ISRAEL JOURNAL OF MATHEMATICS 80 (1992), 359–379

EXPONENTIAL SUMS, THE GEOMETRY OF HYPERPLANE SECTIONS, AND SOME DIOPHANTINE PROBLEMS

BY

ALEXEI N. SKOROBOGATOV

Institute for Problems of Information Transmission,
The Academy of Sciences of Russia,
19 Ermolovoi, Moscow 101447, Russia

ABSTRACT

We estimate exponential sums with additive character along an affine variety given by a system of homogeneous equations, with a homogeneous function in the exponent. The proof uses the results of Deligne's Weil Conjectures II and a generalization of Lefschetz hyperplane theorem to singular varieties. We apply our estimate to obtain an upperbound for the number of integer solutions of a system of homogeneous equations in a box. Another application is devoted to uniform distribution of solutions of a system of homogeneous congruences modulo a prime in the following sense: the portion of solutions in a box is proportional to the volume of the box, provided the box is not very small.

1. Introduction

This paper is devoted to the study of exponential sums of "homogeneous" type, and to their applications. In the first part we consider exponential sums along an affine variety given by a system of homogeneous equations, with a homogeneous function in the exponent (Section 3). Such a sum is often computed in terms of the number of points on the corresponding projective variety and on its hyperplane section (Lemma 3.1). To estimate it we obtain a version of Lefschetz hyperplane theorem valid on singular varieties (Theorem 2.1). To the best of our knowledge, this theorem, though its proof follows the proof of the classical Lefschetz theorem (see, e.g., [15], VI.7.1), does not seem to exist in the literature. The defect to which the classical Lefschetz theorem fails is measured by

Received November 25, 1991 and in revised form May 19, 1992

the dimension of the singular locus of the hyperplane section. Appealing to the Weil Conjectures II we obtain bounds for exponential sums which hold without a non-singularity condition (normally indispensable if one uses Deligne's formalism [5], cf. [3], 8.4, [12], 5.1.2, [1], 4.20, [13], 5.7.0).

Bounds of this kind can be used in various diophantine problems, notably in estimating the number of integer solutions of a system of homogeneous equations in a box, e.g., via the circle method of Hardy–Littlewood. This method gives an expression for the leading term, but it applies only if the number of variables is large in comparison with the number of equations and their degrees (cf. [16] and references therein). A simpler approach was suggested by Heath–Brown ([9], Appendix 2). Although less powerful, it has the advantage that the analytic part is more or less reduced to the Poisson summation formula, and that one encounters only exponential sums of prime modulus. The method results in the statement that the number of points in the square box of size a is at most a^β for a certain $\beta > 0$.

By a similar argument, Fujiwara ([7], Thm.1) proved that the solutions of a system of homogeneous congruences modulo prime p are uniformly distributed in the following sense: the portion of solutions in a box is proportional to the volume of the box, provided its size is at least p^γ for a certain $\gamma > 0$.

In the second part of this paper we employ the techniques of Heath–Brown and Fujiwara, using the estimates of exponential sums obtained in Section 3. To estimate β and γ we need to know "how many" hyperplane sections of our variety have singularities of given dimension. We summarize some information of this kind in Section 4, where the most general bound follows from the work of Zak [18]. The proofs of Theorems 5.1 and 5.2, where the bounds for the number of solutions in a box are deduced, closely follow the corresponding proofs in [7]. We reproduce them for the sake of completeness. However, now we are in an advantageous position with the results of Section 3 and 4 at our disposal. Consequently we improve and generalize the previous results ([9], App.2), [14], [2], [6], [7], [17] to (absolutely irreducible) varieties that need not be complete intersections, and may be singular, in other words, to (almost) arbitrary systems of homogeneous equations with integer coefficients.

We previously used the method of this paper for complete intersections [17], where the bounds can be made more precise.

This work has benefited from helpful discussions with Nicholas Katz and

Feodor Zak. I am grateful to Igor Shparlinskii and Serge Vlăduţ for their interest in this work.

I would like to express my gratitude to University of Puerto–Rico, University Paris-7, and the Mathematical Institute of the Technical University of Denmark, where parts of this work have been carried out.

2. A Generalization of Lefschetz Hyperplane Theorem to Singular Varieties

In this section k is an algebraically closed field. Let V be a vector space over k, $\dim(V) = N$, and let $\mathbb{P} = \mathbb{P}(V)$ be the corresponding projective space.

Let $X \subset \mathbb{P}$ be a closed irreducible scheme. We are interested in the following question: how different is the cohomology of X from that of the intersection of X with a hypersurface? Applying the Veronese embedding if necessary, we can restrict ourselves to considering hyperplane sections. So let us fix a linear form $f \in V^*$. Let $H \subset \mathbb{P}$ be a hyperplane given by $f = 0$, and let $X_H = X \cap H$ be the (scheme-theoretic) intersection of X and H. Let us denote by $\operatorname{Sing} X$ the minimal subscheme of X such that $X \setminus \operatorname{Sing} X$ is regular. Let $n = \dim(X)$, $s = \dim(\operatorname{Sing} X_H)$. We can assume without loss of generality that X is not contained in H. Then $s \leq \dim(X_H) = n - 1$.

We consider étale cohomology with coefficients in $\Lambda = \mathbb{Z}/\ell^m\mathbb{Z}$, where ℓ is a prime different from char (k).

THEOREM 2.1: *Let X be irreducible and not contained in H. For $j \geq n + s + 1$ there are canonical isomorphisms*

$$\Phi_j : H^j(X_H, \Lambda(-1)) \xrightarrow{\sim} H^{j+2}(X, \Lambda).$$

If $s \leq n - 2$ there is also a canonical surjection

$$\Phi_{n+s} : H^{n+s}(X_H, \Lambda(-1)) \twoheadrightarrow H^{n+s+2}(X, \Lambda).$$

If X and X_H are regular, Φ_j are the Gysin maps.

Proof: Let $U = X \setminus X_H$, $W = X_H \setminus \operatorname{Sing} X_H$, $V = X \setminus (\operatorname{Sing} X \cup \operatorname{Sing} X_H)$. Note that $H \cap \operatorname{Sing} X \subset \operatorname{Sing} X_H$, therefore $W \subset V$, $V \setminus W = U \setminus \operatorname{Sing} X$. Consider the natural embeddings:

$$\begin{array}{ccccc} X_H & \xrightarrow{i} & X & \xleftarrow{j} & U, \\ \operatorname{Sing} X_H & \xrightarrow{i'} & X_H & \xleftarrow{j'} & W, \\ W & \xrightarrow{i''} & V & \xleftarrow{j''} & V \setminus W. \end{array}$$

For a sheaf F we define

$$\dim\operatorname{supp}(F) := \sup\{\dim(x) | F_x \neq 0\},$$

where $x \hookrightarrow X$ is a closed point. It is clear that

$$R^o j_* \Lambda_U = \Lambda_X, \quad R^q j_* \Lambda_U = i^* R^q j_* \Lambda_U, \quad q \geq 1.$$

Let us remark that $i'' : W \hookrightarrow V$ is a closed embedding of smooth schemes. By the purity theorem for the smooth pair (W, V) of codimension one (cf. [15], VI.5.1 and VI.6.1) we have a canonical isomorphism:

$$i''^* R^1 j''_* \Lambda_{V \setminus W} = \Lambda(-1)_W.$$

We can compute this sheaf locally in any neighbourhood of W, for instance, in $X \setminus \operatorname{Sing} X_H = W \cup U$. Thus we obtain

$$j'^* i^* R^1 j_* \Lambda_U = \Lambda(-1)_W \tag{2.1}$$

Likewise, it follows from [loc.cit.] that $j'^* i^* R^q j_* \Lambda_U = 0$ for $q \geq 2$. By the affine Lefschetz theorem (cf. [15], VI 7.3) we have $\dim\operatorname{supp}(R^q j_* \Lambda_U) \leq n - q$, hence $\dim\operatorname{supp}(R^q j_* \Lambda_U) \leq \min\{s, n-q\}$ for $q \geq 2$. This implies

$$H^p(X, R^q j_* \Lambda_U) = 0, \quad p > \min\{2s, 2n - 2q\}, \quad q \geq 2. \tag{2.2}$$

