ACTA ARITHMETICA
130.1 (2007)

An effective Bertini theorem and the number of rational points of a normal complete intersection over a finite field

by

ANTONIO CAFURE and GUILLERMO MATERA (Buenos Aires)

1. Introduction. Let $\mathbb{F}_q$ be the finite field of q elements and let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. We denote the n-dimensional projective and affine spaces defined over $\mathbb{F}_q$ and $\overline{\mathbb{F}}_q$ by $\mathbb{P}^n(\mathbb{F}_q)$, $\mathbb{P}^n := \mathbb{P}^n(\overline{\mathbb{F}}_q)$, $\mathbb{A}^n(\mathbb{F}_q)$ and $\mathbb{A}^n := \mathbb{A}^n(\overline{\mathbb{F}}_q)$ respectively. Let V be an affine or a projective variety defined over $\mathbb{F}_q$ (an $\mathbb{F}_q$-*variety* for short). Counting or estimating the number $|V(\mathbb{F}_q)|$ of q-rational points of V is a classical problem. Here by a *q-rational point* of V we mean a point of V with coordinates in $\mathbb{F}_q$.

In [19] (see also [15]), S. Lang and A. Weil establish a "prototype" estimate on $|V(\mathbb{F}_q)|$ for absolutely irreducible $\mathbb{F}_q$-varieties. They prove that for an absolutely irreducible $\mathbb{F}_q$-variety $V \subset \mathbb{P}^n$ of dimension r and degree δ,

$$\big||V(\mathbb{F}_q)| - p_r\big| \le (\delta-1)(\delta-2)\, q^{r-1/2} + C(n,r,\delta)\, q^{r-1}, \tag{1}$$

where $p_r := q^r + q^{r-1} + \cdots + q + 1 = |\mathbb{P}^r(\mathbb{F}_q)|$ and $C(n,r,\delta)$ is a constant independent of q. We remark that [19] does not provide an explicit expression for $C(n,r,\delta)$.

From the point of view of practical applications, it is usually necessary to provide explicit expressions of the constant $C := C(n,r,\delta)$ (see, e.g., [14], [16], [24], [2]). Further, particular families of varieties for which better estimates hold are also of interest (see, e.g., [32], [33], [21], [25]).

S. Ghorpade and G. Lachaud ([10], [9]) show that one can take $C = 9\cdot 2^s(sd+3)^{n+1}$ in (1), provided that the variety V is defined by s equations of degree at most d. The proof of this result relies on the Grothendieck–Lefschetz trace formula and estimates of the Betti numbers of suitable spaces of étale ℓ-adic cohomology.

2000 *Mathematics Subject Classification*: Primary 11G25, 14G05; Secondary 11G20, 14M10.

Key words and phrases: varieties over finite fields, rational points, normal complete intersection, second Bertini theorem.

This research was partially supported by the following grants: UBACyT X112, PIP CONICET 2461, UNGS 30/3005 and MTM2004-01167 (2004–2007).

W. Schmidt ([27], [28]) develops an alternative approach based on combinatorial arguments and an effective version of the first Bertini theorem in order to obtain for the first time an explicit value of C for an absolutely irreducible $\mathbb{F}_q$-hypersurface. The authors of this article [3] combine Schmidt's approach with tools of effective elimination theory and an improved effective version of the first Bertini theorem in order to prove that one can take $C = 5\delta^{13/3}$ in (1), provided that the *regularity* condition $q > 2(r+1)\delta^2$ holds. The estimate (1) holds for hypersurfaces without any regularity condition.

These two are the best *general* estimates known. Nevertheless, in many particular cases they are far from being sharp. In fact, in the presence of better geometric conditions significant improvements can be obtained, as shown by the work of P. Deligne [7], C. Hooley [13] and others. This article is devoted to obtaining an estimate of type (1) for the number of q-rational points of a normal complete-intersection $\mathbb{F}_q$-variety $V \subset \mathbb{P}^n$.

This case has already been considered in [10], [9]. The authors prove that if $V \subset \mathbb{P}^n$ is a normal complete-intersection $\mathbb{F}_q$-variety of degree δ and multidegree $\mathbf{d} := (d_1, \ldots, d_{n-r})$, defined by $n-r$ equations of maximum degree d, then the following estimate holds:

$$(2)\quad \big||V(\mathbb{F}_q)| - p_r\big| \le b'_1(n-r+1, \mathbf{d})q^{r-1/2} + 9 \cdot 2^{n-r}((n-r)d+3)^{n+1}q^{r-1}.$$

Here $b'_1(n-r+1, \mathbf{d})$ is the first primitive Betti number of a nonsingular complete intersection curve in $\mathbb{P}^{n-r+1}$ of multidegree $\mathbf{d}$. As $b'_1(n-r+1, \mathbf{d}) \le (\delta-1)(\delta-2)$, with equality if and only if V is a hypersurface, we conclude that (2) improves (1) with $C = 9 \cdot 2^s(sd+3)^{n+1}$.

Compared with the bound $C \le 5\delta^{13/3}$ obtained in [3] without using the normality assumption, the bound $C \le 9 \cdot 2^{n-r}((n-r)d+3)^{n+1}$ does not seem to be good for low codimension varieties, in particular for hypersurfaces, which are very common in practical situations (see, e.g., [14], [16], [24], [2], [25]). Indeed, in the hypersurface case the bound for C obtained in [3] exponentially improves that of [10], [9]. In this direction, using methods of elimination theory we derive a further estimate of type (2) better adapted to low codimensional situations. Our main result is the following (cf. Theorem 6.1 and Corollary 6.2 below):

THEOREM. *Let $q > 2(n-r)d\delta+1$ and let $V \subset \mathbb{P}^n$ be a normal complete-intersection $\mathbb{F}_q$-variety of degree δ and multidegree $\mathbf{d}$, defined by polynomials of maximum degree d. Then*

$$(3)\qquad \big||V(\mathbb{F}_q)| - p_r\big| \le b'_1(n-r+1, \mathbf{d})q^{r-1/2} + 2(n-r)^2d^2\delta^2q^{r-1},$$

where $b'_1(n-r+1, \mathbf{d})$ denotes the first primitive Betti number of a nonsingular complete-intersection curve in $\mathbb{P}^{n-r+1}$ of multidegree $\mathbf{d}$.

As previously mentioned, our estimate, although valid under the regularity condition $q > 2(n-r)d\delta+1$, clearly improves (2) in the case of a hypersurface. In fact, for a hypersurface (2) becomes

$$\big||V(\mathbb{F}_q)| - p_{n-1}\big| \le (\delta-1)(\delta-2)q^{n-3/2} + 18(\delta+3)^{n+1}q^{n-2}.$$

Our estimate also improves (2) in cases of low dimension (such as $2r \le n-1$) and low degree (such as $d \le 2(n-r)$). Furthermore, we improve the (general) estimate $C = 5\delta^{13/3}$ of [3] and its regularity condition $q > 2(r+1)\delta^2$.

The proof of our main result relies on arguments of elimination theory in the spirit of [3] and an effective version of the second Bertini theorem. More precisely, we express the variety V under consideration as the disjoint union of a suitable number, namely $p_{r-1} := |\mathbb{P}^{r-1}(\mathbb{F}_q)|$, of 1-dimensional linear sections of V defined over $\mathbb{F}_q$. Since the dimension of the singular locus of V is at most $r-2$, a generic 1-dimensional linear section of V is a nonsingular complete-intersection curve. A critical point is to obtain an upper bound on the number of 1-dimensional *singular* linear sections of V defined over $\mathbb{F}_q$. For this purpose, we establish the following effective version of the second Bertini theorem (see Theorem 5.3):

THEOREM. *Let $V \subset \mathbb{P}^n$ be a normal complete-intersection of dimension r and degree δ, and let $\pi : V \to \mathbb{P}^{r-1}$ be a generic linear projection. Then there exists a variety $W \subset \mathbb{P}^{r-1}$ of degree at most $2(n-r)^2(d-1)^2\delta$ such that the fiber $\pi^{-1}(y)$ is a nonsingular curve of degree at most δ for every $y \notin W$.*

The number of q-rational points of V lying in the nonsingular linear sections mentioned above is estimated using Deligne's estimate (see Section 6), while the q-rational points lying in the remaining linear sections are controlled by means of elementary estimates and our effective second Bertini theorem.

