ACTA ARITHMETICA
165.2 (2014)

On the value set of small families of polynomials over a finite field, II

by

Guillermo Matera, Mariana Pérez
and Melina Privitelli (Buenos Aires)

1. Introduction. Let $\mathbb{F}_q$ be the finite field of q elements, let T be an indeterminate over $\mathbb{F}_q$ and let $f \in \mathbb{F}_q[T]$. We define $\mathcal{V}(f) := |\{f(c) : c \in \mathbb{F}_q\}|$, the cardinality of the value set of f (cf. [LN83]). This paper is a continuation of [C–P14] and is concerned with results on the average value set cardinality of certain families of polynomials of $\mathbb{F}_q[T]$.

Let $\mathcal{V}(d,0)$ denote the average value of $\mathcal{V}(f)$ when f ranges over all monic polynomials in $\mathbb{F}_q[T]$ of degree d with $f(0)=0$. It is well-known that

$$\mathcal{V}(d,0) = \sum_{r=1}^{d} (-1)^{r-1} \binom{q}{r} q^{1-r} = \mu_d q + \mathcal{O}(1), \tag{1.1}$$

where $\mu_d := \sum_{r=1}^{d} (-1)^{r-1}/r!$ and the $\mathcal{O}$-constant depends only on d (see [U55a], [Coh73]).

On the other hand, if some of the coefficients of f are fixed, the results on the average value of $\mathcal{V}(f)$ are less precise. More precisely, let $1 \le s \le d-2$ 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

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

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

$$\mathcal{V}(d,s,\boldsymbol{a}) := \frac{1}{q^{d-s-1}} \sum_{\boldsymbol{b} \in \mathbb{F}_q^{d-s-1}} \mathcal{V}(f_{\boldsymbol{b}}) = \mu_d q + \mathcal{O}(q^{1/2}), \tag{1.2}$$

where the $\mathcal{O}$-constant depends only on d and s (see [U55b], [Coh72]). In our

2010 *Mathematics Subject Classification*: Primary 11T06; Secondary 11G25, 14B05, 14G05.

Key words and phrases: finite fields, average value set cardinality, average second moment, singular complete intersections, rational points.

DOI: 10.4064/aa165-2-3

previous paper [C–P14], we obtain the following explicit estimate for $q > d$ and $1 \le s \le d/2 - 1$:

$$(1.3)\qquad |\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d q| \le \frac{e^{-1}}{2} + \frac{(d-2)^5 e^{2\sqrt{d}}}{2^{d-2}} + \frac{7}{q}.$$

This result holds without any restriction on the characteristic p of $\mathbb{F}_q$ and shows that $\mathcal{V}(d,s,\boldsymbol{a}) = \mu_d q + \mathcal{O}(1)$. On the other hand, (1.3) is valid for $1 \le s \le d/2 - 1$, while (1.2) holds for a larger set of values of s, namely for $1 \le s \le d - 2$.

In this paper we obtain an explicit estimate for $\mathcal{V}(d,s,\boldsymbol{a})$ which can be seen as a complement of (1.3):

Theorem 1.1. *Let $p > 2$, $q > d$ and $1 \le s \le d - 3$. Then*

$$(1.4)\qquad |\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d q| \le d^2 2^{d-1} q^{1/2} + 133 d^{d+5} e^{2\sqrt{d}-d}.$$

We observe that (1.4) holds for a larger set of values of s than (1.3), although it does not hold for fields of characteristic 2. It might also be worth remarking that the estimate for $|\mathcal{V}(f_{\boldsymbol{b}}) - \mu_d q|$ in (1.4) does not behave as well as that of (1.3). On the other hand, it strengthens (1.2) in that it provides an explicit estimate for $|\mathcal{V}(f_{\boldsymbol{b}}) - \mu_d q|$ for fields of characteristic greater than 2.

A second aim of this paper is to provide estimates on the second moment of the value set cardinalities of the families of polynomials under consideration. In this connection, in [U56] it is shown that, under the Riemann hypothesis for L-functions, for $p > d$ we have

$$(1.5)\qquad \mathcal{V}_2(d,0) := \frac{1}{q^{d-1}} \sum \mathcal{V}(f)^2 = \mu_d^2 q^2 + \mathcal{O}(q),$$

where the sum ranges over all monic polynomials $f \in \mathbb{F}_q[T]$ of degree d with $f(0) = 0$ (see also [KK90] for results when $d \ge q$). We obtain the following explicit version of (1.5), which also holds for fields $\mathbb{F}_q$ of small characteristic.

Theorem 1.2. *Let $p > 2$ and $q > d$. If $d \ge 3$, then*

$$|\mathcal{V}_2(d,0) - \mu_d^2 q^2| \le (d^2 2^{2d-1} + 28^3 d^{2d+8} e^{4\sqrt{d}-2d}) q.$$

Our second result regarding second moments is an estimate on the average second moment of the set of monic polynomials of degree d with s coefficients fixed:

Theorem 1.3. *Let $p > 2$, $q > d$ and $1 \le s \le d - 3$. Let $\mathcal{V}_2(d,s,\boldsymbol{a}) := q^{-d+s+1} \sum_{\boldsymbol{b} \in \mathbb{F}_q^{d-s-1}} \mathcal{V}(f_{\boldsymbol{b}}^{\boldsymbol{a}})^2$. Then*

$$|\mathcal{V}_2(d,s,\boldsymbol{a}) - \mu_d^2 q^2| \le d^2 2^{2d+1} q^{3/2} + 28^3 d^{2d+6} e^{4\sqrt{d}-2d} q.$$

Our approach to prove Theorem 1.1 shares certain similarities with that of [C–P14]. Indeed, we express the quantity $\mathcal{V}(d,s,\boldsymbol{a})$ in terms of the number $\chi_r^{\boldsymbol{a}}$ of certain "interpolating sets" with $d - s + 1 \le r \le d$. More precisely, for $f^{\boldsymbol{a}} := T^d + a_{d-1}T^{d-1} + \cdots + a_{d-s}T^{d-s}$, we define $\chi_r^{\boldsymbol{a}}$ 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 $d-s-1$. In Section 3 we show that $\chi_r^{\boldsymbol{a}}$ equals the number of $\mathbb{F}_q$-rational points with pairwise distinct coordinates of a given $\mathbb{F}_q$-definable affine variety Γ_r^* in $\overline{\mathbb{F}}_q^{d-s+r}$ for $d-s+1 \le r \le d$. In Section 4 we establish a number of geometric properties of Γ_r^*. This allows us to obtain, in Section 5, a suitable estimate on the quantities $\chi_r^{\boldsymbol{a}}$ for $d-s+1 \le r \le d$, and thus on $\mathcal{V}(d,s,\boldsymbol{a})$.

The proofs of Theorems 1.2 and 1.3 follow a similar scheme to that of Theorem 1.1. We provide a detailed proof of Theorem 1.3 in Sections 6–9, and sketch the proof of Theorem 1.2 in Section 10. In Section 6 we obtain a combinatorial expression for $\mathcal{V}_2(d,s,\boldsymbol{a})$ in terms of the number $\mathcal{S}_{m,n}^{\boldsymbol{a}}$ of certain "interpolating sets" with $d-s+1 \le m+n \le 2d$. In Section 7 the number $\mathcal{S}_{m,n}^{\boldsymbol{a}}$ is expressed as the number of $\mathbb{F}_q$-rational points with pairwise distinct coordinates of a given $\mathbb{F}_q$-definable affine variety $\Gamma_{m,n}^*$ in $\overline{\mathbb{F}}_q^{d-s+1+m+n}$ for each m,n as above. In Section 8 we obtain results concerning the geometry of $\Gamma_{m,n}^*$ which allow us to determine the asymptotic behavior of $\mathcal{V}_2(d,s,\boldsymbol{a})$ in Section 9. Finally, in Section 10 we discuss how the arguments of the previous sections can be adapted in order to obtain a proof of Theorem 1.2.

We remark that the analysis of the singular locus of the varieties underlying the proofs of Theorems 1.1 and 1.3 requires the study of the discriminant locus of the family of polynomials under consideration, that is, the union of the zero loci of the discriminants of all these polynomials. Such a discriminant locus has been considered in [FS84], where it is shown that it is absolutely irreducible for fields of characteristic large enough. In an appendix we show that the discriminant locus is absolutely irreducible for fields of characteristic at least 3, extending the main result of [FS84].

2. Notions and notations. Since our approach relies on tools of algebraic geometry, we briefly collect the basic definitions and facts that we need. We use standard notions and notations which can be found in, e.g., [Kun85], [Sha94].

We denote by $\mathbb{A}^n$ the *n-dimensional affine space* $\overline{\mathbb{F}}_q^n$ and by $\mathbb{P}^n$ the *n-dimensional projective 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 in $\overline{\mathbb{F}}_q[X_1,\dots,X_n]$ or of homogeneous polynomials in $\overline{\mathbb{F}}_q[X_0,\dots,X_n]$. 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 think a projective or affine $\mathbb{K}$-variety as being equipped with the induced Zariski topology. We shall frequently denote by $V(F_1,\dots,F_m)$ or $\{F_1=0,\dots,F_s=0\}$ the affine or projective $\mathbb{K}$-variety consisting of the common zeros of the polynomials $F_1,\dots,F_m$. The set $V(\mathbb{F}_q):=V\cap\mathbb{F}_q^n$ in the affine case, or $V(\mathbb{F}_q):=V\cap\mathbb{P}^n(\mathbb{F}_q)$ in the projective case, 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 an $\overline{\mathbb{F}}_q$-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*, the set of all polynomials in $\mathbb{K}[X_1,\dots,X_n]$, or in $\mathbb{K}[X_0,\dots,X_n]$, vanishing on V. The *coordinate ring* $\mathbb{K}[V]$ of V is defined as 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 linear space L of codimension $\dim V$, for which $V\cap L$ is a finite set. More generally, following [Hei83] (see also [Ful84]), 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 [Hei83], [Ful84], [Vog84]): if V and W are $\mathbb{K}$-varieties, then

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

Let V be a variety contained in $\mathbb{A}^n$ and let $I(V)\subset\overline{\mathbb{F}}_q[X_1,\dots,X_n]$ be the defining ideal of V. Let $\boldsymbol{x}$ be a point of V. The *dimension* $\dim_{\boldsymbol{x}}V$ *of* V *at* $\boldsymbol{x}$ is the maximum of the dimensions of the irreducible components of V that contain $\boldsymbol{x}$. If $I(V)=(F_1,\dots,F_m)$, the *tangent space* $\mathcal{T}_{\boldsymbol{x}}V$ to V at $\boldsymbol{x}$ is the kernel of the Jacobian matrix $(\partial F_i/\partial X_j)_{1\le i\le m,\,1\le j\le n}(\boldsymbol{x})$ of the polynomials $F_1,\dots,F_m$ with respect to $X_1,\dots,X_n$ at $\boldsymbol{x}$. The point $\boldsymbol{x}$ is *regular* if $\dim\mathcal{T}_{\boldsymbol{x}}V=\dim_{\boldsymbol{x}}V$. Otherwise, $\dim\mathcal{T}_{\boldsymbol{x}}V>\dim_{\boldsymbol{x}}V$ and the point $\boldsymbol{x}$ 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.

Elements $F_1, \dots, F_{n-r}$ in $\mathbb{K}[X_1, \dots, X_n]$ or in $\mathbb{K}[X_0, \dots, X_n]$ form a *regular sequence* if F_1 is nonzero and no F_i is a zero divisor in the quotient ring $\mathbb{K}[X_1, \dots, X_n]/(F_1, \dots, F_{i-1})$ or $\mathbb{K}[X_0, \dots, X_n]/(F_1, \dots, F_{i-1})$ for $2 \leq i \leq n-r$. In that case, the (affine or projective) $\mathbb{K}$-variety $V := V(F_1, \dots, F_{n-r})$ they define is equidimensional of dimension r, and is called a *set-theoretic complete intersection.* If the ideal $(F_1, \dots, F_{n-r})$ 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 $F_1, \dots, F_{n-r}$ is a system of generators of $I(V)$, then the degrees $d_1, \dots, d_{n-r}$ depend only on V and not on the system of generators. Arranging the d_i in such a way that $d_1 \geq \dots \geq d_{n-r}$, we call $\boldsymbol{d} := (d_1, \dots, d_{n-r})$ the *multidegree* of V. The so-called *Bézout theorem* (see, e.g., [Har92, Theorem 18.3]) asserts that

$$\deg V = d_1 \cdots d_{n-r}.$$

In what follows we shall deal with a particular class of complete intersections, which we now define. A $\mathbb{K}$-variety V is *regular in codimension* m if its singular locus $\mathrm{Sing}(V)$ has codimension at least $m+1$ in V, that is, $\dim V - \dim \mathrm{Sing}(V) \geq m+1$. A complete intersection V which is regular in codimension 1 is called *normal* (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., [Kun85, Theorem VI.4.2]), which we now state. If $V \subset \mathbb{P}^n$ is a set-theoretic 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 $\mathbb{P}^n$ over $\mathbb{K}$. Applying the Hartshorne connectedness theorem with $W := \mathrm{Sing}(V)$, one deduces the following result.

THEOREM 2.1. *If $V \subset \mathbb{P}^n$ is a normal set-theoretic complete intersection, then V is absolutely irreducible.*

Let V and W be irreducible $\mathbb{K}$-varieties of the same dimension and let $f : V \to W$ be a regular map for which $\overline{f(V)} = W$, where $\overline{f(V)}$ denotes the closure of $f(V)$ with respect to the Zariski $\mathbb{K}$-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, i.e. each $\eta \in \mathbb{K}[V]$ 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 is that the preimage $f^{-1}(S)$ of an irreducible closed subset $S \subset W$ is equidimensional of dimension $\dim S$.

3. Estimating the mean $\mathcal{V}(d, s, \boldsymbol{a})$: a geometric approach.

Let $s, d \in \mathbb{N}$ with $d < q$ and $1 \leq s \leq d-2$ and $\boldsymbol{a} := (a_{d-1}, \dots, a_{d-s}) \in \mathbb{F}_q^s$.

Denote $f^{\boldsymbol{a}} := T^d + a_{d-1}T^{d-1} + \cdots + a_{d-s}T^{d-s}$. For every $\boldsymbol{b} := (b_{d-s-1}, \dots, b_1) \in \mathbb{F}_q^{d-s-1}$, denote by $f_{\boldsymbol{b}} := f_{\boldsymbol{b}}^{\boldsymbol{a}} \in \mathbb{F}_q[T]$ the polynomial

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

Our first objective is to determine the asymptotic behavior of the average value set cardinality

$$\mathcal{V}(d,s,\boldsymbol{a}) := \frac{1}{q^{d-s-1}} \sum_{\boldsymbol{b} \in \mathbb{F}_q^{d-s-1}} \mathcal{V}(f_{\boldsymbol{b}}).$$

For this purpose, we use the following result.

Theorem 3.1 ([C–P14, Theorem 2.1]). *Under the assumptions above,*

$$\mathcal{V}(d,s,\boldsymbol{a}) = \sum_{r=1}^{d-s} (-1)^{r-1} \binom{q}{r} q^{1-r} + \frac{1}{q^{d-s-1}} \sum_{r=d-s+1}^{d} (-1)^{r-1} \chi_r^{\boldsymbol{a}}, \tag{3.1}$$

where $\chi_r^{\boldsymbol{a}}$ denotes the number of r-element subsets χ_r of $\mathbb{F}_q$ such that there exists $(\boldsymbol{b}, b_0) \in \mathbb{F}_q^{d-s}$ for which $(f_{\boldsymbol{b}} + b_0)|_{\chi_r} \equiv 0$.

According to this result, we have to determine the asymptotic behavior of $\chi_r^{\boldsymbol{a}}$ for $d-s+1 \le r \le d$. In [C–P14] we introduce an affine $\mathbb{F}_q$-variety $V_r^{\boldsymbol{a}} \subset \mathbb{A}^r$ such that the number of q-rational points of $V_r^{\boldsymbol{a}}$ with pairwise distinct coordinates equals $\chi_r^{\boldsymbol{a}}$. Here we follow a different approach, considering the incidence variety consisting of the set of points $(\boldsymbol{b}, b_0, \alpha_1, \dots, \alpha_r)$ with $\chi_r := \{\alpha_1, \dots, \alpha_r\}$ and $(f_{\boldsymbol{b}} + b_0)|_{\chi_r} \equiv 0$.

Fix r with $d-s+1 \le r \le d$. Let $T, T_1, \dots, T_r, B_{d-s-1}, \dots, B_1, B_0$ be new indeterminates over $\overline{\mathbb{F}}_q$, let $\boldsymbol{T} := (T_1, \dots, T_r)$, $\boldsymbol{B} := (B_{d-s-1}, \dots, B_1)$ and $\boldsymbol{B}_0 := (\boldsymbol{B}, B_0)$, and let $F \in \mathbb{F}_q[\boldsymbol{B}_0, T]$ be the polynomial

$$F := T^d + \sum_{i=d-s}^{d-1} a_i T^i + \sum_{i=1}^{d-s-1} B_i T^i + B_0. \tag{3.2}$$

Consider the affine quasi-$\mathbb{F}_q$-variety $\Gamma_r \subset \mathbb{A}^{d-s+r}$ defined as follows:

$$\begin{aligned} \Gamma_r := \{(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \mathbb{A}^{d-s} \times \mathbb{A}^r : F(\boldsymbol{b}_0, \alpha_j) = 0 \ (1 \le j \le r), \\ \alpha_i \ne \alpha_j \ (1 \le i < j \le r)\}. \end{aligned}$$

Our next result shows how the number $|\Gamma_r(\mathbb{F}_q)|$ of q-rational points of Γ_r is related to $\chi_r^{\boldsymbol{a}}$.

Lemma 3.2. *Let r be an integer with $d-s+1 \le r \le d$. Then*

$$|\Gamma_r(\mathbb{F}_q)|/r! = \chi_r^{\boldsymbol{a}}.$$

Proof. Let $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Gamma_r(\mathbb{F}_q)$ and let $\sigma : \{1, \dots, r\} \to \{1, \dots, r\}$ be an arbitrary permutation. Let $\sigma(\boldsymbol{\alpha})$ be the image of $\boldsymbol{\alpha}$ under the linear mapping induced by σ. Then it is easy to see that $(\boldsymbol{b}_0, \sigma(\boldsymbol{\alpha}))$ is also in $\Gamma_r(\mathbb{F}_q)$.

Furthermore, $\sigma(\boldsymbol{\alpha}) = \boldsymbol{\alpha}$ if and only if σ is the identity permutation. This shows that $\mathbb{S}_r$, the symmetric group of r elements, acts on $\Gamma_r(\mathbb{F}_q)$ and each orbit of this action has $r!$ elements.

