NUMBER OF SOLUTIONS OF EQUATIONS OVER FINITE FIELDS AND A CONJECTURE OF LANG AND WEIL

SUDHIR R. GHORPADE AND GILLES LACHAUD

ABSTRACT. A brief survey of the conjectures of Weil and some classical estimates for the number of points of varieties over finite fields is given. The case of partial flag manifolds is discussed in some details by way of an example. This is followed by a motivated account of some recent results on counting the number of points of varieties over finite fields, and a related conjecture of Lang and Weil. Explicit combinatorial formulae for the Betti numbers and the Euler characteristics of smooth complete intersections are also discussed.

INTRODUCTION

The general question that we want to discuss in this article may be stated in its simplest form as follows.

Suppose p is a prime number and $f(T_0, T_1, \ldots, T_N)$ is a polynomial with integer coefficients. Then what can we say about the solutions of the congruence equation $f(T_0, T_1, \ldots, T_N) \equiv 0 (\operatorname{mod} p)$?

For example, if f is a quadratic polynomial in one variable of the form $T^2 - a$ (or alternatively, a homogeneous polynomial in two variables of the form $T_0^2 - T_1^2$), then the question is related to the classical study of quadratic residues. As in the classical case, by solutions we really mean solutions (mod p). In other words, we are interested in the set

$$V_f = \{(t_0, t_1, \ldots, t_N) \in \mathbb{F}_p^{N+1} : f(t_0, t_1, \ldots, t_N) = 0\},$$

where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the field with p elements. Note that since f has integer coefficients, the substitution of values from $\mathbb{F}_p$ in f makes sense. In case f is homogeneous, then $(t_0, t_1, \ldots, t_N)$ is a solution if and only if $(\lambda t_0, \lambda t_1, \ldots, \lambda t_N)$ is a solution for any $\lambda \in \mathbb{F}_p$, $\lambda \neq 0$, and the solutions that are proportional to each other ought to be considered equivalent. Thus it is better in this case to look at the set

$$X_f = \{(t_0 : t_1 : \cdots : t_N) \in \mathbb{P}^N_{\mathbb{F}_p} : f(t_0, t_1, \ldots, t_N) = 0\},$$

where $\mathbb{P}^N_{\mathbb{F}_p}$ denotes the N-dimensional projective space over $\mathbb{F}_p$.

Date: November 27, 2001.

1991 *Mathematics Subject Classification.* 11G25, 14F20, 14G15, 14M10.

† The first author is partially supported by the IRCC grant 97IR012 from IIT Bombay.

This is an unofficial electronic version of the paper which has appeared in *Number Theory and Discrete Mathematics* (Chandigarh, 2000), A. K. Agarwal, B. Berndt, C. Krattenthaler, G L Mullen, K Ramachandra and M. Waldschmidt Eds., Hindustan Book Agency, New Delhi/Birkhäuser, Basel (2002), pp. 269-291.

Roughly speaking, sets such as V_f and X_f are known as affine varieties and projective varieties, respectively, especially when f is irreducible. Better still, they are the sets of $\mathbb{F}_p$-rational points of affine or projective varieties, and to emphasize this, the notation $V_f(\mathbb{F}_p)$ or $X_f(\mathbb{F}_p)$ is sometimes used. An important feature of these is that they are finite sets. In fact, instead of $\mathbb{F}_p$, we could look more generally at any finite field $\mathbb{F}_q$ with q elements and the corresponding sets $V_f(\mathbb{F}_q)$ or $X_f(\mathbb{F}_q)$ are well defined and finite. So the general problem mentioned above can, in part, be stated as follows.

Given an affine or projective variety X defined over the finite field $\mathbb{F}_q$, count or estimate the cardinality $|X(\mathbb{F}_q)|$ of the set of $\mathbb{F}_q$-rational points of X.

In this connection, André Weil made a remarkable observation about fifty years ago. Namely, that the arithmetic or combinatorial question of counting the number of points of varieties over finite fields is intimately related to the topology of related objects such as the corresponding variety over the complex numbers. His observation was formulated in the form of a number of conjectures, which are now theorems. This work leads to some nontrivial estimates for the number $|X(\mathbb{F}_q)|$. In the special case such as X_f when the variety is a *hypersurface*, that is, it is defined by a single equation, or in the more general case when it is a *complete intersection*, the estimates one gets are particularly sharp provided that the variety is nonsingular.

In the next section, we shall give a brief introduction to the celebrated conjectures of Weil and some related results, with an emphasis on the resulting estimates for the number of $\mathbb{F}_q$-rational points of varieties over finite fields. The example of partial flag manifolds is worked out in a fairly self-contained manner in the subsequent section, so as to provide an illustration of Weil Conjectures, and also to serve as a ready reference for some material that may be of independent interest. We then turn to certain recent results, where some of the classical estimates for the number of $\mathbb{F}_q$-rational points of varieties over finite fields are extended or refined, and a related conjecture of Lang and Weil is proven. Our aim here is to provide a short and leisurely introduction to these recent results and some background material, in such a way that it can be easily accessible to the non-experts. A reader who wishes to know more may consult [8], [28] and [10] where further details can be found. Additional pointers to the literature appear in the subsequent sections.

1. Weil Conjectures and Classical Estimates

From this section onwards, it will be convenient to use some language of Algebraic Geometry. For most part, it will suffice to know what an affine or projective variety is, and some basic things such as the dimension of a variety, the notion of nonsingular or smooth varieties, etc. In essence, an affine variety over a field k is the locus in the affine space $\mathbb{A}_k^N$ (which means the space of N-tuples of elements from k) of a bunch of polynomial equations in N variables with coefficients in k, while a projective variety is the locus in the projective space $\mathbb{P}_k^N$ of a bunch of homogeneous polynomials in $N+1$ variables with coefficients in k. For more details concerning the basics of Algebraic Geometry, one may consult standard texts such as Hartshorne [13] or Shafarevich [37].

Let X be a variety defined over the finite field $\mathbb{F}_q$. Then X is also defined over any extension $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$. The numbers $a_r = |X(\mathbb{F}_{q^r})|$ of $\mathbb{F}_{q^r}$-rational points of

X are therefore well-defined. Now, the exponential generating function of these numbers, namely,

$$Z(X,T) = \exp\left(\sum_{r=1}^{\infty} a_r \frac{T^r}{r}\right)$$

is a well-defined formal power series with rational coefficients. This is called the *(Weil) zeta function* of X.

For example, if $X = \mathbb{P}^n$, the projective space of dimension n over $\mathbb{F}_q$, then we can easily see that

$$|\mathbb{P}^n(\mathbb{F}_q)| = \pi_n := q^n + q^{n-1} + \cdots + q + 1.$$

Of course, a similar formula holds with q replaced by q^r. Thus,

$$Z(X,T) = \exp\left(\sum_{r=1}^{\infty} \frac{T^r}{r} \sum_{j=0}^{n} q^{rj}\right) = \prod_{j=0}^{n} \frac{1}{1-q^jT},$$

where the last equality follows by remembering the familiar expansion of $\log(1 - q^jT)$. It may be noted here that $Z(X,T)$ is, in fact, a rational function in T, and it satisfies the equation $Z\left(X, 1/(q^nT)\right) = (-q^{n/2}\,T)^{n+1}\,Z(X,T)$. The conjectures of Weil state that the situation in the general case is similar. More precisely, these conjectures may be stated as follows.

Let X be a nonsingular projective variety of dimension n. Then we have the following.

(i) $Z(X,T)$ is a rational function in T.

(ii) $Z(X,T)$ satisfies the functional equation

$$Z\left(X, \frac{1}{q^nT}\right) = (-q^{n/2}\,T)^{\chi}\,Z(X,T), \tag{1}$$

for some integer χ. More precisely, there is a factorization

$$Z(X,T) = \frac{P_1(X,T)P_3(X,T)\cdots P_{2n-1}(X,T)}{P_0(X,T)P_2(X,T)\cdots P_{2n}(X,T)},$$

where $P_0(X,T) = 1-T$, $P_{2n}(X,T) = 1-q^nT$, and for $0 \le i \le 2n$, $P_i(X,T)$ are polynomials with integer coefficients such that if $b_i = \deg P_i(X,T)$, then

$$T^{b_i}P_i\left(X, \frac{1}{q^nT}\right) = (-1)^{b_i}q^{(i-n)b_i/2}P_{2n-i}(X,T).$$

(This implies that $b_i = b_{2n-i}$ and (1) holds with $\chi = \sum_{i=0}^{2n}(-1)^i b_i$.)

(iii) If $P_i(X,T)$ are as above, then there is a factorization

$$P_i(X,T) = \prod_{j=1}^{b_i}(1-\omega_{ij}T), \tag{2}$$

where the reciprocal roots ω_{ij} are algebraic integers with the property that $|\omega_{ij}| = q^{i/2}$ for $1 \le j \le b_i$ and $0 \le i \le 2n$.

(iv) If X is obtained from 'reduction modulo p' of a nonsingular projective variety Y over $\mathbb{Z}$ or more generally, over a ring of algebraic integers, and if $Y_{\mathbb{C}}$ is the complex manifold corresponding to Y, then $b_i = \deg P_i(X,T)$ equals the

ith Betti number of $Y_{\mathbb{C}}$. In particular, the number χ in (ii) is the Euler characteristic of $Y_{\mathbb{C}}$.