The paper is organized as follows. In Section 3 we exhibit an upper bound on the number of q-rational points of an arbitrary projective variety defined over $\mathbb{F}_q$, which illustrates the kind of arguments of elimination theory we use. Section 4 is devoted to obtaining an upper bound on the degree of the genericity condition underlying the choice of linear varieties $\mathcal{L}_r$ and $\mathcal{L}_{n-r-1}$ for which the central projection from $\mathcal{L}_{n-r-1}$ mapping V onto $\mathcal{L}_r$ is a finite morphism and the corresponding field extension is separable. In Section 5 we obtain the effective version of the second Bertini theorem mentioned above, which is applied in Section 6 to obtain (3). We finish by briefly commenting on an application of (3) in the setting of cryptography.

2. Notions and notations.

We use standard notions and notations of commutative algebra and algebraic geometry as can be found in, e.g., [17], [30], [22].

Let K be any of the fields $\mathbb{F}_q$ or $\overline{\mathbb{F}}_q$. We say that $V \subset \mathbb{P}^n$ (resp. $V \subset \mathbb{A}^n$) is a projective (resp. affine) K-variety if it is the set of all common zeros in $\overline{\mathbb{F}}_q^{n+1}$ (resp. $\overline{\mathbb{F}}_q^n$) of a family of homogeneous polynomials $F_1, \dots, F_m \in \mathsf{K}[X_0, \dots, X_n]$ (resp. of polynomials $F_1, \dots, F_m \in \mathsf{K}[X_1, \dots, X_n]$). In this section, unless otherwise stated, all results referring to K-varieties in general should be understood as valid for both projective and affine varieties.

For a K-variety V in the n-dimensional (affine or projective) space, we denote by $I(V)$ its defining ideal and by $\mathsf{K}[V]$ its coordinate ring. The *dimension* $\dim V$ of a K-variety V is the (Krull) dimension of the ring $\mathsf{K}[V]$. The *degree* $\deg V$ of an irreducible K-variety V is the maximum number of points lying in the intersection of V with a generic linear space L of codimension $\dim V$, for which $V \cap L$ is a finite set (a zero-dimensional variety). More generally, if $V = V_1 \cup \cdots \cup V_s$ is the decomposition of V into irreducible K-components, we define the degree of V as $\deg V := \sum_{i=1}^{s} \deg V_i$ (cf. [11]).

We say that V has *pure dimension* r if every irreducible K-component of V has dimension r. A K-variety V is *absolutely irreducible* if it is irreducible as an $\overline{\mathbb{F}}_q$-variety.

A K-variety V of dimension r in an n-dimensional space is called an (ideal-theoretic) *complete intersection* if its ideal $I(V)$ over K can be generated by $n-r$ polynomials. If V is a complete intersection in $\mathbb{P}^n$ of dimension r and degree δ and $F_1, \dots, F_{n-r}$ is a system of generators of $I(V)$, 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 $d_1 \geq \cdots \geq d_{n-r}$, we call $\mathbf{d} := (d_1, \dots, d_{n-r})$ the *multidegree* of the complete intersection V. In particular, it follows that $\delta = \prod_{i=1}^{n-r} d_i$.

An irreducible projective K-variety V is *normal* if for every $x \in V$ there is an affine neighborhood U of x such that the affine coordinate ring $\mathsf{K}[U]$ is integrally closed. Nonsingular varieties are normal, and when V is a curve, normality and nonsingularity are equivalent conditions. We recall Serre's criterion for normality: *A projective complete intersection V is normal if and only if V is regular in codimension* 1. If V is a normal complete-intersection curve it is connected and so absolutely irreducible.

Let V and W be irreducible K-varieties of the same dimension and $f : V \to W$ be a regular dominant map. The degree of the field extension $f^*(\mathsf{K}(W)) \subset \mathsf{K}(V)$ is called the *degree* of f. Suppose further that W is normal and f is a finite morphism. We say that f is *unramified* at $y \in W$ if the number of inverse images of y equals the degree of f.

An important tool for our estimates is the following *Bézout inequality* (see [11] for the affine case and [5] for the projective case; see also [8], [34]): if V and W are K-varieties, then

$$\deg(V \cap W) \leq \deg V \deg W. \tag{4}$$

We shall also make use of the following well-known identities relating the degree of an affine K-variety $V \subset \mathbb{A}^n$, the degree of its projective closure (with respect to the projective Zariski K-topology) $\overline{V} \subset \mathbb{P}^n$ and the degree of the affine cone $\widetilde{V}$ of $\overline{V}$ (see, e.g., [4, Proposition 1.11]):

$$\deg V = \deg \overline{V} = \deg \widetilde{V}. \tag{5}$$

Finally, we have the following result concerning the behavior of the degree under linear maps.

LEMMA 2.1. *Let $\phi : V \to W$ be a regular linear map between K-varieties. Then* $\deg \overline{\phi(V)} \leq \deg V$.

Proof. From (5) we see that it is enough to prove the statement for affine varieties. But for affine varieties this is a well-known fact (see, e.g., [11, Lemma 2]). ∎

3. An elementary upper bound. Following the notations of the preceding section, $\mathbb{P}^n$ and $\mathbb{A}^n$ stand for $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ and $\mathbb{A}^n(\overline{\mathbb{F}}_q)$ respectively. For a given variety V, we denote by $V(\mathbb{F}_q)$ the set of q-rational points of V and by $|V(\mathbb{F}_q)|$ its cardinality.

In this section we obtain an elementary upper bound on $|V(\mathbb{F}_q)|$. Notice that in some cases it is possible to determine the exact value of $|V(\mathbb{F}_q)|$. For instance, the number of points p_n of $\mathbb{P}^n(\mathbb{F}_q)$ is given by $p_n := |\mathbb{P}^n(\mathbb{F}_q)| = q^n + q^{n-1} + \cdots + q + 1$.

For an affine variety V of dimension r and degree δ we have the following upper bound on the number of q-rational points of V [3, Lemma 2.1]:

$$|V(\mathbb{F}_q)| \leq \delta q^r. \tag{6}$$

The corresponding upper bound for a projective hypersurface is classical ([28], [20]). Our next result extends this bound to arbitrary projective varieties:

PROPOSITION 3.1. *Let V be a projective variety of dimension r and degree δ. Then*

$$|V(\mathbb{F}_q)| \leq \delta p_r.$$

Proof. The proof is by induction on r. If $r = 0$ then it is clear that $|V(\mathbb{F}_q)| \leq \delta$. Hence we may assume that $r \geq 1$. Suppose now that V is irreducible. After a linear change of coordinates we may assume that the hyperplane at infinity $\{X_0 = 0\}$ does not contain V.

Then $V_{\mathrm{aff}} := V \cap \{X_0 = 1\}$ is an affine r-dimensional variety with projective closure V. Therefore, $\deg V_{\mathrm{aff}} = \delta$ by (5) and thus (6) implies $|V_{\mathrm{aff}}(\mathbb{F}_q)| \leq \delta q^r$.

On the other hand, by assumption, $V_\infty := V \cap \{X_0 = 0\} = V \setminus V_{\mathrm{aff}}$ is a projective variety of dimension at most $r-1$ and degree at most δ. Then by the induction hypothesis we have $|V_\infty(\mathbb{F}_q)| \leq \delta p_{r-1}$.