Consider now the Leray spectral sequence for the morphism $j : U \longrightarrow X$, whose E_2 terms are of the form

$$H^p(X, R^q j_* \Lambda_U) \Longrightarrow H^{p+q}(U, \Lambda).$$

By (2.2) we obtain the long exact sequence

$$\begin{aligned} H^{n+s}(X_H, i^* R^1 j_* \Lambda_U) \longrightarrow\ & H^{n+s+2}(X, \Lambda) \longrightarrow H^{n+s+2}(U, \Lambda) \\ & \longrightarrow H^{n+s+1}(X_H, i^* R^1 j_* \Lambda_U) \longrightarrow \quad \ldots \end{aligned}$$

By the theorem on cohomological dimension of affine vareties (cf. [15], VI. 7.2) we have $H^q(U, \Lambda) = 0$ for $q > n$. Since $s \geq -1$ we obtain the canonical isomorphisms

$$\Phi_q : H^q(X_H, i^* R^1 j_* \Lambda_U) \xrightarrow{\sim} H^{q+2}(X, \Lambda), \quad q \geq n + s + 1, \tag{2.3}$$

and the canonical surjection

$$\Phi_{n+s} : H^{n+s}(X_H, i^*R^1j_*\Lambda_U) \twoheadrightarrow H^{n+s+2}(X, \Lambda). \tag{2.4}$$

If $i : X_H \hookrightarrow X$ is an embedding of smooth varieties, then (2.1) reduces to $i^*R^1j_*\Lambda_U = \Lambda(-1)_{X_H}$. Now $s = -1$, and we get the classical Gysin isomorphisms

$$H^q(X_H, \Lambda(-1)) \xrightarrow{\sim} H^{q+2}(X, \Lambda), \quad q \geq n,$$

and the classical Lefschetz hyperplane theorem follows. In the singular case we must do some extra work.

Let us show that

$$H^q(X_H, i^*R^1j_*\Lambda) = H^q(X_H, \Lambda(-1)), \quad q \geq 2s+2. \tag{2.5}$$

Consider the two long exact sequences in cohomology with compact supports:

$$\begin{array}{c} \to H^{q-1}(\operatorname{Sing} X_H, \Lambda(-1)) \to H^q_c(W, \Lambda(-1)) \to H^q(X_H, \Lambda(-1)) \\ \| \\ \to H^{q-1}(\operatorname{Sing} X_H, i''^*i^*R^1j_*\Lambda_U) \to H^q_c(W, j''^*i^*R^1j_*\Lambda_U) \to H^q(X_H, i^*R^1j_*\Lambda_U) \end{array}$$

where the vertical isomorphism comes from (2.1). Since $\dim(\operatorname{Sing} X_H) = s$, we obtain (2.5).

Now note that $s \leq \dim(X_H) = n-1$, hence $2s+2 \leq n+s+1$, and we can put together (2.3) and (2.5) to get the first claim of the theorem. If $s \leq \dim(X_H) - 1 = n-2$, hence $2s+2 \leq n+s$, then our second claim follows from (2.4) combined with (2.5). ∎

Remark: A slightly different proof may be given using the theory developed in SGA 7, Exposé 1, especially, Cor. 4.3 (cf. the proof of Thm. 2.3 of [17]).

COROLLARY 2.2: *Let X be irreducible and not contained in H. There are canonical isomorphisms*

$$\Phi_j : H^j(X_H, \mathbb{Q}_\ell(-1)) \xrightarrow{\sim} H^{j+2}(X, \mathbb{Q}_\ell), \quad j \geq n+s+1.$$

If $s \leq n-2$ there is a canonical surjection

$$\Phi_{n+s} : H^{n+s}(X_H, \mathbb{Q}_\ell(-1)) \twoheadrightarrow H^{n+s+2}(X, \mathbb{Q}_\ell).$$

Let us note than if k is an algebraic closure of a finite field $\mathbb{F}_q$, and X and H come from schemes defined over $\mathbb{F}_q$, then the maps Φ_j commute with the action of the Frobenius endomorphism.

3. Exponential Sums of "Homogeneous" Type

Let q be a prime power, $q = p^r$, $\mathbb{F}_q$ be the field with q elements. Let k be an algebraic closure of $\mathbb{F}_q$. We keep the notation of Section 2, except that we now assume that all objects are defined over $\mathbb{F}_q$, unless otherwise stated. Let $Y \subset \mathbf{A}^N$ be the affine cone over a projective variety $X \subset \mathbb{P}^{N-1}$, and $Y(\mathbb{F}_{q^i})$ be the set of $\mathbb{F}_{q^i}$–points of Y. Let G be a form of degree d with coefficients in $\mathbb{F}_q$. For each i fix a nontrivial additive character $\chi_i : \mathbb{F}_{q^i} \to \mathbb{C}^*$. We are interested in the following exponential sum:

$$S_i(Y,G) := \sum_{x\in Y(\mathbb{F}_{q^i})} \chi_i(G(x))$$

We shall refer to $S_i(Y,G)$ as to a "homogeneous" exponential sum. The condition that G and the defining equations of Y are homogeneous, is fairly strong, as revealed by the following elementary

PROPOSITION 3.1 ([17], 3.1): *Let X_G be the intersection of X with the hypersurface given by $G(x) = 0$. Then for i such that $q^i - 1$ is coprime with $d = deg(G)$, and for any non-trivial additive character $\chi_i : \mathbb{F}_{q^i} \to \mathbb{C}^*$, we have*

$$S_i(Y,G) = q^i \# X_G(\mathbb{F}_{q^i}) - \# X(\mathbb{F}_{q^i}) + 1. \tag{3.1}$$

Proof:

$$\begin{aligned} S_i(Y,G) &= 1 + (q^i-1)^{-1} \sum_{t\in\mathbb{F}_{q^i}} \sum_{x\in Y(\mathbb{F}_{q^i})\setminus\{0\}} \chi_i(G(tx)) \\ &= 1 - (q^i-1)^{-1}(\# Y(\mathbb{F}_{q^i}) - 1) \\ &+ (q^i-1)^{-1} \sum_{t\in\mathbb{F}_{q^i}} \sum_{x\in Y(\mathbb{F}_{q^i})\setminus\{0\}} \chi_i(t^d G(x)) \\ &= 1 - \# X(\mathbb{F}_{q^i}) + q^i \# X_G(\mathbb{F}_{q^i}). \qquad \blacksquare \end{aligned}$$

Note that under the assumptions of this proposition $S_i(Y,G)$ is an integer which does not depend on the choice of the character χ_i. The proposition is not true without the assumption $(d, q^i - 1) = 1$. For instance, let $i = 1$, $N = 2$, $X = \mathbb{P}^1$, $Y = \mathbf{A}^2$, $G(x,y) = x^{q-1} - y^{q-1}$. Then

$$S_1(\mathbf{A}^2, x^{q-1} - y^{q-1}) = |1 + (q-1)\chi_1(1)|^2.$$

Let us introduce some more notation. Define $X_G = X \cap \{G = 0\}$. Let $\overline{X}$ be the variety obtained from X by extension of the ground field to k, $\overline{X} = X \times_{\mathbb{F}_q} k$, and similarly, $\overline{X}_G = X_G \times_{\mathbb{F}_q} k$.