These conjectures were proved in the case of curves, i.e., when $n = 1$, by Weil himself in the 40's. In this particular case when X is a nonsingular projective curve, we have $b_0 = b_2 = 1$ and $b_1 = 2g$ where g is the *genus* of X. Thus if we write ω_j for ω_{1j}, then from (ii) and (iii), we see that

$$a_r = |X(\mathbb{F}_{q^r})| = 1 + q^r - \sum_{j=1}^{2g} w_j^r\,. \tag{3}$$

Now $|\omega_j| = \sqrt{q}$, and so we obtain our first classical estimate:

$$\Big|\, |X(\mathbb{F}_q)| - \pi_1 \,\Big| \le 2g\sqrt{q} \quad \text{where } \dim X = 1 \text{ and } \pi_1 = 1 + q. \tag{4}$$

This is known as *Weil's inequality.* We remark that if in (3), we write $\omega_j = \sqrt{q}e^{2\pi i\theta_j}$, where $0 \le \theta_j \le 1$, then by a classical theorem of Kronecker (see, for example, [12, Ch. XXIII]), for every $\epsilon > 0$, we can find (infinitely many) $r \ge 1$ such that

$$\Big| \sum_{j=1}^{2g} e^{2\pi i r\theta_j} - 2g \Big| < \epsilon.$$

Thus it follows that the constant $2g$ in (4) is the best possible, in general. However, for a given q, improvements can be made. This was observed, for example, by Serre who refined (4) to obtain the following estimate.

$$\Big|\, |X(\mathbb{F}_q)| - \pi_1 \,\Big| \le g[2\sqrt{q}] \quad \text{where } \dim X = 1 \text{ and } \pi_1 = 1 + q. \tag{5}$$

Here $[2\sqrt{q}]$ denotes, as usual, the greatest integer $\le 2\sqrt{q}$. For example, if $q = 2$ and $g = 50$, the Weil bound for $|X(\mathbb{F}_q)|$ is 144 while the Serre bound is 103.

The genus g of a nonsingular projective curve X is, in general, difficult to determine, especially if we describe X by its defining equations. However, if we fix an embedding of X in a projective space, and let d denote the degree of X, then the genus satisfies the bound $g \le (d-1)(d-2)/2$. Thus (4) implies a similar inequality with $2g$ replaced by $(d-1)(d-2)$. This weaker inequality was generalized by Lang and Weil [24] in 1954 to varieties of arbitrary dimension. They proved that if X is a projective variety in $\mathbb{P}^N$ defined over $\mathbb{F}_q$ and of dimension n and degree d, then

$$\Big|\, |X(\mathbb{F}_q)| - \pi_n \,\Big| \le (d-1)(d-2)q^{n-(1/2)} + Cq^{n-1}, \tag{6}$$

where C is a constant depending only on N, n and d (so that it is independent of q). We will refer to (6) as the *Lang–Weil inequality.*

The first part of Weil's conjecture about the rationality of $Z(X, T)$ was proved in 1960 by Dwork [7]. In fact, the rationality was conjectured and proved for arbitrary varieties that are not necessarily projective or nonsingular. Dwork's proof used methods from p-adic analysis, which were quite different from the heuristic approach suggested by Weil for proving his conjectures. Weil's idea was based on the simple observation that an element a in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ is in $\mathbb{F}_q$ if and only if $a^q = a$. In other words, a is the fixed point of the Frobenius map $F : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$ which sends x to x^q. The Frobenius map can be extended to an affine or projective space over $\overline{\mathbb{F}}_q$ by simply raising each coordinate to its

qth power. It follows, then, that the number of $\mathbb{F}_q$-rational points of a variety X (in the projective space over $\overline{\mathbb{F}}_q$) is the number of fixed points of X under the Frobenius map. Similarly, the points of $X(\mathbb{F}_{q^r})$ correspond to the fixed points of the r-fold composite F^r of the Frobenius map. Now we remember from Topology, the Lefschetz Fixed Point Formula which says that if Y is a complex manifold and $f : Y \to Y$ is a map with isolated fixed points, then the number of fixed points of f^r is the alternating sum of the traces of the (linear) maps induced by f^r on the cohomology spaces of Y. Thus,

$$\text{Number of fixed points of } f^r = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}\left(f^r | H^i(Y, \mathbb{C})\right).$$

To carry this idea to varieties over finite fields, it was felt desirable to develop a suitable cohomology theory in which a similar trace formula holds. This task was accomplished by Artin and Grothendieck around 1963. They showed that if p is the characteristic of $\mathbb{F}_q$ and ℓ is any prime different from p, then to a projective variety X over $\mathbb{F}_q$, we can associate the *étale ℓ-adic cohomology spaces* $H^i(\bar{X}, \mathbb{Q}_\ell)$. Here, $\bar{X} = X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ denotes the variety corresponding to X over the algebraic closure of $\mathbb{F}_q$, and $\mathbb{Q}_\ell$ denotes, as usual, the field of ℓ-adic numbers. These cohomology spaces are finite-dimensional vectors spaces over $\mathbb{Q}_\ell$. Moreover, if $n = \dim X$, then $H^i(\bar{X}, \mathbb{Q}_\ell)$ vanish if $i < 0$ or $i > 2n$. The Frobenius map on $\bar{X}$ induces an endomorphism of $H^i(\bar{X}, \mathbb{Q}_\ell)$, and the following analogue of the Lefschetz Trace Formula holds.

$$|X(\mathbb{F}_{q^r})| = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}\left(F^r | H^i(\bar{X}, \mathbb{Q}_\ell)\right). \tag{7}$$

We will refer to (7) as the *Grothendieck-Lefschetz Trace Formula.* Now if we let $P_{i,\ell}(X,T) = \det(1 - TF | H^i(\bar{X}, \mathbb{Q}_\ell))$, for $0 \le i \le 2n$, then it is a formal and easy consequence of (7) that

$$Z(X,T) = \frac{P_{1,\ell}(X,T) P_{3,\ell}(X,T) \cdots P_{2n-1,\ell}(X,T)}{P_{0,\ell}(X,T) P_{2,\ell}(X,T) \cdots P_{2n,\ell}(X,T)}. \tag{8}$$

Thus, the rationality of $Z(X,T)$ is proved. Notice that if we factor $P_{i,\ell}(X,T)$ as in (2), then we see that the reciprocal roots $\omega_{ij} = \omega_{ij,\ell}$ are the eigenvalues of the Frobenius endomorphism on $H^i(\bar{X}, \mathbb{Q}_\ell)$, and so we can rewrite (7) as

$$|X(\mathbb{F}_{q^r})| = \sum_{i=1}^{2n} (-1)^i \sum_{j=1}^{b_{i,\ell}} \omega_{ij}^r, \quad \text{where } b_{i,\ell} = \dim_{\mathbb{Q}_\ell} H^i(\bar{X}, \mathbb{Q}_\ell). \tag{9}$$

In case X is nonsingular, then it was shown that the ℓ-adic Betti numbers $b_{i,\ell}$ are independent of ℓ and moreover, Poincaré duality holds, which means, in particular, that $b_{i,\ell} = b_{2n-i,\ell}$ for $0 \le i \le 2n$. These facts and some elementary Linear Algebra imply the functional equation for $Z(X,T)$ conjectured by Weil. Independent proofs of rationality and the functional equation for $Z(X,T)$ were also given by Lubkin [25, 26] around 1967.

For the étale cohomology spaces $H^i(\bar{X}, \mathbb{Q}_\ell)$, a *Comparison Theorem* holds in the case when X is nonsingular and obtained by 'reduction mod p' from a nonsingular variety in characteristic zero. This implies (iv) in the list of Weil conjectures. Thus, what remains to be proved is (iii), which is commonly referred to as the

Riemann hypothesis[1] for varieties over finite fields. This Riemann hypothesis was finally proved by Deligne [5] in 1973. As a first application of his work, Deligne [5, Thm. 8.1] gave the following estimate for the number of points of nonsingular complete intersections:

$$\Big| |X(\mathbb{F}_q)| - \pi_n \Big| \le b'_n \, q^{n/2}. \tag{10}$$

Here X is assumed to be a nonsingular complete intersection in $\mathbb{P}^N$, of dimension n, defined over $\mathbb{F}_q$ and b'_n is its primitive nth Betti number. We will explain these terms and describe explicit formulae for b'_n in Section 3. Returning to the general case, another proof of the Riemann hypothesis and a weaker version of it for varieties that are not necessarily nonsingular, was obtained by Deligne in a subsequent paper [6]. In effect, Deligne's result for arbitrary projective varieties states that

(11) *the eigenvalues* $\omega_{ij,\ell}$ *of* $F \mid H^i_c(\bar{X}, \mathbb{Q}_\ell)$ *are pure of weight* $\le i$.

Here, we call $\alpha \in \bar{\mathbb{Q}}_\ell$ *pure of weight* r if α is an algebraic integer and if $|\iota(\alpha)| = q^{r/2}$ for any embedding ι of $\bar{\mathbb{Q}}_\ell$ into $\mathbb{C}$. We will refer to (11) as *Deligne's Main Theorem.*

Both Grothendieck-Lefschetz Trace Formula (7) and Deligne's Main Theorem (11) are, in fact, valid for objects X that are more general than projective varieties (namely, separated schemes of finite type[2] over $\mathbb{F}_q$, of dimension n), and these two results are the most fundamental tools for much of the subsequent work on the number of points of varieties over finite fields.