In conclusion,

$$|V(\mathbb{F}_q)| = |V_{\mathrm{aff}}(\mathbb{F}_q)| + |V_\infty(\mathbb{F}_q)| \leq \delta q^r + \delta p_{r-1} = \delta p_r.$$

This completes the inductive step when V is irreducible. Next, for an arbitrary projective variety V, let $V = V_1 \cup \cdots \cup V_s$ be its decomposition into irreducible projective varieties. Then $\dim V_i \leq r$ and $\delta = \sum_{i=1}^s \delta_i$, where $\delta_i := \deg V_i$ for $1 \leq i \leq s$. Therefore

$$|V(\mathbb{F}_q)| \leq \sum_{i=1}^s |V_i(\mathbb{F}_q)| \leq \sum_{i=1}^s \delta_i p_r \leq \delta p_r.$$

This finishes the proof of the proposition. ∎

A somewhat different proof is given in [10, Proposition 12.1] (see also [18, Proposition 2.3]). Nevertheless, we have included our proof because it illustrates the kind of arguments of elimination theory we use. We also observe that in the case of an $\mathbb{F}_q$-hypersurface $H \subset \mathbb{P}^n$ of degree $\delta \leq q+1$ we have the upper bound $|H(\mathbb{F}_q)| \leq \delta q^{n-1} + p_{n-2}$ due to J.-P. Serre [29]. Unfortunately, the hypersurfaces we consider in the next sections are not in general defined over $\mathbb{F}_q$, and thus Serre's bound cannot be applied.

4. On the existence of good linear projections.

In this section we establish some results which are crucial to obtaining our effective version of the second Bertini theorem of Section 5.

Let $V \subset \mathbb{P}^n$ be an absolutely irreducible complete-intersection $\mathbb{F}_q$-variety of dimension r and degree δ. Let $F_1, \dots, F_{n-r} \in \mathbb{F}_q[X_0, \dots, X_n]$ be homogeneous polynomials which form a regular sequence and generate the ideal of the variety V. We denote by d_i the degree of F_i for $1 \leq i \leq n-r$, and we set $d := \max_{1 \leq i \leq n-r} d_i$.

Since V has pure dimension r, for a generic choice of linear varieties $\mathcal{L}_r$ and $\mathcal{L}_{n-r-1}$ of $\mathbb{P}^n$ of dimension r and $n-r-1$ respectively, we have

$$\mathcal{L}_r \cap \mathcal{L}_{n-r-1} = \emptyset, \qquad V \cap \mathcal{L}_{n-r-1} = \emptyset.$$

Furthermore, V is mapped onto $\mathcal{L}_r$ by the central projection π_r from $\mathcal{L}_{n-r-1}$, and finitely many points of V lie over any point of $\mathcal{L}_r$ under this projection. Finally, if $Y_0, \dots, Y_r$ are linear forms on $\overline{\mathbb{F}}_q[X_0, \dots, X_n]$ whose zero set defines the linear variety $\mathcal{L}_{n-r-1}$, and π_r is defined by

$$\pi_r : V \to \mathcal{L}_r, \qquad x \mapsto (Y_0(x) : \cdots : Y_r(x)),$$

then π_r is a finite morphism. Our first result yields a suitable choice for the linear variety $\mathcal{L}_{n-r-1}$:

Lemma 4.1. *There exist indices $0 \leq i_{r+1} < \cdots < i_n \leq n$ such that, if we define $Y_j := X_{i_j}$ for $r+1 \leq j \leq n$, then $Y_{r+1}, \dots, Y_n$ are $\overline{\mathbb{F}}_q$-linearly* *independent and* $\mathcal{U} := \{x \in V : (\partial F_i/\partial Y_{r+j})_{1\le i,j\le n-r}(x) \neq 0\}$ *is a nonempty Zariski open subset of* V.

Proof. Since V is absolutely irreducible, from, e.g., [28, Chapter 6, Corollary 6.C], we conclude that there exist linear forms $Y_0,\dots,Y_r \in \overline{\mathbb{F}}_q[X_0,\dots,X_n]$ such that $\overline{\mathbb{F}}_q(Y_0,\dots,Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$ is an algebraic separable field extension. Further, these linear forms can be chosen in such a way that the projection mapping $\pi_r : V \to \mathbb{P}^r$ defined by $\pi_r(x) := (Y_0(x) : \cdots : Y_r(x))$ is a finite morphism, as asserted above. For the sake of the argument, fix arbitrarily such linear forms and denote by $\lambda \in \overline{\mathbb{F}}_q^{(r+1)\times(n+1)}$ the matrix whose rows are the coefficients of these forms.

From, e.g., [31, II.6.3, Theorem 4], we see that there exists $y \in \mathbb{P}^r$ such that $\pi_r^{-1}(y)$ is an unramified fiber of π_r, i.e., the number of inverse images of y equals the degree of the field extension $\overline{\mathbb{F}}_q(Y_0,\dots,Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$. Fix arbitrarily $x \in \pi_r^{-1}(y)$. The unramifiedness of π_r at x means that the differential $d_x\pi_r : T_xV \to T_y\mathbb{P}^r$ between the tangent spaces is injective (see [6, §5, 5.2]). This in turns means that the following $(n+1)\times(n+1)$ matrix is nonsingular:

$$D_r(x) := \begin{pmatrix} \lambda_{0,0} & \cdots & \lambda_{0,n} \\ \vdots & & \vdots \\ \lambda_{r,0} & \cdots & \lambda_{r,n} \\ \frac{\partial F_1}{\partial X_0}(x) & \cdots & \frac{\partial F_1}{\partial X_n}(x) \\ \vdots & & \vdots \\ \frac{\partial F_{n-r}}{\partial X_0}(x) & \cdots & \frac{\partial F_{n-r}}{\partial X_n}(x) \end{pmatrix}.$$

Considering the Laplace expansion of the determinant of $D_r(x)$, we conclude that there exist two disjoint sets of indices $0 \le i_0 < i_1 < \cdots < i_r \le n$ and $0 \le i_{r+1} < \cdots < i_n \le n$ such that both the square Jacobian matrices $(\partial Y_i/\partial X_{i_j})_{0\le i,j\le r}$ and $((\partial F_i/\partial X_{i_{r+j}})(x))_{1\le i,j\le n-r}$ are nonsingular.

From the nonsingularity of $(\partial Y_i/\partial X_{i_j})_{0\le i,j\le r}$ we conclude that the linear forms $Y_0,\dots,Y_r,X_{i_{r+1}},\dots,X_{i_n}$ are $\overline{\mathbb{F}}_q$-linearly independent. Furthermore, defining $Y_j := X_{i_j}$ for $r+1 \le j \le n$, we see that the matrix $((\partial F_i/\partial Y_{r+j})(x))_{1\le i,j\le n-r}$ is nonsingular, which implies that $\mathcal{U} := \{x \in V : (\partial F_i/\partial Y_{r+j})_{1\le i,j\le n-r}(x) \neq 0\}$ is a nonempty Zariski open subset of V. ∎

From now on we fix linear forms $Y_{r+1},\dots,Y_n$ satisfying the statement of Lemma 4.1. Our next result yields an upper bound on the degree of the genericity condition underlying the choice of the linear variety $\mathcal{L}_r$. Before stating it, we introduce some notations. Let $\Lambda := (\Lambda_{i,j})_{0\le i\le r,\,0\le j\le n}$ be a matrix of indeterminates and let $\Lambda^{(i)}$ denote the ith row of Λ for $0 \le i \le r$. Set $X := (X_0,\dots,X_n)$ and $\widetilde{Y} := (\widetilde{Y}_0,\dots,\widetilde{Y}_r) := \Lambda X$.