THEOREM 3.2: *Let $X \subset \mathbb{P}$ be an absolutely irreducible projective variety of dimension n over $\mathbb{F}_q$, and Y the affine cone over X. Let G be a homogeneous form in N variables with coefficients in $\mathbb{F}_q$ of degree d, $(d, q-1) = 1$, not vanishing identically on X. Then for i such that $(d, q^i - 1) = 1$, we have*

$$(3.2) \qquad |S_i(Y,G)| \leq Cq^{i\frac{n+s+2}{2}}.$$

where $s = \dim(\operatorname{Sing} X_G)$. The constant C depends only on the topology of $\overline{X}$ and $\overline{X}_G$:

$$(3.3) \qquad C \leq \sum_{j=0}^{n+s} \dim_{\mathbb{Q}_\ell}(H^j(\overline{X}, \mathbb{Q}_\ell)) + \sum_{j=0}^{n+s-2} \dim_{\mathbb{Q}_\ell}(H^j(\overline{X}_G, \mathbb{Q}_\ell)).$$

Proof: By the Grothendieck trace formula (cf. [15], VI.13.4) we have

$$\#X(\mathbb{F}_{q^i}) = \sum_{j=0}^{2n} (-1)^j Tr(F^i | H^j(\overline{X}, \mathbb{Q}_\ell)),$$

where F is the Frobenius endomorphism. Likewise, for X_G we have

$$q^i \# X_G(\mathbb{F}_{q^i}) = q^i \sum_{j=0}^{2n-2} (-1)^j Tr(F^i | H^j(\overline{X}_G, \mathbb{Q}_\ell)) =$$
$$= \sum_{j=0}^{2n-2} (-1)^j Tr(F^i | H^j(\overline{X}_G, \mathbb{Q}_\ell(-1))).$$

It follows from Corollary 2.2 that for $j \geq n+s+1$ we have

$$Tr(F^i | H^j(\overline{X}, \mathbb{Q}_\ell)) = Tr(F^i | H^{j-2}(\overline{X}_G, \mathbb{Q}_\ell(-1))).$$

According to ([4], 3.3.1) the eigenvalues of F^i on $H^j(\overline{X}, \mathbb{Q}_\ell)$ are algebraic numbers whose absolute values (with respect to any complex valuation) are at most $q^{ij/2}$. Now the theorem follows from Proposition 3.1 and Corollary 2.2. ∎

The bound (3.3) is certainly very rough. One may hope that the theorem is true without the assumption $(d, q^i - 1) = 1$.

Let us consider a particular case of the above result.

COROLLARY 3.3: *If $X = \mathbb{P}^{N-1}$, $Y = \mathbb{A}^N$, then for i such that $(d, q^i - 1) = 1$, we have*

$$|S_i(\mathbb{A}^N, G)| = |\sum_{x\in(\mathbb{F}_{q^i})^N} \chi_i(G(X))| \le Cq^{i\frac{N+s+1}{2}} \tag{3.4}$$

where C depends only on the topology of $\overline{Z}$, where $Z \subset \mathbb{P}$ is given by $G(x) = 0$; $s = \dim(\operatorname{Sing} Z)$.

If $(d,p) = 1$, and G has no singular point, that is, $\partial G/\partial x_1 = \ldots = \partial G/\partial x_n = 0$ has no solutions for $(x_1, \ldots, x_n) \in k^n \setminus \{0\}$, then $s = -1$, and we get the bound with the same exponent as that of Deligne ([3], 8.4). As an easy example shows, if we fix $s = \dim(\operatorname{Sing} Z)$, the exponent in Corollary 3.3 is in a sense best possible.

Example 3.4: Let $G(x_1, \ldots, x_N) = G_1(x_1, \ldots, x_{N-r-1})$ be a form which actually contains only variables $x_1, \ldots, x_{N-r-1}$. We further assume that the projective hypersurface Z_1 in $\mathbb{P}^{N-r-2}$ given by $G_1(x_1, \ldots, x_{N-r-1}) = 0$ is non-singular. In other words, $Z \subset \mathbb{P}^{N-1}$ given by $G(x_1, \ldots, x_N) = 0$ is a cone with the vertex $\mathbb{P}^r$ over the non-singular $N - r - 3$-dimentional variety Z_1. In particular, $s = \dim(\operatorname{Sing} Z) = r$. We have (under the usual assumption $(d, q^i - 1) = 1$):

$$\begin{aligned} S_i(\mathbb{A}^N, G) &= q^{i(s+1)} S_i(\mathbb{A}^{N-s-1}, G_1) \\ &= q^{i(s+1)}(q^i \# Z_1(\mathbb{F}_{q^i}) - q^{i(N-s-2)} - q^{i(N-s-3)} - \ldots - q^i) \\ &= q^{i(s+2)}(-1)^{N-s-3} Tr(F^i | H^{N-s-3}_{\text{prim}}(\overline{Z}_1, \mathbb{Q}_\ell)). \end{aligned}$$

where $H^{N-s-3}_{\text{prim}}(\overline{Z}_1, \mathbb{Q}_\ell)$ is the primitive part of $H^{N-s-3}(\overline{Z}_1, \mathbb{Q}_\ell)$. By [3] the eigenvalues of F^i on $H^{N-s-3}(\overline{Z}_1, \mathbb{Q}_\ell)$ have complex absolute values $q^{i(N-s-3)/2}$, thus in general it is not reasonable to expect an exponent in Corollary 3.3 better than $i\frac{N+s+1}{2}$.

Other corrollaries from Theorem 3.2 can also be deduced, for example, homogeneous singular analogs of [12], 5.1.2.

In case of varieties given by equations with integer coefficients, the bound (3.2) holds for all but a finite number of primes.

Let us consider an absolutely irreducible affine variety $Y \subset \mathbb{A}^N_{\mathbb{Q}}$ defined by a system of homogeneous equations with integer coefficients

$$F_1(x_1, \ldots, x_N) = \ldots = F_m(x_1, \ldots, x_N) = 0. \tag{3.5}$$

We denote $\delta_i := \deg(F_i)$, $i = 1, \ldots, m$. Let $G = G(x_1, \ldots, x_N)$ be a form of degree d with coefficients in $\mathbb{Z}$, not vanishing identically on Y. Define $Y_G \subset \mathbb{A}^N_{\mathbb{Q}}$ by the equations

$$(3.6) \qquad G(x_1, \ldots, x_N) = F_1(x_1, \ldots, x_N) = \ldots = F_m(x_1, \ldots, x_N) = 0.$$

$\operatorname{Sing} Y_G$ denotes the singular locus of Y_G.

THEOREM 3.5: *There exists a constant $C = C(N; d; \delta_1, \ldots, \delta_m)$, and a finite set $\mathcal{B}$ of primes depending on the forms $G, F_1, \ldots, F_m$, such that for any prime power p^i, $p \notin \mathcal{B}$ and $(d, p^i - 1) = 1$, and for any non-trivial additive character $\chi_i : \mathbb{F}_{p^i} \to \mathbb{C}^*$, we have*

$$(3.7) \qquad \Big| \sum_{x \in Y(\mathbb{F}_{p^i})} \chi_i(G(x)) \Big| \le C \sqrt{p^i}^{\dim(Y) + \dim(\operatorname{Sing} Y_G)}.$$

Here the sum is over $x \in (\mathbb{F}_{p^i})^N$ satisfying (3.5).

Proof: It will be convenient for us to consider the corresponding projective varieties $X \subset \mathbb{P}^{N-1}_{\mathbb{Q}}$ (respectively, $X_G \subset \mathbb{P}^{N-1}_{\mathbb{Q}}$) given by (3.5) (respectively, (3.6)). Let $\dim(X) = n$, $\dim(\operatorname{Sing} X_G) = s$. Then the right hand side of (3.7) is $Cp^{i\frac{n+s+2}{2}}$.