To end this section, we provide some pointers to the references for the results described in this section. Weil's conjectures were formally stated in his article [42] in the *Bulletin.* The improvement in Weil's inequality by Serre is given in [36]. The proof of Serre bound is rather short and elementary — it mainly uses things like the AM-GM inequality! For the Lang-Weil inequality, the original paper [24] is probably the best reference. An overview of Dwork's proof [7] can be found in the memorial article by Katz and Tate [21] in the *Notices.* The idea of using a suitable analogue of the Lefschetz fixed point formula for counting points of varieties over finite fields appears in Weil's ICM address [43]. The theory of étale topology first appeared in the Harvard notes of Artin [2], and later in SGA [3]. One of the earlier elementary exposition can be found in an article [32] by Mumford. A more recent review is given by Katz [18]. There is also the book of Milne [28] as well as his lecture notes [29] that are more elementary and available for free! An overview of Deligne's proof of Riemann hypothesis and some of its spectacular applications such as the proof of Ramanujan-Peterson conjecture, is given in the article of Katz [17]. The book by Freitag and Kiehl [8] contains a proof of Weil conjectures along with some background material and furthermore, an article by Dieudonné giving a historical introduction to Weil conjectures. An overview of the Weil conjectures also appears in an appendix to Hartshorne's book [13]. There are now shorter proofs of the Riemann hypothesis for varieties over finite fields: by Laumon in 1984 and most recently by Katz [20]. For an account of Laumon's work and for

[1] This nomenclature will be clear if we translate (iii) as a condition for the function $\zeta(X, s) = Z(X, q^{-s})$.

[2] In the case of schemes of this type, it is better to work with étale ℓ-adic cohomology with *compact supports.*

more on Deligne's Main Theorem (11), we refer to the recent book [22] by Kiehl and Weissauer.

2. An Example

In this section, we shall illustrate the conjectures of Weil and the Trace Formula by a rather substantial example. This example involves the partial flag manifolds, which are not only of interest in Algebraic Geometry, but also in Combinatorics, Representation Theory and Topology. However, for the general results described in later sections, this example is of no direct relevance, and it may be skipped at a first reading.

Let k be a field and V be a vector space of dimension m over k. Let $\underline{\ell} = (\ell_1, \dots, \ell_s)$ be a sequence of integers such that $0 < \ell_1 < \cdots < \ell_s < m$. By a *partial flag* of dimension $\underline{\ell}$ we mean a sequence $(V_1, \dots, V_s)$ of subspaces of V such that $V_1 \subset \cdots \subset V_s$ and $\dim V_i = \ell_i$ for $1 \le i \le s$. Let $\mathcal{F}_{\underline{\ell}}(V)$ denote the set of partial flags of dimension $\underline{\ell}$. Two special cases of this arise more frequently. If $s = 1$ and we write $l = \ell_1$, then $\mathcal{F}_{\underline{\ell}}(V)$ is the *Grassmannian* $\mathrm{Gr}_l(V)$ of l-planes in the m-space (over k). At the other extreme, if $s = m-1$, then we necessarily have $\ell_i = i$ for $1 \le i \le s$, and in this case $\mathcal{F}_{\underline{\ell}}(V)$ is the space of *full flags* or *complete flags*. It is elementary and well-known that any Grassmannian embeds in a projective space[3] as a projective variety given by the vanishing of certain quadratic homogeneous polynomials. Using this, we obtain natural maps

$$\mathcal{F}_{\underline{\ell}}(V) \hookrightarrow \mathrm{Gr}_{\ell_1}(V) \times \cdots \times \mathrm{Gr}_{\ell_1}(V) \hookrightarrow \mathbb{P}\left(\bigwedge^{\ell_1} V\right) \times \cdots \times \mathbb{P}\left(\bigwedge^{\ell_s} V\right)$$

and the latter product of projective spaces embeds naturally into a big projective space via the so called Segre embedding. In this way, $\mathcal{F}_{\underline{\ell}}(V)$ becomes a projective algebraic variety, and the defining equations are known to have integer coefficients (see, for example, [9, Sec. 9.1] or [16, Sec. 1.8]). Moreover, $\mathcal{F}_{\underline{\ell}}(V)$ is smooth and to see this, it suffices to note that $\mathcal{F}_{\underline{\ell}}(V)$ is a homogeneous space of the form G/P, where $G = \mathrm{GL}(V)$ is the group of invertible linear transformations of V (which is identified with $\mathrm{GL}_m(k)$ once we fix a basis of V) and P is the stabilizer of a partial flag with respect to the natural action of G on $\mathcal{F}_{\underline{\ell}}(V)$[4].

Now suppose $k = \mathbb{F}_q$. Then we can easily calculate the number $|\mathcal{F}_{\underline{\ell}}(V)(\mathbb{F}_q)|$ of $\mathbb{F}_q$-rational points of $\mathcal{F}_{\underline{\ell}}(V)$. For this, first note that the number of l-dimensional subspaces W of the m-dimensional vector space V over $\mathbb{F}_q$ can be computed as follows. A basis $\{w_1, \dots, w_l\}$ of a l-dimensional subspace is obtained by successively choosing w_1 in $V \setminus \{0\}$, w_2 in $V \setminus (\mathbb{F}_q\, w_1)$, w_3 in $V \setminus (\mathbb{F}_q\, w_1 + \mathbb{F}_q\, w_2)$, and so on. Thus, there are $(q^m - 1)(q^m - q)(q^m - q^2) \cdots (q^m - q^{l-1})$ choices. Two bases determine the same subspace if and only if the corresponding $l \times m$ matrices differ by a factor in $\mathrm{GL}_l(\mathbb{F}_q)$. The cardinality of $\mathrm{GL}_l(\mathbb{F}_q)$ is the number of choices of l

[3] This embedding is known as *Plücker embedding*, and it may be described as follows. To a subspace W in the Grassmannian $\mathrm{Gr}_l(V)$, we associate the point of the projective space $\mathbb{P}(\bigwedge^l V) = \mathbb{P}_k^{\binom{m}{l}-1}$ corresponding to the 1-dimensional subspace of the exterior product $\bigwedge^l V$ spanned by $w_1 \wedge \cdots \wedge w_l$, where $\{w_1, \dots, w_l\}$ is any k-basis of W.

[4] Fix a basis $\{e_1, \dots, e_m\}$ of V. If we consider the partial flag $(E_{\ell_1}, \dots, E_{\ell_s})$ where $E_{\ell_i} = \mathrm{span}\{e_1, \dots, e_{\ell_i}\}$, then its stabilizer P corresponds to matrices $g = (g_{uv}) \in \mathrm{GL}_m(k)$ with $g_{uv} = 0$ for $\ell_{i-1} < u \le \ell_i$ and $1 \le v \le \ell_i$ $(i = 1, \dots, s+1)$ with the convention that $\ell_0 = 0$ and $\ell_{s+1} = m$.

linearly independent row vectors in ${\mathbb{F}_q}^m$, and arguing as before, we see that this number is $(q^l-1)(q^l-q)\cdots(q^l-q^{l-1})$. It follows that

$$|\mathrm{Gr}_l(V)(\mathbb{F}_q)| = \begin{bmatrix} m \\ l \end{bmatrix}_q := \frac{(q^m-1)(q^m-q)\cdots(q^m-q^{l-1})}{(q^l-1)(q^l-q)\cdots(q^l-q^{l-1})}.$$

The expression on the right is known as the *Gaussian binomial coefficient* corresponding to m and l. As for calculating $\mathcal{F}_{\underline{\ell}}(V)(\mathbb{F}_q)$, we note that the inclusion relations in a partial flag $(V_1,\dots,V_s)$ will disappear if we consider instead the subspaces $V_1, V_2/V_1, \dots, V_s/V_{s-1}$ of $V, V/V_1, \dots, V/V_{s-1}$, respectively. This leads to the following formula for the number of $\mathbb{F}_q$-rational points of $\mathcal{F}_{\underline{\ell}}(V)$ as a *Gaussian multinomial coefficient*:

$$|\mathcal{F}_{\underline{\ell}}(V)(\mathbb{F}_q)| = \begin{bmatrix} m \\ \ell_1, \ell_2-\ell_1, \dots, \ell_s-\ell_{s-1}, m-\ell_s \end{bmatrix}_q := \prod_{i=1}^{s+1} \begin{bmatrix} m-\ell_{i-1} \\ \ell_i-\ell_{i-1} \end{bmatrix}_q$$

with the convention that $\ell_0 = 0$ and $\ell_{s+1} = m$.

Now suppose $k=\mathbb{C}$. Then $\mathcal{F}_{\underline{\ell}}(V)$ is a compact complex manifold[5]. Moreover, its Betti numbers can be computed easily since we have a nice cellular decomposition. This decomposition is obtained as follows. Fix a basis $\{e_1,\dots,e_m\}$ of V, and consider the standard full flag $(E_1,\dots,E_{m-1})$ where $E_j = \mathrm{span}\{e_1,\dots,e_j\}$ for $1 \le j \le m-1$. Set $E_0 = \{0\}$ and $E_m = V$. Given any $(V_1,\dots,V_s) \in \mathcal{F}_{\underline{\ell}}(V)$, set $V_{s+1} = V$, $\ell_{s+1} = m$, and define $r(i,j) = \dim V_i \cap E_j$ for $1 \le i \le s+1$ and $0 \le j \le m$. Note that

$$0 = r(i,0) \le r(i,1) \le r(i,2) \le \cdots \le r(i,m) = \ell_i \quad \text{for } i = 1,\dots,s+1.$$

The consecutive terms of the sequence $(r(i,1),\dots,r(i,m))$ differ by at most 1 [because the jth coordinate map $V_i \cap E_j \to \mathbb{C}$ has kernel $V_i \cap E_{j-1}$], and there are exactly ℓ_i jumps in this sequence [a *jump* is an index $j \in \{1,\dots,m\}$ such that $r(i,j) = r(i,j-1)+1$]. Moreover, since $V_{i+1} \cap E_{j-1} = V_{i+1} \cap E_j$ implies that $V_i \cap E_{j-1} = V_i \cap E_j$, we see that the ℓ_i jumps in $(r(i,1),\dots,r(i,m))$ are included in the ℓ_{i+1} jumps in $(r(i+1,1),\dots,r(i+1,m))$. It follows that there is a unique permutation σ of $\{1,\dots,m\}$ such that $\sigma(1),\dots,\sigma(\ell_i)$ are precisely the jumps in $(r(i,1),\dots,r(i,m))$, and

$$\sigma(\ell_{i-1}+1) < \sigma(\ell_{i-1}+2) < \cdots < \sigma(\ell_i) \quad \text{for } i = 1,\dots,s+1. \tag{12}$$