Proposition 4.2. *There exists a nonzero polynomial* $A \in \overline{\mathbb{F}}_q[\Lambda]$ *of degree at most* $2\delta + 1$ *in each group of variables* $\Lambda^{(i)}$ *for* $0 \le i \le r$ *with the following property. For any* $\lambda \in \overline{\mathbb{F}}_q^{(r+1)(n+1)}$ *with* $A(\lambda) \ne 0$, *the linear forms* $(Y_0, \dots, Y_r) := \lambda X$ *satisfy the following conditions*:

(i) *the map* $\pi_r : V \to \mathbb{P}^r$ *defined by* $Y_0, \dots, Y_r$ *is a finite morphism*,
(ii) $\overline{\mathbb{F}}_q(Y_0, \dots, Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$ *is a separable field extension*,
(iii) *if* $Y_{r+1}, \dots, Y_n$ *denote the linear forms of Lemma* 4.1, *then* $Y_0, \dots, Y_n$ *are* $\overline{\mathbb{F}}_q$*-linearly independent.*

Proof. Let $\Lambda^{(r+1)}$ be a vector of $n+1$ new indeterminates and let $\widetilde{Y}_{r+1} := \Lambda^{(r+1)}X$. Let $P_V \in \overline{\mathbb{F}}_q[\Lambda, \Lambda^{(r+1)}, \widetilde{Y}_0, \dots, \widetilde{Y}_{r+1}]$ be the Chow form of V (cf. [26], [12]). It is a well-known fact that P_V is an irreducible polynomial in $\overline{\mathbb{F}}_q[\Lambda, \Lambda^{(r+1)}, \widetilde{Y}_0, \dots, \widetilde{Y}_{r+1}]$ which is separable in each of the variables $\widetilde{Y}_0, \dots, \widetilde{Y}_{r+1}$ and homogeneous in $\widetilde{Y}_0, \dots, \widetilde{Y}_{r+1}$ and in each group of variables $\Lambda^{(i)}$ for $0 \le i \le r+1$. Furthermore, P_V satisfies the following degree estimates:

- $\deg_{\widetilde{Y}} P_V = \deg_{\widetilde{Y}_{r+1}} P_V = \delta$,
- $\deg_{\Lambda^{(i)}} P_V \le \delta$ for $0 \le i \le r+1$.

Considering the expansion of P_V in powers of $\widetilde{Y}_{r+1}$, let $\widetilde{A}_1 \in \overline{\mathbb{F}}_q[\Lambda, \Lambda^{(r+1)}]$ be the nonzero polynomial which arises as the coefficient of the monomial $\widetilde{Y}_{r+1}^{\delta}$ in P_V, and let $\widetilde{A}_2 \in \overline{\mathbb{F}}_q[\Lambda, \Lambda^{(r+1)}, \widetilde{Y}_0, \dots, \widetilde{Y}_r]$ be the coefficient of a monomial $\widetilde{Y}_{r+1}^{j_0}$, with j_0 not divisible by the characteristic of $\mathbb{F}_q$. Let $A_1, A_2 \in \overline{\mathbb{F}}_q[\Lambda]$ be nonzero coefficients of $\widetilde{A}_1$ and $\widetilde{A}_2$, respectively, where we consider $\widetilde{A}_1$ as an element of $\overline{\mathbb{F}}_q[\Lambda][\Lambda^{(r+1)}]$ and $\widetilde{A}_2$ as an element of $\overline{\mathbb{F}}_q[\Lambda][\Lambda^{(r+1)}, \widetilde{Y}_0, \dots, \widetilde{Y}_r]$. The above estimates imply that both A_1 and A_2 have degree at most δ in each group of variables $\Lambda^{(i)}$ for $0 \le i \le r+1$.

Let $\lambda \in \overline{\mathbb{F}}_q^{(r+1)(n+1)}$ be any point for which $A_1(\lambda) \ne 0$ and $A_2(\lambda) \ne 0$, and define the $r+1$ linear forms $(Y_0, \dots, Y_r) := \lambda X$. Since $\widetilde{A}_1(\lambda, \Lambda^{(r+1)})$ and $\widetilde{A}_2(\lambda, \Lambda^{(r+1)}, Y_0, \dots, Y_r)$ are nonzero polynomials, we deduce the existence of $\overline{\mathbb{F}}_q$-linearly independent vectors $w_0, \dots, w_n \in \overline{\mathbb{F}}_q^{n+1}$ such that $P_V(\lambda, w_j, Y_0, \dots, Y_r, \widetilde{Y}_{r+1}) \in \overline{\mathbb{F}}_q[Y_0, \dots, Y_r][\widetilde{Y}_{r+1}]$ is a nonzero, monic (up to elements of $\overline{\mathbb{F}}_q$) and separable polynomial, for every $0 \le j \le n$.

If we define $\ell_j := w_j X$ for $0 \le j \le n$, it turns out that the polynomial $P_V(\lambda, w_j, Y_0, \dots, Y_r, \ell_j)$ yields an integral dependence equation for the coordinate function induced by ℓ_j in the ring extension $\mathbb{F}_q[Y_0, \dots, Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$. On the other hand, $P_V(\lambda, w_j, Y_0, \dots, Y_r, \ell_j)$ also yields a separable equation for ℓ_j in the field extension $\overline{\mathbb{F}}_q(Y_0, \dots, Y_r) \hookrightarrow \overline{\mathbb{F}}_q(V)$. Since $\overline{\mathbb{F}}_q[\ell_0, \ell_1, \dots, \ell_n] = \overline{\mathbb{F}}_q[X_0, \dots, X_n]$, we conclude that conditions (i) and (ii) are satisfied.

Finally, to prove (iii), let $A_3 \in \overline{\mathbb{F}}_q[\Lambda]$ be the nonzero determinant of the matrix defined by the vectors of the coefficients of the linear forms $\widetilde{Y}_0, \dots, \widetilde{Y}_r$,

$Y_{r+1},\dots,Y_n$, where $Y_{r+1},\dots,Y_n$ are the linear forms of the statement of Lemma 4.1. It is clear that if $A_3(\lambda)\neq 0$ and we define $(Y_0,\dots,Y_r):=\lambda X$, then condition (iii) will be satisfied. Observe that $\deg_{\Lambda^{(i)}} A_3\leq 1$ for $0\leq i\leq r$.

Define $A:=A_1A_2A_3$; our previous arguments show that A satisfies the requirements of the statement of the proposition. ■

From Lemma 4.1 and Proposition 4.2 we deduce the main result of this section:

COROLLARY 4.3. *Let $q>2(n-r)d\delta+1$. Then there exist linear forms $Y_0,\dots,Y_r\in\mathbb{F}_q[X_0,\dots,X_n]$ satisfying the following conditions*:

(i) *the map $\pi_r:V\to\mathbb{P}^r$ defined by $Y_0,\dots,Y_r$ is a finite morphism*,
(ii) *the map $\pi_{r-1}:V\setminus\mathcal{U}\to\mathbb{P}^{r-1}$ defined by $Y_0,\dots,Y_{r-1}$ is a finite morphism*,
(iii) *$\overline{\mathbb{F}}_q(Y_0,\dots,Y_r)\hookrightarrow\overline{\mathbb{F}}_q(V)$ is a separable field extension*,
(iv) *$\overline{\mathbb{F}}_q(Y_0,\dots,Y_{r-1})\hookrightarrow\overline{\mathbb{F}}_q(\mathcal{C})$ is a separable field extension for every absolutely irreducible component $\mathcal{C}$ of $V\setminus\mathcal{U}$*,
(v) *the linear forms $Y_0,\dots,Y_r,Y_{r+1},\dots,Y_n$ are $\overline{\mathbb{F}}_q$-linearly independent.*

Proof. From Proposition 4.2 it follows that there exists a nonzero polynomial $A\in\overline{\mathbb{F}}_q[\Lambda]$ of degree at most $2\delta+1$ in each group of variables $\Lambda^{(i)}$ for $0\leq i\leq r+1$ such that, for every $\lambda\in\overline{\mathbb{F}}_q{}^{(r+1)(n+1)}$ with $A(\lambda)\neq 0$, defining $(Y_0,\dots,Y_r):=\lambda X$, we see that conditions (i), (iii) and (v) are satisfied.

Let $V\setminus\mathcal{U}=\bigcup_{j=1}^{s}\mathcal{C}_j$ be the decomposition of $V\setminus\mathcal{U}$ into absolutely irreducible components. We have $\dim\mathcal{C}_j=r-1$ for $1\leq j\leq s$. From the proof of Proposition 4.2 we conclude that for $1\leq j\leq s$ there exists a nonzero polynomial $A^{(j)}\in\overline{\mathbb{F}}_q[\Lambda]$ of degree at most $2\deg\mathcal{C}_j$ in each group of variables $\Lambda^{(i)}$ such that for every $\lambda\in\overline{\mathbb{F}}_q{}^{(r+1)(n+1)}$ with $A^{(j)}(\lambda)\neq 0$, the linear forms $(Y_0,\dots,Y_r):=\lambda X$ satisfy conditions (ii) and (iv) for $\mathcal{C}_j$.