The orbit of $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Gamma_r(\mathbb{F}_q)$ uniquely determines a polynomial $F(\boldsymbol{b}_0, T) \in \mathbb{F}_q[T]$ and a set $\chi_r := \{\alpha_1, \dots, \alpha_r\} \subset \mathbb{F}_q$ with $|\chi_r| = r$ and $F(\boldsymbol{b}_0, T)|_{\chi_r} \equiv 0$. On the other hand, each subset $\chi_r := \{\alpha_1, \dots, \alpha_r\}$ as in the statement of Theorem 3.1 determines a unique $\boldsymbol{b}_0 \in \mathbb{F}_q^{d-s}$ such that the polynomial $F(\boldsymbol{b}_0, T)$ vanishes on χ_r, and thus a unique orbit as above. This implies that the number of orbits of $\Gamma_r(\mathbb{F}_q)$ is equal to $\chi_r^{\boldsymbol{a}}$ and finishes the proof of the lemma. ∎

To estimate $|\Gamma_r(\mathbb{F}_q)|$ we shall consider the Zariski closure $\mathrm{cl}(\Gamma_r)$ of $\Gamma_r \subset \mathbb{A}^{d-s+r}$. The equations defining $\mathrm{cl}(\Gamma_r)$ will be expressed using the following notation. Let $T, X_1, \dots, X_{l+1}$ be indeterminates over $\overline{\mathbb{F}}_q$ and let $f \in \overline{\mathbb{F}}_q[T]$ be a polynomial of degree at most l. For notational convenience, we define the *0th divided difference* $\Delta^0 f \in \overline{\mathbb{F}}_q[X_1]$ of f as $\Delta^0 f := f(X_1)$. Further, for $1 \le i \le l$ we define the *ith divided difference* $\Delta^i f \in \overline{\mathbb{F}}_q[X_1, \dots, X_{i+1}]$ of f as

$$\Delta^i f(X_1, \dots, X_{i+1}) = \frac{\Delta^{i-1} f(X_1, \dots, X_i) - \Delta^{i-1} f(X_1, \dots, X_{i-1}, X_{i+1})}{X_i - X_{i+1}}.$$

With these notations, consider the affine $\mathbb{F}_q$-variety $\Gamma_r^* \subset \mathbb{A}^{d-s+r}$ defined as

$$\Gamma_r^* := \{(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \mathbb{A}^{d-s} \times \mathbb{A}^r : \Delta^{i-1} F(\boldsymbol{b}_0, \alpha_1, \dots, \alpha_i) = 0 \ (1 \le i \le r)\},$$

where $\Delta^{i-1} F(\boldsymbol{b}_0, T_1, \dots, T_i)$ is the $(i-1)$th divided difference of $F(\boldsymbol{b}_0, T)$. The next result establishes the relation between the varieties Γ_r and Γ_r^*.

Lemma 3.3. *With the notations above,*

$$\Gamma_r = \Gamma_r^* \cap \{(\boldsymbol{b}_0, \boldsymbol{\alpha}) : \alpha_i \neq \alpha_j \ (1 \le i < j \le r)\}. \tag{3.3}$$

Proof. Let $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Gamma_r$. By the definition of the divided differences of $F(\boldsymbol{b}_0, T)$ we easily conclude that $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Gamma_r^*$. Conversely, let $(\boldsymbol{b}_0, \boldsymbol{\alpha})$ be in the set on the right-hand side of (3.3). We claim that $F(\boldsymbol{b}_0, \alpha_k) = 0$ for $1 \le k \le r$. We observe that $F(\boldsymbol{b}_0, \alpha_1) = \Delta^0 F(\boldsymbol{b}_0, \alpha_1) = 0$. Arguing inductively, suppose that $F(\boldsymbol{b}_0, \alpha_1) = \dots = F(\boldsymbol{b}_0, \alpha_{i-1}) = 0$. By definition, $\Delta^{i-1} F(\boldsymbol{b}_0, \alpha_1 \cdots \alpha_i)$ can be expressed as a linear combination with nonzero coefficients of the differences $F(\boldsymbol{b}_0, \alpha_{j+1}) - F(\boldsymbol{b}_0, \alpha_j)$ with $1 \le j \le i-1$. Therefore, combining the inductive hypothesis with the fact that $\Delta^{i-1} F(\boldsymbol{b}_0, \alpha_1, \dots, \alpha_i) = 0$, we easily see that $F(\boldsymbol{b}_0, \alpha_i) = 0$, finishing the proof of the claim. ∎

4. On the geometry of Γ_r^*. From now on we assume that the characteristic p of $\mathbb{F}_q$ is strictly greater than 2. This section is devoted to establishing several facts concerning the geometry of the affine $\mathbb{F}_q$-variety Γ_r^*.

We first show that the defining polynomials of $\varGamma_r^*$ form a regular sequence, which in particular allows us to determine the dimension of $\varGamma_r^*$. Then we analyze the singular locus of $\varGamma_r^*$, showing that it has codimension at least 2 in $\varGamma_r^*$. Finally, we show a number of results concerning the projective closure $\mathrm{pcl}(\varGamma_r^*)$ of $\varGamma_r^*$ and the set of points of $\mathrm{pcl}(\varGamma_r^*)$ at infinity. The final outcome is that both $\mathrm{pcl}(\varGamma_r^*)$ and the set of points of $\mathrm{pcl}(\varGamma_r^*)$ at infinity are normal complete intersections, which will allow us to obtain a suitable estimate of the number of q-rational points of $\varGamma_r^*$.

Lemma 4.1. *$\varGamma_r^*$ is a (set-theoretic) complete intersection of dimension $d-s$.*

Proof. Consider the graded lexicographic order of $\overline{\mathbb{F}}_q[\boldsymbol{B}_0, \boldsymbol{T}]$ with $T_r > \cdots > T_1 > B_{d-s-1} > \cdots > B_0$. It is easy to see that for each i the polynomial $\varDelta^{i-1}F(\boldsymbol{B}_0, T_1, \ldots, T_i)$ has degree $d-i+1$ in the variables $\boldsymbol{T}$, and the monomial T_i^{d-i+1} occurs in the dense representation of such a polynomial with nonzero coefficient. We deduce that the leading term of $\varDelta^{i-1}F(\boldsymbol{B}_0, T_1, \ldots, T_i)$ is T_i^{d-i+1} for $1 \le i \le r$ in the monomial order defined above. Hence, the leading terms of $\varDelta^{i-1}F(\boldsymbol{B}_0, T_1, \ldots, T_i)$ $(1 \le i \le r)$ are relatively prime and thus they form a Gröbner basis of the ideal $\mathcal{J}$ that they generate (see, e.g., [CLO92, §2.9, Proposition 4]), the initial ideal of $\mathcal{J}$ being generated by $\{T_i^{d-i+1} : 1 \le i \le r\}$. Furthermore, since $\{T_i^{d-i+1} : 1 \le i \le r\}$ forms a regular sequence in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0, \boldsymbol{T}]$, from, e.g., [Eis95, Proposition 15.15], we conclude that $\{\varDelta^{i-1}F(\boldsymbol{B}_0, T_1, \ldots, T_i) : 1 \le i \le r\}$ also forms a regular sequence in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0, \boldsymbol{T}]$. This finishes the proof of the lemma. ∎

4.1. The dimension of the singular locus of $\varGamma_r^*$ and consequences. As announced above, we study the dimension of the singular locus of $\varGamma_r^*$. Our aim is to show that such a singular locus has codimension at least 2 in $\varGamma_r^*$.

We start with the following simple criterion of nonsingularity.

Lemma 4.2. *Let $J_F \in \mathbb{F}_q[\boldsymbol{B}_0, \boldsymbol{T}]^{r \times (d-s+r)}$ be the Jacobian matrix of the polynomials $F(\boldsymbol{B}_0, T_i)$ $(1 \le i \le r)$ with respect to $\boldsymbol{B}_0, \boldsymbol{T}$ and let $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \varGamma_r^*$. If $J_F(\boldsymbol{b}_0, \boldsymbol{\alpha})$ has full rank, then $(\boldsymbol{b}_0, \boldsymbol{\alpha})$ is a nonsingular point of $\varGamma_r^*$.*

Proof. Considering the Newton form of the polynomial interpolating $F(\boldsymbol{b}_0,T)$ at $\alpha_1, \ldots, \alpha_r$, we easily deduce that $F(\boldsymbol{b}_0, \alpha_i) = 0$ for $1 \le i \le r$. This shows that $F(\boldsymbol{B}_0, T_i)$ vanishes on $\varGamma_r^*$ for $1 \le i \le r$. As a consequence, any element of the tangent space $\mathcal{T}_{(\boldsymbol{b}_0, \boldsymbol{\alpha})}\varGamma_r^*$ belongs to the kernel of the Jacobian matrix $J_F(\boldsymbol{b}_0, \boldsymbol{\alpha})$.

By hypothesis, the $(r \times (d-s+r))$-matrix $J_F(\boldsymbol{b}_0, \boldsymbol{\alpha})$ has full rank r, and thus its kernel has dimension $d-s$. We conclude that $\mathcal{T}_{(\boldsymbol{b}_0, \boldsymbol{\alpha})}\varGamma_r^*$ has dimension at most $d-s$. Since $\varGamma_r^*$ is equidimensional of dimension $d-s$, it follows that $(\boldsymbol{b}_0, \boldsymbol{\alpha})$ is a nonsingular point of $\varGamma_r^*$. ∎

Let $(\boldsymbol{b}_0,\boldsymbol{\alpha}) \in \varGamma_r^*$ with $\boldsymbol{\alpha} := (\alpha_1,\dots,\alpha_r)$, and let $f_{\boldsymbol{b}_0} := F(\boldsymbol{b}_0,T)$. Then

$$J_F(\boldsymbol{b}_0,\boldsymbol{\alpha}) = \begin{pmatrix} \alpha_1^{d-s-1} & \cdots & \alpha_1 & 1 & f'_{\boldsymbol{b}_0}(\alpha_1) & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_r^{d-s-1} & \cdots & \alpha_r & 1 & 0 & \cdots & f'_{\boldsymbol{b}_0}(\alpha_r) \end{pmatrix}.$$

We observe that if all the roots in $\overline{\mathbb{F}}_q$ of $f_{\boldsymbol{b}_0}$ are simple, then $J_F(\boldsymbol{b}_0,\boldsymbol{\alpha})$ has full rank and $(\boldsymbol{b}_0,\boldsymbol{\alpha})$ is a regular point of $\varGamma_r^*$. Therefore, to prove that the singular locus of $\varGamma_r^*$ is a subvariety of codimension at least 2, it suffices to consider the set of points $(\boldsymbol{b}_0,\boldsymbol{\alpha}) \in \varGamma_r^*$ for which at least one coordinate of $\boldsymbol{\alpha}$ is a multiple root of $f_{\boldsymbol{b}_0}$. In particular, $f_{\boldsymbol{b}_0}$ must have multiple roots. We start by considering the "extreme" case where $f'_{\boldsymbol{b}_0} = 0$.

Lemma 4.3. *If $d-s \geq 3$, then the set $\mathcal{W}_1$ of points $(\boldsymbol{b}_0,\boldsymbol{\alpha}) \in \varGamma_r^*$ with $f'_{\boldsymbol{b}_0} = 0$ is contained in a subvariety of codimension 2 of $\varGamma_r^*$.*

Proof. Consider the morphism of $\mathbb{F}_q$-varieties defined as follows:

$$\varPsi_r : \varGamma_r^* \to \mathbb{A}^{d-s}, \qquad (\boldsymbol{b}_0,\boldsymbol{\alpha}) \mapsto \boldsymbol{b}_0. \tag{4.1}$$

We claim that $\varPsi_r$ is a finite morphism. To prove this, it is enough to show that the coordinate function t_j of $\overline{\mathbb{F}}_q[\varGamma_r^*]$ defined by T_j satisfies a monic equation with coefficients in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]$ for $1 \leq j \leq r$. Since the polynomial $F(\boldsymbol{B}_0,T_j)$ vanishes on $\varGamma_r^*$ and is a monic element of $\overline{\mathbb{F}}_q[\boldsymbol{B}_0][T_j]$, it provides the monic equation annihilating t_j that we are looking for.

Since $d-s \geq 3$, we have $d-s-1 \geq 2$ and the condition $f'_{\boldsymbol{b}_0} = (f^{\boldsymbol{a}})' + \sum_{j=1}^{d-s-1} jb_jT^{j-1} = 0$ implies $b_1 = b_2 = 0$. It follows that the set of points $(\boldsymbol{b}_0,\boldsymbol{\alpha}) \in \varGamma_r^*$ with $f'_{\boldsymbol{b}_0} = 0$ is a subset of $\varPsi_r^{-1}(\mathcal{Z}_{1,2})$, where $\mathcal{Z}_{1,2} \subset \mathbb{A}^{d-s}$ is the variety of dimension $d-s-2$ defined by $B_1 = B_2 = 0$. Taking into account that $\varPsi_r$ is a finite morphism, we deduce that $\varPsi_r^{-1}(\mathcal{Z}_{1,2})$ has dimension $d-s-2$. ∎

In what follows we shall assume that $f'_{\boldsymbol{b}_0}$ is nonzero and $f_{\boldsymbol{b}_0}$ has multiple roots. We analyze the case where exactly one of the coordinates of $\boldsymbol{\alpha}$ is a multiple root of $f_{\boldsymbol{b}_0}$.

Lemma 4.4. *Suppose that $f'_{\boldsymbol{b}_0} \neq 0$ and there exists a unique coordinate α_i of $\boldsymbol{\alpha}$ which is a multiple root of $f_{\boldsymbol{b}_0}$. Then $(\boldsymbol{b}_0,\boldsymbol{\alpha})$ is a regular point of $\varGamma_r^*$.*

Proof. Assume without loss of generality that α_1 is the only multiple root of $f_{\boldsymbol{b}_0}$ among the coordinates of $\boldsymbol{\alpha}$. According to Lemma 4.2, it suffices to show that $J_F(\boldsymbol{b}_0,\boldsymbol{\alpha})$ has full rank. For this purpose, we observe that the $(r \times r)$-submatrix of $J_F(\boldsymbol{b}_0,\boldsymbol{\alpha})$ consisting of the $(d-s)$th column and the last $r-1$ columns,

$$\hat{J}_F(\boldsymbol{b}_0,\boldsymbol{\alpha}) := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & f'_{\boldsymbol{b}_0}(\alpha_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & f'_{\boldsymbol{b}_0}(\alpha_r) \end{pmatrix},$$

is nonsingular. Indeed, by hypothesis α_i is a simple root of $f'_{\boldsymbol{b}_0}$, which implies $f'_{\boldsymbol{b}_0}(\alpha_i) \neq 0$ for $i \geq 2$. We conclude that $J_F(\boldsymbol{b}_0,\boldsymbol{\alpha})$ has full rank. ∎

The next case to be discussed is when two distinct multiple roots of $f_{\boldsymbol{b}_0}$ occur among the coordinates of $\boldsymbol{\alpha}$.

Lemma 4.5. *Let $\mathcal{W}_2$ denote the set of points $(\boldsymbol{b}_0,\boldsymbol{\alpha}) \in \Gamma_r^*$ for which there exist $1 \leq i < j \leq r$ such that $\alpha_i \neq \alpha_j$ and α_i, α_j are multiple roots of $f_{\boldsymbol{b}_0}$. Then $\mathcal{W}_2$ is contained in a subvariety of codimension 2 of Γ_r^*.*

Proof. Let $(\boldsymbol{b}_0,\boldsymbol{\alpha}) \in \mathcal{W}_2$. We may assume that $f'_{\boldsymbol{b}_0} \neq 0$. Since $f_{\boldsymbol{b}_0}$ has at least two distinct multiple roots, the greatest common divisor of $f_{\boldsymbol{b}_0}$ and $f'_{\boldsymbol{b}_0}$ has degree at least 2. Hence,

$$\mathrm{Res}(f_{\boldsymbol{b}_0}, f'_{\boldsymbol{b}_0}) = \mathrm{Subres}(f_{\boldsymbol{b}_0}, f'_{\boldsymbol{b}_0}) = 0,$$

where $\mathrm{Res}(f_{\boldsymbol{b}_0}, f'_{\boldsymbol{b}_0})$ and $\mathrm{Subres}(f_{\boldsymbol{b}_0}, f'_{\boldsymbol{b}_0})$ denote the resultant and the first-order subresultant of $f_{\boldsymbol{b}_0}$ and $f'_{\boldsymbol{b}_0}$ respectively. Furthermore, since $f_{\boldsymbol{b}_0}$ has degree d, by basic properties of resultants and subresultants it follows that

$$\mathrm{Res}(f_{\boldsymbol{b}_0}, f'_{\boldsymbol{b}_0}) = \mathrm{Res}\big(F(\boldsymbol{B}_0,T), \Delta^1 F(\boldsymbol{B}_0,T,T),T\big)\big|_{\boldsymbol{B}_0=\boldsymbol{b}_0},$$
$$\mathrm{Subres}(f_{\boldsymbol{b}_0}, f'_{\boldsymbol{b}_0}) = \mathrm{Subres}\big(F(\boldsymbol{B}_0,T), \Delta^1 F(\boldsymbol{B}_0,T,T),T\big)\big|_{\boldsymbol{B}_0=\boldsymbol{b}_0},$$

where

$$\mathcal{R} := \mathrm{Res}\big(F(\boldsymbol{B}_0,T), \Delta^1 F(\boldsymbol{B}_0,T,T),T\big),$$
$$\mathcal{S}_1 := \mathrm{Subres}\big(F(\boldsymbol{B}_0,T), \Delta^1 F(\boldsymbol{B}_0,T,T),T\big)$$

are the resultant and the first-order subresultant, with respect to T, of $F(\boldsymbol{B}_0,T)$ and $\Delta^1 F(\boldsymbol{B}_0,T,T)$. It follows that $\mathcal{W}_2 \cap \Gamma_r^* \subset \Psi_r^{-1}(\mathcal{Z}_2)$, where Ψ_r is the morphism (4.1) and $\mathcal{Z}_2 \subset \mathbb{A}^{d-s}$ is the variety defined by

$$\mathcal{R}(\boldsymbol{B}_0) = 0, \quad \mathcal{S}_1(\boldsymbol{B}_0) = 0. \tag{4.2}$$

Observe that $\mathcal{R}$ is a nonzero polynomial because $F(\boldsymbol{B}_0,T)$ is a separable element of $\mathbb{F}_q[\boldsymbol{B}_0][T]$. We claim that $\mathcal{S}_1$ is also nonzero. Indeed, if p does not divide $d(d-1)$, then the nonzero term $d(d-1)^{d-2}B_1^{d-2}$ occurs in the dense representation of $\mathcal{S}_1$. On the other hand, if p divides $d(d-1)$, since $p > 2$, the nonzero term $2\,(-1)^d(d-2)^{d-2}B_2^{d-1}$ appears in the dense representation of $\mathcal{S}_1$.

We claim that $\mathcal{R}$ and $\mathcal{S}_1$ form a regular sequence in $\mathbb{F}_q[\boldsymbol{B}_0]$. Indeed, since $p > 2$, $\mathcal{R}$ is an irreducible element of $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]$ (see Theorem A.3 below). If $\mathcal{S}_1$ were a zero divisor in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]/(\mathcal{R})$, then it would be a multiple of $\mathcal{R}$ in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]$, which is impossible because $\max\{\deg_{B_1}\mathcal{R}, \deg_{B_2}\mathcal{R}\} = d$, while $\max\{\deg_{B_1}\mathcal{S}_1, \deg_{B_2}\mathcal{S}_1\} \leq d-1$. It follows that $\dim \mathcal{Z}_2 = d-s-2$, and hence $\dim \Psi_r^{-1}(\mathcal{Z}_2) = d-s-2$. Therefore, $\mathcal{W}_2$ is contained in a subvariety of Γ_r^* of codimension 2. ■

It remains to consider the case where only one multiple root of $f_{\boldsymbol{b}_0}$ occurs among the coordinates of $\boldsymbol{\alpha}$, but at least two distinct coordinates of $\boldsymbol{\alpha}$ take that value. Then either all the remaining coordinates of $\boldsymbol{\alpha}$ are simple roots of $f_{\boldsymbol{b}_0}$, or at least one more coordinate is the same multiple root. Our next result deals with the first of these two cases.

Lemma 4.6. *Let $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Gamma_r^*$ satisfy the following conditions:*

- *there exist $1 \leq i < j \leq r$ such that $\alpha_i = \alpha_j$ and α_i is a multiple root of $f_{\boldsymbol{b}_0}$;*
- *for any $k \notin \{i, j\}$, α_k is a simple root of $f_{\boldsymbol{b}_0}$.*

Then $(\boldsymbol{b}_0, \boldsymbol{\alpha})$ is a regular point of Γ_r^*.