We let $W_{\underline{\ell}}$ denote the set of permutations $\sigma \in S_m$ satisfying (12). The dimension array $(r(i,j))$ is determined by the corresponding $\sigma \in W_{\underline{\ell}}$ as follows:

$$r(i,j) = r_\sigma(i,j), \quad \text{where } r_\sigma(i,j) := \Big| \{u \in \{1,\dots,\ell_i\} : \sigma(u) \le j\} \Big|.$$

Therefore, we have a decomposition of $\mathcal{F}_{\underline{\ell}}(V)$ as a disjoint union:

$$\mathcal{F}_{\underline{\ell}}(V) = \coprod_{\sigma \in W_{\underline{\ell}}} \Omega_\sigma, \tag{13}$$

[5]When $k=\mathbb{C}$, we can consider orthonormal bases, and note that there is a transitive action of the unitary group $U(n)$ on the partial flags so that $\mathcal{F}_{\underline{\ell}}(V)$ is a quotient of $U(n)$. The compactness of $\mathcal{F}_{\underline{\ell}}(V)$ is essentially a consequence of the fact that $U(n)$ is a compact group.

where for any $\sigma \in W_{\underline{\ell}}$,

$$\Omega_\sigma = \left\{ (V_1, \dots, V_s) \in \mathcal{F}_{\underline{\ell}}(V) : \begin{array}{l} \dim V_i \cap E_j = r_\sigma(i,j), \text{ for} \\ 1 \le i \le s+1, \ 1 \le j \le m \end{array} \right\}.$$

We now show that every Ω_σ is isomorphic to a cell, i.e., an affine space over $\mathbb{C}$. Fix $\sigma \in W_{\underline{\ell}}$. Given $(V_1, \dots, V_s) \in \Omega_\sigma$, we can recursively find vectors $\mathbf{x}_1, \dots, \mathbf{x}_m$ in V such that $\{\mathbf{x}_1, \dots, \mathbf{x}_{\ell_i}\}$ is a basis of $V_i = V_i \cap E_m$, and more generally, for $1 \le i \le s+1$ and $1 \le j \le m$,

$$\{\mathbf{x}_u : 1 \le u \le \ell_i \text{ and } \sigma(u) \le j\} \text{ is a basis of } V_i \cap E_j, \tag{14}$$

and further, if $(x_{u1}, \dots, x_{um})$ are the coordinates of $\mathbf{x}_u$ (with respect to the basis $\{e_1 \dots, e_m\}$ of V), then

$$x_{u\sigma(u)} = 1, \ x_{uv} = 0 = x_{u\sigma(u')} \text{ for } v > \sigma(u) \text{ and } u' < u, \tag{15}$$

where u, v, u' vary in $\{1, \dots, m\}$. The partial flag $(V_1, \dots, V_s) \in \Omega_\sigma$ and the matrix (x_{uv}) with rows $\mathbf{x}_1, \dots, \mathbf{x}_m$ satisfying (14) and (15) clearly determine each other uniquely. Moreover from (15) it is clear that the number of 'free entries' in this matrix are those x_{uv} for which $v = \sigma(u')$ with $u < u'$ and $\sigma(u) > \sigma(u')$. It follows that

$$\Omega_\sigma \simeq \mathbb{C}^{\mathrm{inv}(\sigma)} \simeq \mathbb{R}^{2\,\mathrm{inv}(\sigma)},$$

where $\mathrm{inv}(\sigma)$ denotes the number of inversions in the permutation σ. Therefore, (13) is a cellular decomposition of $\mathcal{F}_{\underline{\ell}}(V)$. Since there are no (real) cells in odd dimensions, it follows from standard topological arguments that the odd dimensional Betti numbers of $\mathcal{F}_{\underline{\ell}}(V)$ are zero while

$$b_{2\nu}(\mathcal{F}_{\underline{\ell}}(V)) = \left| \{\sigma \in W_{\underline{\ell}} : \mathrm{inv}(\sigma) = \nu\} \right|, \quad \text{for } \nu \ge 0. \tag{16}$$

The reason why the formula for the number of $\mathbb{F}_q$-rational points of $\mathcal{F}_{\underline{\ell}}(V)$ is in accordance with (16) and the Weil conjectures is the following combinatorial identity that is about 90 years old and goes back to MacMahon (cf [1, Thm. 3.4]):

$$\begin{bmatrix} m \\ \ell_1, \ell_2 - \ell_1, \dots, \ell_s - \ell_{s-1}, m - \ell_s \end{bmatrix}_q = \sum_{\nu \ge 0} \mathrm{Inv}(\underline{\ell}\,; \nu) q^\nu, \tag{17}$$

where $\mathrm{Inv}(\underline{\ell}\,;\nu)$ denotes the number of permutations $\tau_1\tau_2\dots\tau_m$ of the multiset $M_{\underline{\ell}} := \{1^{\ell_1} 2^{\ell_2 - \ell_1} \dots s^{\ell_s - \ell_{s-1}} (s+1)^{m-\ell_s}\}$ with exactly ν inversions[6]. There is a natural inversion-preserving bijection between the permutations in $W_{\underline{\ell}}$ and the permutations of the multiset $M_{\underline{\ell}}$[7]. Thus, from (16) and (17), we obtain the identity

$$\left| \mathcal{F}_{\underline{\ell}}(V)(\mathbb{F}_q) \right| = \sum_{\nu \ge 0} b_{2\nu}(\mathcal{F}_{\underline{\ell}}(V)) q^\nu,$$

which implies that the zeta function of $\mathcal{F}_{\underline{\ell}}(V)(\mathbb{F}_q)$ is a rational function of the desired form and the Riemann hypothesis is satisfied.

---

[6] Just like permutations, the inversions of a multiset permutation $\tau_1\tau_2\dots\tau_m$ are the pairs (τ_i, τ_j) such that $1 \le i < j \le m$ and $\tau_i > \tau_j$.

[7] This bijection is obtained as follows. Given $\sigma \in W_{\underline{\ell}}$, let τ be the permutation of $M_{\underline{\ell}}$ with i in the spots marked by $\sigma(\ell_{i-1}+1), \dots, \sigma(\ell_i)$, that is, $\tau_j = i$ if $\ell_{i-1} < \sigma^{-1}(j) \le \ell_i$. For example, if $\ell_1 = 4$, $\ell_2 = 6$, $\ell_3 = 7$ and $\ell_4 = 8 = m$, then the multiset permutation corresponding to $\sigma = 12586734$ is $\tau = 11341221$.

2.1. *Remarks.* 1. The cellular decomposition (13) and the equivalence between Ω_σ and an affine space of dimension $\mathrm{inv}(\sigma)$ is, in fact, valid when $\mathbb{C}$ is replaced by any field k. If we take $k = \mathbb{F}_q$, then in view of the abovementioned bijection between $W_{\underline{\ell}}$ and multiset permutations, we obtain another proof of MacMahon's identity (17).
2. In another direction, we can use MacMahon's identity (17) together with Weil Conjectures to deduce the description (16) for the Betti numbers, and consequently, a description of the Poincaré polynomial of $\mathcal{F}_{\underline{\ell}}(V)$ as the multinomial coefficient in (17) with q replaced by q^2. Here, one has to make use of the fact that $\mathcal{F}_{\underline{\ell}}(V)$ is smooth and the number of $\mathbb{F}_{q^r}$-rational points of $\mathcal{F}_{\underline{\ell}}(V)$ is a polynomial in q^r, for every $r \geq 1$. Alternative descriptions of $b_{2\nu}(\mathcal{F}_{\underline{\ell}}(V))$ are also possible using combinatorial identities such as MacMahon's identity for $\mathrm{Inv}(\underline{\ell}\,; \nu)$ in terms of the number of multiset permutations with 'major index' ν. In the Grassmannian case ($s = 1$), this Betti number has an interpretation in terms of partitions, namely $b_{2\nu}(\mathrm{Gr}_l(V))$ is the number of partitions of ν with at most l parts, each part $\leq m - l$. For proofs of these combinatorial facts, we refer to [1, Sec. 3.4].
3. Using the cellular decomposition (13), or alternatively, the formula for the number of $\mathbb{F}_q$-rational points of $\mathcal{F}_{\underline{\ell}}(V)$ coupled with Weil conjectures, we see that the dimension of $\mathcal{F}_{\underline{\ell}}(V)$ (as a projective variety) is equal to

$$\sum_{1 \leq i < j \leq s+1} (\ell_i - \ell_{i-1})(\ell_j - \ell_{j-1}) = \binom{m+1}{2} - \sum_{i=1}^{s+1} \binom{\ell_i - \ell_{i-1} + 1}{2}.$$

This number is simply $l(m - l)$ in the Grassmannian case ($s = 1$ and $l = \ell_1$), whereas in the case of the full flag manifold ($s = m - 1$), this is $m(m - 1)/2$.
4. We indicated earlier that $\mathcal{F}_{\underline{\ell}}(V)$ can be identified as a quotient G/P of $G = \mathrm{GL}(V)$. In this setting, $W_{\underline{\ell}}$ can be identified as W/W_P, where W and W_P are the Weyl groups of G and P, respectively [in fact, $W \simeq S_m$ whereas $W_P \simeq S_{\ell_1} \times S_{\ell_2 - \ell_1} \times \cdots \times S_{\ell_{s+1} - \ell_s}$]. Moreover, if we let B denote the subgroup of G consisting of all upper triangular invertible matrices, then the cell Ω_σ can be identified with the double coset $B\sigma P/P$. Thus (13) is an instance of the so called Bruhat decomposition. Note also that if σ is any permutation, then $\mathrm{inv}(\sigma)$ is the *length* of σ, as an element of a Coxeter group. For more on this point of view, see, for example, [16].