Since $\sum_{j=1}^{s}\deg\mathcal{C}_j=\deg(V\setminus\mathcal{U})\leq(n-r)(d-1)\delta$, we conclude that the polynomial $A^*:=A\cdot A^{(1)}\cdots A^{(s)}$ has degree at most $2\delta+1+2(n-r)(d-1)\delta\leq 2(n-r)d\delta+1$ in each group of variables $\Lambda^{(i)}$, and for every $\lambda\in\overline{\mathbb{F}}_q{}^{(r+1)(n+1)}$ with $A^*(\lambda)\neq 0$, the linear forms $(Y_0,\dots,Y_r):=\lambda X$ satisfy conditions (i)–(v).

Let $a^{(0)}\in\overline{\mathbb{F}}_q[\Lambda^{(0)}]$ be a nonzero coefficient of A^*, considering A^* as a polynomial in $\overline{\mathbb{F}}_q[\Lambda^{(0)}][\Lambda^{(1)},\dots,\Lambda^{(r)}]$. By (6) it follows that $a^{(0)}$ has at most $(2(n-r)d\delta+1)q^n$ zeros in $\mathbb{F}_q^{n+1}$. Since $q>2(n-r)d\delta+1$, we conclude that there exists $\lambda^{(0)}\in\mathbb{F}_q^{n+1}$ such that $A^*(\lambda^{(0)},\Lambda^{(1)},\dots,\Lambda^{(r)})$ is a nonzero polynomial. Arguing in a similar way, we successively deduce the existence of $\lambda^{(1)},\dots,\lambda^{(r)}\in\mathbb{F}_q^{n+1}$ such that $A^*(\lambda)\neq 0$ for $\lambda:=(\lambda^{(0)},\dots,\lambda^{(r)})$. The linear forms $(Y_0,\dots,Y_r):=\lambda X$ satisfy the conditions of the corollary. ■

We remark that, from the proof of Corollary 4.3, we deduce that there exist linear forms $Y_0,\dots,Y_r\in\mathbb{F}_q[X]$ such that the map $\pi_r:V\to\mathbb{P}^r$ defined by $Y_0, \ldots, Y_r$ is a finite morphism for $q > \delta - 1$. This is also proved in [18, Proposition 2.3].

5. An effective second Bertini theorem. This section is devoted to establishing an effective version of the second Bertini theorem suitable for our requirements. The second Bertini theorem (see, e.g., [31, II.6.2, Theorem 2]) asserts that, given a dominant morphism of irreducible varieties $f : V_1 \to V_2$ defined over a field of characteristic zero with V_1 nonsingular, there exists a dense open set U of V_2 such that the fiber $f^{-1}(y)$ is nonsingular for every $y \in U$. Our effective version holds without any restriction on the characteristic of the ground field and gives an upper bound on the degree of the subvariety of points of V_2 defining singular fibers. An effective version of a weak form of the Bertini theorem is given in [1]. Nevertheless, the bound given there is exponentially higher than ours and therefore is not suitable for our purposes.

Let notations and assumptions be as in Section 4. Assume that $q > 2(n-r)d\delta + 1$, and let $Y_0, \ldots, Y_n \in \mathbb{F}_q[X_0, \ldots, X_n]$ be linear forms satisfying conditions (i)–(v) of Corollary 4.3. Consider the linear mappings $\pi_r : V \to \mathbb{P}^r$ and $\pi_{r-1} : V \to \mathbb{P}^{r-1}$ defined by $\pi_r(x) := (Y_0(x) : \cdots : Y_r(x))$ and $\pi_{r-1}(x) := (Y_0(x) : \cdots : Y_{r-1}(x))$. Then π_r is a well-defined finite morphism, π_{r-1} is well-defined outside (the 0-dimensional subvariety) $\pi_r^{-1}(0 : \cdots : 0 : 1)$, and the choice of the linear forms $Y_0, \ldots, Y_{r-1}$ implies that $\pi_{r-1}^{-1}(y)$ is a pure dimensional curve on V for every $y \in \mathbb{P}^{r-1}$. We shall prove that there exists a proper subvariety W of $\mathbb{P}^{r-1}$ such that $\pi_{r-1}^{-1}(y)$ is nonsingular for every $y \notin W$, and we shall provide an upper bound for the degree of W.

For a given $x \in V$ and $y := \pi_{r-1}(x) \in \mathbb{P}^{r-1}$, we denote by T_xV and $T_y\mathbb{P}^{r-1}$ the respective tangent spaces. Further, we denote by $d_x\pi_{r-1} : T_xV \to T_y\mathbb{P}^{r-1}$ the differential of π_{r-1} at x and for any $y \in \mathbb{P}^{n-1}$ we set $V_y := \pi_{r-1}^{-1}(y)$. We start with the following lemma, which yields a sufficient condition for the nonsingularity of the fiber V_y.

Lemma 5.1. *Let y be a point of $\mathbb{P}^{r-1}$ such that for any point $x \in V_y$ the following conditions are satisfied*:

(i) *x is a regular point of V*,
(ii) *$d_x\pi_{r-1}$ is surjective.*

Then V_y is a nonsingular curve.

Proof. Let x be an arbitrary point of V_y. Since the composite of $T_xV_y \hookrightarrow T_xV$ with $d_x\pi_{r-1}$ is the zero map, the tangent space T_xV_y is contained in the kernel of $d_x\pi_{r-1}$. By the surjectivity of $d_x\pi_{r-1}$ the dimension of the image of $d_x\pi_{r-1}$ equals $r-1$. Hence

$$\dim T_xV_y \le \dim \operatorname{Ker} d_x\pi_{r-1} = \dim T_xV - \dim T_y\mathbb{P}^{r-1} = 1,$$

where the last equality follows from the fact that x is a nonsingular point of V. Since V_y is of pure dimension 1, we conclude that $\dim T_x V_y = 1$ and therefore x is regular point of V_y. This shows that V_y is nonsingular. ∎

Next we give a sufficient condition for the surjectivity of $d_x\pi_{r-1}$.

Lemma 5.2. *Let $\mathcal{U} = \{x \in V : \det(\partial F_i/\partial Y_{r+j})_{1\le i,j\le n-r}(x) \neq 0\}$ be the nonempty Zariski open subset of V of Lemma 4.1. Then $d_x\pi_{r-1}$ is surjective for every $x \in \mathcal{U} \setminus \pi_r^{-1}(0 : \cdots : 0 : 1)$.*

Proof. Let x be an arbitrary point of $\mathcal{U}$. Then x is a regular point of V, which implies that T_xV has dimension r. Therefore, from the identity $\dim \operatorname{Ker} d_x\pi_{r-1} = r - \dim \operatorname{Im} d_x\pi_{r-1}$, we conclude that the surjectivity of $d_x\pi_{r-1}$ is equivalent to the condition $\dim \operatorname{Ker} d_x\pi_{r-1} = 1$. Suppose without loss of generality that $Y_0(x) \neq 0$. Then we may assume that we are in an affine situation, and π_{r-1} is locally defined by $\pi_{r-1}(x) := (Y_1(x), \ldots, Y_{r-1}(x))$. Now $\operatorname{Ker} d_x\pi_{r-1}$ is the affine linear space defined by the equations $\sum_{j=1}^{n}(\partial F_i/\partial Y_j)(x)(Y_j - Y_j(x)) = 0$ $(1 \le i \le n-r)$, $Y_k - Y_k(x) = 0$ $(1 \le k \le r-1)$. From the definition of $\mathcal{U}$ we see that these equations are $\overline{\mathbb{F}}_q$-linearly independent, which proves that $\operatorname{Ker} d_x\pi_{r-1}$ has dimension 1. This completes the proof. ∎

Now we are ready to state our effective version of the second Bertini theorem.