Proof. The argument is similar to that of the proof of Lemma 4.2. We can assume that $i = 1$ and $j = 2$. Since the polynomials $\Delta^1 F(\boldsymbol{B}_0, T_1, T_2)$ and $F(\boldsymbol{B}_0, T_i)$ $(2 \leq i \leq r)$ vanish on Γ_r^*, the tangent space $\mathcal{T}_{(\boldsymbol{b}_0,\boldsymbol{\alpha})}\Gamma_r^*$ is included in the kernel of the Jacobian matrix $J_{\Delta,F}(\boldsymbol{b}_0, \boldsymbol{\alpha})$ of $\Delta^1 F(\boldsymbol{B}_0, T_1, T_2)$ and $F(\boldsymbol{B}_0, T_i)$ $(2 \leq i \leq r)$ with respect to $\boldsymbol{B}_0, \boldsymbol{T}$. If $J_{\Delta,F}(\boldsymbol{b}_0, \boldsymbol{\alpha})$ has full rank r, then its kernel has dimension $d-s$. Hence $\dim \mathcal{T}_{(\boldsymbol{b}_0,\boldsymbol{\alpha})}\Gamma_r^* \leq d-s$, which proves that $(\boldsymbol{b}_0, \boldsymbol{\alpha})$ is regular point of Γ_r^*.

It is easy to see that $\frac{\partial \Delta^1 F}{\partial B_0}(\boldsymbol{b}_0, \alpha_1, \alpha_1) = 0$ and $\frac{\partial \Delta^1 F}{\partial B_i}(\boldsymbol{b}_0, \alpha_1, \alpha_1) = i\alpha_1^{i-1}$ for $i \geq 1$. Therefore,

$$J_{\Delta,F}(\boldsymbol{b}_0, \boldsymbol{\alpha}) := \begin{pmatrix} (d-s-1)\alpha_1^{d-s-2} & \cdots & 1 & 0 & * & * & 0 & \cdots & 0 \\ \alpha_2^{d-s-1} & \cdots & \alpha_2 & 1 & 0 & 0 & 0 & \cdots & 0 \\ \alpha_3^{d-s-1} & \cdots & \alpha_3 & 1 & 0 & 0 & \gamma_3 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_r^{d-s-1} & \cdots & \alpha_r & 1 & 0 & 0 & 0 & \cdots & \gamma_r \end{pmatrix},$$

where $\gamma_i := f'_{\boldsymbol{b}_0}(\alpha_i)$ for $i \geq 3$. Since α_i is a simple root of $f_{\boldsymbol{b}_0}$ for $i \geq 3$, it follows that $\gamma_i \neq 0$ for $i \geq 3$, which implies that $J_{\Delta,F}(\boldsymbol{b}_0, \boldsymbol{\alpha})$ has rank r. This finishes the proof. ■

Finally, we consider the set of points $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Gamma_r^*$ such that the value of at least three distinct coordinates of $\boldsymbol{\alpha}$ is the same multiple root of $f_{\boldsymbol{b}_0}$.

Lemma 4.7. *Let $\mathcal{W}_3 \subset \Gamma_r^*$ be the set of points $(\boldsymbol{b}_0, \boldsymbol{\alpha})$ for which there exist $1 \le i < j < k \le r$ such that $\alpha_i = \alpha_j = \alpha_k$ and α_i is a multiple root of $f_{\boldsymbol{b}_0}$. If $d - s \ge 3$, then $\mathcal{W}_3$ is contained in a codimension-2 subvariety of Γ_r^*.*

Proof. Let $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \mathcal{W}_3$. We may assume that $\alpha_1 = \alpha_2 = \alpha_3$ is a multiple root of $f_{\boldsymbol{b}_0}$. Taking into account that $(\boldsymbol{b}_0, \boldsymbol{\alpha})$ satisfies the equations

$$F(\boldsymbol{B}_0, T_1) = \Delta F(\boldsymbol{B}_0, T_1, T_2) = \Delta^2 F(\boldsymbol{B}_0, T_1, T_2, T_3) = 0,$$

we see that α_1 is a common root of $f_{\boldsymbol{b}_0}$, $\Delta F(\boldsymbol{b}_0, T, T)$ and $\Delta^2 F(\boldsymbol{b}_0, T, T, T)$. Hence,

$$\operatorname{Res}(f_{\boldsymbol{b}_0}, f'_{\boldsymbol{b}_0}) = \operatorname{Res}\big(F(\boldsymbol{B}_0, T), \Delta^1 F(\boldsymbol{B}_0, T, T), T\big)\big|_{\boldsymbol{B}_0 = \boldsymbol{b}_0} = 0. \tag{4.3}$$

Here the first equality holds by elementary properties of resultants, because $\deg_T F(\boldsymbol{B}_0, T) = \deg_T F(\boldsymbol{b}_0, T)$.

Suppose first that $\Delta^2 F(\boldsymbol{b}_0, T, T, T) = 0$. Then

$$0 = 2\Delta^2 F(\boldsymbol{b}_0, T, T, T) = (f^{\boldsymbol{a}})'' + \sum_{j=2}^{d-s-1} j(j-1) b_j T^{j-2} = 0.$$

This in particular implies $2b_2 = 0$, and thus $b_2 = 0$, since $p > 2$ by hypothesis. As a consequence of this identity and (4.3), the set $\mathcal{W}'_3$ of points $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Gamma_r^*$ with $\Delta^2 F(\boldsymbol{b}_0, T, T, T) = 0$ is contained in $\Psi_r^{-1}(\mathcal{Z}'_3)$, where $\mathcal{Z}'_3 \subset \mathbb{A}^{d-s}$ is the variety defined by the equations

$$B_2 = 0, \qquad \mathcal{R}(\boldsymbol{B}_0) := \operatorname{Res}\big(F(\boldsymbol{B}_0, T), \Delta^1 F(\boldsymbol{B}_0, T, T), T\big) = 0.$$

Theorem A.3 below asserts that $\mathcal{R}$ is an irreducible element of $\mathbb{F}_q[\boldsymbol{B}_0]$, which has degree $d-1$ in B_0. Thus $\mathcal{R}$ and B_2 form a regular sequence in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]$, and the variety $\mathcal{Z}'_3 \subset \mathbb{A}^{d-s}$ they define has dimension $d - s - 2$. Let Ψ_r be the mapping (4.1). Since Ψ_r is a finite morphism, $\Psi_r^{-1}(\mathcal{Z}'_3)$ has dimension $d - s - 2$. Therefore, we may assume that $\Delta^2 F(\boldsymbol{b}_0, T, T, T)$ is a nonzero polynomial.

Now suppose that p does not divide d. Then $f_{\boldsymbol{b}_0}$ and $f'_{\boldsymbol{b}_0}$ are nonzero polynomials of degree d and $d-1$ respectively. Hence, by elementary properties of resultants,

$$\begin{aligned}\operatorname{Res}(f_{\boldsymbol{b}_0}, f'_{\boldsymbol{b}_0}) &= \operatorname{Res}\big(F(\boldsymbol{B}_0, T), \Delta^1 F(\boldsymbol{B}_0, T, T), T\big)\big|_{\boldsymbol{B}_0 = \boldsymbol{b}_0},\\ \operatorname{Res}(f'_{\boldsymbol{b}_0}, \Delta^2 f_{\boldsymbol{b}_0}) &= \operatorname{Res}\big(\Delta^1 F(\boldsymbol{B}_0, T, T), \Delta^2 F(\boldsymbol{B}_0, T, T, T), T\big)\big|_{\boldsymbol{B}_0 = \boldsymbol{b}_0}.\end{aligned}$$

We conclude that $(\mathcal{W}_3 \setminus \mathcal{W}'_3) \cap \Gamma_r^* \subset \Psi_r^{-1}(\mathcal{Z}_3)$, where Ψ_r is the morphism of (4.1) and $\mathcal{Z}_3$ is the subvariety of $\mathbb{A}^{d-s}$ defined by the equations

$$\begin{aligned}\mathcal{R} &:= \operatorname{Res}\big(F(\boldsymbol{B}_0, T), \Delta^1 F(\boldsymbol{B}_0, T, T), T\big) = 0,\\ \mathcal{R}' &:= \operatorname{Res}\big(\Delta^1 F(\boldsymbol{B}_0, T, T), \Delta^2 F(\boldsymbol{B}_0, T, T, T), T\big) = 0.\end{aligned}$$

As asserted by Theorem A.3, $\mathcal{R}$ is an irreducible element of $\mathbb{F}_q[\boldsymbol{B}_0]$ of degree $d-1$ in B_0. On the other hand, the nonzero polynomial $\mathcal{R}'$ has degree 0 in B_0. As a consequence, the two polynomials form a regular sequence in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]$, which shows that $\mathcal{Z}_3$ has codimension 2 in $\mathbb{A}^{d-s}$. This proves that $\Psi_r^{-1}(\mathcal{Z}_3)$ is a codimension-2 subvariety of Γ_r^*.

Next suppose that p divides d. If there exists l such that $la_l \not\equiv 0 \bmod p$, then $f'_{\boldsymbol{b}_0}$ and $\Delta^1F(\boldsymbol{B}_0, T, T)$ are of the same degree in T and the argument above works *mutatis mutandis.*

On the other hand, if $la_l \equiv 0 \bmod p$ for $d-s \leq l \leq d-1$, we have two possibilities, according to whether or not $(d-s-1)b_{d-s-1} = 0$. If not, then $f'_{\boldsymbol{b}_0}$ and $\Delta^1F(\boldsymbol{B}_0, T, T)$ are of the same degree in T and the previous argument works. If $b_{d-s-1} = 0$, then $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Psi_r^{-1}(\mathcal{Z}_4)$, where $\mathcal{Z}_4$ is the subvariety of $\mathbb{A}^{d-s}$ defined by

$$\mathcal{R}(\boldsymbol{B}_0) = 0, \qquad B_{d-s-1} = 0.$$

It is easy to see that $\mathcal{R}$ and B_{d-s-1} form a regular sequence in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]$, which shows that $\Psi_r^{-1}(\mathcal{Z}_4)$ is a subvariety of codimension 2 in Γ_r^*. Finally, if p divides $d-s-1$, then p does not divide $d-s-2$, and we can repeat previous arguments considering the cases $b_{d-s-2} = 0$ and $b_{d-s-2} \neq 0$. This finishes the proof of the lemma. ■

Now we are in a position to prove the main result of this section. According to Lemmas 4.3–4.7, the set of singular points of Γ_r^* is contained in union of $\mathcal{W}_1$, $\mathcal{W}_2$ and $\mathcal{W}_3$, defined in the relevant statements. Since each $\mathcal{W}_i$ is contained in a codimension-2 subvariety of Γ_r^*, we obtain the following result.

THEOREM 4.8. *Let $p > 2$ and $q > d$. If $d - s \geq 3$, then the singular locus of Γ_r^* has codimension at least* 2 *in Γ_r^*.*

We finish the section by discussing a few consequences of the analysis underlying the proof of Theorem 4.8.

COROLLARY 4.9. *Under the assumptions of Theorem* 4.8, *the ideal $\mathcal{J} \subset \mathbb{F}_q[\boldsymbol{B}_0, \boldsymbol{T}]$ generated by $\Delta^{i-1}F(\boldsymbol{B}_0, T_1, \ldots, T_i)$ $(1 \leq i \leq r)$ is radical, and the variety Γ_r^* is an ideal-theoretic complete intersection of dimension $d-s$.*

Proof. Let $J_\Delta(\boldsymbol{B}_0, \boldsymbol{T})$ be the Jacobian matrix of the polynomials $\Delta^{i-1}F(\boldsymbol{B}_0, T_1, \ldots, T_i)$ $(1 \leq i \leq r)$ with respect to $\boldsymbol{B}_0, \boldsymbol{T}$. We claim that the set of points $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Gamma_r^*$ for which $J_\Delta(\boldsymbol{b}_0, \boldsymbol{\alpha})$ does not have full rank is contained in a subvariety of Γ_r^* of codimension 1.

Indeed, let $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Gamma_r^*$. In the proof of Lemma 4.2 we showed that $F(\boldsymbol{B}_0, T_j) \in \mathcal{J}$ for $1 \leq j \leq r$. This implies that $\nabla F(\boldsymbol{b}_0, \alpha_j)$ is a linear combination of the gradients of the polynomials $\Delta^{i-1}F(\boldsymbol{b}_0, \boldsymbol{\alpha})$ for $1 \leq i \leq r$. Hence $\operatorname{rank} J_F(\boldsymbol{b}_0, \boldsymbol{\alpha}) \leq \operatorname{rank} J_\Delta(\boldsymbol{b}_0, \boldsymbol{\alpha})$.

Moreover, if $J_F(\boldsymbol{b}_0, \boldsymbol{\alpha})$ does not have full rank, then $f_{\boldsymbol{b}_0}$ has multiple roots. By Lemma 4.3, the set of points $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \Gamma_r^*$ for which $f'_{\boldsymbol{b}_0} = 0$ is contained in a subvariety of codimension 2 of $\varGamma_r^*$. On the other hand, if $(\boldsymbol{b}_0,\boldsymbol{\alpha}) \in \varGamma_r^*$ is such that $f_{\boldsymbol{b}_0}$ has multiple roots and $f'_{\boldsymbol{b}_0} \neq 0$, then $(\boldsymbol{b}_0,\boldsymbol{\alpha}) \in \varPsi_r^{-1}(\mathcal{Z})$, where $\mathcal{Z}$ is the subvariety of $\mathbb{A}^{d-s}$ defined by

$$\mathrm{Res}\big(F(\boldsymbol{B}_0,T),\varDelta^1F(\boldsymbol{B}_0,T,T),T\big)=0.$$

We see that $\varPsi_r^{-1}(\mathcal{Z})$ has codimension 1 in $\varGamma_r^*$, finishing the proof of our claim.

By Lemma 4.1 the polynomials $\varDelta^{i-1}F(\boldsymbol{B}_0,T_1,\dots,T_i)$ $(1\le i\le r)$ form a regular sequence in $\mathbb{F}_q[\boldsymbol{B}_0,\boldsymbol{T}]$. Therefore, by [Eis95, Theorem 18.15], $\mathcal{J}$ is a radical ideal, which in turn implies that $\varGamma_r^*$ is an ideal-theoretic complete intersection of dimension $d-s$. ∎

4.2. The geometry of the projective closure of $\varGamma_r^*$. To estimate the number of q-rational points of $\varGamma_r^*$ we need information on the behavior of $\varGamma_r^*$ at infinity. For this purpose, we consider its projective closure $\mathrm{pcl}(\varGamma_r^*) \subset \mathbb{P}^{d-s+r}$, whose definition we now recall. Consider the embedding of $\mathbb{A}^{d-s+r}$ into the projective space $\mathbb{P}^{d-s+r}$ which assigns to any point $(\boldsymbol{b}_0,\boldsymbol{\alpha}) \in \mathbb{A}^{d-s+r}$ the point $(b_{d-s-1}:\dots:b_0:1:\alpha_1:\dots:\alpha_r) \in \mathbb{P}^{d-s+r}$. The closure of the image of $\varGamma_r^*$ under this embedding in the Zariski topology of $\mathbb{P}^{d-s+r}$ is called the *projective closure* of $\varGamma_r^*$. The points of $\mathrm{pcl}(\varGamma_r^*)$ lying in the hyperplane $\{T_0=0\}$ are called the *points of* $\mathrm{pcl}(\varGamma_r^*)$ *at infinity*.

It is well-known that $\mathrm{pcl}(\varGamma_r^*)$ is the $\mathbb{F}_q$-variety of $\mathbb{P}^{d-s+r}$ defined by the homogenizations $F^h \in \mathbb{F}_q[\boldsymbol{B}_0,T_0,\boldsymbol{T}]$ of all polynomials F in the ideal $\mathcal{J} \subset \mathbb{F}_q[\boldsymbol{B}_0,\boldsymbol{T}]$ generated by $\varDelta^{i-1}F(\boldsymbol{B}_0,T_1,\dots,T_i)$ $(1\le i\le r)$. We denote by $\mathcal{J}^h$ the ideal generated by all the polynomials F^h with $F\in\mathcal{J}$. Since $\mathcal{J}$ is radical, so is $\mathcal{J}^h$ (see, e.g., [Kun85, §I.5, Exercise 6]). Furthermore, $\mathrm{pcl}(\varGamma_r^*)$ is equidimensional of dimension $d-s$ (see, e.g., [Kun85, Propositions I.5.17 and II.4.1]) and of degree equal to $\deg\varGamma_r^*$ (see, e.g., [CGH91, Proposition 1.11]).

Lemma 4.10. *The homogenized polynomials* $\varDelta^{i-1}F(\boldsymbol{B}_0,T_1,\dots,T_i)^h$ $(1\le i\le r)$ *generate the ideal* $\mathcal{J}^h$. *Furthermore,* $\mathrm{pcl}(\varGamma_r^*)$ *is an ideal-theoretic complete intersection of dimension* $d-s$ *and degree* $d!/(d-r)!$.

Proof. According to Lemma 4.1, the polynomials $\varDelta^{i-1}F(\boldsymbol{B}_0,T_1,\dots,T_i)$ $(1\le i\le r)$ form a Gröbner basis of the ideal $\mathcal{J}$ with the graded lexicographical order defined by $T_r>\dots>T_1>B_{d-s-1}>\dots>B_0$. Therefore, the first assertion follows from, e.g., [CLO92, §8.4, Theorem 4]. In particular, $\mathrm{pcl}(\varGamma_r^*)$ is an ideal-theoretic complete intersection. Hence, [Har92, Theorem 18.3] proves that the degree of $\mathrm{pcl}(\varGamma_r^*)$ is $d!/(d-r)!$. ∎

Our next purpose is to study the singular points of $\mathrm{pcl}(\varGamma_r^*)$. We start with the following characterization of the points of $\mathrm{pcl}(\varGamma_r^*)$ at infinity.

LEMMA 4.11. $\mathrm{pcl}(\varGamma_r^*) \cap \{T_0 = 0\} \subset \mathbb{P}^{d-s-1+r}$ *is a linear variety of dimension* $d-s-1$.

Proof. According to Lemma 4.10, the homogeneous polynomials $\varDelta^{i-1}F(\boldsymbol{B}_0, T_1, \dots, T_i)^h$ $(1 \leq i \leq r)$ generate the ideal $\mathcal{J}^h$. Since $\varDelta^{i-1}F(\boldsymbol{B}_0, T_1, \dots, T_i)^h|_{T_0=0} = T_i^{d-i+1} +$ monomials of positive degree in $T_1, \dots, T_{i-1}$, we conclude that $\mathrm{pcl}(\varGamma_r^*) \cap \{T_0 = 0\}$ is the linear $\mathbb{F}_q$-variety $\{T_1 = 0, \dots, T_r = 0\}$, which finishes the proof. ∎

Now we are able to prove the main result of this section, which summarizes all the facts we need concerning the projective variety $\mathrm{pcl}(\varGamma_r^*)$.

THEOREM 4.12. *Under the assumptions of Theorem* 4.8, *the projective variety* $\mathrm{pcl}(\varGamma_r^*) \subset \mathbb{P}^{d-s+r}$ *is a normal absolutely irreducible ideal-theoretic complete intersection of dimension* $d-s$ *and degree* $d!/(d-r)!$.

Proof. Lemma 4.10 shows that $\mathrm{pcl}(\varGamma_r^*)$ is an ideal-theoretic complete intersection. On the other hand, combining Theorem 4.8 and Lemma 4.11 we see that the singular locus of $\mathrm{pcl}(\varGamma_r^*)$ has codimension at least 2 in $\mathrm{pcl}(\varGamma_r^*)$. This implies that $\mathrm{pcl}(\varGamma_r^*)$ is regular in codimension 1, and thus normal. Finally, by Theorem 2.1 we conclude that $\mathrm{pcl}(\varGamma_r^*)$ is absolutely irreducible. ∎

As a consequence of Theorem 4.12, $\varGamma_r^* \subset \mathbb{A}^{d-s+r}$ is also absolutely irreducible of dimension $d-s$ and degree $d!/(d-r)!$. Furthermore, Lemma 3.3 shows that $\varGamma_r$ is a nonempty Zariski open subset of $\varGamma_r^*$. Since $\varGamma_r^*$ is absolutely irreducible, we conclude that the Zariski closure of $\varGamma_r$ is equal to $\varGamma_r^*$.