Let us fix a prime ℓ. In the natural way, X extends to the scheme $\mathfrak{X} \subset \mathbb{P}^{N-1}_{\mathbb{Z}}$ given by (3.5). Then $\mathfrak{X}_p = \mathfrak{X} \times_{\mathbb{Z}} \mathbb{F}_p$ is "the reduction of X modulo p". There exists an integer L, $\ell | L$, large enough such that $\mathfrak{X} \times_{\mathbb{Z}} \mathbb{Z}[L^{-1}]$ is flat over $\mathbb{Z}[L^{-1}]$ with absolutely irreducible fibres. This implies that $\dim(\mathfrak{X}_p) = \dim(X) = n$ for $p \nmid L$. In the same way, let $\mathfrak{X}_G$ be the subscheme of $\mathfrak{X}$ given by (3.6). Let $\mathfrak{X}_{G,p} = \mathfrak{X}_G \times_{\mathbb{Z}[L^{-1}]} \mathbb{F}_p$. We can enlarge L so that $\mathfrak{X}_G$ is flat over $\mathbb{Z}[L^{-1}]$, hence $\dim(\mathfrak{X}_{G,p})$ equals the dimension of the generic fibre X_G of $\mathfrak{X}_G$, that is $n-1$. This provides that the reduction of G modulo p does not vanish identically on $\mathfrak{X}_p$. Consider also the subscheme $\operatorname{Sing} \mathfrak{X}_G \subset \mathfrak{X}_G$ given by adding to (3.6) the equations describing that the rank of the Jacobian matrix of (3.6) is less than $N-n$. Clearly $\mathfrak{X}_G \setminus \operatorname{Sing} \mathfrak{X}_G$ is smooth over $\mathbb{Z}[L^{-1}]$. Let $\operatorname{Sing} \mathfrak{X}_{G,p} = \operatorname{Sing} \mathfrak{X}_G \times_{\mathbb{Z}[L^{-1}]} \mathbb{F}_p$. Once again we enlarge L so that $\operatorname{Sing} \mathfrak{X}_G$ is flat over $\mathbb{Z}[L^{-1}]$, hence $\dim(\operatorname{Sing} \mathfrak{X}_{G,p}) = \dim(\operatorname{Sing} X_G) = s$. Finally, we choose $\mathcal{B}$ as the set of primes dividing L. Now it remains to apply Theorem 3.2 to $q = p^i$, $\mathfrak{X}_p \times_{\mathbb{F}_p} \mathbb{F}_q$, and $\mathfrak{X}_{G,p} \times_{\mathbb{F}_p} \mathbb{F}_q$, and to use the following lemma. ∎

LEMMA 3.6: *Let ℓ be a prime. Let $X \subseteq \mathbb{P} = \mathbb{P}_k^{N-1}$ be a closed subscheme defined by the vanishing of m forms of degrees $\delta_1, \dots, \delta_m$, over an algebraically closed field k of characteristic different from ℓ. Then there exists a constant C depending only on N and $\delta_1, \dots, \delta_m$, such that $\dim_{\mathbb{Q}_\ell} H^i(X, \mathbb{Q}_\ell) \leq C$ for any $i \geq 0$.*

Proof: Let $r_i = \binom{\delta_i + N-1}{N-1}$, and let $\mathbf{A}_{\mathbf{Z}}^{r_i}$ be the scheme parametrizing homogeneous polynomials of degree δ_i in N variables. Consider the "universal" polynomial of degree δ_i:

$$\Xi_i(x_1, \dots, x_N) := \sum \xi_{i;a_1,\dots,a_N} x_1^{a_1} \dots x_N^{a_N},$$

here $\xi_{i;a_1,\dots,a_N}$ for $a_1 + \dots + a_N = \delta_i$ are coordinates in $\mathbf{A}_{\mathbf{Z}}^{r_i}$. Let $r := r_1 + \dots + r_m$, $\mathbf{A}_{\mathbf{Z}}^r := \mathbf{A}_{\mathbf{Z}}^{r_1} \times \dots \times \mathbf{A}_{\mathbf{Z}}^{r_m}$. Define $\mathfrak{N} \subset \mathbb{P}_{\mathbf{Z}}^{N-1} \times \mathbf{A}_{\mathbf{Z}}^r$ to be the scheme given by $\Xi_1 = \dots = \Xi_m = 0$. Let π be the natural projection $\mathfrak{N} \to \mathbf{A}_{\mathbf{Z}}^r$. Let $x \to \mathbf{A}_{\mathbf{Z}}^r$ be the closed point such that X is the fibre of π at x, $\mathfrak{N}_x = X$. By the finiteness theorem (cf. [15], VI.2.1) $R^i\pi_*\mathbb{Q}_\ell$ is a constructible sheaf. By the proper base change theorem (cf.[15], VI.2.5) we have $(R^i\pi_*\mathbb{Q}_\ell)_x = H^i(X, \mathbb{Q}_\ell)$. We have $R^i\pi_*\mathbb{Q}_\ell = 0$ for $i > 2(N-1)$. It remains to choose C as the maximum of the dimensions of the fibres of $R^i\pi_*\mathbb{Q}_\ell$. ∎

4. Singularities of Hyperplane Sections

In this section we work over an algebraically closed field k. Let $X \subset \mathbb{P} = \mathbb{P}^{N-1}$ be an irreducible projective variety not contained in a hyperplane. We shall summarize our knowledge concerning the following questions:

1) How singular a hyperplane section $X_H = X \cap H$ can be?
2) What is the dimension of the set of hyperplanes H when the number $\dim(\operatorname{Sing} X_H)$ is fixed ?

With this purpose in mind, let us introduce some notation. Let $\check{P} \cong \mathbb{P}^{N-1}$ be the dual projective space. For $i \geq -1$ define Z_i to be the closed subset of $\check{P}$ consisting of hyperplanes $H \subset \mathbb{P}$ such that

$$\dim(\operatorname{Sing} X_H) \geq i.$$

In particular, if X is smooth, Z_0 is no other than the dual variety $\check{X}$. Let us define $d_i := \dim(Z_i)$, $\sigma := \max\{i | Z_i \neq \emptyset\}$. Thus σ is the maximal possible dimension of $\operatorname{Sing} X_H$. The following parameter of purely geometric nature contains all geometric information about X which we shall use in the arithmetical applications in Section 5:

$$\alpha(X) := \min_{-1\le i\le\sigma} \frac{1}{2}\left\{\frac{n-i}{d_i+1}\right\}.$$

In this section we obtain some lower bounds on $\alpha(X)$ via upper bounds on σ and d_i. We start with some elementary remarks.

LEMMA 4.1:

(a) *If X is smooth, then $d_i \le N-i-2$.*

(b) *Assume that* $\operatorname{Sing} X \ne \emptyset$, $m = \dim(\operatorname{Sing} X)$. *Then*

$$d_i \le \min\{N-1, N+m-i-2\}.$$

Proof: Consider the following diagram:

$$\begin{array}{ccccc} \mathbb{P} & \xleftarrow{\pi_1} & \mathbb{P}\times\check{\mathbb{P}} & \xrightarrow{\pi_2} & \check{\mathbb{P}} \\ \cup & & \cup & & \cup \\ X & \longleftarrow & T & \longrightarrow & Z_0 \end{array}$$

where π_1 and π_2 are the natural projections, T is the set of pairs $\{(x,H)| x \in X, H \in \check{\mathbb{P}}, x \in \operatorname{Sing} X_H\}$. In particular, $\pi_2^{-1}(H) = \operatorname{Sing} X_H$. We have $Z_0 = \pi_2(T)$, $Z_i = \{H \in Z_0 | \dim(\pi_2^{-1}(H)) \ge i\}$, thus $\dim(Z_i) + i \le \dim(T)$. So let us compute $\dim(T)$. If $x \notin \operatorname{Sing} X$, then $\dim(\pi_1^{-1}(x)) = N-n-2$, thus $\dim(\pi_1^{-1}(X \setminus \operatorname{Sing} X)) = N-2$. This proves (a). On the other hand , for $x \in \operatorname{Sing} X$ we have $\dim(\pi_1^{-1}(x)) = N-2$, hence $\dim(\pi_1^{-1}(\operatorname{Sing} X)) = N-2+m$, and (b) follows. ∎