Theorem 5.3. *There exists a proper subvariety $W \subset \mathbb{P}^{r-1}$ of degree at most $2(n-r)^2(d-1)^2\delta$ such that the fiber V_y is a nonsingular curve of degree at most δ for every $y \notin W$.*

Proof. Let Z be the proper closed subset of V consisting of the points of V where $d_x\pi_{r-1}$ is not surjective, and let V_{reg} and V_{sing} denote the sets of regular and singular points of V, respectively. Then Z can be expressed as

$$Z = (Z \cap V_{\mathrm{reg}}) \cup (Z \cap V_{\mathrm{sing}}) = \overline{Z \cap V_{\mathrm{reg}}} \cup (Z \cap V_{\mathrm{sing}}),$$

where $\overline{Z \cap V_{\mathrm{reg}}}$ denotes the Zariski closure of $Z \cap V_{\mathrm{reg}}$. From Lemma 5.2 we conclude that $Z \subset V \setminus \mathcal{U}$, i.e.,

$$Z \subset \{x \in V : F_1(x) = \cdots = F_{n-r}(x) = \det(\partial F_i/\partial Y_{r+j})_{1\le i,j\le n-r}(x) = 0\}.$$

Since V is a normal variety, the set of singular points V_{sing} has codimension at least two in V.

Claim 1. *There exists a closed subset $Z_{\mathrm{sing}} \subset V$ of codimension two in V and degree bounded by $(n-r)^2(d-1)^2\delta$ such that $V_{\mathrm{sing}} \subset Z_{\mathrm{sing}}$.*

Proof of Claim 1. The Jacobian matrix $(\partial F_i/\partial X_j)_{1\le i\le n-r,\,1\le j\le n+1}$ has $N_r := \binom{n+1}{n-r}$ maximal minors $M_1, \ldots, M_{N_r}$. If $x \in V$ is a regular point, at least one of these minors is not zero at x. As a consequence we may choose $\gamma_1, \ldots, \gamma_{N_r} \in \overline{\mathbb{F}}_q$ such that $\sum_{j=1}^{N_r} \gamma_j M_j(x) \neq 0$. Setting $G := \sum_{j=1}^{n} \gamma_j M_j$, from the Jacobian criterion we see that $V_{\text{sing}} \subset V \cap \{G = 0\} \subset V$. Moreover, the absolute irreducibility of V implies that $V \cap \{G = 0\}$ is an equidimensional projective variety of dimension $r - 1$.

Consider now the decomposition $V \cap \{G = 0\} = \bigcup_{i=1}^{s} \mathcal{C}_i$ into absolutely irreducible components. Since V_{sing} has dimension at most $r - 2$, it follows that $\mathcal{C}_i \cap V_{\text{reg}}$ is nonempty for $1 \leq i \leq s$. Hence, arguing as above, we conclude that there exist $x_i \in V_{\text{reg}} \cap \mathcal{C}_i$ for $1 \leq i \leq s$ and $\widetilde{\gamma}_1, \ldots, \widetilde{\gamma}_{N_r} \in \overline{\mathbb{F}}_q$ such that no x_i is a zero of the polynomial $H := \sum_{j=1}^{N_r} \widetilde{\gamma}_j M_j$. Observe that both G and H have degree at most $(n - r)(d - 1)$.

We define $Z_{\text{sing}} := V \cap \{G = 0, H = 0\}$. By construction, $V_{\text{sing}} \subset Z_{\text{sing}} \subset V$ and Z_{sing} is an equidimensional projective variety of dimension $r - 2$. Furthermore, from the Bézout inequality (4) we conclude that $\deg Z_{\text{sing}} \leq \delta \deg G \deg H \leq (n - r)^2(d - 1)^2\delta$. This finishes the proof of our claim.

Claim 2. *There exists a proper closed subset $Z_{\text{reg}} \subset V$ of degree bounded by $(n - r)^2(d - 1)^2\delta$ such that $Z \cap V_{\text{reg}} \subset Z_{\text{reg}}$ and $\pi_{r-1}(Z_{\text{reg}})$ is a proper closed subset of $\mathbb{P}^{r-1}$.*

Proof of Claim 2. We consider separately the cases $\dim \overline{Z \cap V_{\text{reg}}} = r - 1$ and $\dim \overline{Z \cap V_{\text{reg}}} < r - 1$.

First, suppose that $\overline{Z \cap V_{\text{reg}}}$ has dimension $r - 1$. Let $\overline{Z \cap V_{\text{reg}}} = \bigcup_{i=1}^{t} \mathcal{D}_i$ be the decomposition into absolutely irreducible components. We are going to prove that the image of each $\mathcal{D}_i$ under π_{r-1} is a proper closed subset of $\mathbb{P}^{r-1}$. For components having dimension less than $r - 1$ this is clear, hence we only have to deal with components of dimension $r - 1$.

Assume that there exists an irreducible component $\mathcal{D}_i$ of $\overline{Z \cap V_{\text{reg}}}$ of dimension $r - 1$ for which $\pi_{r-1}(\mathcal{D}_i) = \mathbb{P}^{r-1}$. Since $\mathcal{D}_i \subset Z \subset V \setminus \mathcal{U}$, and $V \setminus \mathcal{U}$ has dimension $r - 1$, it follows that $\mathcal{D}_i$ is an absolutely irreducible component of $V \setminus \mathcal{U}$, and Corollary 4.3 implies that the field extension $\overline{\mathbb{F}}_q(Y_0, \ldots, Y_{r-1}) \hookrightarrow \overline{\mathbb{F}}_q(\mathcal{D}_i)$ is separable. Applying, e.g., [31, II.6.2, Lemma 2], we conclude that there exists a nonempty Zariski open subset $\mathcal{O}_i \subset \mathcal{D}_i$ such that $d_x\pi_{r-1}$ is surjective for every $x \in \mathcal{O}_i$, contrary to $\mathcal{D}_i \subset Z$. This shows that $\pi_{r-1}(\mathcal{D}_i)$ is a proper closed subset of $\mathbb{P}^{r-1}$ for every $1 \leq i \leq t$.

Let $M(x)$ denote the Jacobian matrix of $F_1, \ldots, F_{n-r}, Y_0, \ldots, Y_{r-1}$ with respect to the variables $X_0, \ldots, X_n$ evaluated at x. A point $x \in V_{\text{reg}}$ belongs to Z if and only if $M(x)$ does not have full rank n. If $x \in V_{\text{reg}}$ is a point for which $d_x\pi_{r-1}$ is surjective (for instance, x can be chosen in the nonempty open set $\mathcal{U}$ of Lemma 5.2), the matrix $M(x)$ has full rank n, and hence it has at least one nonzero $n \times n$ minor. Denoting by $M^{(1)}, \ldots, M^{(n+1)}$ the maximal minors of M, we define the polynomial $\widetilde{G} := \sum_{j=1}^{n+1} \eta_j M^{(j)}$, where $\eta_1, \ldots, \eta_{n+1}$ are elements of $\overline{\mathbb{F}}_q$ such that $\widetilde{G}(x) \neq 0$. It follows that $V \cap \{\widetilde{G} = 0\}$ is an equidimensional projective variety of dimension $r - 1$.

Furthermore, by our characterization of the points of $Z \cap V_{\mathrm{reg}}$ we easily conclude that $Z \cap V_{\mathrm{reg}} \subset V \cap \{\widetilde{G} = 0\}$ and so $\overline{Z \cap V_{\mathrm{reg}}} \subset V \cap \{\widetilde{G} = 0\}$.

Let $V \cap \{\widetilde{G} = 0\} = \bigcup_{i=1}^{t'} \mathcal{E}_i$ be the decomposition into absolutely irreducible components. As before, given that $\dim V_{\mathrm{sing}} \leq r-2$ and that each $\mathcal{E}_i$ has dimension $r-1$, the intersection $\mathcal{E}_i \cap V_{\mathrm{reg}}$ is nonempty for each $1 \leq i \leq t'$. Assume that $\mathcal{E}_1, \ldots, \mathcal{E}_{t''}$ are all the components contained in $\overline{Z \cap V_{\mathrm{reg}}}$ for certain $t'' \leq t'$. This means that for $t''+1 \leq i \leq t'$ there exists a point $x_i \in \mathcal{E}_i \cap (V_{\mathrm{reg}} \setminus Z)$. Hence, arguing as for Claim 1 we conclude that there exist $\widetilde{\eta}_1, \ldots, \widetilde{\eta}_{n+1} \in \overline{\mathbb{F}}_q$ such that no x_i is a root of the polynomial $\widetilde{H} := \sum_{j=1}^{n+1} \widetilde{\eta}_j M_j$.