5. The number of q-rational points of $\varGamma_r$.

As before, let $p > 2$ and let d and s be positive integers with $q > d$ and $1 \leq s \leq d-3$. In this section we determine the asymptotic behavior of the average value set cardinality $\mathcal{V}(d, s, \boldsymbol{a})$ of the family of polynomials $\{f_{\boldsymbol{b}} : \boldsymbol{b} \in \mathbb{F}_q^{d-s-1}\}$. By Theorem 3.1 we have

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

where $\chi_r^{\boldsymbol{a}}$ denotes the number of r-element subsets χ_r of $\mathbb{F}_q$ such that there exists $\boldsymbol{b}_0 \in \mathbb{F}_q^{d-s}$ with $f_{\boldsymbol{b}_0}|_{\chi_r} \equiv 0$. Combining Lemmas 3.2 and 3.3 shows that

$$\chi_r^{\boldsymbol{a}} = \frac{|\varGamma_r(\mathbb{F}_q)|}{r!} = \frac{1}{r!} \Big| \varGamma_r^*(\mathbb{F}_q) \setminus \bigcup_{i \neq j} \{T_i = T_j\} \Big|$$

for each r with $d-s+1 \leq r \leq d$. In the next section we apply the results of Section 4 on the geometry of $\varGamma_r^*$ to estimate the number of q-rational points of $\varGamma_r^*$.

5.1. Estimates on the number of q-rational points of normal complete intersections. We shall use an estimate on the number of q-rational points of a projective normal complete intersection of [CMP12] (see also [CM07] or [GL02] for other estimates). More precisely, if $V \subset \mathbb{P}^n$ is a normal complete intersection defined over $\mathbb{F}_q$ of dimension $m \geq 2$, degree δ and multidegree $\boldsymbol{d} := (d_1, \dots, d_{n-m})$, then (see [CMP12, Theorem 1.3])

$$\big||V(\mathbb{F}_q)| - p_m\big| \leq (\delta(D-2)+2)q^{m-1/2} + 14D^2\delta^2 q^{m-1}, \tag{5.1}$$

where $p_m := q^m + q^{m-1} + \cdots + q + 1 = |\mathbb{P}^m(\mathbb{F}_q)|$ and $D := \sum_{i=1}^{n-m}(d_i - 1)$.

From Theorem 4.12 we know that $\mathrm{pcl}(\varGamma_r^*) \subset \mathbb{P}^{d-s+r}$ is a normal complete intersection defined over $\mathbb{F}_q$. Therefore, applying (5.1) we obtain

$$\big||\mathrm{pcl}(\varGamma_r^*)(\mathbb{F}_q)| - p_{d-s}\big| \leq (\delta_r(D_r-2)+2)q^{d-s-1/2} + 14D_r^2\delta_r^2 q^{d-s-1},$$

where $D_r := \sum_{i=1}^{r}(d-i) = rd - r(r+1)/2$ and $\delta_r := d!/(d-r)!$. On the other hand, since $\mathrm{pcl}(\varGamma_r^*)^\infty := \mathrm{pcl}(\varGamma_r^*) \cap \{T_0 = 0\} \subset \mathbb{P}^{d-s-1+r}$ is a linear variety of dimension $d-s-1$, the number of q-rational points of $\mathrm{pcl}(\varGamma_r^*)^\infty$ is p_{d-s-1}. Hence,

$$\begin{aligned} \big||\varGamma_r^*(\mathbb{F}_q)| - q^{d-s}\big| &= \big||\mathrm{pcl}(\varGamma_r^*)(\mathbb{F}_q)| - |\mathrm{pcl}(\varGamma_r^*(\mathbb{F}_q))^\infty| - p_{d-s} + p_{d-s-1}\big| \\ &= \big||\mathrm{pcl}(\varGamma_r^*)(\mathbb{F}_q)| - p_{d-s}\big| \\ &\leq (\delta_r(D_r-2)+2)q^{d-s-1/2} + 14D_r^2\delta_r^2 q^{d-s-1}. \end{aligned} \tag{5.2}$$

We also need an estimate on the number q-rational points of the affine $\mathbb{F}_q$-variety

$$\varGamma_r^{*,=} := \varGamma_r^* \cap \bigcup_{1\leq i<j\leq r} \{T_i = T_j\}.$$

We observe that $\varGamma_r^{*,=} = \varGamma_r^* \cap \mathcal{H}_r$, where $\mathcal{H}_r \subset \mathbb{A}^{d-s+r}$ is the hypersurface defined by the polynomial $F_r := \prod_{1\leq i<j\leq r}(T_i - T_j)$. By the Bézout inequality (2.1),

$$\deg \varGamma_r^{*,=} \leq \delta_r \binom{r}{2}. \tag{5.3}$$

Furthermore, we claim that $\varGamma_r^{*,=}$ has dimension at most $d-s-1$. Indeed, let $(\boldsymbol{b}_0, \boldsymbol{\alpha}) \in \varGamma_r^{*,=}$. We can assume that $\alpha_1 = \alpha_2$. From the definition of divided differences we deduce that $f'_{\boldsymbol{b}_0}(\alpha_1) = 0$, which implies that $f_{\boldsymbol{b}_0}$ has multiple roots. By Corollary 4.9 the set of points $(\boldsymbol{b}_0, \boldsymbol{\alpha})$ of $\varGamma_r^*$ for which $f_{\boldsymbol{b}_0}$ has multiple roots is contained in a subvariety of $\varGamma_r^*$ of codimension at least 1. This yields the claim.

Combining the claim with (5.3), applying, e.g., [CM06, Lemma 2.1], we obtain

$$|\varGamma_r^{*,=}(\mathbb{F}_q)| \leq \delta_r \binom{r}{2} q^{d-s-1}. \tag{5.4}$$

Since $\Gamma_r(\mathbb{F}_q) = \Gamma_r^*(\mathbb{F}_q) \setminus \Gamma_r^{*,=}(\mathbb{F}_q)$, from (5.2) and (5.4) we deduce that

$$\begin{aligned}\big||\Gamma_r(\mathbb{F}_q)| - q^{d-s}\big| &\leq \big||\Gamma_r^*(\mathbb{F}_q)| - q^{d-s}\big| + |\Gamma_r^{*,=}(\mathbb{F}_q)| \\ &\leq (\delta_r(D_r-2)+2)q^{d-s-1/2} \\ &\quad + (14D_r^2\delta_r^2 + r(r-1)\delta_r/2)q^{d-s-1}.\end{aligned}$$

As a consequence, we obtain the following result.

Theorem 5.1. *Let $p > 2$ and $q > d$. If $1 \leq s \leq d-3$, then for any r with $d-s+1 \leq r \leq d$ we have*

$$\begin{aligned}\left|\chi_r^{\boldsymbol{a}} - \frac{q^{d-s}}{r!}\right| &\leq \frac{1}{r!}(\delta_r(D_r-2)+2)q^{d-s-1/2} \\ &\quad + \frac{1}{r!}(14D_r^2\delta_r^2 + r(r-1)\delta_r/2)q^{d-s-1},\end{aligned}$$

where $D_r := rd - r(r+1)/2$ and $\delta_r := d!/(d-r)!$.

5.2. An estimate for $\mathcal{V}(d,s,\boldsymbol{a})$. Theorem 5.1 is the critical step in estimating $\mathcal{V}(d,s,\boldsymbol{a})$.

Corollary 5.2. *Under the assumptions of Theorem 5.1,*

$$|\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d q| \leq d^2 2^{d-1} q^{1/2} + \frac{7}{2}d^4 \sum_{k=0}^{s-1} \binom{d}{k}^2 (d-k)!. \tag{5.5}$$

Proof. According to Theorem 3.1, we have

$$\begin{aligned}&\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d q \\ &\quad = \sum_{r=1}^{d-s}(-q)^{1-r}\left(\binom{q}{r} - \frac{q^r}{r!}\right) + \frac{1}{q^{d-s-1}} \sum_{r=d-s+1}^{d} (-1)^{r-1}\left(\chi_r^{\boldsymbol{a}} - \frac{q^{d-s}}{r!}\right).\end{aligned} \tag{5.6}$$

In [C–P14, Corollary 14] we obtained the following upper bound for the absolute value of the first term on the right-hand side of (5.6):

$$A(d,s) := \left|\sum_{r=1}^{d-s}(-q)^{1-r}\left(\binom{q}{r} - \frac{q^r}{r!}\right)\right| \leq \frac{1}{2(d-s-1)!} + \frac{7}{q} + \frac{1}{2e} \leq d.$$

Next we consider the second term. From Theorem 5.1 we have

$$\begin{aligned}B(d,s) &:= \frac{1}{q^{d-s-1}} \sum_{r=d-s+1}^{d} \left|\chi_r^{\boldsymbol{a}} - \frac{q^{d-s}}{r!}\right| \\ &\leq q^{1/2} \sum_{r=d-s+1}^{d} \frac{\delta_r(D_r-2)+2}{r!} + 14 \sum_{r=d-s+1}^{d} \frac{D_r^2\delta_r^2}{r!} + \sum_{r=d-s+1}^{d} \frac{\delta_r}{2(r-2)!}.\end{aligned}$$

Concerning the first term on the right-hand side, we see that

$$\sum_{r=d-s+1}^{d} \frac{\delta_r(D_r-2)+2}{r!} \le \sum_{r=d-s+1}^{d} \binom{d}{r}\frac{r(2d-1-r)}{2} \le d^2 2^{d-1}.$$

Moreover,

$$\begin{aligned}\sum_{r=d-s+1}^{d} \frac{D_r^2\delta_r^2}{r!} &= \sum_{r=d-s+1}^{d} \binom{d}{r}^2 \frac{r^2(2d-1-r)^2\, r!}{4}\\ &\le \frac{1}{64}(2d-1)^4 \sum_{k=0}^{s-1}\binom{d}{k}^2 (d-k)!.\end{aligned}$$

Finally,

$$\sum_{r=d-s+1}^{d} \frac{\delta_r}{2(r-2)!} = \sum_{r=d-s+1}^{d} \binom{d}{r}\frac{r(r-1)}{2} = \sum_{k=0}^{s-1}\binom{d}{k}\frac{(d-k)!}{2\,(d-k-2)!}.$$

Therefore,

$$B(d,s) \le q^{1/2} d^2 2^{d-1} + \frac{1}{4}\sum_{k=0}^{s-1}\binom{d}{k}(d-k)! + \frac{7}{32}(2d-1)^4 \sum_{k=0}^{s-1}\binom{d}{k}^2 (d-k)!.$$

Combining the bounds for $A(d,s)$ and $B(d,s)$, we obtain the statement of the corollary. ∎

5.3. On the behavior of (5.5). In this section we analyze the behavior of the right-hand side of (5.5). The analysis consists of elementary calculations, which will only be sketched.

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

Remark 5.3. Let $k_0 := -1/2+\sqrt{5+4d}/2$. Then h is either an increasing function or a unimodal function in the integer interval $[0, s-1]$, which reaches its maximum at $\lfloor k_0 \rfloor$.

From Remark 5.3 we see that

$$\sum_{k=0}^{s-1}\binom{d}{k}^2(d-k)! \le s\binom{d}{\lfloor k_0\rfloor}^2 (d-\lfloor k_0\rfloor)! = \frac{s\,(d!)^2}{(d-\lfloor k_0\rfloor)!\,(\lfloor k_0\rfloor !)^2}. \tag{5.7}$$

To obtain an upper bound for the right-hand side of (5.7) we shall use the Stirling formula (see, e.g., [FS08, p. 747]): for $m \in \mathbb{N}$, there exists θ with $0 \le \theta < 1$ such that $m! = (m/e)^m\sqrt{2\pi m}\, e^{\theta/(12m)}$.

Applying the Stirling formula, we see that there exist θ_i $(i = 1, 2, 3)$ with $0 \le \theta_i < 1$ such that

$$\begin{aligned} C(d,s) &:= \frac{s(d!)^2}{(d-\lfloor k_0\rfloor)!\,(\lfloor k_0\rfloor!)^2} \\ &\le \frac{sd^{2d+1}e^{-d+\lfloor k_0\rfloor}e^{\frac{\theta_1}{6d}-\frac{\theta_2}{12(d-\lfloor k_0\rfloor)}-\frac{\theta_3}{6\lfloor k_0\rfloor}}}{(d-\lfloor k_0\rfloor)^{d-\lfloor k_0\rfloor}\sqrt{2\pi(d-\lfloor k_0\rfloor)}\,\lfloor k_0\rfloor^{2\lfloor k_0\rfloor+1}}. \end{aligned}$$

By elementary calculations we obtain

$$(d-\lfloor k_0\rfloor)^{-d+\lfloor k_0\rfloor} \le d^{-d+\lfloor k_0\rfloor}e^{\lfloor k_0\rfloor(d-\lfloor k_0\rfloor)/d}, \qquad \frac{d^{\lfloor k_0\rfloor}}{\lfloor k_0\rfloor^{2\lfloor k_0\rfloor}} \le e^{(d-\lfloor k_0\rfloor^2)/\lfloor k_0\rfloor}.$$

It follows that

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

By the definition of $\lfloor k_0\rfloor$, it is easy to see that $d/(\lfloor k_0\rfloor\sqrt{d-\lfloor k_0\rfloor}) \le 5/2$ and $2\lfloor k_0\rfloor \le -1+\sqrt{5+4d} \le -1/5+2\sqrt{d}$. Therefore, taking into account that $d \ge 4$, we conclude that

$$C(d,s) \le \frac{5}{2}\,\frac{e^{109/30}sd^de^{2\sqrt{d}}}{\sqrt{2\pi}\,e^d}.$$

Combining this bound with Corollary 5.2 we obtain the following result.

Theorem 5.4. *Under the assumptions and notations of Theorem* 5.1,

$$|\mathcal{V}(d,s,\boldsymbol{a}) - \mu_d q| \le d^2 2^{d-1}q^{1/2} + 133d^{d+5}e^{2\sqrt{d}-d}.$$

6. Estimating the second moment $\mathcal{V}_2(d,s,\boldsymbol{a})$: combinatorial preliminaries. Now we consider the second objective of this paper: estimating the second moment of the value set cardinalities for the families of polynomials under consideration.

As before, we assume that the characteristic p of $\mathbb{F}_q$ is greater than 2, and fix integers d and s with $d < q$ and $1 \le s \le d-3$. We also fix $\boldsymbol{a} := (a_{d-1}, \ldots, a_{d-s}) \in \mathbb{F}_q^s$ and set $f^{\boldsymbol{a}} := T^d + a_{d-1}T^{d-1} + \cdots + a_{d-s}T^{d-s}$. Further, for any $\boldsymbol{b} := (b_{d-s-1}, \ldots, b_1) \in \mathbb{F}_q^{d-s-1}$, we denote

$$f_{\boldsymbol{b}} := T^d + a_{d-1}T^{d-1} + \cdots + a_{d-s}T^{d-s} + b_{d-s-1}T^{d-s-1} + \cdots + b_1T.$$

We wish to estimate the sum

$$\mathcal{V}_2(d,s,\boldsymbol{a}) := \frac{1}{q^{d-s-1}} \sum_{\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}} \mathcal{V}(f_{\boldsymbol{b}})^2. \tag{6.1}$$

We start with the following result, which plays a similar role to Theorem 3.1 in estimating $\mathcal{V}(d,s,\boldsymbol{a})$.

Theorem 6.1. *Under the assumptions above,*

$$\mathcal{V}_2(d,s,\boldsymbol{a}) = \mathcal{V}(d,s,\boldsymbol{a}) + \sum_{\substack{1\le m,n\le d\\ 2\le m+n\le d-s}} (-1)^{m+n}\binom{q}{m}\binom{q}{n} q^{2-n-m} + \frac{1}{q^{d-s-1}} \sum_{\substack{1\le m,n\le d\\ d-s+1\le m+n\le 2d}} (-1)^{m+n} \sum_{\substack{\Gamma_1,\Gamma_2\subset\mathbb{F}_q\\ |\Gamma_1|=m,\,|\Gamma_2|=n}} |S^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2}|,$$

where $\mathcal{S}^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2}$ is the set of points $(\boldsymbol{b}, b_{0,1}, b_{0,2}) \in \mathbb{F}_q^{d-s+1}$ with $b_{0,1}\neq b_{0,2}$ such that $(f_{\boldsymbol{b}}+b_{0,1})|_{\Gamma_1}\equiv 0$ and $(f_{\boldsymbol{b}}+b_{0,2})|_{\Gamma_2}\equiv 0$.

Proof. Fix $\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}$. Let $\mathbb{F}_q[T]_d$ denote the set of polynomials in $\mathbb{F}_q[T]$ of degree at most d, let $\mathcal{N} : \mathbb{F}_q[T]_d \to \mathbb{Z}_{\ge 0}$ be the counting function of the number of roots in $\mathbb{F}_q$ 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 $\mathbb{F}_q$. Taking into account that $\mathcal{V}(f_{\boldsymbol{b}}) = \sum_{b_0\in\mathbb{F}_q} \mathbf{1}_{\{\mathcal{N}>0\}}(f_{\boldsymbol{b}}+b_0)$, we obtain

$$q^{d-s-1}\mathcal{V}_2(d,s,\boldsymbol{a}) = \sum_{\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}} \Big(\sum_{b_{0,1}\in\mathbb{F}_q} \mathbf{1}_{\{\mathcal{N}>0\}}(f_{\boldsymbol{b}}+b_{0,1})\Big)\Big(\sum_{b_{0,2}\in\mathbb{F}_q} \mathbf{1}_{\{\mathcal{N}>0\}}(f_{\boldsymbol{b}}+b_{0,2})\Big).$$

For $(\boldsymbol{b}, b_{0,1}, b_{0,2}) \in \mathbb{F}_q^{d-s+1}$, we denote $f_{\boldsymbol{b}_1} := f_{\boldsymbol{b}} + b_{0,1}$ and $f_{\boldsymbol{b}_2} := f_{\boldsymbol{b}} + b_{0,2}$. We have

$$(6.2)\qquad q^{d-s-1}\mathcal{V}_2(d,s,\boldsymbol{a}) = \sum_{\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}} \sum_{(b_{0,1},b_{0,2})\in\mathbb{F}_q^2} \mathbf{1}_{\{\mathcal{N}>0\}^2}(f_{\boldsymbol{b}_1}, f_{\boldsymbol{b}_2})$$

$$= \sum_{\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}} \sum_{\substack{(b_{0,1},b_{0,2})\in\mathbb{F}_q^2\\ b_{0,1}=b_{0,2}}} \mathbf{1}_{\{\mathcal{N}>0\}^2}(f_{\boldsymbol{b}_1}, f_{\boldsymbol{b}_2}) + \sum_{\boldsymbol{b}\in\mathbb{F}_q^{d-s-1}} \sum_{\substack{(b_{0,1},b_{0,2})\in\mathbb{F}_q^2\\ b_{0,1}\neq b_{0,2}}} \mathbf{1}_{\{\mathcal{N}>0\}^2}(f_{\boldsymbol{b}_1}, f_{\boldsymbol{b}_2}).$$

For the first term on the right-hand side of (6.2), we have

$$(6.3)\qquad \sum_{\substack{(\boldsymbol{b},b_{0,1},b_{0,2})\in\mathbb{F}_q^{d-s+1}\\ b_{0,1}=b_{0,2}}} \mathbf{1}_{\{\mathcal{N}>0\}^2}(f_{\boldsymbol{b}_1}, f_{\boldsymbol{b}_2}) = \sum_{\boldsymbol{b}_1\in\mathbb{F}_q^{d-s}} \mathbf{1}_{\{\mathcal{N}>0\}}(f_{\boldsymbol{b}_1}) = q^{d-s-1}\mathcal{V}(d,s,\boldsymbol{a}).$$

