound we have

$$\big||V_{r,\neq}^{\boldsymbol{a}}(\mathbb{F}_q)|-q^{d-s}\big|\le\frac{r(r-1)}{2}\delta(d,s,r)q^{d-s-1}+14D(s,d,r)^3\delta(s,d,r)^2(q+1)q^{d-s-2}.$$

From this inequality we easily deduce the statement of the theorem. □

The estimate of Theorem **??** is the essential step in order to determine the behavior of the average value set $\mathcal{V}(d,s,\boldsymbol{a})$. More precisely, we have the following result.

Corollary 4.2. *With assumptions and notations as in Theorem* **??***, we have*

$$|\mathcal{V}(d,s,\boldsymbol{a})-\mu_d\,q|\le\frac{e^{-1}}{2}+3\frac{s^6(s!)^2}{d!}\sum_{k=0}^{s-1}\binom{d}{k}\frac{1}{k!}+\frac{2(d-s)}{q}. \tag{4.3}$$

Proof. According to Theorem **??**, we have

$$\mathcal{V}(d,s,\boldsymbol{a})-\mu_d q=\sum_{r=1}^{d-s}(-q)^{r-1}\left(\binom{q}{r}-\frac{q^r}{r!}\right)+\frac{1}{q^{d-s-1}}\sum_{r=d-s+1}^{d}(-1)^{r-1}\left(\chi(\boldsymbol{a},r)-\frac{q^{d-s}}{r!}\right). \tag{4.4}$$

First we obtain an upper bound for the absolute value $A(d,s)$ of the first term in the right–hand side of (**??**). For this purpose, given positive integers k,n with $k\le n$, we shall denote by $\left[{n \atop k}\right]$ the unsigned Stirling number of the first kind, namely the number of permutations of n elements with k disjoint cycles. The following properties of the Stirling numbers are well–known (see, e.g., [**?**, §A.8]):

$$\left[{r \atop r}\right]=1,\ \left[{r \atop r-1}\right]=\binom{r}{2},\ \sum_{k=0}^{r}\left[{r \atop k}\right]=r!.$$

It follows that $\left[{r \atop k}\right]/r!\le 1$ for $0\le k\le r$.

Taking into account the identity

$$\binom{q}{r} = \sum_{k=0}^{r} \frac{(-1)^{r-k}}{r!} \begin{bmatrix} r \\ k \end{bmatrix} q^k,$$

we obtain

$$\begin{aligned} A(d,s) := \left| \sum_{r=2}^{d-s} (-q)^{1-r} \left(\binom{q}{r} - \frac{q^r}{r!} \right) \right| &= \left| \sum_{r=2}^{d-s} q^{1-r} \sum_{k=0}^{r-1} \frac{(-1)^{k+1}}{r!} \begin{bmatrix} r \\ k \end{bmatrix} q^k \right| \\ &\leq \sum_{r=0}^{d-s-2} \frac{(-1)^r}{2r!} + \left| \sum_{r=2}^{d-s} q^{1-r} \sum_{k=0}^{r-2} \frac{(-1)^{k+1}}{r!} \begin{bmatrix} r \\ k \end{bmatrix} q^k \right| \\ &\leq \frac{e^{-1}}{2} + \sum_{r=2}^{d-s} \frac{1}{q-1} \leq \frac{e^{-1}}{2} + \frac{2(d-s)}{q}. \end{aligned}$$

Next we consider the absolute value of the second term in the right–hand side of (**??**). From Theorem **??** we have that

$$\begin{aligned} B(d,s) \quad &:= \quad \frac{1}{q^{d-s-1}} \sum_{r=d-s+1}^{d} \left| \chi(\boldsymbol{a}, r) - \frac{q^{d-s}}{r!} \right| \\ &\leq \quad \sum_{r=d-s+1}^{d} \frac{r(r-1)}{2r!} \delta(d,s,r) + \sum_{r=d-s+1}^{d} \frac{14}{r!} D(s,d,r)^3 \delta(s,d,r)^2 \left(1 + \frac{1}{q}\right). \end{aligned}$$

Concerning the first term in the right–hand side, we see that

$$\begin{aligned} \sum_{r=d-s+1}^{d} \frac{r(r-1)}{2r!} \delta(d,s,r) &= \frac{s!}{2(d-2)!} \sum_{r=d-s+1}^{d} \binom{d-2}{r-2} \\ &\leq \frac{s \cdot s!}{2(d-2)!} \binom{d-2}{s-1} = \frac{s^2}{2(d-s-1)!}. \end{aligned}$$

On the other hand,

$$\sum_{r=d-s+1}^{d} \frac{14}{r!} D(s,d,r)^3 \delta(s,d,r)^2 \leq \frac{7}{4} \sum_{r=d-s+1}^{d} \frac{s^3(s-1)^3(s!)^2}{r!((d-r)!)^2} = \frac{7}{4} \sum_{k=0}^{s-1} \frac{s^6(s!)^2}{(d-k)!(k!)^2}.$$

Therefore, we obtain

$$B(d,s) \leq \frac{s^2}{2(d-s-1)!} + \frac{7s^6(s!)^2}{4d!} \sum_{k=0}^{s-1} \binom{d}{k} \frac{1}{k!}.$$

Combining the upper bounds for $A(d,s)$ and $B(d,s)$ the statement of the corollary follows. □

4.2. **On the behavior of (??).** In this section we analyze the behavior of the right–hand side of (**??**). Such an analysis consists of elementary calculations, which shall only be sketched.