A general restriction on σ follows from a powerful theorem of Zak ([18], 2, Cor.5):

$$\sigma \le N-n+m-1. \tag{4.1}$$

LEMMA 4.2: *Assume that X is smooth, and* $\dim(\check{X}) = N-2$. *Then*

$$d_i \le N-i-3, \quad i \ge 1.$$

Proof: For a smooth X, T is a $\mathbb{P}^{N-n-2}$-bundle over X, in particular, T is irreducible. We have $Z_0 \ne Z_1$, otherwise

$$\dim(T) = \dim(\pi_2^{-1}(Z_0)) = \dim(\pi_2^{-1}(Z_1)) \ge 1 + \dim(\check{X}) = N-1.$$

Thus $\pi_2^{-1}(Z_0 \setminus Z_1)$ is a non-empty subset of T, but since $\dim(\check{X}) = \dim(T)$, we must conclude that it is open. It follows that $\dim(\pi_2^{-1}(Z_1)) \leq N-3$, hence $i + \dim(Z_i) \leq N-3$ for $i \geq 1$. ∎

Not for every smooth X the dual variety $\check{X}$ is a hypersurface. For instance, if X is the Grassmannian $G(2, 2n+1)$ with its Plücker embedding, then $\check{X}$ is of codimension 3. See [10] for a formula for $\dim(\check{X})$ in terms of the Chern classes of X.

I have learnt the following nice lemma from F. L. Zak (cf. [11], Appendix, Thm. 2).*

Lemma 4.3: *Let X be a complete intersection, then $\sigma \leq m+1$.*

Proof: It is known that a hyperplane section of a smooth complete intersection can have at most isolated singularities [8]. This proves the lemma in the smooth case. In the singular case, take a projective subspace $L \subset \mathbb{P}$, $\mathrm{codim}(L) = m+1$, in general position, that is, not contained in H, and such that $\dim(L \cap X) = n - m - 1$, $L \cap X$ is smooth, $\dim(L \cap \mathrm{Sing}\, X_H) = \dim(\mathrm{Sing}\, X_H) - m - 1$. Then $X_H \cap L$ is a hyperplane section of a smooth complete intersection $X \cap L$. Thus $\mathrm{Sing}(X_H \cap L)$ is at most 0-dimensional by [8]. Clearly $L \cap \mathrm{Sing}\, X_H \subseteq \mathrm{Sing}(X_H \cap L)$, therefore $\dim(\mathrm{Sing}\, X_H) - m - 1 \leq 0$. ∎

In case of hypersurfaces a more precise statement was communicated to me by N. M. Katz (cf. [11], Lemma 1).

Lemma 4.4: *Let $X \subset \mathbb{P}$ be a hypersurface. Then for any hyperplane $H \subset \mathbb{P}$ we have*

$$\dim(\mathrm{Sing}\, X_H) \leq \dim(H \cap \mathrm{Sing}\, X) + 1 \leq \dim(\mathrm{Sing}\, X) + 1.$$

Proof: Let X be given by a form f in variables $x = (x_1, \ldots, x_N)$, and H be given by $x_1 = 0$. We have

$$H \cap \mathrm{Sing}\, X = X \cap H \cap \{x | \frac{\partial f}{\partial x_i}(x) = 0, \quad i = 1, \ldots, N\},$$

$$\mathrm{Sing}\, X_H = X \cap H \cap \{x | \frac{\partial f}{\partial x_i}(x) = 0, \quad i = 2, \ldots, N\}.$$

Thus $H \cap \mathrm{Sing}\, X$ is a subset of $\mathrm{Sing}\, X_H$ given by one equation $\frac{\partial f}{\partial x_i}(x) = 0$, hence $\dim(H \cap \mathrm{Sing}\, X) \geq \dim(\mathrm{Sing}\, X_H) - 1$. ∎

* This is also proved in: S. Ishii, A characterization of hyperplane cuts of smooth complete intersection, Proc. Japan. Acad. Ser. A. 58 (1982) 309–311.

Recall that if X is singular, the dual variety $\check{X}$ is defined as the Zariski closure of the set of hyperplanes which are tangent to X at its smooth points.

LEMMA 4.5: *Let $P \in X \subset \mathbb{P}$ be an isolated singular point.*

(a) *If $H \ni P$ is a generic hyperplane passing through P, then P is an isolated singular point on X_H.*
(b) *If the dual variety $\check{X}$ is not contained in a hyperplane, then the set of H such that P is a non–isolated singularity of X_H, is of dimension at most $N-4$.*
(c) *If X is a hypersurface of degree d, which is not a cone, and* $\mathrm{char}(k) > d$ *or* $\mathrm{char}(k) = 0$*, then we have the same conclusion as in (b).*

Proof: The statement is local, so we can replace X by $X' = (X \setminus \operatorname{Sing} X) \cup \{P\}$, which is an irreducible n–dimensional quasi–projective variety. We introduce some notation:

$$V = \{(x, H) | H \in \check{\mathbb{P}}, x \in \operatorname{Sing}((X' \setminus \{P\}) \cap H)\},$$
$$V_0 = \{(x, H) \in V | H \ni P\}.$$

It is easy to see that V is a $\mathbb{P}^{N-n-2}$–bundle over $X' \setminus \{P\}$, thus $\dim(V) = N-2$. Since $V_0 \subset V$, we have $\dim(V_0) \leq N-2$. Now let us assume that (a) is not true. Then for a generic H passing through P we would have $\dim(\operatorname{Sing}(X' \cap H)) \geq 1$, implying $\dim(V_0) \geq N-1$, which is a contradiction.

Let us now explore the situation when $\dim(V_0) = N-2$. Since V is irreducible, and V_0 is closed in V, we have $V_0 = V$. This says that every hyperplane tangent to X at its smooth point passes through P. Thus $\check{X}$ is contained in the hyperplane dual to P, hence (b).

Assume that $p = (1, 0, ..., 0)$, and X is given by the vanishing of an irreducible form $f(x)$ of degree d. The tangent hypersurface at a smooth point $x \in X$ passes through P if and only if $\frac{\partial f}{\partial x_1}(x) = 0$. Thus the proof of (b) implies that $\frac{\partial f}{\partial x_1}(x) = 0$ for all $x \in X \setminus \operatorname{Sing} X$, hence X is contained in $\{x | \frac{\partial f}{\partial x_1}(x) = 0\}$. Since X is not contained in a hypersurface of degree $d-1$, the form $\frac{\partial f}{\partial x_1}(x)$ is zero. Under the assumption that $\mathrm{char}(k) > d$ or $\mathrm{char}(k) = 0$, X is a cone with vertex P if and only if $\frac{\partial f}{\partial x_1}(x)$ is identically zero. This proves (c). ∎

Let us now concentrate on the case of hypersurfaces with isolated singular points.

COROLLARY 4.6: *Let X be a hypersurface of degree $\deg(X)$, with at most isolated singular points, then $\sigma = 1$, $d_0 = N-2$, $d_1 \leq N-3$. If one of the following conditions is satisfied:*

(i) *the dual variety $\check{X}$ is not contained in a hyperplane,*
(ii) *X is not a cone, and $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > \deg(X)$,*

then $d_1 \leq N-4$.