Next we express the second term on the right-hand side of (6.2) in terms of the sets

$$S^{\boldsymbol{a}}_{\{\alpha\},\{\beta\}} := \{(\boldsymbol{b}, b_{0,1}, b_{0,2}) \in \mathbb{F}_q^{d-s+1} : b_{0,1}\neq b_{0,2},\ f_{\boldsymbol{b}_1}(\alpha) = f_{\boldsymbol{b}_2}(\beta) = 0\}$$

with $\alpha, \beta \in \mathbb{F}_q$. We have

$$\sum_{\substack{(\boldsymbol{b},b_{0,1},b_{0,2})\in\mathbb{F}_q^{d-s+1}\\ b_{0,1}\neq b_{0,2}}} \mathbf{1}_{\{\mathcal{N}>0\}^2}(f_{\boldsymbol{b}_1}, f_{\boldsymbol{b}_2}) = \Big| \bigcup_{\substack{\{\alpha,\beta\}\subseteq\mathbb{F}_q\\ \alpha\neq\beta}} \mathcal{S}^{\boldsymbol{a}}_{\{\alpha\},\{\beta\}} \Big| = \Big| \bigcup_{\alpha\in\mathbb{F}_q} \bigcup_{\substack{\beta\in\mathbb{F}_q\\ \alpha\neq\beta}} \mathcal{S}^{\boldsymbol{a}}_{\{\alpha\},\{\beta\}} \Big|.$$

Let $\mathcal{T}^{\boldsymbol{a}}_\alpha := \bigcup_{\beta\in\mathbb{F}_q} \mathcal{S}^{\boldsymbol{a}}_{\{\alpha\},\{\beta\}}$. By the inclusion-exclusion principle we obtain

$$\begin{aligned}
\Big| \bigcup_{\alpha\in\mathbb{F}_q} \bigcup_{\beta\in\mathbb{F}_q} \mathcal{S}^{\boldsymbol{a}}_{\{\alpha\},\{\beta\}} \Big| &= \sum_{m=1}^{q} (-1)^{m-1} \sum_{\{\alpha_1,\dots,\alpha_m\}\subset\mathbb{F}_q} |\mathcal{T}^{\boldsymbol{a}}_{\alpha_1} \cap \dots \cap T^{\boldsymbol{a}}_{\alpha_m}| \\
&= \sum_{m=1}^{q} (-1)^{m-1} \sum_{\{\alpha_1,\dots,\alpha_m\}\subset\mathbb{F}_q} \Big| \bigcup_{\beta\in\mathbb{F}_q} \mathcal{S}^{\boldsymbol{a}}_{\{\alpha_1,\dots,\alpha_m\},\{\beta\}} \Big| \\
&= \sum_{\substack{m=1\\ n=1}}^{q} (-1)^{m+n} \sum_{\substack{\{\alpha_1,\dots,\alpha_m\}\subset\mathbb{F}_q\\ \{\beta_1,\dots,\beta_n\}\subset\mathbb{F}_q}} |\mathcal{S}^{\boldsymbol{a}}_{\{\alpha_1,\dots,\alpha_m\},\{\beta_1,\dots,\beta_n\}}| \\
&= \sum_{\substack{m=1\\ n=1}}^{q} (-1)^{m+n} \sum_{\substack{\Gamma_1,\Gamma_2\subseteq\mathbb{F}_q\\ |\Gamma_1|=m,\,|\Gamma_2|=n}} |S^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2}|.
\end{aligned}$$

If $\Gamma_1 \cap \Gamma_2 \neq \emptyset$, then $\mathcal{S}^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2} = \emptyset$, while $\mathcal{S}^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2} = \emptyset$ for $m > d$ or $n > d$. We conclude that

$$\sum_{\substack{(\boldsymbol{b},b_{0,1},b_{0,2})\in\mathbb{F}_q^{d-s+1}\\ b_{0,1}\neq b_{0,2}}} \mathbf{1}_{\{\mathcal{N}>0\}^2}(f_{\boldsymbol{b}_1}, f_{\boldsymbol{b}_2}) = \sum_{1\le m,\,n\le d} (-1)^{m+n} \sum_{\substack{\Gamma_1,\Gamma_2\subseteq\mathbb{F}_q\\ |\Gamma_1|=m,\,|\Gamma_2|=n\\ \Gamma_1\cap\Gamma_2=\emptyset}} |\mathcal{S}^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2}|.$$

Fix $n, m \in \mathbb{N}$ and fix subsets $\Gamma_1 = \{\alpha_1, \dots, \alpha_m\} \subset \mathbb{F}_q$ and $\Gamma_2 = \{\beta_1, \dots, \beta_n\} \subset \mathbb{F}_q$ with $\Gamma_1 \cap \Gamma_2 = \emptyset$. If $(\boldsymbol{b}, b_{0,1}, b_{0,2}) \in \mathcal{S}^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2}$, then $b_{0,1} \neq b_{0,2}$, $f_{\boldsymbol{b}_1}|_{\Gamma_1} \equiv 0$ and $f_{\boldsymbol{b}_2}|_{\Gamma_2} \equiv 0$. These two identities can be expressed in matrix form as follows:

$$M(\Gamma_1, \Gamma_2) \cdot \boldsymbol{v} = -f_{\boldsymbol{a}}(\Gamma_1, \Gamma_2) \tag{6.4}$$

where $\boldsymbol{v}^t := (\boldsymbol{b}, b_{0,1}, b_{0,2}) \in \mathbb{F}_q^{d-s+1}$, and $M(\Gamma_1, \Gamma_2) \in \mathbb{F}_q^{(m+n)\times(d-s+1)}$ and $f_{\boldsymbol{a}}(\Gamma_1, \Gamma_2) \in \mathbb{F}_q^{(m+n)\times 1}$ are the following matrices:

$$M(\Gamma_1, \Gamma_2) := \begin{pmatrix} \alpha_1^{d-s-1} & \cdots & \alpha_1 & 1 & 0 \\ \vdots & & \vdots & \vdots & \vdots \\ \alpha_m^{d-s-1} & \cdots & \alpha_m & 1 & 0 \\ \beta_1^{d-s-1} & \cdots & \beta_1 & 0 & 1 \\ \vdots & & \vdots & \vdots & \vdots \\ \beta_n^{d-s-1} & \cdots & \beta_n & 0 & 1 \end{pmatrix}, \quad f_{\boldsymbol{a}}(\Gamma_1, \Gamma_2) := \begin{pmatrix} -f_{\boldsymbol{a}}(\alpha_1) \\ \vdots \\ -f_{\boldsymbol{a}}(\alpha_m) \\ -f_{\boldsymbol{a}}(\beta_1) \\ \vdots \\ -f_{\boldsymbol{a}}(\beta_n) \end{pmatrix}.$$

It follows that $(\boldsymbol{b}, b_{0,1}, b_{0,2}) \in \mathcal{S}^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2}$ if and only if $(\boldsymbol{b}, b_{0,1}, b_{0,2})$ is a solution of (6.4).

For $m+n < d-s+1$, the rank of $M(\Gamma_1,\Gamma_2)$ is $m+n$, and the set $\mathcal{S}^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2}$ of solutions is a linear $\mathbb{F}_q$-variety of dimension $d-s+1-m-n$. From (6.4) we conclude that

$$|\mathcal{S}^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2}| = q^{d-s+1-m-n}.$$

This implies

$$\sum_{\substack{(\boldsymbol{b},b_{0,1},b_{0,2})\in\mathbb{F}_q^{d-s+1}\\ b_{0,1}\neq b_{0,2}}} \mathbf{1}_{\{\mathcal{N}>0\}^2}(f_{\boldsymbol{b}_1}, f_{\boldsymbol{b}_2}) = \sum_{\substack{1\le m,\, n\le d\\ 2\le m+n\le d-s}} (-1)^{m+n} q^{d-s+1-m-n}\binom{q}{m}\binom{q}{n}$$
$$+ \sum_{\substack{1\le m\,,n\le d\\ d-s+1\le m+n\le 2d}} (-1)^{m+n} \sum_{\substack{\Gamma_1,\,\Gamma_2\subseteq\mathbb{F}_q\\ |\Gamma_1|=m,\,|\Gamma_2|=n\\ \Gamma_1\cap\Gamma_2=\emptyset}} |\mathcal{S}^{\boldsymbol{a}}_{\Gamma_1,\Gamma_2}|.$$

Combining this with (6.3) yields the statement of the theorem. ■

Fix s, d and $\boldsymbol{a}$ as in the statement of Theorem 6.1. According to Theorem 6.1, to determine the behavior of $\mathcal{V}_2(d,s,\boldsymbol{a})$ we have to estimate

$$\mathcal{S}^{\boldsymbol{a}}_{m,n} := \sum_{\substack{\Gamma_1,\,\Gamma_2\subset\mathbb{F}_q\\ |\Gamma_1|=m,\,|\Gamma_2|=n}} |\mathcal{S}^{\boldsymbol{a}}_{\Gamma_1,\,\Gamma_2}| \tag{6.5}$$

for each pair (m,n) with $1\le m,n\le d$ and $d-s+1\le m+n\le 2d$.

7. A geometric approach to estimating $\mathcal{S}^{\boldsymbol{a}}_{m,n}$. Fix m and n with $1\le m,n\le d$ and $d-s+1\le m+n\le 2d$. To estimate $\mathcal{S}^{\boldsymbol{a}}_{m,n}$, we introduce new indeterminates $T, T_1,\dots,T_m$, $U, U_1,\dots,U_n$, $B, B_{d-s-1},\dots,B_1$, $B_{0,1}$, $B_{0,2}$ over $\overline{\mathbb{F}}_q$ and denote $\boldsymbol{T} := (T_1,\dots,T_m)$, $\boldsymbol{U} := (U_1,\dots,U_n)$, $\boldsymbol{B} := (B_{d-s-1},\dots,B_1)$, $\boldsymbol{B}_1 := (\boldsymbol{B}, B_{0,1})$ and $\boldsymbol{B}_2 := (\boldsymbol{B}, B_{0,2})$. Furthermore, we consider the polynomial $F\in\mathbb{F}_q[\boldsymbol{B},B,T]$ defined as follows:

$$F := T^d + \sum_{i=d-s}^{d-1} a_i T_j^i + \sum_{i=1}^{d-s-1} B_i T^i + B. \tag{7.1}$$

If $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{F}_q^{d-s+1+m+n}$, then we have $F(\boldsymbol{b}, b_{0,1}, \alpha_j) = f_{\boldsymbol{b}_1}(\alpha_j)$ and $F(\boldsymbol{b}, b_{0,2}, \beta_k) = f_{\boldsymbol{b}_2}(\beta_k)$ for $1\le j\le m$ and $1\le k\le n$. Let $\Gamma_{m,n}\subset\mathbb{A}^{d-s+1+m+n}$ be the affine quasi-$\mathbb{F}_q$-variety defined as

$$\Gamma_{m,n} := \{(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{A}^{d-s+1+m+n} : F(\boldsymbol{b}, b_{0,1}, \alpha_j) = 0\ (1\le j\le m),$$
$$\alpha_i\neq\alpha_j\ (i\neq j),\ F(\boldsymbol{b}, b_{0,2}, \beta_k) = 0\ (1\le k\le n),\ \beta_i\neq\beta_j\ (i\neq j),\ b_{0,1}\neq b_{0,2}\}.$$

Similarly to Lemma 3.2, we have the following result.

LEMMA 7.1. *Let m and n be integers with $1 \leq m, n \leq d$ and $d-s+1 \leq m+n \leq 2d$. Then*

$$\frac{|\mathit{\Gamma}_{m,n}(\mathbb{F}_q)|}{m!n!} = \mathcal{S}^{\boldsymbol{a}}_{m,n}.$$

Proof. Let $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathit{\Gamma}_{m,n}(\mathbb{F}_q)$ and let

$$\sigma : \{1, \ldots, m\} \to \{1, \ldots, m\} \quad \text{and} \quad \tau : \{1, \ldots, n\} \to \{1, \ldots, n\}$$

be any permutations. Let $\sigma(\boldsymbol{\alpha})$ and $\tau(\boldsymbol{\beta})$ be the images of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ under the linear mappings induced by these permutations. Then it is clear that $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \sigma(\boldsymbol{\alpha}), \tau(\boldsymbol{\beta})) \in \mathit{\Gamma}_{m,n}(\mathbb{F}_q)$. Furthermore, $\sigma(\boldsymbol{\alpha}) = \boldsymbol{\alpha}$ if and only if σ is the identity permutation, and similarly for $\tau(\boldsymbol{\beta})$. This shows that the product $\mathbb{S}_m \times \mathbb{S}_n$ of symmetric groups acts on $\mathit{\Gamma}_{m,n}(\mathbb{F}_q)$ and each orbit of this action has $m!n!$ elements.

The orbit of an arbitrary point $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ uniquely determines polynomials $f_{\boldsymbol{b}_1}$ and $f_{\boldsymbol{b}_2}$ and sets $\mathit{\Gamma}_1 := \{\alpha_1, \ldots, \alpha_m\} \subset \mathbb{F}_q$ and $\mathit{\Gamma}_2 := \{\beta_1, \ldots, \beta_n\} \subset \mathbb{F}_q$ with $|\mathit{\Gamma}_1| = m$ and $|\mathit{\Gamma}_2| = n$ such that $f_{\boldsymbol{b}_1}|_{\mathit{\Gamma}_1} \equiv 0$ and $f_{\boldsymbol{b}_2}|_{\mathit{\Gamma}_2} \equiv 0$. Therefore, each orbit uniquely determines sets $\mathit{\Gamma}_1, \mathit{\Gamma}_2 \subset \mathbb{F}_q$ with $|\mathit{\Gamma}_1| = m$ and $|\mathit{\Gamma}_2| = n$ and an element of $S^{\boldsymbol{a}}_{\mathit{\Gamma}_1, \mathit{\Gamma}_2}$. Conversely, to each element of $S^{\boldsymbol{a}}_{\mathit{\Gamma}_1, \mathit{\Gamma}_2}$ there corresponds a unique orbit of $\mathit{\Gamma}_{m,n}(\mathbb{F}_q)$. This implies that

$$\text{number of orbits of } \mathit{\Gamma}_{m,n}(\mathbb{F}_q) = \sum_{\substack{\mathit{\Gamma}_1,\, \mathit{\Gamma}_2 \subset \mathbb{F}_q \\ |\mathit{\Gamma}_1| = m,\, |\mathit{\Gamma}_2| = n}} |S^{\boldsymbol{a}}_{\mathit{\Gamma}_1, \mathit{\Gamma}_2}|,$$

finishing the proof. ∎

To estimate $|\mathit{\Gamma}_{m,n}(\mathbb{F}_q)|$ we shall consider the Zariski closure $\mathrm{cl}(\mathit{\Gamma}_{m,n})$ in $\mathbb{A}^{d-s+1+m+n}$. Our aim is to provide explicit equations defining $\mathrm{cl}(\mathit{\Gamma}_{m,n})$. Let $\mathit{\Gamma}^*_{m,n} \subset \mathbb{A}^{d-s+1+m+n}$ be the affine $\mathbb{F}_q$-variety defined as

$$\begin{aligned} \mathit{\Gamma}^*_{m,n} := \{(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{A}^{d-s+1+m+n} : \mathit{\Delta}^{i-1} F(\boldsymbol{b}, b_{0,1}, \alpha_1, \ldots, \alpha_i) = 0 \\ (1 \leq i \leq m),\ \mathit{\Delta}^{j-1} F(\boldsymbol{b}, b_{0,2}, \beta_1, \ldots, \beta_j) = 0\ (1 \leq j \leq n)\}, \end{aligned}$$

where $\mathit{\Delta}^{i-1} F(\boldsymbol{b}, b_{0,1}, T_1, \ldots, T_i)$ and $\mathit{\Delta}^{j-1} F(\boldsymbol{b}, b_{0,2}, U_1, \ldots, U_j)$ denote the corresponding divided differences of $F(\boldsymbol{b}, b_{0,1}, T) \in \overline{\mathbb{F}}_q[T]$ and $F(\boldsymbol{b}, b_{0,2}, U) \in \overline{\mathbb{F}}_q[U]$ respectively. The following relation between the varieties $\mathit{\Gamma}_{m,n}$ and $\mathit{\Gamma}^*_{m,n}$ is an easy consequence of Lemma 3.3.

LEMMA 7.2. *With the notations above,*

$$\mathit{\Gamma}_{m,n} = \mathit{\Gamma}^*_{m,n} \cap \{\alpha_i \neq \alpha_j\ (1 \leq i < j \leq m),\ \beta_i \neq \beta_j\ (1 \leq i < j \leq n),\ b_{0,1} \neq b_{0,2}\}. \tag{7.2}$$

8. Geometry of $\mathit{\Gamma}^*_{m,n}$. Let $1 \leq m, n \leq d$ and $d-s+1 \leq m+n \leq 2d$. In this section we obtain critical information on the geometry of $\mathit{\Gamma}^*_{m,n}$, from which we conclude that $\mathit{\Gamma}^*_{m,n}$ is the Zariski closure of $\mathit{\Gamma}_{m,n}$.

Several arguments in this section are similar to those of Section 4. Therefore, to avoid repetition, some proofs will only be sketched.

LEMMA 8.1. *The variety $\Gamma^*_{m,n}$ is a set-theoretic complete intersection of dimension $d-s+1$.*

Proof. Consider the graded lexicographic order of $\overline{\mathbb{F}}_q[\boldsymbol{B}, B_{0,1}, B_{0,2}, \boldsymbol{T}, \boldsymbol{U}]$ with $U_n > \cdots > U_1 > T_m > \cdots > T_1 > B_{d-s-1} > \cdots > B_{0,1} > B_{0,2}$. Arguing as in Lemma 4.1 it is easy to see that the leading terms of $\Delta^{i-1}F(\boldsymbol{B}_1, T_1, \ldots, T_i)$ and $\Delta^{j-1}F(\boldsymbol{B}_2, U_1, \ldots, U_j)$ are T_i^{d-i+1} and U_j^{d-j+1} respectively. This shows that $\Delta^{i-1}F(\boldsymbol{B}_1, T_1, \ldots, T_i)$ $(1 \le i \le m)$ and $\Delta^{j-1}F(\boldsymbol{B}_2, U_1, \ldots, U_j)$ $(1 \le j \le n)$ form a Gröbner basis of the ideal $\mathcal{J}_{m,n}$ they generate (see, e.g., [CLO92, §2.9, Proposition 4]). Furthermore, since the leading terms of $\Delta^{i-1}F(\boldsymbol{B}_1, T_1, \ldots, T_i)$ $(1 \le i \le m)$ and $\Delta^{j-1}F(\boldsymbol{B}_2, U_1, \ldots, U_j)$ $(1 \le j \le n)$ form a regular sequence in $\overline{\mathbb{F}}_q[\boldsymbol{B}, B_{0,1}, B_{0,2}, \boldsymbol{T}, \boldsymbol{U}]$, by [Eis95, Proposition 15.15] we conclude that $\Delta^{i-1}F(\boldsymbol{B}_1, T_1, \ldots, T_i)$ $(1 \le i \le m)$ and $\Delta^{j-1}F(\boldsymbol{B}_2, U_1, \ldots, U_j)$ $(1 \le j \le n)$ also form a regular sequence. Then $\Gamma^*_{m,n}$ is a set-theoretic complete intersection of dimension $d-s+1$. ■

8.1. The singular locus of $\Gamma^*_{m,n}$. The aim of this section is to prove that the singular locus of $\Gamma^*_{m,n}$ has codimension at least 2 in $\Gamma^*_{m,n}$.

Arguing as in the proof of Lemma 4.2 it is easy to see that the polynomials $F(\boldsymbol{B}_1, T_i)$ $(1 \le i \le m)$ and $F(\boldsymbol{B}_2, U_j)$ $(1 \le j \le n)$ vanish on $\Gamma^*_{m,n}$. Hence, we have the following criterion of nonsingularity.