Fix k with $0 \leq k \leq s-1$ and denote $h(k) := \binom{d}{k} \frac{1}{k!}$. Analyzing the sign of the differences $h(k+1) - h(k)$ for $0 \leq k \leq s-2$, we deduce the following remark, which is stated without proof.

Remark 4.3. Let $k_0 := -1/2 + \sqrt{5+4d}/2$. Then h is a unimodal function in the integer interval $[0, s-1]$ which reaches its maximum at $\lfloor k_0 \rfloor$.

From Remark **??** we see that

$$\frac{s^6(s!)^2}{d!}\sum_{k=0}^{s-1}\binom{d}{k}\frac{1}{k!} \le \frac{s^7(s!)^2}{d!}\binom{d}{\lfloor k_0\rfloor}\frac{1}{\lfloor k_0\rfloor!} = \frac{s^7(s!)^2}{(d-\lfloor k_0\rfloor)!(\lfloor k_0\rfloor!)^2}. \tag{4.5}$$

In order to obtain an upper bound for the right–hand side of (**??**) we shall use the Stirling formula (see, e.g., [**?**, p. 747]): for $m \in \mathbb{N}$, there exists θ with $0 \le \theta < 1$ such that $m! = (m/e)^m\sqrt{2\pi m}\, e^{\theta/12m}$ holds.

Applying the Stirling formula and taking into account that $2(s+1) \le d$ we see that there exist θ_i $(i = 1, 2, 3)$ with $0 \le \theta_i < 1$ such that

$$C(d,s) := \frac{s^7(s!)^2}{(d-\lfloor k_0\rfloor)!(\lfloor k_0\rfloor!)^2} \le \frac{(\frac{d}{2}-1)^8(\frac{d}{2}-1)^{d-2}\, e^{2+\lfloor k_0\rfloor+\frac{\theta_1}{3d-6}-\frac{\theta_2}{12(d-\lfloor k_0\rfloor)}-\frac{\theta_3}{6\lfloor k_0\rfloor}}}{\big(d-\lfloor k_0\rfloor\big)^{d-\lfloor k_0\rfloor}\sqrt{2\pi(d-\lfloor k_0\rfloor)}\,\lfloor k_0\rfloor^{2\lfloor k_0\rfloor+1}}.$$

By elementary calculations we obtain

$$\begin{aligned}
(d-\lfloor k_0\rfloor)^{-d+\lfloor k_0\rfloor} &\le d^{-d+\lfloor k_0\rfloor}e^{\lfloor k_0\rfloor(d-\lfloor k_0\rfloor)/d},\\
\frac{d^{\lfloor k_0\rfloor}}{\lfloor k_0\rfloor^{2\lfloor k_0\rfloor}} &\le e^{(d-\lfloor k_0\rfloor^2)/\lfloor k_0\rfloor},\\
\left(\frac{d}{2}-1\right)^{d-2} &\le \left(\frac{d}{2}\right)^{d-2} e^{4/d-2}.
\end{aligned}$$

It follows that

$$C(d,s) \le \left(\frac{d}{2}-1\right)^8 \frac{e^{\lfloor k_0\rfloor+\frac{1}{3d-6}+\frac{4}{d}+\frac{\lfloor k_0\rfloor}{d}(d-\lfloor k_0\rfloor)+\frac{1}{\lfloor k_0\rfloor}(d-\lfloor k_0\rfloor^2)}}{d^2 2^{d-2}\sqrt{2\pi(d-\lfloor k_0\rfloor)}\lfloor k_0\rfloor}.$$

By the definition of $\lfloor k_0\rfloor$, it is easy to see that

$$\begin{aligned}
\lfloor k_0\rfloor + \tfrac{\lfloor k_0\rfloor}{d}(d-\lfloor k_0\rfloor) &\le 2\lfloor k_0\rfloor - \tfrac{4}{5},\\
\tfrac{1}{\lfloor k_0\rfloor}(d-\lfloor k_0\rfloor^2) &\le 4,\\
\tfrac{(\frac{d}{2}-1)^3}{d^2\lfloor k_0\rfloor\sqrt{d-\lfloor k_0\rfloor}} &\le \tfrac{3}{20}.
\end{aligned}$$

Therefore, taking into account that $d \ge 2$, we conclude that

$$C(d,s) \le \frac{3(\frac{d}{2}-1)^5 e^{\frac{1}{3d-6}+\frac{4}{d}+2\lfloor k_0\rfloor-\frac{4}{5}+3+\sqrt{5+4d}}}{5\sqrt{2\pi}\,2^d}. \tag{4.6}$$

Combining this bound with Corollary **??** we obtain the main result of this section.

Theorem 4.4. *With assumptions and notations as in Theorem **??**, we have*

$$|\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d\, q| \le \frac{e^{-1}}{2} + 2\,\frac{(d-2)^5e^{2\sqrt{d}}}{2^d} + \frac{2(d-s)}{q}.$$

Proof. From (**??**) and the fact that $\sqrt{5+4d} \le 4/5 + 2\sqrt{d}$ holds for $d \ge 2$, we conclude that

$$\frac{3s^6(s!)^2}{d!}\sum_{k=0}^{s-1}\binom{d}{k}\frac{1}{k!} \le 2\,\frac{(d-2)^5e^{2\sqrt{d}}}{2^d}.$$

From this inequality the statement of the theorem easily follows. □

[1]Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Buenos Aires, Argentina
E-mail address: {ecesarat, gmatera, vperez}@ungs.edu.ar

[2] National Council of Science and Technology (CONICET), Argentina
E-mail address: mprivitelli@conicet.gov.ar

[3]Instituto de Ciencias, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Buenos Aires, Argentina