Proof: There are two possibilities: $H \cap \mathrm{Sing}\, X = \emptyset$, or H passes through a singular point of X. In the first case $\dim(\mathrm{Sing}\, X_H) \leq 0$ by Lemma 4.4. In the second case $\dim(\mathrm{Sing}\, X_H) \leq 1$ by the same lemma. We bound d_1 using Lemma 4.5. ∎

COROLLARY 4.7: *Let $X \subset \mathbb{P} = \mathbb{P}^{N-1}$ be an irreducible projective variety not contained in a hyperplane, $\dim(X) = n$, $\dim(\mathrm{Sing}\, X) = m$.*

(a) *If X is singular ($m \geq 0$), then $\alpha(X) \geq 1 - \frac{N+m-1}{2n}$ for $n \geq \frac{1}{2}(N+m)$, and $\alpha(X) \geq \frac{1}{2(N+m-n)}$ for $n < \frac{1}{2}(N+m)$;*
(b) *If X is smooth, and the dual variety $\check{X}$ is a hypersurface, then*

$$\alpha(X) \geq \frac{1}{2(N-n)} \text{for } n \leq \frac{1}{2}(N-1),$$
$$\alpha(X) \geq 1 - \frac{N-2}{2n} \text{ for } N-1-\sqrt{N-1} \geq n \geq \frac{1}{2}(N-1),$$
$$\alpha(X) \geq \frac{n}{2(N-1)} \text{ for } n \geq N-1-\sqrt{N-1}.$$

(c) *If X is a singular complete intersection, then $\alpha(X) \geq \frac{n-m-1}{2(N-2)}$;*
(d) *If X is smooth complete intersection, then $\alpha(X) \geq \frac{n}{2(N-1)}$;*
(e) *If X is a hypersurface with at most isolated singularities, such that X is not a cone, and $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > \deg(X)$, then $\alpha(X) \geq \frac{N-2}{2(N-1)}$.*

Proof: (a) easily follows from Lemma 4.1 (b), (4.1), and the trivial bound $\sigma \leq n-1$. The statement (b) is a combination of Lemma 4.1 (a), Lemma 4.2, and (4.1). The statements (c) and (d) follow from Lemmas 4.1 and 4.3. Finally, (e) follows from Corollary 4.6. ∎

Note that the bound in (e) is the same as that in (d) for $n = N-2$, that is the bound for smooth hypersurfaces is the same as that for hypersurfaces with only isolated singularities. Note also that (d) coincides with (b) for small codimension. This is certainly no surprise. A stronger result would follow from Hartshorne's conjecture that a smooth variety $X \subset \mathbf{P}^{N-1}$ is a complete intersection as soon as $n = \dim(X) > \frac{2}{3}(N-1)$.

5. Applications to Distribution of Rational Points

Let $x = (x_1, \dots, x_N)$ and $G(x) = \{G_1(x), \dots, G_r(x)\}$ be a system of forms with integer coefficients defining an absolutely irreducible variety $X \subset \mathbf{P}_{\mathbf{Q}}^{N-1}$ not contained in a hyperplane. By $Y \subset \mathbf{A}_{\mathbf{Q}}^N$ we denote the corresponding affine cone, that is, the affine variety defined by the same system $G(x) = 0$.

Consider the box of size $b > 0$ with the center in $a \in \mathbf{R}^N$:

$$B(b) := \{x | x_i \in \mathbf{R}, \quad |x_i - a_i| < b, \quad i = 1, \dots, N\},$$

vol $B(b) = (2b)^N$. We shall assume that b is an integer. If $p \neq 2$ is a prime and $b = (p+1)/2$, we identify $B(b) \cap \mathbf{Z}^N$ with $\mathbf{F}_p^N$.

Let $\mathfrak{X}_p \subset \mathbf{P}_{\mathbf{F}_p} = \mathbf{P}_{\mathbf{F}_p}^{N-1}$ be the variety given by $G(x) = 0$ over $\mathbf{F}_p$ (the reduction of X modulo p), and similarly, $\mathcal{Y}_p \subset \mathbf{A}_{\mathbf{F}_p}^N$. For $p \neq 2$ the set of $\mathbf{F}_p$-points $\mathcal{Y}_p(\mathbf{F}_p)$ is identified with the set of solutions of the system of congruences $G(x) \equiv 0 (\operatorname{mod} p)$ in $B((p+1)/2)$. Define

$$L(G, b) := \#\{x \in B(b) | G(x) = 0\},$$
$$N_p(G, b) := \#\{x \in B(b) | G(x) \equiv 0 (\operatorname{mod} p)\}.$$

The computation of $N_p(G, b)$ for $b = (p+1)/2$ follows from the Weil conjecture proved by Deligne. The aim of this section is to estimate $N_p(G, b)$ for b not too small, $b < p$, and to obtain an upper bound for $L(G, b)$ for large b.

We start with some remarks of scheme-theoretic nature similar to those in the proof of Theorem 3.5. In a natural way, X extends to the scheme $\mathfrak{X} \subset \mathbf{P}_{\mathbf{Z}} = \mathbf{P}_{\mathbf{Z}}^{N-1}$, such that $\mathfrak{X}_p = \mathfrak{X} \times_{\mathbf{Z}} \mathbf{F}_p$. There exists an integer L large enough such that $\mathfrak{X} \times_{\mathbf{Z}} \mathbf{Z}[L^{-1}]$ is flat over $\mathbf{Z}[L^{-1}]$. This implies that $\dim(\mathfrak{X}_p) = \dim(X)$, $\deg(\mathfrak{X}_p) = \deg(X)$, for $p \nmid L$. Let $\operatorname{Sing} \mathfrak{X}$ be the subscheme of $\mathfrak{X}$ given by adding to $G(x) = 0$ the equations describing that the rank of the Jacobian matrix of $G(x) = 0$ is less than $N - 1 - \dim(X)$. The closed points of $\operatorname{Sing} \mathfrak{X}$ over $\mathbf{Z}[L^{-1}]$ are the singular points of their fibres, $(\operatorname{Sing} \mathfrak{X})_p = \operatorname{Sing} \mathfrak{X}_p$, $p \nmid L$. Making L larger we can arrange that $\operatorname{Sing} \mathfrak{X}$ is flat over $\mathbf{Z}[L^{-1}]$. In particular, $\dim(\operatorname{Sing} \mathfrak{X}_p) = \dim(\operatorname{Sing} X)$.

In the same way, let $\mathfrak{T}$ be the scheme in $\mathbb{P} \times_{\mathbb{Z}[L^{-1}]} \check{\mathbb{P}}$ whose closed points are the pairs (x, H) such that x is a singular point of the hyperplane section of a fibre of $\mathfrak{X}$ by H. Let π_2 be the second projection $\mathbb{P} \times_{\mathbb{Z}[L^{-1}]} \check{\mathbb{P}} \to \check{\mathbb{P}}$. Define the relative version of Z_i as $\mathcal{Z}_i := \{H \in \check{\mathbb{P}} | \dim(\pi_2^{-1}(H)) \geq i\}$. Once again, we enlarge L so that all $\mathcal{Z}_i$ are flat over $\mathbb{Z}[L^{-1}]$. Let $\mathcal{Z}_{i,p} = \mathcal{Z}_i \times_{\mathbb{Z}[L^{-1}]} \mathbb{F}_p$, then $\dim(\mathcal{Z}_{i,p}) = \dim(Z_i)$, and therefore $\alpha(\mathfrak{X}_p) = \alpha(X)$ for $p \nmid L$.

THEOREM 5.1: *Let* $\dim(X) = n$. *Choose a small* $\varepsilon > 0$, *then for any prime* p, $p > C_1(\varepsilon, G)$, *and for any integer* b, $p \geq b \geq C_2(\varepsilon, G)p^{1-\alpha(X)}$, *we have*

$$(1-\varepsilon)p^{n-N+1} \operatorname{vol} B(b) \leq N_p(Y, b) \leq (1+\varepsilon)p^{n-N+1} \operatorname{vol} B(b).$$

Remark: In particular, we get a bound for the smallest non-trivial solution of a system of congruences. For p large enough, $G(x) \equiv 0 (\operatorname{mod} p)$ has a non-trivial solution in the box $B(b)$ of size $b \geq b(G)p^{1-\alpha(X)}$.