REMARK 8.2. Let $J_{F_{1,2}}$ be the Jacobian matrix of the polynomials $F(\boldsymbol{B}_1, T_i)$ $(1 \le i \le m)$ and $F(\boldsymbol{B}_2, U_j)$ $(1 \le j \le n)$ with respect to $\boldsymbol{B}, B_{0,1}, B_{0,2}, \boldsymbol{T}, \boldsymbol{U}$. If the point $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \in \Gamma^*_{m,n}$ is such that $\operatorname{rank} J_{F_{1,2}}(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) = m+n$, then it is nonsingular.

Let $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \in \Gamma^*_{m,n}$, and denote $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_m)$ and $\boldsymbol{\beta} := (\beta_1, \ldots, \beta_n)$. Set $\boldsymbol{b}_1 := (\boldsymbol{b}, b_{0,1})$ and $\boldsymbol{b}_2 := (\boldsymbol{b}, b_{0,2})$. Then the Jacobian matrix $J_{F_{1,2}}(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ has the expression

(8.1)
$$J_{F_{1,2}}(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \begin{pmatrix} \alpha_1^{d-s-1} & \cdots & \alpha_1 & 1 & 0 & \gamma_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ \alpha_m^{d-s-1} & \cdots & \alpha_m & 1 & 0 & 0 & \cdots & \gamma_m & 0 & \cdots & 0 \\ \beta_1^{d-s-1} & \cdots & \beta_1 & 0 & 1 & 0 & \cdots & 0 & \eta_1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots \\ \beta_n^{d-s-1} & \cdots & \beta_n & 0 & 1 & 0 & \cdots & 0 & 0 & \cdots & \eta_n \end{pmatrix},$$

where $\gamma_i := f'_{\boldsymbol{b}}(\alpha_i)$ and $\eta_j := f'_{\boldsymbol{b}}(\beta_j)$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. Therefore, from Remark 8.2 we immediately deduce the following remark.

Remark 8.3. If there exist at most one α_i and at most one β_j which are multiple roots of $f_{\boldsymbol{b}_1}$ and $f_{\boldsymbol{b}_2}$ respectively, then $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ is a nonsingular point of $\Gamma^*_{m,n}$.

Consider the following morphism of $\mathbb{F}_q$-varieties:

$$\Psi_{m,n} : \Gamma^*_{m,n} \to \mathbb{A}^{d-s+1}, \qquad (\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \mapsto (\boldsymbol{b}, b_{0,1}, b_{0,2}). \tag{8.2}$$

As in the proof of Lemma 4.3, we easily deduce that $\Psi_{m,n}$ is a finite morphism.

Let $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ be a singular point of $\Gamma^*_{m,n}$. According to Remark 8.3, either $f_{\boldsymbol{b}_1}$ or $f_{\boldsymbol{b}_2}$ has multiple roots. We now observe that we may assume without loss of generality that $f'_{\boldsymbol{b}} \neq 0$ and $\Delta^2 F(\boldsymbol{b}_1, T, T, T) \neq 0$. More precisely, from the proofs of Lemmas 4.3 and 4.7 we deduce the following remark.

Remark 8.4. If $d - s \geq 3$, then the set $\mathcal{W}'_1$ of points $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ of $\Gamma^*_{m,n}$ such that $f'_{\boldsymbol{b}} = 0$ or $\Delta^2 F(\boldsymbol{b}_1, T, T, T) = 0$ is contained in a subvariety of $\Gamma^*_{m,n}$ of codimension 2.

Next we study the set of singular points of $\Gamma^*_{m,n}$ for which $f'_{\boldsymbol{b}} \neq 0$. We first consider the case where $f_{\boldsymbol{b}_1}$ and $f_{\boldsymbol{b}_2}$ have multiple roots in $\overline{\mathbb{F}}_q$.

Lemma 8.5. *Let $\mathcal{W}' \subset \Gamma^*_{m,n}$ be the set of points $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ such that $f'_{\boldsymbol{b}} \neq 0$ and $f_{\boldsymbol{b}_1}$ and $f_{\boldsymbol{b}_2}$ have multiple roots in $\overline{\mathbb{F}}_q$. Then $\mathcal{W}'$ is contained in a codimension-2 subvariety of $\Gamma^*_{m,n}$.*

Proof. Let $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathcal{W}'$. Then $\mathrm{Res}(f_{\boldsymbol{b}_1}, f'_{\boldsymbol{b}_1}) = \mathrm{Res}(f_{\boldsymbol{b}_2}, f'_{\boldsymbol{b}_2}) = 0$, where Res denotes resultant. Since $f_{\boldsymbol{b}_1}$ and $f_{\boldsymbol{b}_2}$ have degree d and $f'_{\boldsymbol{b}_1}$ and $f'_{\boldsymbol{b}_2}$ are nonzero polynomials, it follows that

$$\mathrm{Res}(f_{\boldsymbol{b}_1}, f'_{\boldsymbol{b}_1}) = \mathrm{Res}\big(F(\boldsymbol{B}_1, T_1), \Delta^1 F(\boldsymbol{B}_1, T_1, T_1), T_1\big)\big|_{\boldsymbol{B}_1 = \boldsymbol{b}_1},$$
$$\mathrm{Res}(f_{\boldsymbol{b}_2}, f'_{\boldsymbol{b}_2}) = \mathrm{Res}\big(F(\boldsymbol{B}_2, U_1), \Delta^1 F(\boldsymbol{B}_2, U_1, U_1), U_1\big)\big|_{\boldsymbol{B}_2 = \boldsymbol{b}_2}.$$

Here $\mathcal{R}_1 := \mathrm{Res}(F(\boldsymbol{B}_1, T_1), \Delta^1 F(\boldsymbol{B}_1, T_1, T_1), T_1)$ is the resultant of the polynomials $F(\boldsymbol{B}_1, T_1)$ and $\Delta^1 F(\boldsymbol{B}_1, T_1, T_1)$ with respect to T_1, and $\mathcal{R}_2 := \mathrm{Res}(F(\boldsymbol{B}_2, U_1), \Delta^1 F(\boldsymbol{B}_2, U_1, U_1), U_1)$ is the resultant of $F(\boldsymbol{B}_2, U_1)$ and $\Delta^1 F(\boldsymbol{B}_2, U_1, U_1)$ with respect to U_1. Then $\mathcal{W}' \subset \Psi^{-1}_{m,n}(\mathcal{Z})$, where $\Psi_{m,n}$ is the morphism (8.2) and $\mathcal{Z}$ is the subvariety of $\mathbb{A}^{d-s+1}$ defined by

$$\mathcal{R}_1(\boldsymbol{B}_1) = 0, \qquad \mathcal{R}_2(\boldsymbol{B}_2) = 0.$$

Since $F(\boldsymbol{B}_1, T_1)$ is a separable element of $\mathbb{F}_q[\boldsymbol{B}_1][T_1]$, the resultant $\mathcal{R}_1$ is nonzero element of $\mathbb{F}_q[\boldsymbol{B}_1]$. Furthermore, from, e.g., [FS84, §1], one deduces that $\mathcal{R}_1 \in \mathbb{F}_q[\boldsymbol{B}][B_{0,1}] \setminus \mathbb{F}_q[\boldsymbol{B}]$. Analogously, $\mathcal{R}_2$ is a nonconstant polynomial of $\mathbb{F}_q[\boldsymbol{B}][B_{0,2}]$. According to Theorem A.3 (see Appendix), $\mathcal{R}_1$ is an irreducible element of $\mathbb{F}_q[\boldsymbol{B}][B_{0,1},B_{0,2}]$ and $\mathcal{R}_2 \in \mathbb{F}_q[\boldsymbol{B}][B_{0,1},B_{0,2}]$ is not a multiple of $\mathcal{R}_1(\boldsymbol{B}_1)$ in $\mathbb{F}_q[\boldsymbol{B}][B_{0,1},B_{0,2}]$. This implies that $\mathcal{R}_1(\boldsymbol{B}_1)$ and $\mathcal{R}_2(\boldsymbol{B}_2)$ form a regular sequence in $\overline{\mathbb{F}}_q[\boldsymbol{B},B_{0,1},B_{0,2}]$. It follows that $\mathcal{Z}$ has dimension $d-s-1$, and hence $\dim \Psi_{m,n}^{-1}(\mathcal{Z}) = d-s-1$. This finishes the proof. ■

According to Lemma 8.5, it remains to analyze the set of singular points $(\boldsymbol{b},b_{0,1},b_{0,2},\boldsymbol{\alpha},\boldsymbol{\beta})$ of $\Gamma_{m,n}^*$ for which either $f_{\boldsymbol{b}_1}$ or $f_{\boldsymbol{b}_2}$ has only simple roots in $\overline{\mathbb{F}}_q$. In what follows we shall assume that the latter holds. By Remark 8.3 there must be at least two distinct coordinates of $\boldsymbol{\alpha}$ which are multiple roots of $f_{\boldsymbol{b}_1}$.

Suppose first that there exist two coordinates of $\boldsymbol{\alpha}$ which are distinct multiple roots of $f_{\boldsymbol{b}_1}$. Arguing as in Lemma 4.5 we easily deduce the following remark.

Remark 8.6. Let $\mathcal{W}_2'$ denote the set of points $(\boldsymbol{b},b_{0,1},b_{0,2},\boldsymbol{\alpha},\boldsymbol{\beta}) \in \Gamma_{m,n}^*$ for which:

- $f_{\boldsymbol{b}_2}$ has only simple roots in $\overline{\mathbb{F}}_q$,
- there exist $1 \le i < j \le m$ such that $\alpha_i \neq \alpha_j$ and α_i,α_j are multiple roots of $f_{\boldsymbol{b}_1}$.

Then $\mathcal{W}_2'$ is contained in a subvariety of codimension 2 of $\Gamma_{m,n}^*$.

Next we consider the points of $\Gamma_{m,n}^*$ for which there exist exactly two distinct coordinates of $\boldsymbol{\alpha}$ whose common value is a multiple root of $f_{\boldsymbol{b}_1}$. Arguing as in Lemma 4.6 we obtain the following remark.

Remark 8.7. Let $(\boldsymbol{b},b_{0,1},b_{0,2},\boldsymbol{\alpha},\boldsymbol{\beta}) \in \Gamma_{m,n}^*$ satisfy:

- $f_{\boldsymbol{b}_2}$ has only simple roots in $\overline{\mathbb{F}}_q$,
- there exist $1 \le i < j \le m$ such that $\alpha_i = \alpha_j$ and α_i is a multiple root of $f_{\boldsymbol{b}_1}$,
- for any $k \notin \{i,j\}$, α_k is a simple root of $f_{\boldsymbol{b}_1}$.

Then $(\boldsymbol{b},b_{0,1},b_{0,2},\boldsymbol{\alpha},\boldsymbol{\beta})$ is a regular point of $\Gamma_{m,n}^*$.

Finally, we analyze the set of points of $\Gamma_{m,n}^*$ such that there exist three distinct coordinates of $\boldsymbol{\alpha}$ with value the same multiple root of $f_{\boldsymbol{b}_1}$. By Lemma 4.7 we deduce the following remark.

Remark 8.8. Let $\mathcal{W}_3'$ be the set of points $(\boldsymbol{b},b_{0,1},b_{0,2},\boldsymbol{\alpha},\boldsymbol{\beta}) \in \Gamma_{m,n}^*$ for which $f_{\boldsymbol{b}_2}$ has only simple roots in $\overline{\mathbb{F}}_q$ and there exist $1 \le i < j < k \le m$ such that $\alpha_i = \alpha_j = \alpha_k$ and α_i is a multiple root of $f_{\boldsymbol{b}_1}$. If $d-s \ge 3$, then $\mathcal{W}_3'$ is contained in a codimension-2 subvariety of $\Gamma_{m,n}^*$.

Now we are able to obtain our lower bound on the codimension of the singular locus of $\Gamma_{m,n}^*$. Remarks 8.3, 8.4, 8.6, 8.7 and 8.8 and Lemma 8.5 show that the set of singular points of $\Gamma_{m,n}^*$ is contained in the union of $\mathcal{W}_1'$, $\mathcal{W}'$, $\mathcal{W}_2'$ and $\mathcal{W}_3'$ defined in the remarks and the lemma. Since that union is contained in a codimension-2 subvariety of $\varGamma_{m,n}^*$, we obtain the following result.

THEOREM 8.9. *Let $p > 2$ and $q > d$. If $d-s \geq 3$, then the singular locus of $\varGamma_{m,n}^*$ has codimension at least 2 in $\varGamma_{m,n}^*$.*

We finish this section with a consequence of the analysis underlying the proof of Theorem 8.9. As the proof of this result is similar to that of Corollary 4.9, it will only be sketched.

COROLLARY 8.10. *Under the assumptions of Theorem 8.9, the ideal $\mathcal{J}_{m,n} \subset \mathbb{F}_q[\boldsymbol{B}, B_{0,1}, B_{0,2}, \boldsymbol{T}, \boldsymbol{U}]$ generated by $\varDelta^{i-1}F(\boldsymbol{B}_1, T_1, \dots, T_i)$ $(1 \leq i \leq m)$ and $\varDelta^{j-1}F(\boldsymbol{B}_2, U_1, \dots, U_j)$ $(1 \leq j \leq n)$ is radical.*

Proof. By Lemma 8.1, the polynomials $\varDelta^{i-1}F(\boldsymbol{B}_1, T_1, \dots, T_i)$ $(1 \leq i \leq m)$ and $\varDelta^{j-1}F(\boldsymbol{B}_2, U_1, \dots, U_j)$ $(1 \leq j \leq n)$ form a regular sequence. Let $J_{\varDelta_{1,2}}$ be their Jacobian matrix with respect to $\boldsymbol{B}, B_{0,1}, B_{0,2}, \boldsymbol{T}, \boldsymbol{U}$. We claim that the set of points $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \in \varGamma_{m,n}^*$ for which $J_{\varDelta_{1,2}}(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ does not have full rank has codimension at least 1 in $\varGamma_{m,n}^*$. Indeed, if $J_{\varDelta_{1,2}}(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ does not have full rank, then neither does the matrix $J_{F_{1,2}}(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ of (8.1). On the other hand, the latter implies that $f_{\boldsymbol{b}_1}$ or $f_{\boldsymbol{b}_2}$ has multiple roots in $\overline{\mathbb{F}}_q$. Therefore, by the arguments of the proofs of Remark 8.4 and Lemma 8.5 we deduce the claim. By [Eis95, Theorem 18.15], the statement of the corollary follows. ∎

8.2. The geometry of the projective closure of $\varGamma_{m,n}^*$. Similarly to Section 4.2, in this section we discuss the behavior of $\varGamma_{m,n}^*$ at infinity. For this purpose, we shall consider the projective closure $\mathrm{pcl}(\varGamma_{m,n}^*) \subset \mathbb{P}^{d-s+1+m+n}$, and the set of point of $\mathrm{pcl}(\varGamma_{m,n}^*)$ at infinity, i.e., lying in the hyperplane $\{T_0 = 0\}$.

Let $\mathcal{J}_{m,n}^h \subset \mathbb{F}_q[\boldsymbol{B}, B_{0,1}, B_{0,2}, T_0, \boldsymbol{T}, \boldsymbol{U}]$ be the ideal generated by the homogenizations F^h of all $F \in \mathcal{J}_{m,n}$.

LEMMA 8.11. *Under the assumptions of Theorem 8.9, the homogenized polynomials $\varDelta^{i-1}F(\boldsymbol{B}_1, T_1, \dots, T_i)^h$ $(1 \leq i \leq m)$ and $\varDelta^{j-1}F(\boldsymbol{B}_2, U_1, \dots, U_j)^h$ $(1 \leq j \leq n)$ generate the ideal $\mathcal{J}_{m,n}^h$. Furthermore, $\mathrm{pcl}(\varGamma_{m,n}^*)$ is an ideal-theoretic complete intersection of dimension $d-s+1$ and degree $(d!)^2/((d-m)!(d-n)!)$.*

Proof. The proof repeats *mutatis mutandis* the proof of Lemma 4.10, considering the graded lexicographical order of $\mathbb{F}_q[\boldsymbol{B}, B_{0,1}, B_{0,2}, \boldsymbol{T}, \boldsymbol{U}]$ defined by $U_n > \dots > U_1 > T_m > \dots > T_1 > B_{d-s-1} > \dots > B_1 > B_{0,1} > B_{0,2}$. ∎

Similarly to Lemma 4.11, the set of points of $\mathrm{pcl}(\varGamma_{m,n}^*)$ at infinity is a linear variety. We shall skip the proof of this result, because it is similar to that of Lemma 4.11.

Lemma 8.12. *$\mathrm{pcl}(\Gamma^*_{m,n}) \cap \{T_0 = 0\} \subset \mathbb{P}^{d-s+m+n}$ is a linear $\mathbb{F}_q$-variety of dimension $d - s$.*

Combining Theorem 8.9 and Lemmas 8.11 and 8.12, as in the proof of Theorem 4.12, we obtain the main result of this section.

Theorem 8.13. *Under the assumptions of Theorem 8.9, the projective variety $\mathrm{pcl}(\Gamma^*_{m,n}) \subset \mathbb{P}^{d-s+1+m+n}$ is a normal absolutely irreducible ideal-theoretic complete intersection defined over $\mathbb{F}_q$ of dimension $d - s + 1$ and degree $(d!)^2/((d-m)!(d-n)!)$.*

We deduce that $\Gamma^*_{m,n} \subset \mathbb{A}^{d-s+1+m+n}$ is an absolutely irreducible ideal-theoretic complete intersection of dimension $d - s + 1$ and degree $(d!)^2/((d-m)!(d-n)!)$. Lemma 7.2 shows that $\Gamma_{m,n}$ coincides with the subset of points of $\Gamma^*_{m,n}$ with $b_{0,1} \neq b_{0,2}$, $\alpha_i \neq \alpha_j$ and $\beta_k \neq \beta_l$. Hence, by the absolute irreducibility of $\Gamma^*_{m,n}$ we deduce that $\mathrm{cl}(\Gamma_{m,n}) = \Gamma^*_{m,n}$.

9. The asymptotic behavior of $\mathcal{V}_2(d, s, \boldsymbol{a})$.

As before, let $p > 2$ and let d and s be positive integers such that $q > d$ and $d - s \geq 3$. As mentioned before, our objective is to determine the asymptotic behavior of the quantity $\mathcal{V}_2(d, s, \boldsymbol{a})$ of (6.1) for a given $\boldsymbol{a} := (a_{d-1}, \ldots, a_{d-s}) \in \mathbb{F}_q^s$. According to Theorem 6.1, this behavior is determined by that of the number $\mathcal{S}^{\boldsymbol{a}}_{m,n}$ defined in (6.5) for all pairs (m, n) with $1 \leq m, n \leq d$ and $d - s + 1 \leq m + n \leq 2d$.

9.1. An estimate for $\mathcal{S}^{\boldsymbol{a}}_{m,n}$.

Lemma 7.1 expresses $\mathcal{S}^{\boldsymbol{a}}_{m,n}$ in terms of the number $|\Gamma_{m,n}(\mathbb{F}_q)|$ of q-rational points of the affine quasi-$\mathbb{F}_q$-variety $\Gamma_{m,n}$. Therefore, we estimate $|\Gamma_{m,n}(\mathbb{F}_q)|$ for each pair (m, n) as above.

Lemma 7.2 relates $|\Gamma_{m,n}(\mathbb{F}_q)|$ to the number $|\Gamma^*_{m,n}(\mathbb{F}_q)|$ of q-rational points of the affine $\mathbb{F}_q$-variety $\Gamma^*_{m,n}$. We shall express the latter in terms of the number of q-rational points of the projective closure $\mathrm{pcl}(\Gamma^*_{m,n})$ and its set $\mathrm{pcl}(\Gamma^*_{m,n})^\infty := \mathrm{pcl}(\Gamma^*_{m,n}) \cap \{T_0 = 0\}$ of points at infinity.