Basic facts about Grassmannians can be found in several texts. The cellular decomposition for Grassmannians is explained beautifully in the book of Milnor and Stasheff [31]. The relation of the Betti numbers of Grassmannians with the Gaussian binomial coefficient, in light of Weil conjectures, is pointed out, for instance, in Stanley's paper [41]. This paper also discusses the example of partial flag manifolds, albeit rather briefly. As remarked by Stanley [41], the known results about Grassmannians were one of the original pieces of evidence for the Weil conjectures. The cellular decomposition for full flag manifolds is given nicely in the *cours* of Manivel [27, Sec. 3.6]. A relatively recent book by Fulton [9] contains a good exposition of the basic facts about partial flag manifolds and the connection with Representation Theory. Although the cellular decomposition and a presentation for the cohomology (á la Borel) is discussed mostly in the case of full flag manifolds, a quick outline of its generalizations to partial flag manifolds is given towards the end of Ch. 10 in [9]. As for the various combinatorial facts mentioned in this section, it suffices to consult the encyclopedia volume of Andrews [1]; see also the book of Stanley [40] for some of this material and more.

3. Complete Intersections over Finite Fields

An algebraic variety defined by a single equation is called a hypersurface. This has codimension 1 in the ambient space. Conversely, if a variety is of codimension 1, then it can be shown that the variety can be defined by a single equation (see, for example, [37, Ch. 1, §6]). For arbitrary varieties, a similar result is not true. In case a variety of codimension r is defined by r equations, it is called a complete intersection. To be more precise, by a *complete intersection* over a field k, we shall mean in this article an irreducible projective variety[8] X in $\mathbb{P}_k^N$ of dimension n such that its homogeneous ideal $I(X)$ can be generated by $N-n$ homogeneous polynomials in $N+1$ variables over k. If $f_1, \ldots, f_r$ is a set of $r = N-n$ homogeneous generators for $I(X)$, then the degrees $d_1, \ldots, d_r$ depend only on $X \subseteq \mathbb{P}^N$ and not on the choice of generators. This follows, for example, by noting that the Hilbert series of X (cf. [34, Ex. 7.15, p. 350]) is given by

$$\mathcal{H}_X(T) := \sum_{m=0}^{\infty} (\dim_k R_m) T^m = \frac{(1-T^{d_1})(1-T^{d_2})\cdots(1-T^{d_r})}{(1-T)^{N+1}} \tag{18}$$

where R denotes the homogeneous coordinate ring of X and R_m its mth homogeneous component. It is customary to arrange $d_1, \ldots, d_r$ such that $d_1 \geq d_2 \geq \cdots \geq d_r$, and call the r-tuple $\mathbf{d} = (d_1, \ldots, d_r)$ the *multidegree* of X. Notice that an easy consequence of (18) is that the degree of X equals the product $d_1 d_2 \cdots d_r$.

The cohomology spaces of nonsingular complete intersections have a particularly simple structure, at least for all except one. Since we are mainly interested in varieties over finite field, we let $k = \mathbb{F}_q$ and consider étale ℓ-adic cohomology where ℓ is a prime different from $p = \operatorname{char} \mathbb{F}_q$.

Now if X is a nonsingular complete intersection in $\mathbb{P}^N$ defined over $\mathbb{F}_q$ and of dimension n, then for $0 \leq i \leq 2n$, we have

$$H^i(\bar{X}, \mathbb{Q}_\ell) = \begin{cases} \mathbb{Q}_\ell(-i/2) & \text{if } i \text{ is even and } i \neq n \\ 0 & \text{if } i \text{ is odd and } i \neq n. \end{cases} \tag{19}$$

Here $\mathbb{Q}_\ell(-i/2)$ denotes the 1-dimensional space $\mathbb{Q}_\ell$ with a 'twist' by the integer $-i/2$; the twist signifies that the Frobenius endomorphism[9] acts on this space as multiplication by $q^{i/2}$. At any rate, the Betti numbers $b_{i,\ell}(\bar{X})$ are either 1 or 0 according as i is even or odd, except if $i = n$. As for the middle cohomology $H^n(\bar{X}, \mathbb{Q}_\ell)$, it can be shown that its dimension, namely, $b_{i,\ell}(\bar{X})$ depends only on n, N and the multidegree $\mathbf{d}$. Thus we denote this by $b_n(N, \mathbf{d})$. Also we let

$$b'_n(N, \mathbf{d}) = \begin{cases} b_n(N, \mathbf{d}) - 1 & \text{if } n \text{ is even} \\ b_n(N, \mathbf{d}) & \text{if } n \text{ is odd.} \end{cases}$$

---

[8] Actually, by a *variety* we mean an irreducible variety, but still, the word *irreducible* is sometimes added for emphasis. More precisely, by a *projective variety* defined over a field k, we mean a closed subscheme of $\mathbb{P}_k^N$ which is geometrically integral.

[9] For technical reasons, we consider here (and hereafter) the *geometric Frobenius* which is induced not by the map $x \mapsto x^q$ but by its inverse.

We call $b'_n(N, \mathbf{d})$ the *primitive* nth *Betti number* of the nonsingular complete intersection X in $\mathbb{P}^N$ of dimension n and multidegree $\mathbf{d}$. This primitive Betti number is given explicitly by the following formula.

$$b'_n(N, \mathbf{d}) = (-1)^{n+1}(n+1) + \sum_{c=r}^{N} (-1)^{N+c} \binom{N+1}{c+1} \sum_{\nu \in M(c)} \mathbf{d}^{\nu}, \tag{20}$$

where $M(c)$ denotes the set of all r-tuples $\nu = (\nu_1, \ldots, \nu_r)$ of positive integers such that $\nu_1 + \cdots + \nu_r = c$, and for any such tuple ν, $\mathbf{d}^{\nu}$ denotes the product $d_1^{\nu_1} \cdots d_r^{\nu_r}$, and where $r = N - n$, as before.

We remark that the formula (20) is equivalent to the following formula for the Euler characteristic of a nonsingular complete intersection X in $\mathbb{P}^N$ of dimension n and multidegree $\mathbf{d} = (d_1, \ldots, d_r)$:

$$\chi(X) := \sum_{i=0}^{2n} (-1)^i b_i(X) = d \sum_{c=0}^{n} (-1)^c \binom{N+1}{c+r+1} \sum_{\nu \in M_0(c)} \mathbf{d}^{\nu}, \tag{21}$$

where $M_0(c)$ denotes the set of all r-tuples $\nu = (\nu_1, \ldots, \nu_r)$ of nonnegative integers such that $\nu_1 + \cdots + \nu_r = c$, and d denotes the product $d_1 \cdots d_r$. The equivalence of (20) and (21) follows from (19), which gives the relation $\chi(X) = n + 1 + (-1)^n b'_n(N, \mathbf{d})$. In fact, the genesis of (20) and (21) is in a classical formula of Hirzebruch [14, Satz 2.4], which shows that for smooth complete intersections V_n in $\mathbb{P}^N_{\mathbb{C}}$ of dimension $n = N - r$, the generating function for the Euler characteristics is given as follows.

$$\sum_{n=0}^{\infty} \chi(V_n) T^n = \frac{d_1 \ldots d_r}{(1-T)^2} \prod_{i=1}^{r} \frac{1}{1 + (d_i - 1)T}\ . \tag{22}$$

It is an elementary exercise to derive (20) and/or (21) from (22) when X is obtained by 'reduction mod p' of a smooth complete intersection in characteristic zero. To pass from the complex case to positive characteristic, one appeals to an appropriate Comparison Theorem (see, for example, [28, Rem. 4.20]).

The formula for $b'_n(N, \mathbf{d})$ given above is rather complicated, and in applications, it is sometimes necessary to quickly find an estimate for this number. To this end, some bounds are obtained in [10]. First, we note that there is the following simple bound:

$$b'_n(N, \mathbf{d}) \le \binom{N+1}{n} (\delta + 1)^N \quad \text{where} \quad \delta = \max\{d_1, \ldots, d_r\}.$$

A more precise, but slightly complicated, bound is the following.

$$b'_n(N, \mathbf{d}) \le (-1)^{n+1}(n+1) + d \binom{N+1}{n} (\delta + 1)^n,$$

where δ is as above and d denotes the product $d_1 \cdots d_r$. In some special cases, we can work directly with the explicit formula and get a bound which is better than the two bounds above. For example, if $n = 1$ and d is as above, then it can be seen that

$$b'_1(N, \mathbf{d}) \le (d-1)(d-2), \text{ with equality } \Leftrightarrow N = 2. \tag{23}$$

In other words, the equality holds if and only if X is a plane curve.

From the explicit formula and the bounds for $b'_n = b'_n(N, \mathbf{d})$, it is clear that Deligne's inequality (10) can be effectively used in applications. There is, however, the hypothesis that X has to be nonsingular. The following result from [10] extends Deligne's inequality to the case of complete intersections that are possibly singular. We use here the notion of the singular locus $\operatorname{Sing} X$ of a variety X. Its dimension $s = \dim \operatorname{Sing} X$ measures how far X is from being singular. If X is nonsingular, $\operatorname{Sing} X$ is empty and $s = -1$, by convention. If, for example X is normal, then $s \leq n-2$. In general, if X is an irreducible projective variety of dimension n, then $-1 \leq s \leq n-1$.