Proof: By the previous remarks, there exists $L \in \mathbb{Z}$ depending on the equations $G(x)$, such that $p \nmid L$ implies that $\mathfrak{X}_p$ satisfies the same geometric assumptions as X: $\mathfrak{X}_p$ is absolutely irreducible, not contained in a hyperplane, $\dim(\mathfrak{X}_p) = \dim(X)$, $\deg(\mathfrak{X}_p) = \deg(X)$, and $\alpha(\mathfrak{X}_p) = \alpha(X)$. We assume that $C_1(\varepsilon, G) > L$.

Let us recall the method of Fujiwara ([7], Thm.1). Let $x = (x_1, \dots, x_N)$ be real variables. Define the counting function $F(x) = 2^N(1 - |x_1|, \dots, (1 - |x_N|)$ in the box $|x_i| \leq 1$, $i = 1, \dots, N$, and let $F(x) = 0$ elsewhere. Let $e(z) := \exp((2\pi\sqrt{-1}z)$, $e_p(z) := e(z/p)$ for $z \in \mathbb{Z}$.

LEMMA ([7], Lemma 1)): *Assume that for any small* $\varepsilon > 0$, *for any prime* $p > C_1(\varepsilon, G)$, *and any* b *such that* $p \geq b \geq c_1(\varepsilon, G)p^{1-\alpha(X)}$ *we have*

$$(5.1)\quad (1-\varepsilon)p^{n-N+1} \operatorname{vol} B(b) \leq \sum_{\substack{x \in \mathbb{Z}^N \\ p | G(x)}} F(b^{-1}(x-a)) \leq (1+\varepsilon)p^{n-N+1} \operatorname{vol} B(b).$$

Then the conclusion of Theorem 5.1 is true. ∎

We continue to follow the proof of [7], Thm.1. Let $x_i = y_i + pz_i$, $z_i \in \mathbb{Z}$, $y_i \in \{0, 1, \dots, p-1\}$. Note that $p | G(x)$ if and only if $p | G(y)$, that is, $y \in \mathcal{Y}_p(\mathbb{F}_p)$.

Using the Poisson summation formula we obtain

$$\sum_{\substack{x\in\mathbb{Z}^N\\ p|G(x)}} F(b^{-1}(x-a)) = \sum_{y\in\mathcal{Y}_p(\mathbb{F}_p)}\sum_{z\in\mathbb{Z}^N} F(b^{-1}(y-a+pz)) =$$

$$= \sum_{y\in\mathcal{Y}_p(\mathbb{F}_p)}\sum_{u\in\mathbb{Z}^N}\int_{z\in\mathbb{R}^N} F(b^{-1}(y-a+pz))e(\langle u.z\rangle)dz =$$

$$= \frac{b^N}{p^N}\sum_{y\in\mathcal{Y}_p(\mathbb{F}_p)}\sum_{u\in\mathbb{Z}^N} e_p(-\langle u.(y-a)\rangle)\hat{F}(bp^{-1}u),$$

where $\langle u.z\rangle = u_1z_1 + \ldots + u_Nz_N$, and $\hat{F}(x)$ is the inverse Fourier transform of $F(x)$, $\hat{F}(x) = 2^N g(x_1)\ldots g(x_N)$, $g(z) = \sin^2(\pi z)/\pi^2 z^2$. Since $\hat{F}(0) = 2^N$ we get

$$= \frac{b^N}{p^N}\sum_{u\in\mathbb{Z}^N}\sum_{y\in\mathcal{Y}_p(\mathbb{F}_p)} e_p(-\langle u.(y-a)\rangle)\hat{F}(bp^{-1}u)$$

$$(5.2)\qquad = \frac{\operatorname{vol} B(b)}{p^N}\Big\{\#\mathcal{Y}_p(\mathbb{F}_p) + 2^{-N}\sum_{u\in\mathbb{Z}^N\setminus\{0\}} e_p(\langle u.a\rangle)\hat{F}(bp^{-1}u)S_1(\mathcal{Y}_p,-u)\Big\},$$

where $S_1(\mathcal{Y}_p,-u) = \sum_{y\in\mathcal{Y}_p(\mathbb{F}_p)} e_p(-\langle u.y\rangle)$ in the notation of Section 3. Let $n = \dim(X)$. Since $\dim(\mathfrak{X}_p) = n$, $\deg(\mathfrak{X}_p) = \deg(X)$, the Lang-Weil theorem writes as

$$(5.3)\qquad |\#\mathcal{Y}_p(\mathbb{F}_p) - p^{n+1}| \le A(N,n,\deg(X))p^{n+1/2}.$$

The right hand side in (5.3) is at most $\frac{1}{2}\varepsilon p^{n+1}$ if only $p > (2A(N,n,\deg(X))/\varepsilon)^2$. It remains to show that for such a p and $b \ge C_2(\varepsilon)p^{1-\alpha(X)}$, the sum in (5.2) is less than $\frac{1}{2}\varepsilon p^{n+1}$. Since $\hat{F}$ vanishes at the non-zero integer points, and we assumed $b \in \mathbb{Z}$, the terms with $u \in (p\mathbb{Z})^N \setminus \{0\}$ do not contribute to our sum. Let us divide $\mathbb{Z}^N\setminus(p\mathbb{Z})^N$ into subsets A_s, $s = -1,0,1,\ldots,n-1$, defined by the following property: $u_p := u(\operatorname{mod} p)$ is a $\mathbb{E}_p$-point on the affine cone of $\mathcal{Z}_{s,p}\setminus\mathcal{Z}_{s-1,p}$. We now estimate the corresponding sums. Let us write $\sum_s$ for the sum over $u \in A_s$. We have

$$|\Sigma_s| \le |S_1(\mathcal{Y}_p,-u)|\sum_{u\in A_s}\hat{F}(bp^{-1}u).$$

Since we have here that $\dim(\operatorname{Sing}\mathfrak{X}_{p,u}) = s$, where $\mathfrak{X}_{p,u}$ is the hyperplane section of $\mathfrak{X}_p$ by $\langle u_p.x\rangle = 0$, we can use the bound (3.2): $|S_1(\mathcal{Y}_p,-u)| \le Cp^{\frac{n+s+2}{2}}$. The constant C depends only on N and the degrees of the equations of G by Lemma 3.6.

Recall that d_s stands for $\dim(Z_s)$. We now claim that if $Z_s \neq 0$, then

$$\sum_{u\in A_s} \hat{F}(bp^{-1}u) \leq C'(G)(b^{-1}p)^{d_s+1}. \tag{5.4}$$

Let us assume (5.4) for a moment, and show how to complete the proof of the theorem. Since $b \geq C_2(\varepsilon, G)p^{1-\alpha(X)}$, where $C_2(\varepsilon, G)$ is not yet specified, we get

$$\begin{aligned}|\Sigma_s| &\leq C(G)C'(G)p^{\frac{n+s+2}{2}}(b^{-1}p)^{d_s}\\ &\leq C(G)C'(G)C_2(\varepsilon,G)^{-(d_s+1)}p^{\frac{n+s+2}{2}+\alpha(X)(d_s+1)}\\ &\leq C(G)C'(G)C_2(\varepsilon,G)^{-(d_s+1)}p^{n+1}.\end{aligned}$$

Choosing $C_2(\varepsilon, G)$ large enough we arrange that $|\Sigma_s| < \frac{1}{2}(n+1)^{-1}\varepsilon p^{n+1}$, thus the sum in (5.2) is less than $\frac{1}{2}\varepsilon p^{n+1}$. Combining this with (5.3) we obtain (5.1), and thus prove the theorem.