Theorem 8.13 shows that $\mathrm{pcl}(\Gamma^*_{m,n})$ is a normal ideal-theoretic complete intersection of dimension $d - s + 1$ defined over $\mathbb{F}_q$, and thus (5.1) yields

$$\big||\mathrm{pcl}(\Gamma^*_{m,n})(\mathbb{F}_q)| - p_{d-s+1}\big| \leq \big(\delta_{m,n}(D_{m,n} - 2) + 2\big)q^{d-s+1/2} + 14D^2_{m,n}\delta^2_{m,n}q^{d-s},$$

where $D_{m,n} := \sum_{i=1}^m (d-i) + \sum_{j=1}^n (d-j) = (m+n)d - (m(m+1) + n(n+1))/2$ and $\delta_{m,n} := (d!)^2/((d-m)!(d-n)!)$. On the other hand, Lemma 8.12 proves that $\mathrm{pcl}(\Gamma^*_{m,n})^\infty$ is a linear $\mathbb{F}_q$-variety of dimension $d - s$. Thus we obtain

$$\begin{aligned} \big||\Gamma^*_{m,n}(\mathbb{F}_q)| - q^{d-s+1}\big| &= \big||\mathrm{pcl}(\Gamma^*_{m,n})| - |\mathrm{pcl}(\Gamma^*_{m,n})^\infty| - p_{d-s+1} + p_{d-s}\big| \\ &\leq (\delta_{m,n}(D_{m,n} - 2) + 2)q^{d-s+1/2} + 14D^2_{m,n}\delta^2_{m,n}q^{d-s}. \end{aligned} \tag{9.1}$$

Next we estimate $|\Gamma_{m,n}(\mathbb{F}_q)|$. To this end, according to Lemma 7.2 we obtain an upper bound on the number of q-rational points $(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta})$

of $\mathit{\Gamma}^*_{m,n}$ such that either $b_{0,1} = b_{0,2}$, or there exist $1 \le i < j \le m$ with $\alpha_i = \alpha_j$, or there exist $1 \le k < l \le n$ with $\beta_k = \beta_l$. This subset of $\mathit{\Gamma}^*_{m,n}$ is the following $\mathbb{F}_q$-variety:

$$\mathit{\Gamma}^{*,=}_{m,n} := \mathit{\Gamma}^*_{m,n} \cap \Big(\{B_{0,1} = B_{0,2}\} \cup \bigcup_{1\le i<j\le m} \{T_i = T_j\} \cup \bigcup_{1\le k<l\le n} \{U_k = U_l\}\Big).$$

Observe that $\mathit{\Gamma}^{*,=}_{m,n} = \mathit{\Gamma}^*_{m,n} \cap \mathcal{H}_{m,n}$, where $\mathcal{H}_{m,n} \subset \mathbb{A}^{d-s+1+m+n}$ is the hypersurface defined by the polynomial

$$F := (B_{0,1} - B_{0,2}) \prod_{1\le i<j\le m} (T_i - T_j) \prod_{1\le k<l\le n} (U_k - U_l).$$

By the Bézout inequality (2.1) we have

$$\deg \mathit{\Gamma}^{*,=}_{m,n} \le \delta_{m,n}\bigg(\binom{m}{2} + \binom{n}{2} + 1\bigg), \tag{9.2}$$

The set $\mathit{\Gamma}^*_{m,n} \cap \{B_{0,1} = B_{0,2}\}$ is contained in the codimension-1 subvariety of $\mathit{\Gamma}^*_{m,n}$ given by $\mathit{\Psi}^{-1}_{m,n}(\{B_{0,1} = B_{0,2}\})$. Furthermore, if $\alpha_i = \alpha_j$ for $1 \le i < j \le m$, then α_i is a multiple root of $f_{\boldsymbol{b}_1}$, and similarly for $f_{\boldsymbol{b}_2}$ if $\beta_k = \beta_l$ for $1 \le k < l \le m$. Then, by Remark 8.4 and Lemma 8.5, $\mathit{\Gamma}^{*,=}_{m,n}$ has dimension at most $d - s$. Therefore, combining, e.g., [CM06, Lemma 2.1] with (9.2) we obtain

$$\big|\mathit{\Gamma}^{*,=}_{m,n}(\mathbb{F}_q)\big| \le \delta_{m,n}\bigg(\binom{m}{2} + \binom{n}{2} + 1\bigg) q^{d-s}. \tag{9.3}$$

Since $\mathit{\Gamma}_{m,n}(\mathbb{F}_q) = (\mathit{\Gamma}^*_{m,n})(\mathbb{F}_q) \setminus (\mathit{\Gamma}^{*,=}_{m,n})(\mathbb{F}_q)$, from (9.1) and (9.3) we see that

$$\begin{aligned} \big||\mathit{\Gamma}_{m,n}(\mathbb{F}_q)| - q^{d-s+1}\big| &\le \big||\mathit{\Gamma}^*_{m,n}(\mathbb{F}_q)| - q^{d-s+1}\big| + |(\mathit{\Gamma}^{*,=}_{m,n})(\mathbb{F}_q)| \\ &\le (\delta_{m,n}(D_{m,n} - 2) + 2) q^{d-s+1/2} + (14 D^2_{m,n}\delta^2_{m,n} + \xi_{m,n}\delta_{m,n}) q^{d-s}, \end{aligned} \tag{9.4}$$

where $\xi_{m,n} := \binom{m}{2} + \binom{n}{2} + 1$.

Finally, by Lemma 7.1 and (9.4) we obtain the following result.

Theorem 9.1. *Let $p > 2$ and let d and s satisfy $q > d$ and $d - s \ge 3$. For each (m, n) with $1 \le m, n \le d$, and $d - s + 1 \le m + n \le 2d$, we have*

$$\begin{aligned} \bigg|\mathcal{S}^{\boldsymbol{a}}_{m,n} - \frac{q^{d-s+1}}{m!n!}\bigg| &\le \frac{1}{m!n!}\big(\delta_{m,n}(D_{m,n} - 2) + 2\big) q^{d-s+1/2} \\ &\quad + \frac{1}{m!n!}(14 D^2_{m,n}\delta^2_{m,n} + \xi_{m,n}\delta_{m,n}) q^{d-s}, \end{aligned}$$

where $\xi_{m,n} := \binom{m}{2} + \binom{n}{2} + 1$, $D_{m,n} := (m+n)d - \binom{m+1}{2} - \binom{n+1}{2}$ and $\delta_{m,n} := (d!)^2/((d-m)!(d-n)!)$.

9.2. The asymptotic behavior of $\mathcal{V}_2(d, s, \boldsymbol{a})$. Theorem 9.1 is the fundamental step towards the determination of the asymptotic behavior of

$\mathcal{V}_2(d,s,\boldsymbol{a})$. Indeed, by Theorem 6.1 we have

$$\begin{aligned}(9.5)\quad &\mathcal{V}_2(d,s,\boldsymbol{a})-\mu_d^2q^2\\ &\quad=\mathcal{V}(d,s,\boldsymbol{a})+\sum_{\substack{1\le m,n\le d\\ 2\le m+n\le d-s}}(-q)^{2-m-n}\bigg(\binom{q}{n}\binom{q}{m}-\frac{q^{m+n}}{m!n!}\bigg)\\ &\qquad+\frac{1}{q^{d-s-1}}\sum_{\substack{1\le m,n\le d\\ d-s+1\le m+n\le 2d}}(-1)^{m+n}\bigg(\mathcal{S}^{\boldsymbol{a}}_{m,n}-\frac{q^{d-s+1}}{m!n!}\bigg).\end{aligned}$$

From Corollary 5.2 it follows that

$$(9.6)\qquad \mathcal{V}(d,s,\boldsymbol{a})\le\mu_dq+d^22^{d-1}q^{1/2}+\frac{7}{2}d^4\sum_{k=0}^{s-1}\binom{d}{k}^2(d-k)!.$$

Next we obtain an upper bound for the absolute value $A_1(d,s)$ of the second term on the right-hand side of (9.5). Indeed, taking into account that

$$\binom{q}{n}\binom{q}{m}-\frac{q^{m+n}}{m!n!}=\binom{q}{m}\bigg(\binom{q}{n}-\frac{q^n}{n!}\bigg)+\frac{q^n}{n!}\bigg(\binom{q}{m}-\frac{q^m}{m!}\bigg),$$

we see that

$$\begin{aligned}A_1(d,s)\le&\bigg|\sum_{\substack{1\le m,n\le d\\ 2\le m+n\le d-s}}(-q)^{2-m-n}\binom{q}{m}\bigg(\binom{q}{n}-\frac{q^n}{n!}\bigg)\bigg|\\ &+\bigg|\sum_{\substack{1\le m,n\le d\\ 2\le m+n\le d-s}}\frac{(-1)^n}{n!}(-q)^{2-m}\bigg(\binom{q}{m}-\frac{q^m}{m!}\bigg)\bigg|.\end{aligned}$$

Arguing as in the proof of [C–P14, Corollary 14], we have

$$\bigg|\sum_{n=1}^{d-s-m}(-q)^{1-n}\bigg(\binom{q}{n}-\frac{q^n}{n!}\bigg)\bigg|\le\frac{1}{2e}+\frac{1}{2}+\frac{7}{q}\le d.$$

Therefore,

$$\begin{aligned}&\bigg|\sum_{\substack{1\le m,n\le d\\ 2\le m+n\le d-s}}(-q)^{1-m-n}\binom{q}{m}\bigg(\binom{q}{n}-\frac{q^n}{n!}\bigg)\bigg|\\ &\qquad\le d\sum_{m=1}^{d-s-1}\binom{q}{m}q^{-m}\le d\bigg(1+\frac{1}{q}\bigg)^q\le ed.\end{aligned}$$

On the other hand,

$$\bigg|\sum_{\substack{1\le m,n\le d\\ 2\le m+n\le d-s}}\frac{(-1)^n}{n!}(-q)^{1-m}\bigg(\binom{q}{m}-\frac{q^m}{m!}\bigg)\bigg|\le d\sum_{n=1}^{d-s-1}\frac{1}{n!}\le ed.$$

Combining the above two bounds we obtain $A_1(d,s)\le 2edq$.

Finally, we consider the absolute value $B_1(d,s)$ of the last term of (9.5). We have

$$\begin{aligned}(9.7)\qquad B_1(d,s) \le \sum_{m,n=1}^{d} &\frac{\delta_{m,n}(D_{m,n}-2)+2}{m!n!}q^{3/2}\\ &+14\sum_{m,n=1}^{d}\frac{D_{m,n}^2\delta_{m,n}^2}{m!n!}q+\sum_{m,n=1}^{d}\frac{\xi_{m,n}\delta_{m,n}}{m!n!}q.\end{aligned}$$

First we obtain an upper bound for the first term on the right-hand side:

$$\begin{aligned}(9.8)\qquad \sum_{m,n=1}^{d}\frac{\delta_{m,n}(D_{m,n}-2)+2}{m!n!} &\le 2\sum_{n=1}^{d}\binom{d}{n}\frac{n(2d-n-1)}{2}\sum_{m=1}^{d}\binom{d}{m}\\ &\le d^2 2^d(2^d-1).\end{aligned}$$

Next, since $D_{m,n}^2 \le (2d-1)^4/16$ for $1 \le m,n \le d$, we see that

$$\begin{aligned}(9.9)\qquad \sum_{m,n=1}^{d}\frac{D_{m,n}^2\delta_{m,n}^2}{m!n!} &\le \frac{1}{16}(2d-1)^4\Bigg(\sum_{n=1}^{d}\binom{d}{n}^2 n!\Bigg)^2\\ &\le \frac{1}{16}(2d-1)^4\Bigg(\sum_{k=0}^{d-1}\binom{d}{k}^2(d-k)!\Bigg)^2.\end{aligned}$$

Finally, we consider the last term of (9.7):

$$\begin{aligned}(9.10)\qquad \sum_{m,n=1}^{d}\frac{\delta_{m,n}\,\xi_{m,n}}{m!n!} &\le 2\sum_{n=1}^{d}\binom{d}{n}\sum_{m=1}^{d}\binom{d}{m}\binom{m}{2}+\sum_{n=1}^{d}\binom{d}{n}\sum_{m=1}^{d}\binom{d}{m}\\ &\le d^2\,2^{d-2}(2^d-1).\end{aligned}$$

Putting together (9.8)–(9.10), we obtain

$$B_1(d,s) \le d^2\,2^{d-2}(2^d-1)(4q^{3/2}+q)+\frac{7}{8}(2d-1)^4\Bigg(\sum_{k=0}^{d-1}\binom{d}{k}^2(d-k)!\Bigg)^2 q.$$

Combining (9.6) and the upper bounds for $A_1(d,s)$ and $B_1(d,s)$, we deduce the following result.

Corollary 9.2. *Under the assumptions of Theorem* 9.1,

$$(9.11)\qquad |\mathcal{V}_2(d,s,\boldsymbol{a})-\mu_d^2q^2| \le d^2 2^{2d+1}q^{3/2}+14d^4\Bigg(\sum_{k=0}^{d-1}\binom{d}{k}^2(d-k)!\Bigg)^2 q.$$

We finish this section with a brief analysis of the behavior of the right-hand side of (9.11). The analysis is similar to that of Section 5.3, and will be only briefly sketched.

Fix k with $0 \leq k \leq d-1$ and denote $h(k) := \binom{d}{k}^2(d-k)!$. Similarly to Remark 5.3, h is a unimodal function in the integer interval $[0, d-1]$ which reaches its maximum at $\lfloor k_0 \rfloor$, where $k_0 := -1/2 + \sqrt{5+4d}/2$. As a consequence,

$$\sum_{k=0}^{d-1} \binom{d}{k}^2 (d-k)! \leq d \binom{d}{\lfloor k_0 \rfloor}^2 (d - \lfloor k_0 \rfloor)! = \frac{d\,(d!)^2}{(d-\lfloor k_0 \rfloor)!\,(\lfloor k_0 \rfloor !)^2}.$$

With a similar analysis to Section 5.3, we conclude that

$$\left(\sum_{k=0}^{d-1} \binom{d}{k}^2 (d-k)! \right)^2 \leq 8 \cdot 14^2 d^{2d+2} e^{4\sqrt{d}-2d}.$$

Hence, we obtain the following result.

Theorem 9.3. *Let $p > 2$, $q > d$ and $1 \leq s \leq d-3$. Then*

$$|\mathcal{V}_2(d, s, \boldsymbol{a}) - \mu_d^2 q^2| \leq d^2\, 2^{2d+1} q^{3/2} + 28^3 d^{2d+6} e^{4\sqrt{d}-2d} q.$$

10. On the second moment for $s = 0$. As before, let $p > 2$ and let d be a positive integer with $d < q$. In this section by a similar analysis to the one underlying Sections 6–9 we establish the asymptotic behavior of the quantity

$$\mathcal{V}_2(d, 0) := \frac{1}{q^{d-1}} \sum_{\boldsymbol{b} \in \mathbb{F}_q^{d-1}} \mathcal{V}(f_{\boldsymbol{b}})^2,$$

the average second moment of $\mathcal{V}(f_{\boldsymbol{b}})$ when $f_{\boldsymbol{b}} := T^d + b_{d-1}T^{d-1} + \cdots + b_1 T$ ranges over all monic polynomials in $\mathbb{F}_q[T]$ of degree d with $f_{\boldsymbol{b}}(0) = 0$. As stated in the introduction, an explicit expression for $\mathcal{V}_2(d, 0)$ is obtained for $d \geq q$ in [KK90]. On the other hand, in [U56] it is shown that, for $p := \mathrm{char}(\mathbb{F}_q) > d$ and assuming the Riemann hypothesis for L-functions, one has $\mathcal{V}_2(d, 0) = \mu_d^2 q^2 + \mathcal{O}(q)$. Observe that no explicit expression for the $\mathcal{O}$-constant is provided in [U56].

A similar argument to the proof of Theorem 6.1 yields the following result.

Theorem 10.1. *Under the assumptions and notations above, we have*

$$\mathcal{V}_2(d, 0) = \mathcal{V}(d, 0) + \sum_{\substack{1 \leq m, n \leq d \\ 2 \leq m+n \leq d}} \binom{q}{m}\binom{q}{n}(-q)^{2-n-m}$$
$$+ \frac{1}{q^{d-1}} \sum_{\substack{1 \leq m, n \leq d \\ d+1 \leq m+n \leq 2d}} (-1)^{m+n} \sum_{\substack{\Gamma_1, \Gamma_2 \subset \mathbb{F}_q \\ |\Gamma_1| = m,\, |\Gamma_2| = n}} |S_{\Gamma_1, \Gamma_2}|,$$

where $\mathcal{S}_{\Gamma_1, \Gamma_2}$ is the set of points $(\boldsymbol{b}, b_{0,1}, b_{0,2}) \in \mathbb{F}_q^{d+1}$ with $b_{0,1} \neq b_{0,2}$ such that $(f_{\boldsymbol{b}} + b_{0,1})|_{\Gamma_1} \equiv 0$ and $(f_{\boldsymbol{b}} + b_{0,2})|_{\Gamma_2} \equiv 0$.

In view of Theorem 10.1, we fix m and n with $1 \leq m, n \leq d$ and $d+1 \leq m+n \leq 2d$ and consider the sum

$$\mathcal{S}_{m,n} := \sum_{\substack{\Gamma_1, \Gamma_2 \subset \mathbb{F}_q \\ |\Gamma_1| = m, |\Gamma_2| = n}} |\mathcal{S}_{\Gamma_1, \Gamma_2}|.$$

In order to find an estimate for $\mathcal{S}_{m,n}$ we introduce new indeterminates $T, T_1, \dots, T_m$, $U, U_1, \dots, U_n$, $B, B_{d-1}, \dots, B_1$, $B_{0,1}$, $B_{0,2}$ over $\overline{\mathbb{F}}_q$ and denote $\boldsymbol{B} := (B_{d-1}, \dots, B_1)$. Furthermore, we consider the polynomial $F := T^d + \sum_{i=1}^{d-1} B_i T^i + B \in \mathbb{F}_q[\boldsymbol{B}, B, T]$ and the affine $\mathbb{F}_q$-variety

$$\Gamma^0_{m,n} := \{(\boldsymbol{b}, b_{0,1}, b_{0,2}, \boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{A}^{d+1+m+n} : \Delta^{i-1} F(\boldsymbol{b}, b_{0,1}, \alpha_1, \dots, \alpha_i) = 0 \\ (1 \leq i \leq m),\ \Delta^{j-1} F(\boldsymbol{b}, b_{0,2}, \beta_1, \dots, \beta_j) = 0\ (1 \leq j \leq n)\},$$

where $\Delta^{i-1} F(\boldsymbol{b}, b_{0,1}, T_1, \dots, T_i)$ and $\Delta^{j-1} F(\boldsymbol{b}, b_{0,2}, U_1, \dots, U_j)$ denote the corresponding divided differences of $F(\boldsymbol{b}, b_{0,1}, T) \in \overline{\mathbb{F}}_q[T]$ and $F(\boldsymbol{b}, b_{0,2}, U) \in \overline{\mathbb{F}}_q[U]$ respectively.

Arguing as in the proof of Lemmas 7.1 and 7.2, we conclude that

$$(10.1) \qquad m!n!\mathcal{S}_{m,n} = \big|\Gamma^0_{m,n}(\mathbb{F}_q) \cap \{\alpha_i \neq \alpha_j\ (1 \leq i < j \leq m), \\ \beta_i \neq \beta_j\ (1 \leq i < j \leq n),\ b_{0,1} \neq b_{0,2}\}\big|.$$

The next step is to analyse the geometry of the affine $\mathbb{F}_q$-variety $\Gamma^0_{m,n}$, its projective closure $\mathrm{pcl}(\Gamma^0_{m,n}) \subset \mathbb{P}^{d+1+m+m}$ and the set $\mathrm{pcl}(\Gamma^0_{m,n})^\infty$ of points of $\mathrm{pcl}(\Gamma^0_{m,n})$ at infinity. We refrain from giving details, as the proofs are similar to those of Theorem 8.9, Lemma 8.12 and Theorem 8.13. We obtain the following result.