We consider the variety $Z_{\mathrm{reg}} := V \cap \{\widetilde{G} = 0, \widetilde{H} = 0\}$. By construction, $Z \cap V_{\mathrm{reg}} \subset Z_{\mathrm{reg}} \subset V$ and Z_{reg} is a projective variety of dimension $r-1$. Furthermore, Z_{reg} can be expressed as $Z_{\mathrm{reg}} = \bigcup_{i=1}^{t''} \mathcal{E}_i \cup \widetilde{Z}$ with $\dim \widetilde{Z} \leq r-2$ and $\dim \pi_{r-1}(\mathcal{E}_i) \leq r-2$ for $1 \leq i \leq t''$, which proves that $\pi_{r-1}(Z_{\mathrm{reg}})$ is strictly contained in $\mathbb{P}^{r-1}$. Finally, from the Bézout inequality (4) we conclude that $\deg Z_{\mathrm{reg}} \leq \delta \deg \widetilde{G} \deg \widetilde{H} \leq (n-r)^2(d-1)^2\delta$. This finishes the proof of our claim in the case $\dim \overline{Z \cap V_{\mathrm{reg}}} = r-1$.

The analysis of the case $\dim \overline{Z \cap V_{\mathrm{reg}}} < r-1$ is simpler since we do not have to deal with components of $\overline{Z \cap V_{\mathrm{reg}}}$ of dimension $r-1$. Therefore, choosing the polynomials $\widetilde{G}, \widetilde{H}$ as above guarantees that $\dim \pi_{r-1}(Z_{\mathrm{reg}}) \leq r-2$. This finishes the proof of Claim 2.

From the claims above we know that $Z \cup V_{\mathrm{sing}} \subset Z_{\mathrm{sing}} \cup Z_{\mathrm{reg}}$ and $Z_{\mathrm{sing}} \cup Z_{\mathrm{reg}}$ is a proper subvariety of V of dimension $r-1$ and degree at most $2(n-r)^2(d-1)^2\delta$. Furthermore, $W := \pi_{r-1}(Z_{\mathrm{reg}} \cup Z_{\mathrm{sing}})$ is a proper subvariety of $\mathbb{P}^{r-1}$ which, by Lemma 2.1, has degree at most $2(n-r)^2(d-1)^2\delta$. For $y \in \mathbb{P}^{r-1} \setminus W$ every $x \in V_y$ is a regular point of V not belonging to Z. Then Lemma 5.1 shows that V_y is a nonsingular curve of V, which by (4) has degree at most δ. This finishes the proof of the theorem. ∎

Since the curve V_y is a nonsingular projective complete intersection for $y \notin W$, Hartshorne's connectedness theorem (see, e.g., [17, VI, Theorem 4.2]) shows that V_y is connected, which implies that V_y is absolutely irreducible.

6. The estimate. In this section we obtain an estimate on the number of q-rational points of a normal complete-intersection $\mathbb{F}_q$-variety $V \subset \mathbb{P}^n$ of dimension r, degree δ and multidegree $\mathbf{d} := (d_1, \ldots, d_{n-r})$. Our estimate relies on the following estimate, due to P. Deligne ([7]), on the number of q-rational points of a nonsingular complete-intersection $\mathbb{F}_q$-curve $\mathcal{C} \subset \mathbb{P}^n$ of degree δ and multidegree $\mathbf{d}$:

$$\big||\mathcal{C}(\mathbb{F}_q)| - p_1\big| \leq b_1'(n, \mathbf{d})q^{1/2}, \tag{7}$$

where $b_1'(n, \mathbf{d})$ denotes the first primitive Betti number of any nonsingular complete intersection $\mathcal{C} \subset \mathbb{P}^n$ of dimension 1 and multidegree $\mathbf{d}$. We have $b_1'(n, \mathbf{d}) \leq (\delta - 1)(\delta - 2)$, with equality if and only if $n = 2$.

Set $d := \max_{1 \leq i \leq n-r} d_i$ and assume that $q > 2(n-r)d\delta + 1$. Then there exist linear forms $Y_0, \ldots, Y_n \in \mathbb{F}_q[X_0, \ldots, X_n]$ satisfying conditions (i)–(v) of Corollary 4.3. We recall that the choice of $Y_0, \ldots, Y_{r-1}$ implies that $V_y := \pi_{r-1}^{-1}(y)$ is a pure dimensional curve on V for every $y \in \mathbb{P}^{r-1}$.

Denote by N_y the number of q-rational points of V_y for any $y \in \mathbb{P}^{r-1}(\mathbb{F}_q)$. We are going to estimate $|V(\mathbb{F}_q)|$ in terms of the quantities N_y. For this purpose, we apply our effective version of the second Bertini theorem (Theorem 5.3), which asserts that there exists a variety $W \subset \mathbb{P}^{r-1}$ of dimension at most $r-2$ such that for every $y \in \mathbb{P}^{r-1} \setminus W$ the fiber V_y is a nonsingular complete intersection of degree at most δ. Since V_y is an $\mathbb{F}_q$-curve for every $y \in \mathbb{P}^{r-1}(\mathbb{F}_q)$, for each y in $(\mathbb{P}^{r-1} \setminus W)(\mathbb{F}_q)$ we can estimate N_y by means of (7). We have the following result:

Theorem 6.1. *Let $V \subset \mathbb{P}^n$ be a normal complete-intersection $\mathbb{F}_q$-variety of dimension r, degree $\delta \geq 2$ and multidegree* $\mathbf{d}$. *For* $q > 2(n-r)d\delta + 1$,

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq b_1'(n-r+1, \mathbf{d})q^{r-1/2} + (b_1'(n-r+1, \mathbf{d}) + \delta \deg W + 2)q^{r-1},$$

where $W \subset \mathbb{P}^{r-1}$ is the variety of the statement of Theorem 5.3.

Proof. We begin by expressing $|V(\mathbb{F}_q)|$ in terms of the numbers N_y with $y \in \mathbb{P}^{r-1}(\mathbb{F}_q)$:

$$|V(\mathbb{F}_q)| = \sum_{y \in \mathbb{P}^{r-1}(\mathbb{F}_q)} N_y + e, \tag{8}$$

where e is the number of q-rational points of $\pi_r^{-1}(0 : \cdots : 0 : 1)$. Since π_r is a finite morphism and $\mathbb{P}^r$ is a normal variety, the cardinality of every fiber of π_r is upper bounded by δ. In particular, $e \leq \delta$.

Subtracting p_r from both sides of (8) and using the identity $p_r = p_1 p_{r-1} - q p_{r-2}$, we obtain:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq \sum_{y \in \mathbb{P}^{r-1}(\mathbb{F}_q)} |N_y - p_1| + q p_{r-2} + \delta. \tag{9}$$

We decompose the first summand of the right-hand side of (9) as

$$\sum_{y \in \mathbb{P}^{r-1}(\mathbb{F}_q)} |N_y - p_1| = \sum_{y \notin W(\mathbb{F}_q)} |N_y - p_1| + \sum_{y \in W(\mathbb{F}_q)} |N_y - p_1|.$$

Thus, we have to estimate the quantities $|N_y - p_1|$ in two different cases: for y belonging to $W(\mathbb{F}_q)$ and for y belonging to $(\mathbb{P}^{r-1} \setminus W)(\mathbb{F}_q)$.