3.1. Theorem. *Let X be an irreducible complete intersection of dimension n in $\mathbb{P}^N_{\mathbb{F}_q}$, defined by $r = N - n$ equations, with multidegree $\mathbf{d} = (d_1, \ldots, d_r)$, and let s be an integer such that* $\dim \operatorname{Sing} X \leq s \leq n-1$. *Then*

$$\Big| |X(\mathbb{F}_q)| - \pi_n \Big| \leq b'_{n-s-1}(N-s-1, \mathbf{d})\, q^{(n+s+1)/2} + C_s(X) q^{(n+s)/2},$$

where $C_s(X)$ is a constant independent of q. If X is nonsingular, then $C_{-1}(X) = 0$. If $s \geq 0$, then

$$C_s(X) \leq 9 \times 2^r \times (r\delta + 3)^{N+1} \quad \text{where} \quad \delta = \max\{d_1, \ldots, d_r\}.$$

The above theorem has some interesting corollaries, which may be worth noting. Let us mention them briefly.

For any irreducible complete intersection, we can take $s = n-1$, and since $b'_0 = b_0 - 1 = 0$, the result implies that

$$\Big| |X(\mathbb{F}_q)| - \pi_n \Big| = O(q^{n-(1/2)}). \tag{24}$$

This may be viewed as a weak version of the Lang-Weil inequality (6). Further, if X happens to be normal, then we can take $s = n-2$, and now Theorem 3.1 yields

$$\Big| |X(\mathbb{F}_q)| - \pi_n \Big| \leq b'_1(N-n+1, \mathbf{d}) q^{n-(1/2)} + C_{n-2}(X) q^{n-1}.$$

This is a stronger result than the Lang-Weil inequality (6) because using (23), we see that $b'_1(N-n+1, \mathbf{d}) \leq (d-1)(d-2)$, with equality if and only if X is a hypersurface. On the other hand, when $s = -1$, the result is the same as Deligne's inequality (10). Thus, the inequality in Theorem 3.1 may be viewed as a common refinement of Deligne's inequality and the Lang-Weil inequality, at least for normal complete intersections. Other corollaries of Theorem 3.1 include a result of Aubry and Perret [4] on the number of points of singular curves, and a result of Shparlinskiĭ and Skorobogatov [38] on the number of points of complete intersections with at most isolated singularities. For the latter, one needs also an additional hypothesis about resolution of singularities. Finally, we remark that the inequality in Theorem 3.1 may be viewed as a more precise version of the estimate about the order of $|X(\mathbb{F}_q)|$, which was obtained by Hooley and Katz [15] in 1991.

The proof given in [10] of Theorem 3.1 can be very briefly sketched as follows. First, we use a variant of Bertini's Theorem to successively construct good hyperplane sections of X. In this way, we obtain a nonsingular complete intersection as a linear section of X. To deal with the corresponding cohomology spaces, we need a suitable generalization of the Weak Lefschetz Theorem for singular varieties. This is obtained using some work of Skorobogatov [39]. These ingredients together with the fundamental tools, namely (9) and (11), and also some recent work of Katz [19] yield the estimates in Theorem 3.1.

4. On the Lang-Weil Inequality

We have seen that if X is a smooth complete intersection of dimension n, defined over $\mathbb{F}_q$, then the difference between $|X(\mathbb{F}_q)|$ and the number $\pi_n = |\mathbb{P}^n(\mathbb{F}_q)|$ is of the order of $q^{n/2}$, thanks to Deligne's inequality (10). This estimate is the same as that given by Weil's inequality (4) or the Lang-Weil inequality (6) when $n = 1$. But it is significantly better than (6) when $n > 1$. In the case of general complete intersections with a singular locus of dimension s, the above difference is of the order of $q^{(n+s+1)/2}$, thanks to the Hooley-Katz estimate or its more precise version stated in the previous section. Again, this is usually much better than (6) when $n > 1$. However, for general projective varieties, essentially the only estimate that we have at our disposal is (24), which is given by the Lang-Weil inequality (6). Recall that for X in $\mathbb{P}^N$ with $\deg X = d$, the Lang-Weil inequality (6) states that

$$\Big| |X(\mathbb{F}_q)| - \pi_n \Big| \le (d-1)(d-2)q^{n-(1/2)} + Cq^{n-1},$$

where C is a constant which is independent of q (and depends only on N, n and d). A possible drawback in this result, particularly from the viewpoint of practical applications, is that almost no information is available about the size of C other than the fact that it is constant with respect to q. This situation is partially remedied by the following 'effective version' of the Lang-Weil inequality which is proved in [10].

We first make a preliminary definition. A projective algebraic variety X in the projective space $\mathbb{P}_k^N$ over a field k is said to be of *type* $(m, N, \mathbf{d})$, with $\mathbf{d} = (d_1, \dots, d_m)$, if X can be defined by the vanishing of m homogeneous polynomials, in $N+1$ variables with coefficients in k, of degrees $d_1, \dots, d_m$. Likewise, an affine algebraic variety X in $\mathbb{A}_k^N$ over a field k is said to be of *type* $(m, N, \mathbf{d})$, with $\mathbf{d} = (d_1, \dots, d_m)$, if X can be defined by the vanishing of m polynomials, in N variables with coefficients in k, of degrees $d_1, \dots, d_m$.

4.1. Theorem. *Suppose X is a projective variety in $\mathbb{P}^N_{\mathbb{F}_q}$ or an affine variety in $\mathbb{A}^N_{\mathbb{F}_q}$ defined over $\mathbb{F}_q$. Let $n = \dim X$ and $d = \deg X$. Then*

$$\Big| |X(\mathbb{F}_q)| - \pi_n \Big| \le (d-1)(d-2)q^{n-(1/2)} + C_+(\bar{X})\, q^{n-1},$$

where $C_+(\bar{X})$ is independent of q. Moreover if X is of type $(m, N, \mathbf{d})$, with $\mathbf{d} = (d_1, \dots, d_m)$, and if $\delta = \max\{d_1, \dots, d_m\}$, then we have

$$C_+(\bar{X}) \le \begin{cases} 9 \times 2^m \times (m\delta + 3)^{N+1} & \text{if } X \text{ is projective} \\ 6 \times 2^m \times (m\delta + 3)^{N+1} & \text{if } X \text{ is affine.} \end{cases}$$

It may be noted that the statement is applicable to projective as well as affine varieties. In fact, the proof given in [10] is different from the one in the original paper of [24] and has the advantage of being applicable to varieties that are affine or projective apart from yielding an explicit bound for the constant C appearing in (6).

The fact that Theorem 4.1 is applicable to affine varieties gives as a corollary, the following lower bound for the number of points on a hypersurface H in $\mathbb{A}^N_{\mathbb{F}_q}$ defined by the vanishing of a polynomial in $\mathbb{F}_q[T_1, \ldots, T_N]$ which is irreducible over $\overline{\mathbb{F}}_q$:

$$|H(\mathbb{F}_q)| \geq q^{N-1} - (d-1)(d-2)q^{N-(3/2)} - 12(d+3)^{N+1}q^{N-2}.$$

This is analogous to the result of Schmidt [35], which gives a lower bound for $|H(\mathbb{F}_q)|$. Actually, in the lower bound of Schmidt, one is able to replace $12(d+3)^{N+1}$ by a much better constant, namely $6d^2$, but Schmidt's bound is only valid for large values of q.

In the remainder of this section, we will briefly outline the proof in [10] of Theorem 4.1. In fact, the basic idea is quite simple and natural. First of all, since X is irreducible, we have $H^{2n}(X, \mathbb{Q}_\ell) \simeq \mathbb{Q}_\ell(-n)$, which implies that $b_{2n,\ell} = 1$ and the only eigenvalue of $F|H^{2n}(\bar{X}, \mathbb{Q}_\ell)$ is $\omega_{2n\,1,\ell} = q^{2n/2} = q^n$. Next comes $H^{2n-1}(\bar{X}, \mathbb{Q}_\ell)$ and by Deligne's Main Theorem (11), this can be split into two parts as follows.

$$H^{2n-1}(\bar{X}, \mathbb{Q}_\ell) = H^{2n-1}_{+}(\bar{X}, \mathbb{Q}_\ell) \oplus H^{2n-1}_{-}(\bar{X}, \mathbb{Q}_\ell),$$

where $H^{2n-1}_{+}(\bar{X}, \mathbb{Q}_\ell)$ is the subspace spanned by the eigenvectors of F corresponding to the eigenvalues $\omega_{2n-1\,j,\ell}$ that are pure of weight $2n-1$, while $H^{2n-1}_{-}(\bar{X}, \mathbb{Q}_\ell)$ is an orthogonal complement of $H^{2n-1}_{+}(\bar{X}, \mathbb{Q}_\ell)$ in $H^{2n-1}(\bar{X}, \mathbb{Q}_\ell)$ (as a $\mathbb{Q}_\ell$-vector space). Following Serre, we call the $\mathbb{Q}_\ell$-vector space dimension of $H^{2n-1}_{+}(\bar{X}, \mathbb{Q}_\ell)$ the $(2n-1)$th *virtual Betti number* of X and denote it by $b^{+}_{2n-1,\ell}(\bar{X})$. Also, we let $b^{-}_{2n-1,\ell}(\bar{X}) = \dim H^{2n-1}_{-}(\bar{X}, \mathbb{Q}_\ell)$. Now it is clear from (9) and (11) that

$$\Big|\, |X(\mathbb{F}_q)| - q^n \,\Big| \leq b^{+}_{2n-1,\ell}(\bar{X}) q^{(n-\frac{1}{2})} + \left(b^{-}_{2n-1,\ell}(\bar{X}) + \sum_{i=0}^{2n-1} b^{+}_{i,\ell}(\bar{X}) \right) q^{n-1}.$$

Using arguments similar to those in Section 1 following Weil's inequality (4), we see that the virtual $(2n-1)$th Betti number $b^{+}_{2n-1,\ell}(\bar{X})$ is, in fact, the best possible constant for the above inequality to hold (not only for q but for all its powers). Moreover, we can show that $b^{+}_{2n-1,\ell}(\bar{X})$ is a birational invariant and is independent of ℓ. Now, to complete the proof of Theorem 4.1, we have to bound $b^{+}_{2n-1,\ell}(\bar{X})$ in terms of the degree, and to effectively bound sums of Betti numbers such as those appearing in large parentheses in the above inequality. The former is done in two stages: first, by finding a 'typical curve' Y on X through degree-preserving linear sections in such a way that $b^{+}_{2n-1,\ell}(\bar{X}) \leq b^{+}_{1}(\bar{Y})$, and next, by showing that if Y is a curve of degree d, then $b^{+}_{1}(\bar{Y}) \leq (d-1)(d-2)$. The latter task of effectively bounding sums of Betti numbers is facilitated by some recent results of Katz [19] that were also used in the proof of Theorem 4.1. These results of Katz are, in fact, analogues of some classical results of Milnor [30] which show, for example, that if V is a complex affine algebraic variety of type $(m, N, \mathbf{d})$, with $\mathbf{d} = (d_1, \ldots, d_m)$, then $\sum b_i(V) \leq \delta(2\delta - 1)^{2N-1}$, where, as before, $\delta = \max\{d_1, \ldots, d_m\}$.