Theorem 10.2. *Assume that $p > 2$ and $q > d \geq 3$. Then:*

- $\mathrm{pcl}(\Gamma^0_{m,n})$ *is an absolutely irreducible ideal-theoretic complete intersection of dimension $d+1$ and degree $(d!)^2/((d-m)!(d-n)!)$.*
- $\mathrm{pcl}(\Gamma^0_{m,n})$ *is regular in codimension* 2, *namely the singular locus of* $\mathrm{pcl}(\Gamma^0_{m,n})$ *has codimension at least* 3 *in* $\mathrm{pcl}(\Gamma^0_{m,n})$.
- $\mathrm{pcl}(\Gamma^0_{m,n})^\infty$ *is a linear $\mathbb{F}_q$-variety of dimension d.*

To estimate the number of q-rational points of $\Gamma^0_{m,n}$ we shall use a further estimate of [CMP12] on the number of q-rational points of a projective complete intersection. More precisely, if $V \subset \mathbb{P}^N$ is a complete intersection defined over $\mathbb{F}_q$ of dimension $r \geq 2$, degree δ and multidegree $\boldsymbol{d} := (d_1, \dots, d_{N-r})$, which is regular in codimension 2, then (see [CMP12, Theorem 1.3])

$$(10.2) \qquad \big||V(\mathbb{F}_q)| - p_r\big| \leq 14 D^3 \delta^2 q^{r-1},$$

where $D := \sum_{i=1}^{N-r} (d_i - 1)$.

According to Theorem 10.2, the projective variety $\mathrm{pcl}(\varGamma_{m,n}^0)$ satisfies the hypothesis of [CMP12, Theorem 1.3]. Therefore, applying (10.2) we obtain

$$\big||\mathrm{pcl}(\varGamma_{m,n}^0)(\mathbb{F}_q)| - p_{d+1}\big| \le 14D_{m,n}^3\delta_{m,n}^2 q^d,$$

where

$$D_{m,n} := (m+n)d - (m(m+1)+n(n+1))/2$$

and

$$\delta_{m,n} := \frac{(d!)^2}{(d-m)!(d-n)!}.$$

Since $\mathrm{pcl}(\varGamma_{m,n}^0)^\infty$ is a linear $\mathbb{F}_q$-variety of dimension d, we have

$$\begin{aligned}(10.3)\qquad \big||\varGamma_{m,n}^0(\mathbb{F}_q)| - q^{d+1}\big| &= \big||\mathrm{pcl}(\varGamma_{m,n}^0)| - |\mathrm{pcl}(\varGamma_{m,n}^0)^\infty| - p_{d+1} + p_d\big| \\ &\le 14D_{m,n}^3\delta_{m,n}^2 q^d.\end{aligned}$$

Arguing as in Section 9.1, we obtain

(10.4)

$$\Big|\varGamma_{m,n}^0(\mathbb{F}_q) \cap \Big(\{B_{0,1} = B_{0,2}\} \cup \bigcup_{1\le i<j\le m}\{T_i = T_j\} \cup \bigcup_{1\le k<l\le n}\{U_k = U_l\}\Big)\Big| \le \xi_{m,n}\delta_{m,n}q^d,$$

where $\xi_{m,n} := \binom{m}{2} + \binom{n}{2} + 1$. Combining (10.1), (10.3) and (10.4) we deduce the following result.

Theorem 10.3. *Under the assumptions of Theorem* 10.2, *for each* (m,n) *with* $1 \le m,n \le d$, *and* $d+1 \le m+n \le 2d$, *we have*

$$\left|\mathcal{S}_{m,n} - \frac{q^{d+1}}{m!n!}\right| \le \frac{q^d}{m!n!}(14D_{m,n}^3\delta_{m,n}^2 + \xi_{m,n}\delta_{m,n}),$$

where

$$\xi_{m,n} := \binom{m}{2} + \binom{n}{2} + 1, \qquad D_{m,n} := (m+n)d - \binom{m+1}{2} - \binom{n+1}{2}$$

and $\delta_{m,n} := (d!)^2/((d-m)!(d-n)!)$.

Now we proceed as in Section 9.2. By Theorem 10.1, we have

(10.5)

$$\begin{aligned}\mathcal{V}_2(d,0) - \mu_d^2q^2 = \mathcal{V}(d,0) &+ \sum_{\substack{1\le m,n\le d\\ 2\le m+n\le d}} (-q)^{2-n-m}\left(\binom{q}{m}\binom{q}{n} - \frac{q^{m+n}}{m!n!}\right) \\ &+ \frac{1}{q^{d-1}}\sum_{\substack{1\le m,n\le d\\ d+1\le m+n\le 2d}} (-1)^{m+n}\Big(\mathcal{S}_{m,n} - \frac{q^{m+n}}{m!n!}\Big).\end{aligned}$$

In Section 9.2 we have obtained the following upper bound for the absolute value $A_1(d,0)$ of the second term on the right-hand side of (10.5):

$$A_1(d,0) \leq 2edq. \tag{10.6}$$

To bound the last term on the right-hand side of (10.5), by Theorem 10.3 we have

$$\begin{aligned} B_1(d,0) &:= \frac{1}{q^{d-1}} \sum_{\substack{1\leq m,n\leq d\\ d+1\leq m+n\leq 2d}} \left| \mathcal{S}_{m,n} - \frac{q^{d+1}}{m!n!} \right| \\ &\leq \sum_{\substack{1\leq m,n\leq d\\ d+1\leq m+n\leq 2d}} \left(\frac{14D_{m,n}^3 \delta_{m,n}^2}{m!n!} + \frac{\delta_{m,n}\xi_{m,n}}{m!n!} \right) q. \end{aligned}$$

With a similar argument to the proof of Corollary 9.2, we see that

$$B_1(d,0) \leq \left(d^2\, 2^{2d-1} + 14d^6 \left(\sum_{k=0}^{d-1} \binom{d}{k}^2 (d-k)! \right)^2 \right) q. \tag{10.7}$$

Finally, combining (1.1), (10.5), (10.6) and (10.7) with the arguments of the proof of Theorem 9.3, we deduce the main result of this section.

Theorem 10.4. *Assume that $p > 2$, $q > d$ and $d \geq 3$. Then*

$$|\mathcal{V}_2(d,0) - \mu_d^2 q^2| \leq (d^2\, 2^{2d-1} + 28^3 d^{2d+8} e^{4\sqrt{d}-2d}) q.$$

Appendix A. Irreducibility of the discriminant of small families of polynomials. Let $\mathbb{K}$ be a field and let $\mathbb{K}[X_1,\dots,X_n]$ be the ring of multivariate polynomials with coefficients in $\mathbb{K}$. For given positive integers $a_1,\dots,a_n$, we define the *weight* $\mathrm{wt}(\boldsymbol{X}^{\boldsymbol{\alpha}})$ of a monomial $\boldsymbol{X}^{\boldsymbol{\alpha}} := X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ as $\mathrm{wt}(\boldsymbol{X}^{\boldsymbol{\alpha}}) := \sum_{i=1}^n a_i \cdot \alpha_i$. The weight $\mathrm{wt}(f)$ of an arbitrary element f in $\mathbb{K}[X_1,\dots,X_n]$ is the highest weight of all the monomials appearing with nonzero coefficients in the dense representation of f.

An element $f \in \mathbb{K}[X_1,\dots,X_n]$ is said to be *weighted homogeneous* (with respect to the weight wt defined above) if all its terms have the same weight. Equivalently, f is weighted homogeneous if and only if $f(X_1^{a_1},\dots,X_n^{a_n})$ is homogeneous of degree $\mathrm{wt}(f)$. Any polynomial $f \in \mathbb{K}[X_1,\dots,X_n]$ can be uniquely written as a sum $\sum_i f_i$, where each f_i is weighted homogeneous with $\mathrm{wt}(f_i) = i$. The polynomials f_i are called the *weighted homogeneous components* of f. We shall use the following elementary property of weights.

Fact A.1 ([HH11, Proposition 3.3.7]). *Let $f \in \mathbb{K}[X_1,\dots,X_n]$ be nonconstant. If the component $f_{\mathrm{wt}(f)}$ of highest weight of f is irreducible in $\mathbb{K}[X_1,\dots,X_n]$, then f is irreducible in $\mathbb{K}[X_1,\dots,X_n]$.*

We shall also use the following simple criterion of irreducibility.

Fact A.2. *Let $f \in \mathbb{K}[X_1, \dots, X_n]$ be nonconstant, $s < n$,*

$$R := \mathbb{K}[X_1, \dots, X_s] \quad \textit{and} \quad Q(R) := \mathbb{K}(X_1, \dots, X_s).$$

If f is a primitive polynomial of $R[X_{s+1}, \dots, X_n]$ and an irreducible element of $Q(R)[X_{s+1}, \dots, X_n]$, then f is irreducible in $\mathbb{K}[X_1, \dots, X_n]$.

Assume that the characteristic p of $\mathbb{F}_q$ is not 2. For d and s with $1 \le s \le d-3$, let $B_{d-s-1}, \dots, B_1, B_0, T$ be indeterminates over $\overline{\mathbb{F}}_q$ and let $\boldsymbol{B}_0 := (B_{d-s-1}, \dots, B_1, B_0)$. In what follows, for a given $\boldsymbol{a} := (a_{d-1}, \dots, a_{d-s}) \in \overline{\mathbb{F}}_q^s$, we shall consider the following polynomial in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0, T]$:

$$f := T^d + a_{d-1}T^{d-1} + \cdots + a_{d-s}T^{d-s} + B_{d-s-1}T^{d-s-1} + \cdots + B_1T + B_0.$$

Denote by $\mathrm{Disc}(f) \in \overline{\mathbb{F}}_q[\boldsymbol{B}_0]$ the discriminant of f with respect to T. We shall consider the weight wt on $\overline{\mathbb{F}}_q[\boldsymbol{B}_0, T]$ defined by setting $\mathrm{wt}(B_j) := d - j$ for $0 \le j \le d-s-1$. We observe that, extending this notion of weight to the polynomial ring $\overline{\mathbb{F}}_q[B_d, \dots, B_0]$ in a similar way, the discriminant of a generic degree-d polynomial of $\overline{\mathbb{F}}_q[B_d, \dots, B_0][T]$ is weighted homogeneous of weight $d(d-1)$ (see, e.g., [FS84, Lemma 2.2]).

Theorem A.3. *Let $p > 2$, $q > d$ and $1 \le s \le d-3$. Then* $\mathrm{Disc}(f)$ *is an irreducible polynomial in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]$.*

Proof. First we suppose that p does not divide $d(d-1)$. Consider $\mathrm{Disc}(f)$ as an element of $\mathbb{K}_2[B_1, B_0] := \overline{\mathbb{F}}_q(B_{d-s-1}, \dots, B_2)[B_1, B_0]$, and consider the weight w_2 on $\mathbb{K}_2[B_1, B_0]$ defined by setting $\mathrm{w}_2(B_0) := d$ and $\mathrm{w}_2(B_1) := d-1$. It is easy to see that the weighted homogeneous component of highest weight of $\mathrm{Disc}(f)$ is $\Delta_2 := d^dB_0^{d-1} + (-1)^{d-1}(d-1)^{d-1}B_1^d$. Our assumption on p implies that Δ_2 is a nonzero polynomial. Furthermore, by the Stepanov criterion (see, e.g., [LN83, Lemma 6.54]), Δ_2 is irreducible in $\mathbb{K}_2[B_1, B_0]$. Then Fact A.1 implies that $\mathrm{Disc}(f)$ is an irreducible element of $\mathbb{K}_2[B_1, B_0]$. Finally, as $\mathrm{Disc}(f)$ is a primitive polynomial in $\overline{\mathbb{F}}_q[B_{d-s-1}, \dots, B_2][B_1, B_0]$, Fact A.2 shows that $\mathrm{Disc}(f)$ is irreducible in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]$.

Assume now that p divides d. Let $\mathbb{K}_3 := \overline{\mathbb{F}}_q(B_{d-s-1}, \dots, B_3)$ and consider $\mathrm{Disc}(f)$ as an element of $\mathbb{K}_3[B_2, B_1, B_0]$. We consider the weight w_3 on $\mathbb{K}_3[B_2, B_1, B_0]$ defined by setting $\mathrm{w}_3(B_0) := d$, $\mathrm{w}_3(B_1) := d-1$ and $\mathrm{w}_3(B_2) := d-2$. If $g := T^d + B_2T^2 + B_1T + B_0$, then $g' = 2B_2T + B_1$. Therefore, applying the Poisson formula for the resultant it is easy to prove that $\mathrm{Disc}(g) = B_1^d + (-1)^{d+1}2^{d-2}B_2^{d-1}B_1^2 + (-1)^d2^dB_2^dB_0$. Since $\deg f = \deg g = d$ and the discriminant of a generic polynomial of degree d is weighted homogeneous of degree $d(d-1)$, it follows that $\mathrm{Disc}(g)$ is the component of highest weight of $\mathrm{Disc}(f)$. Furthermore, we claim that $\mathrm{Disc}(g)$ is irreducible in $\mathbb{K}_3[B_2, B_1, B_0]$. Indeed, considering $\mathrm{Disc}(g)$ as a polynomial in $\mathbb{K}_3(B_0)[B_2, B_1]$, we see that it is the sum of two homogeneous polynomials of degrees d and $d+1$ without common factors, namely $B_1^d + (-1)^d 2^d B_2^d B_0$ and $(-1)^{d+1} 2^{d-2} B_2^{d-1} B_1^2$. Then [Gib98, Lemma 3.15] proves that $\mathrm{Disc}(g)$ is irreducible in $\mathbb{K}_3(B_0)[B_2, B_1]$, which in turn implies it is irreducible in $\mathbb{K}_3[B_2, B_1, B_0]$ by Fact A.2. Combining this with Fact A.1 we deduce that $\mathrm{Disc}(f)$ is irreducible in $\mathbb{K}_3[B_2, B_1, B_0]$, from which we readily conclude that it is irreducible in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]$ by Fact A.2.

Finally, suppose that p divides $d-1$ and consider $\mathrm{Disc}(f)$ as an element of $\mathbb{K}_3[B_2, B_1, B_0]$. Arguing as before we conclude that the discriminant $\mathrm{Disc}(g)$ of $g := T^d + B_2T^2 + B_1T + B_0$ is the component of highest weight of $\mathrm{Disc}(f)$. Observe that $g' = T^{d-1} + 2B_2T + B_1$, and thus

$$\begin{aligned}\mathrm{Disc}(g) &= \frac{\mathrm{Res}_T(g, Tg' - g)}{\mathrm{Res}_T(g, T)} = \frac{\mathrm{Res}_T(g, B_2T^2 - B_0)}{\mathrm{Res}_T(g, T)} \\ &= \frac{\mathrm{Res}_T(T^d + B_1T + 2B_0, B_2T^2 - B_0)}{\mathrm{Res}_T(g, T)}.\end{aligned}$$

Applying the Poisson formula for the resultant, we easily deduce that

$$\mathrm{Disc}(g) = \begin{cases} 4B_2^d B_0 + B_0^{d-1} + 4B_0^{d/2} B_2^{d/2} - B_1^2 B_2^{d-1} & \text{for } d \text{ even}, \\ -4B_2^d B_0 + B_0^{d-1} + 2B_0^{\frac{d-1}{2}} B_2^{\frac{d-1}{2}} - B_1^2 B_2^{d-1} & \text{for } d \text{ odd}. \end{cases}$$

Then $\mathrm{Disc}(g)$ is irreducible in $\overline{\mathbb{F}}_q[B_0, B_2][B_1]$ by the Eisenstein criterion and $\mathrm{Disc}(f)$ is irreducible in $\mathbb{K}_3[B_2, B_1, B_0]$ by Fact A.1. Arguing as above we find that $\mathrm{Disc}(f)$ is irreducible in $\overline{\mathbb{F}}_q[\boldsymbol{B}_0]$, thus finishing the proof of the theorem. ■

Acknowledgments. The authors were partially supported by the grants PIP 11220090100421 CONICET, UNGS 30/3180 and STIC-AmSud 13STIC-02 “Dynalco”. The authors are pleased to thank Eda Cesaratto for several valuable comments and suggestions.

References

[CM06] A. Cafure and G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. 12 (2006), 155–185.

[CM07] 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), 19–35.

[CMP12] A. Cafure, G. Matera, and M. Privitelli, *Polar varieties, Bertini's theorems and number of points of singular complete intersections over a finite field*, arXiv:1209.4938 [math.AG] (2012).

[CGH91] L. Caniglia, A. Galligo, and J. Heintz, *Equations for the projective closure and effective Nullstellensatz*, Discrete Appl. Math. 33 (1991), 11–23.

[C–P14] E. Cesaratto, G. Matera, M. Pérez, and M. Privitelli, *On the value set of small families of polynomials over a finite field, I*, J. Combin. Theory Ser. A 124 (2014), 203–227.

[Coh72] S. Cohen, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. (2) 6 (1972), 93–102.

[Coh73] S. Cohen, *The values of a polynomial over a finite field*, Glasgow Math. J. 14 (1973), 205–208.

[CLO92] 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.

[Eis95] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Grad. Texts in Math. 150, Springer, New York, 1995.

[FS08] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge Univ. Press, Cambridge, 2008.

[FS84] M. Fried and J. Smith, *Irreducible discriminant components of coefficient spaces*, Acta Arith. 44 (1984), 59–72.

[Ful84] W. Fulton, *Intersection Theory*, Springer, Berlin, 1984.

[GL02] S. Ghorpade and G. Lachaud, *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields*, Moscow Math. J. 2 (2002), 589–631.

[Gib98] C. Gibson, *Elementary Geometry of Algebraic Curves: an Undergraduate Introduction*, Cambridge Univ. Press, Cambridge, 1998.

[Har92] J. Harris, *Algebraic Geometry: a First Course*, Grad. Texts in Math. 133, Springer, New York, 1992.

[Hei83] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci. 24 (1983), 239–277.

[HH11] J. Herzog and T. Hibi, *Monomial Ideals*, Grad. Texts in Math. 206, Springer, London, 2011.

[KK90] A. Knopfmacher and J. Knopfmacher, *The distribution of values of polynomials over a finite field*, Linear Algebra Appl. 134 (1990), 145–151.

[Kun85] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Boston, 1985.

[LN83] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MS, 1983.

[Sha94] I. R. Shafarevich, *Basic Algebraic Geometry: Varieties in Projective Space*, Springer, Berlin, 1994.

[U55a] S. Uchiyama, *Note on the mean value of $V(f)$*, Proc. Japan Acad. 31 (1955), 199–201.

[U55b] S. Uchiyama, *Note on the mean value of $V(f)$. II*, Proc. Japan Acad. 31 (1955), 321–323.

[U56] S. Uchiyama, *Note on the mean value of $V(f)$. III*, Proc. Japan Acad. 32 (1956), 97–98.

[Vog84] W. Vogel, *Results on Bézout's Theorem*, Tata Inst. Fund. Res. Lect. Math. 74, Tata Inst. Fund. Res., Bombay, 1984.

Guillermo Matera
Instituto del Desarrollo Humano
Universidad Nacional
de General Sarmiento
J. M. Gutiérrez 1150
(B1613GSX) Los Polvorines
Buenos Aires, Argentina
and
National Council of Science
and Technology (CONICET), Argentina
E-mail: gmatera@ungs.edu.ar

Melina Privitelli
Instituto de Ciencias
Universidad Nacional
de General Sarmiento
J. M. Gutiérrez 1150
(B1613GSX) Los Polvorines
Buenos Aires, Argentina
and
National Council of Science
and Technology (CONICET), Argentina
E-mail: mprivitelli@conicet.gov.ar

Mariana Pérez
Instituto del Desarrollo Humano
Universidad Nacional de General Sarmiento
J. M. Gutiérrez 1150
(B1613GSX) Los Polvorines
Buenos Aires, Argentina
E-mail: vperez@ungs.edu.ar

Received on 4.9.2013 (7574)