The inequality (5.4) follows from (5.5):

$$\sum_{u_p\in \mathcal{W}_p(\mathbf{F}_p)} \hat{F}(m^{-1}u) \leq c(\mathcal{W})m^d, \quad p > p_0(\mathcal{W}), \quad 1 < m < p. \tag{5.5}$$

Here $W \subset \mathbf{A}^N_{\mathbf{Q}}$ is an affine variety defined by equations with integer coefficients, $\dim(W) = d$; $\mathcal{W} \subset \mathbf{A}^N_{\mathbf{Z}}$ is the affine scheme defined by the same equations, $\mathcal{W}_p := \mathcal{W} \times_{\mathbf{Z}} \mathbf{F}_p$. The sum is over $u \in \mathbf{Z}^N$ such that the reduction of u modulo p, denoted by u_p, is a $\mathbf{F}_p$-point of $\mathcal{W}_p$. (The sum (5.4) is dominated by (5.5) with $\mathcal{W}$ equal to the affine cone of Z_s, $m = pb^{-1}$.) Before proving (5.5) note that for $K = K(N)$ we have the following easy estimate (cf. [7], (6)):

$$\sum_{u\in \mathbf{Z}^N} \hat{F}(a + m^{-1}u) \leq Km^N, a \in \mathbf{R}^N, \quad m \geq 1. \tag{5.6}$$

We prove (5.5) by induction on d. For $d = 0$ and $p > K'(\mathcal{W})$, we have $\#W_p(\mathbf{F}_p) \leq \deg(W)$, hence (5.5) is bounded by $K\deg(W)$. In the general case we may assume W irreducible. Let us remove $\operatorname{Sing} W$ as a closed subset of dimension at most $d-1$. Let $W' = W \setminus \operatorname{Sing} W$. Let $\overline{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$. Choose a $\overline{\mathbf{Q}}$-point $z = (z_1, \ldots, z_N)$ on W', and let $T_{z,W}$ be the tangent space to W at z, $\dim(T_{z,W}) = d$. For a subset $I = \{i_1, \ldots, i_d\} \subset \{1, \ldots N\}$ consider the natural projection $\pi_I : \mathbf{A}^N \to \mathbf{A}^d_I$, where $\mathbf{A}^d_I$ is given by $x_i = 0$, $i \notin I$. Clearly there exists such a subset I for which π_I maps $T_{Z,W}$ isomorphically onto $\mathbf{A}^d_I$. The same is true for a Zariski open neighbourhood W'' of z, which we may choose defined over $\mathbb{Q}$. This implies that W'' is Zariski dense in W'. We may remove $W' \setminus W''$ of dimension at most $d-1$. Then π_I restricted on W'' is a finite morphism of degree $\deg(\pi_I) = \deg(W)$. If p is large enough, then the same holds for the reductions of these varieties modulo p. Since $\hat{F}$ is the product of functions in one variable, we can apply (5.6) first to the (zero-dimensional) fibres of π_I, and then to the base. Hence the sum over W'' is bounded by $\deg(W)K^2m^d$. ∎

THEOREM 5.2: *There exists a constant $C_3 = C_3(G)$ such that*

$$L(G,b) \le C_3 b^{N-\frac{N-n-1}{1-\alpha(X)}}.$$

Proof: We follow the proof of [7], Thm. 3. Choose a prime p in the range $b^{(1-\alpha(X))^{-1}} \le p \le 2b^{(1-\alpha(X))^{-1}}$. Note that

$$L(G,b) \le N_p(G,b) \le \sum_{\substack{x\in\mathbb{Z}^N\\ p\mid G(x)}} F((2b)^{-1}x).$$

We have $b \ge c_3(G)p^{1-\alpha(X)}$. The proof of Theorem 5.1 then shows that for b large enough we have (cf. (5.1)):

$$N_p(G,b) \le c_4(G)p^{n-N+1}\operatorname{vol} B(b) \le c_5(G)b^{N-(N-n-1)(1-\alpha(X))^{-1}}. \quad ∎$$

For smooth complete intersections of codimension t, $t = N-n-1$, this result combined with Corollary 4.7 (d) gives ([17], Thm. 3):

$$L(G,b) \le C_3(G)b^{N-2t+\frac{2t^2}{N+t-1}} \tag{5.7}$$

We can note that the exponent in Theorem 5.2 involves the dimension of X and $\alpha(X)$ as the only characteristics of X. In particular, (5.7) is best for complete intersections of least possible degree, that is, for complete intersections of quadrics (cf. the discussion and the references in [17]).

Example 5.3: Let X be a hypersurface with at most isolated singularities, which is not a cone. (Clearly 3 is the least degree for which such hypersurfaces may exist). Then we have $\alpha(X) \ge \frac{N-2}{2(N-1)}$ by Corollary 4.7 (e). Now it follows from Theorem 5.2 that

$$L(G,b) \le C_3(G)b^{N-2+\frac{2}{N}}. \tag{5.8}$$

This bound coincides with Fujiwara's bound for smooth hypersurfaces [6]. (The exponent is the same as in (5.7) for $t = 1$.) ∎

Example 5.4: Let X be a singular complete intersection of codimension $t = N - n - 1$, $\dim(\operatorname{Sing} X) = m$. By Corollary 4.7 (c) we get

$$L(G,b) \leq C_3(G) b^{N-2t+\frac{2t(t+m)}{N+t+m-2}}. \quad \blacksquare$$

Example 5.5: On the other hand, let X be a smooth variety of dimension n, $N - 1 - \sqrt{N-1} \geq n \geq \frac{1}{2}(N-1)$, that is of codimension $t = N - n - 1$, $\sqrt{N-1} \leq t \leq \frac{1}{2}(N-1)$. Then by Corollary 4.7 we have $\alpha(X) \geq 1 - \frac{N-2}{2n}$. Now Theorem 5.2 reads as follows:

$$L(G,b) \leq C_3(G) b^{N-2t+\frac{2t(t-1)}{N-2}}. \quad \blacksquare$$

References

[1] A. Adolphson and S. Sperber, *Exponential sums and Newton polyhedra,* Ann. Math. **130** (1989), 367–406.

[2] R. C. Baker, *Small solution of congruences,* Mathematika **30** (1983), 164–188.

[3] P. Deligne, *La conjecture de Weil I,* Math. IHES **43** (1974), 273–307.

[4] P. Deligne, *La conjecture de Weil II,* Math. IHES **52** (1981), 313–428.

[5] P. Deligne, *Applications de la formule des traces aux sommes trigonométriques,* Cohomologie etále (SGA 4 1/2), Lecture Notes in Math. **569** (1977), 168–232.

[6] M. Fujiwara, *Upper bounds for the number of lattice points on hypersurfaces, in Number Theory and Combinatorics,* World Scientific (1985), 89–96.

[7] M. Fujiwara, *Distribution of rational points on varieties over finite fields,* Mathematika **35** (1988), 155–171.

[8] W. Fulton and R. Lazarsfeld, *Connectivity and its applications in algebraic geometry,* Lecture Notes in Math. **862** (1981), 26–92.

[9] D. R. Heath-Brown, *Cubic forms in ten variables,* Proc. London Math. Soc. (3) **47** (1983), 225–257.

[10] A. Holme, *On the dual of a smooth variety,* Lecture Notes in Math. **732** (1979), 144–156.

[11] C. Hooley, *On the number of points on a complete intersection over a finite field. (With an appendix by N. M. Katz),* J. Number Theory **38** (1991), 338–358.

[12] N. M. Katz, *Sommes exponentielles,* Astérisque **79** (1980).

[13] N. M. Katz and G. Laumon, *Transformation de Fourier et majoration de sommes exponentielles,* Publ. Math. IHES **62** (1985), 165–202.

[14] G. Meyerson, *The distribution of rational points on varieties defined over a finite field,* Mathematika **28** (1981), 153–159.

[15] J. S. Milne, *Etale cohomology,* Princeton Math. Series **33** (1980).

[16] W. M. Schmidt, *The density of integer points on homogeneous varieties,* Acta Math. **154** (1985), 243–296.

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

[18] F. L. Zak, *The structure of Gauss maps. (In Russian),* Funct. Anal. Appl. **21** (1987), 39–50.