5. Conjectural Statements of Lang and Weil

An *abelian variety* is a projective variety, which is also a commutative group in such a way that the group operation and the map taking an element to its inverse are algebraic (morphisms). A classic example is given by an elliptic curve, where the points satisfy a group law. The work of Abel and Jacobi in the nineteenth century on elliptic integrals, and the more general abelian integrals, lead to the construction of an abelian variety, called the *Jacobian variety*, associated to any (smooth projective) curve. The Jacobian variety of a curve has dimension equal to the genus of that curve[10]. To any higher dimensional variety, one can associate certain abelian varieties known as the *Picard* and *Albanese* varieties, which play a role analogous to that of the Jacobian variety of a curve. For general projective varieties X over an arbitrary field, there are in fact, two distinct constructions of the Picard variety, namely, the Picard-Weil variety $\operatorname{Pic}_w X$ and the Picard-Serre variety $\operatorname{Pic}_s X$. Likewise, there is the Albanese-Weil variety $\operatorname{Alb}_w X$ and the Albanese-Serre variety $\operatorname{Alb}_s X$. When X is nonsingular, the two constructions coincide. If X is normal, then $\operatorname{Pic}_w X$ is the dual of $\operatorname{Alb}_w X$ while $\operatorname{Pic}_s X$ is the dual of $\operatorname{Alb}_s X$. For precise definitions of the Picard and Albanese varieties and some basic properties, we refer to [10] and the references therein. General references on abelian varieties are the books of Lang [23] and Mumford [33].

Now suppose X is an irreducible projective variety in $\mathbb{P}^N$ defined over $\mathbb{F}_q$. Let n be the dimension of X and d be the degree of X. For simplicity, we assume that X has at least one $\mathbb{F}_q$-rational point (which can be ensured by passing, if necessary, to a finite extension of $\mathbb{F}_q$).

When Lang and Weil [24] proved the inequality (6), namely,

$$\Big| |X(\mathbb{F}_q)| - \pi_n \Big| \leq (d-1)(d-2)q^{n-(1/2)} + Cq^{n-1},$$

they showed in the same paper that if K is an algebraic function field of dimension n over $k = \mathbb{F}_q$, then there is a constant γ for which (6) holds with $(d-1)(d-2)$ replaced by γ, for any model X of K/k, and moreover, the smallest such constant γ is a birational invariant. Subsequently, Lang and Weil went on to conjecture that this constant γ can be described *algebraically* as being twice the dimension of the associated Picard variety, at least when X is nonsingular. Notice that when X is a smooth curve of genus g, then from the remarks made in Section 1 following Weil's inequality (4), we see that $\gamma = 2g$, and thus the conjecture is verified in this case.

The conjectures of Lang and Weil preceded an analysis of the zeros and poles of the zeta function of X. They showed that the zeros and poles of $Z(X,T)$ in the open disc $|T| < q^{-(n-1)}$ are birational invariants, and that in the smaller disc $|T| < q^{-(n-1/2)}$ there is exactly one pole of order 1 at $T = q^{-n}$ (see Fig. 1). Then they wrote: *about the behavior of $Z(X,T)$ for $|T| \geq q^{-(n-1/2)}$, we can only make the following conjectural statements, which complement the conjectures of Weil.* In addition to the conjecture mentioned above about γ, these *conjectural statements* are to the effect that when X is projective and nonsingular, the quotient

$$\frac{Z(X,T)(1-q^nT)}{f_c(P,T)} \tag{25}$$

[10]For a lucid exposition of basic facts concerning Jacobian varieties, in the classical case of complex curves, see the China lectures of Griffiths [11, Ch. V.].

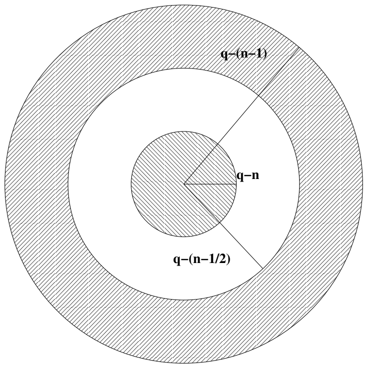

FIGURE 1. Disks in which the zeros and poles of the zeta function $Z(X,T)$ were analyzed by Lang and Weil

has no zeros or poles inside $|T| < q^{-(n-1)}$ and at least one pole on $|T| = q^{-(n-1)}$, where P denotes the Picard variety of X, and $f_c(P,T)$ the 'characteristic polynomial' of P.

The characteristic polynomial of an abelian variety A over $\mathbb{F}_q$ can be defined as follows. Choose a prime $\ell \neq p = \operatorname{char} \mathbb{F}_q$. Let $T_\ell(A)$ denote the *Tate module* of A, which is the projective limit of $\{A_{\ell^n} : n \geq 1\}$ with respect to the maps induced by multiplication by ℓ (for $m \in \mathbb{Z}$, we let $A_m = \{a \in A(\overline{\mathbb{F}}_q) : ma = 0\}$ be the set of m-torsion points of A). If $\dim A = g$, then the Tate module $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$; consequently, $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a $\mathbb{Q}_\ell$-vector space of dimension $2g$. Now if $\varphi : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$ is the Frobenius map given by $\varphi(x) = x^q$, then φ induces an endomorphism of $T_\ell(A)$, which we denote by $T_\ell(\varphi)$. The *characteristic polynomial* $f_c(A,T)$ of A is defined to be the characteristic polynomial of the linear map $T_\ell(\varphi)$ of $T_\ell(A)$; in other words,

$$f_c(A,T) := \det\left(T - T_\ell(\varphi)\right) = T^{2g} - a_1 T^{2g-1} + \cdots + (-1)^{2g} a_{2g},$$

where $a_1, \ldots, a_{2g}$ are in $\mathbb{Z}_\ell$. We call a_1 to be the *trace* of φ and denote it by $\operatorname{Tr}(\varphi)$. The constant coefficient a_{2g} is sometimes called the *degree* of φ and denoted by $\deg \varphi$.

We are now in a position to describe some of the main results from [10] in connection with the conjectural statements of Lang and Weil. To begin with, let us note that from the discussion in the last paragraph of the previous section, it is clear that the birational invariant γ that Lang and Weil talked about is nothing but the virtual $(2n-1)$th Betti number $b^+_{2n-1,\ell}(\bar{X})$. Also, it is clear from the factorization (8) and Deligne's Main Theorem (11) (or the Riemann hypothesis, in the smooth case), that to prove the assertion of Lang and Weil concerning the quotient (25), it suffices to relate the polynomial $f_c(P,T)$ with $P_{2n-1,\ell}(X,T)$. The following result from [10] gives, in fact, a relationship between the corresponding algebraic objects. Note that the hypothesis of this result is fulfilled when X is nonsingular.

5.1. Proposition. *Suppose X is a normal projective variety defined over $\mathbb{F}_q$ and of dimension $n \geq 2$ such that X is also regular in codimension 2. Then the $\mathbb{Q}_\ell$*

vector spaces $V_\ell(\mathrm{Alb}_w X)$ *and* $H^{2n-1}(\bar{X}, \mathbb{Q}_\ell(n))$ *are isomorphic (in fact, by a* $\mathbf{g}$*-equivariant isomorphism, where* $\mathbf{g} = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ *is the absolute Galois group of* $\mathbb{F}_q$*). As a consequence,*

$$b_{2n-1,\ell}(\bar{X}) = 2\dim \mathrm{Alb}_w X = 2\dim \mathrm{Pic}_w X.$$

In particular, the penultimate Betti number is even and independent of ℓ*.*

To extend this result to varieties that are not necessarily regular in codimension 2, we need a weak version of resolution of singularities, namely the condition on X that *X is birationally equivalent to a normal projective variety $\widetilde{X}$ defined over k, which is regular in codimension* 2. We will refer to this condition as (**RS2**).

5.2. Theorem. *Suppose X is a projective variety defined over $\mathbb{F}_q$ and of dimension $n \geq 2$ which satisfies* (**RS2**)*. Then the $\mathbb{Q}_\ell$ vector spaces $V_\ell(\mathrm{Alb}_w X)$ and $H_+^{2n-1}(\bar{X}, \mathbb{Q}_\ell(n))$ are isomorphic (in fact, by a* $\mathbf{g}$*-equivariant isomorphism, where $\mathbf{g} = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is the absolute Galois group of $\mathbb{F}_q$). As a consequence, $b^+_{2n-1,\ell}(\bar{X}) = 2\dim \mathrm{Alb}_w X$.*

If X is nonsingular, one has Poincaré duality for the étale cohomology space and Proposition 5.1 would imply a similar result for H^1 and the first Betti number $b_1(\bar{X})$. But for a general X, this is not true. However, it may be interesting to note the following result in [10], which involves the Serre construction of the Picard or the Albanese varieties. This result can be used, in turn, to obtain a weak version of Poincaré duality when the hypothesis of Proposition 5.1 is met.