For any y in $W(\mathbb{F}_q)$, the number N_y is less than or equal to δp_1. Hence, taking into account that $\delta \geq 2$, we obtain $|N_y - p_1| \leq (\delta - 1)p_1$. From

Proposition 3.1 we have $|W(\mathbb{F}_q)| \leq \deg W p_{r-2}$, and thus

$$\sum_{y \in W(\mathbb{F}_q)} |N_y - p_1| \leq (\delta - 1)p_1 \cdot \deg W p_{r-2} \leq \delta \deg W q^{r-1}. \tag{10}$$

On the other hand, if $y \in (\mathbb{P}^{r-1} \setminus W)(\mathbb{F}_q)$, Theorem 5.3 shows that the fiber V_y is a nonsingular complete-intersection $\mathbb{F}_q$-curve in $\mathbb{P}^{n-r+1}$ of degree at most δ and multidegree at most $\mathbf{d}$. By (7) we obtain the estimate $|N_y - p_1| \leq b_1'(n-r+1, \mathbf{d})q^{1/2}$, where $b_1'(n-r+1, \mathbf{d})$ is the corresponding Betti number. Hence, writing $b_1' := b_1'(n-r+1, \mathbf{d})$, we have

$$\sum_{y \notin W(\mathbb{F}_q)} |N_y - p_1| \leq b_1' q^{r-1/2} + b_1' p_{r-2} q^{1/2} \leq b_1' q^{r-1/2} + b_1' q^{r-1}. \tag{11}$$

Combining (9)–(11) and taking into account that $qp_{r-2} + \delta \leq 2q^{r-1}$, we easily deduce the statement of the theorem. ■

Taking into account the upper bound $\deg W \leq 2(n-r)^2(d-1)^2\delta$ of Theorem 5.3, we deduce the following corollary:

Corollary 6.2. *With notations and assumptions as in Theorem* 6.1, *we have*:

$$\big||V(\mathbb{F}_q)| - p_r\big| \leq (\delta - 1)(\delta - 2)q^{r-1/2} + 2(n-r)^2 d^2 \delta^2 q^{r-1}.$$

In order to illustrate the comparison between the result of Corollary 6.2 and (2) we briefly comment on an application of this kind of estimates in the setting of cryptography.

Boolean functions $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ are used in cryptography in order to design algorithms for block ciphering. It is important for such functions to possess a high resistance to differential cryptanalysis. In order to analyze the resistance of such functions to differential attacks, Nyberg [23] has introduced the notion of almost perfect nonlinearity (APN).

Let $q := 2^m$. In [25, Corollaire 3.1], F. Rodier shows that, if a given function $f : \mathbb{F}_q \to \mathbb{F}_q$ is APN, then a certain absolutely irreducible nonsingular projective $\mathbb{F}_q$-surface V_f of degree δ associated to f has at most $3((\delta-3)q+1)$ q-rational points. Then, as a consequence of [9, Corollary 7.3], he shows that for $m \geq 6$ and $\delta < q^{1/6} + 3.9$ the function f is not APN [25, Théorème 4.1].

By means of our estimates we may strengthen this conclusion. Indeed, from Corollary 6.2 we deduce that, for $q > 2\delta^2 + 1$,

$$|V_f(\mathbb{F}_q)| \geq p_2 - (\delta - 1)(\delta - 2)q^{3/2} - 2\delta^4 q.$$

Therefore, from [25, Corollaire 3.1] it follows that if $q > 2\delta^2 + 1$ and

$$p_2 - (\delta - 1)(\delta - 2)q^{3/2} - 2\delta^4 q > 3((\delta - 3)q + 1),$$

then f is not APN. As a consequence, we see that for $q \geq 4\delta^4$, the function f is not APN, which significantly improves [25, Théorème 4.1].

References

[1] E. Ballico, *An effective Bertini theorem over finite fields*, Adv. Geom. 3 (2003), 361–363.

[2] A. Bogdanov, *Pseudorandom generators for low degree polynomials*, in: H. N. Gabow and R. Fagin (eds.), Proc. 37th Annual ACM Symposium on Theory of Computing (Baltimore, MD, 2005), ACM, New York, 2005, 21–30.

[3] 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.

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

[5] F. Catanese, *Chow varieties, Hilbert schemes, and moduli spaces of surfaces of general type*, J. Algebraic Geom. 1 (1992), 561–595.

[6] V. Danilov, *Algebraic varieties and schemes*, in: I. R. Shafarevich (ed.), Algebraic Geometry I, Encyclopaedia Math. Sci. 23, Springer, Berlin, 1994, 167–307.

[7] P. Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. 43 (1974), 273–307.

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

[9] 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.

[10] —, —, *Number of solutions of equations over finite fields and a conjecture of Lang and Weil*, in: A. K. Agarwal *et al.* (eds.), Number Theory and Discrete Mathematics (Chandigarh, 2000), Hindustan Book Agency, New Delhi, 2002, 269–291.

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

[12] W. Hodge and D. Pedoe, *Methods of Algebraic Geometry*, Vol. II, Cambridge Univ. Press, Cambridge, 1968.

[13] C. Hooley, *On the number of points on a complete intersection over a finite field*, J. Number Theory 38 (1991), 338–358.

[14] M.-D. Huang and Y.-C. Wong, *Solvability of systems of polynomial congruences modulo a large prime*, Comput. Complexity 8 (1999), 227–257.

[15] J.-R. Joly, *Équations et variétés algébriques sur un corps fini*, Enseign. Math. 19 (1973), 1–117.

[16] M. Knapp, *Artin's conjecture for forms of degree 7 and 11*, J. London Math. Soc. (2) 63 (2001), 268–274.

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

[18] G. Lachaud, *Number of points of plane sections and linear codes defined on algebraic varieties*, in: R. Pellikaan *et al.* (eds.), Arithmetic, Geometry and Coding Theory (Luminy, 1993), de Gruyter, Berlin, 1996, 77–104.

[19] S. Lang and A. Weil, *The number of points of varieties in finite fields*, Amer. J. Math. 76 (1954), 819–827.

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

[21] W. Luo, *Rational points on complete intersections over F_p*, Int. Math. Res. Not. 1999, no. 16, 901–907.

[22] H. Matsumura, *Commutative Algebra*, Benjamin, 1980.

[23] K. Nyberg, *Differentially uniform mappings for cryptography*, in: T. Helleseth (ed.), Advances in Cryptology—EUROCRYPT '93 (Lofthus, 1993), Lecture Notes in Comput. Sci. 765, Springer, 1994, 55–64.

[24] J.-F. Ragot, *Probabilistic absolute irreducibility test for polynomials*, J. Pure Appl. Algebra 172 (2002), 87–107.

[25] F. Rodier, *Borne sur le degré des polynômes presque parfaitement non-linéaires*, Preprint IML 2006–13, Institut de Mathématiques de Luminy, France, http://iml.univ-mrs.fr/editions/preprint2006/preprint2006.html, 2006.

[26] P. Samuel, *Méthodes d'algèbre abstraite en géométrie algébrique*, Springer, Berlin, 1967.

[27] W. Schmidt, *A lower bound for the number of solutions of equations over finite fields*, J. Number Theory 6 (1974), 448–480.

[28] —, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Math. 536, Springer, New York, 1976.

[29] J.-P. Serre, *Lettre à M. Tsfasman*, Astérisque 198-200 (1991), 351–353.

[30] I. R. Shafarevich, *Basic Algebraic Geometry*, Grundlehren Math. Wiss. 213, Springer, New York, 1974.

[31] —, *Basic Algebraic Geometry: Varieties in Projective Space*, Springer, Berlin, 1994.

[32] I. Shparlinski and A. Skorobogatov, *Exponential sums and rational points on complete intersections*, Mathematika 37 (1990), 201–208.

[33] A. Skorobogatov, *Exponential sums, the geometry of hyperplane sections, and some diophantine problems*, Israel J. Math. 80 (1992), 359–379.

[34] W. Vogel, *Lectures on Results on Bézout's Theorem*, Tata Inst. Fund. Res. Lecture Math. Phys. 74, Tata Inst. Fund. Res., Bombay, 1984.

Antonio Cafure
Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria, Pabellón I
1428 Buenos Aires, Argentina
E-mail: acafure@dm.uba.ar
and
Instituto de Desarrollo Humano
Universidad Nacional de General Sarmiento
J. M. Gutiérrez 1150
1613 Los Polvorines, Buenos Aires, Argentina

Guillermo Matera
Instituto de Desarrollo Humano
Universidad Nacional de General Sarmiento
J. M. Gutiérrez 1150
1613 Los Polvorines, Buenos Aires, Argentina
E-mail: gmatera@ungs.edu.ar
and
National Council of Science
and Technology (CONICET), Argentina

Received on 23.1.2006
and in revised form on 15.6.2007 (5129)