5.3. Proposition. *Suppose X is a normal projective variety defined over $\mathbb{F}_q$ and of dimension n. Then the $\mathbb{Q}_\ell$ vector spaces $V_\ell(\mathrm{Pic}_s X)$ and $H^1(\bar{X}, \mathbb{Q}_\ell)$ are isomorphic (in fact, by a* $\mathbf{g}$*-equivariant isomorphism, where $\mathbf{g} = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$), provided we twist $V_\ell(\mathrm{Pic}_s X)$ by -1). As a consequence, $b_{1,\ell}(\bar{X}) = 2\dim \mathrm{Pic}_s X$; in particular, the first Betti number is even and independent of ℓ.*

Recall that the space $H_+^{2n-1}(\bar{X}, \mathbb{Q}_\ell)$ and its dimension, the $(2n-1)$th virtual Betti number, $b^+_{2n-1,\ell}(X)$ were defined in the previous section. Let us also define $P^+_{2n-1,\ell}(X,T) = \det\left(1 - TF | H_+^{2n-1}(\bar{X}, \mathbb{Q}_\ell)\right)$.

5.4. Theorem. *Let X be any variety defined over $\mathbb{F}_q$ of dimension $n \geq 2$, and let $g = \dim \mathrm{Alb}_w X$. Then*

$$P^+_{2n-1,\ell}(X,T) = q^{-g} f_c(\mathrm{Alb}_w X, q^n T).$$

In particular,

$$b^+_{2n-1,\ell}(X) = 2g \quad \textit{and} \quad Tr(F \mid H_+^{2n-1}(\bar{X}, \mathbb{Q}_\ell)) = q^{n-1}\,\mathrm{Tr}(\varphi).$$

If X is normal, then $\mathrm{Pic}_w X$ and $\mathrm{Alb}_w X$ are the duals of each other, and $f_c(\mathrm{Alb}_w X, T) = f_c(\mathrm{Pic}_w X, T)$. Thus, in view of the remarks made earlier in this section, the conjectural statements of Lang and Weil follow as a particular case of Theorem 5.4.

Acknowledgements

This article is an expanded version of the talks by the authors at the *International Conference on Number Theory and Discrete Mathematics in honour of*

Srinivasa Ramanujan, which was held at Chandigarh in October 2000. We take this opportunity to thank the organizers, especially Professor Ashok Agarwal, for their invitation and hospitality. We would also like to express our warm gratitude to Professor Michel Waldschmidt for his suggestions and encouragement.

References

[1] Andrews, G. E., *The Theory of Partitions*, Encyclopedia Math. Appl. Vol. 2, Addison-Wesley, Reading, Mass., 1976.

[2] Artin, M., *Grothendieck topologies*, mimeographed notes, Harvard Univ., Cambridge Mass., 1962.

[3] Artin, M., Grothendieck, A., Verdier J.-L., *Théorie des Topos et Cohomologie Étale des Schémas*, Tome 2 and 3, Lect. Notes in Math. Vol. 270 and 305, Springer-Verlag, Berlin, 1972 and 1973.

[4] Aubry, Y., Perret, M., *A Weil Theorem for singular curves*, in: Arithmetic, Geometry, and Coding Theory (Luminy, 1993), de Gruyter, Berlin, 1996, pp. 1-7.

[5] Deligne, P., *La conjecture de Weil I*, Publ. Math. I.H.E.S. **43** (1974), 273-308.

[6] Deligne, P., *La conjecture de Weil II*, Publ. Math. I.H.E.S. **52**(1981), 313-428.

[7] Dwork, B., *On the rationality of the zeta function of an algebraic variety*, Amer J. Math. **82** (1960), 631-648.

[8] Freitag, E., Kiehl, R., *Étale Cohomology and the Weil Conjectures*, Ergeb. Math. Grenzgeb.(3) Vol. 13, Springer-Verlag, Berlin, 1988.

[9] Fulton, W., *Young Tableaux, with Applications to Representation Theory and Geometry*, LMS Student Texts Vol. 35, Cambridge University Press, Cambridge, 1997.

[10] Ghorpade, S. R., Lachaud, G., *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields*, preprint (2001); to appear in: Moscow Math. Journal. [Available: `http://www.math.iitb.ac.in/~srg/Papers.html`]

[11] Griffiths, P., *Introduction to Algebraic Curves*, American Mathematical Society, Providence, 1989.

[12] Hardy, G. H., Wright, E. M., *An Introduction to the Theory of Numbers*, 4th Ed., Clarendon Press, Oxford, 1960. [An online index to this classic text is available at: `http://www.utm.edu/research/primes/notes/hw_index.html`]

[13] Hartshorne, R., *Algebraic Geometry*, Grad. Texts in Math. Vol. 52, Springer-Verlag, Berlin, 1977.

[14] Hirzebruch, F., *Der Satz von Riemann-Roch in Faisceau-theoretischer Formulierung: einige Anwendingen und offene Fragen*, Proc. Int. Cong. Math., (Amsterdam, 1954), Vol. 3, North-Holland, Amsterdam, 1956, pp. 457-473.

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

[16] Humphreys, J. E., *Linear Algebraic Groups*, Grad. Texts in Math. Vol. 21, Springer-Verlag, Berlin, 1975.

[17] Katz, N. M., *An overview of Deligne's proof of Riemann hypothesis for varieties over finite fields*, in: Mathematical Development arising from Hilbert Problems, Proc. Symp. Pure Math. Vol. 28, Part 1, American Mathematical Society, Providence, 1976, pp. 275-305.

[18] Katz, N. M., *Review of ℓ-adic Cohomology*, in: *Motives* (Seattle 1991), Proc. Symp. Pure Math. Vol. 55, American Mathematical Society, Providence, 1994, pp. 21-30.

[19] Katz, N. M., *Sums of Betti numbers in arbitrary characteristic*, Finite Fields and their App. **7** (2001), 29-44.

[20] Katz, N. M., *L-functions and monodromy: four lectures on Weil II*, Adv. Math. **160** (2001), 81-132.

[21] Katz, N. M., Tate, J. *Bernard Dwork (1923–1998)*, Notices Amer. Math. Soc. **46** (1999), 338-343.

[22] Kiehl, R., Weissauer, R., *Weil Conjectures, Perverse Sheaves and ℓ-adic Fourier Transform*, Ergeb. Math. Grenzgeb.(3) Vol. 42, Springer-Verlag, Berlin, 2001.

[23] Lang, S., *Abelian Varieties*, Interscience Publishers, New York, 1959.

[24] Lang, S., Weil, A., *Number of points of varieties over finite fields*, Amer. J. Math. **76** (1954), 819-827.

[25] Lubkin, S., *On a conjecture of André Weil*, Amer. J. Math. **89** (1967), 443-548.

[26] Lubkin, S., *A p-adic proof of Weil's conjectures*, Ann. of Math. **87** (1968), 105-194 and 195-255.

[27] Manivel, L., *Fonctions Symétriques, Polynômes de Schubert et Lieux de Dégénérescence*, Cours Spécialisés N$^{\mathrm{o}}$ 3, Soc. Math. de France, Paris, 1998. [English translation: SMF/AMS Texts and Monographs Vol. 6, Amer. Math. Soc., Providence, 2001.]

[28] Milne, J.S., *Étale Cohomology*, Princeton Math. Series Vol. 33, Princeton University Press, Princeton, 1980.

[29] Milne, J. S., *Lectures on Étale Cohomology*, Course Notes, v2.01, 1998. [Available: `http://www.jmilne.org/math/Coursenotes/math732.html`]

[30] Milnor, J. W., *On the Betti numbers of real varieties*, Proc. Amer. Math. Soc. **15** (1964), 275-280.

[31] Milnor, J. W., Stasheff, J. D., *Characteristic classes*, Ann. of Math. Stud., No. 76. Princeton University Press, Princeton, 1974.

[32] Mumford, D., *Picard groups of moduli problems*, in: Arithmetical Algebraic Geometry (Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 33-81.

[33] Mumford, D., *Abelian Varieties*, 2d ed., Oxford University Press, Bombay, 1974.

[34] Northcott, D. G., *Lessons on Rings, Modules and Multiplicities*, Cambridge University Press, Cambridge, 1968.

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

[36] Serre, J.-P., *Sur les nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), 397-402.

[37] Shafarevich, I. R., *Basic Algebraic Geometry*, Vol 1 and 2, 2nd Ed., Springer-Verlag, Berlin, 1994.

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

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

[40] Stanley, R. P., *Enumerative Combinatorics*, Vol. I, Wadsworth & Brooks/Cole, Monterey, Calif., 1986.

[41] Stanley, R. P., *Some combinatorial aspects of the Schubert calculus*, in: Combinatoire et Représentation du Groupe Symétrique (Strasbourg, 1976), Lect. Notes in Math. Vol. 579, Springer-Verlag, Berlin, 1977, pp. 217-251.

[42] Weil, A., *Number of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497-508.

[43] Weil, A., *Abstract versus classical Algebraic Geometry*, Proc. Int. Cong. Math. (Amsterdam, 1954), Vol. 3, North-Holland, Amsterdam, 1956, pp. 550-558.

Department of Mathematics
Indian Institute of Technology, Bombay
Powai, Mumbai 400076, INDIA
E-mail address: `srg@math.iitb.ac.in`

Équipe "Arithmétique et Théorie de l'Information"
Institut de Mathématiques de Luminy
Luminy Case 907, 13288 Marseille Cedex 9, FRANCE
E-mail address: `lachaud@iml.univ-mrs.fr`