The Riemann Hypothesis for Varieties over Finite Fields

Sander Mack-Crane

16 July 2015

Abstract

We discuss the Weil conjectures, especially the Riemann hypothesis, for varieties over finite fields. Particular detail is devoted to the proof of the Riemann hypothesis for cubic threefolds in projective 4-space, as given by Bombieri and Swinnerton-Dyer. The main idea is to relate the number of points on a cubic threefold to the trace of Frobenius on an associated abelian variety, and we develop the necessary machinery of abelian varieties.

1 Introduction

The Weil conjectures are a set of conjectures (now proven) describing the number of points of varieties over finite fields, as encoded in the zeta function of the variety. They give an analog in finite fields of both the Riemann hypothesis of analytic number theory and the cohomology theory of complex varieties. We will introduce both of these perspectives in turn, partly following [2]. But first, we review an element of algebraic geometry that is essential for our discussion.

1.1 Fields of Definition

In the classical setting, let

$$\mathbb{A}_k^n = \{(a_1, \ldots, a_n) \mid a_i \in k\}$$

be n-dimensional affine space over a field k, $\{f_i\} \subset k[x_1, \ldots, x_n]$ some set of polynomials, and

$$V = V(f_i) = \{(a_1, \ldots, a_n) \in \mathbb{A}_k^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ for all } i\} \subset \mathbb{A}_k^n$$

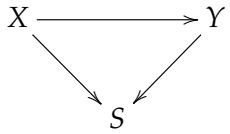
the variety defined by the polynomials $\{f_i\}$.

For any extension K of k, we have $k[x_0, \ldots, x_n] \subset K[x_0, \ldots, x_n]$, and in particular our polynomials f_i defining X are in $K[x_0, \ldots, x_n]$. Thus we may equally well ask for the common solutions of the f_i with coordinates in K:

$$V(K) = \{(a_1, \ldots, a_n) \in \mathbb{A}_K^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ for all } i\} \subset \mathbb{A}_K^n.$$

There is a nice abstraction of "points of a variety with coordinates in some field" to the setting of schemes. Fix a "base" scheme S. A scheme *(defined) over* S, or an *S-scheme*,

is a scheme X with a distinguished morphism $X \to S$. A morphism of S-schemes from X to Y is a morphism of schemes $X \to Y$ respecting the morphisms to S, i.e. making the following diagram commute.



If $S = \operatorname{Spec} A, X = \operatorname{Spec} B, Y = \operatorname{Spec} C$ are affine, then under the equivalence of categories between commutative rings and affine schemes, to give X (or Y) the structure of an S-scheme is to give B (or C) the structure of an A-algebra. Morphisms $X \to Y$ of S-schemes correspond to morphisms $C \to B$ of A-algebras.

Given two S-schemes X and Y, define the *points of X with coordinates in Y* to be $X(Y) = \operatorname{Hom}_{S\text{-}\mathbf{Sch}}(Y, X)$ (here S-**Sch** denotes the category of S-schemes as defined above). In the affine case $S = \operatorname{Spec} R$ we may abuse notation by speaking of schemes "over R" rather than "over $\operatorname{Spec} R$", and writing $X(R)$ rather than $X(\operatorname{Spec} R)$.

This definition agrees to our previous notion in the following way. A point of $V(K)$ (as first defined) is simply a tuple $(a_1, \ldots, a_n)$ of elements of K for which $f_i(a_1, \ldots, a_n) = 0$ for all i. This is the same as a k-algebra morphism

$$\begin{aligned} k[x_1, \ldots, x_n] &\to K \\ x_i &\mapsto a_i \end{aligned}$$

with $f_i \mapsto 0$ for all i, which in turn is the same as a k-algebra morphism

$$k[x_1, \ldots, x_n]/(f_i) \to K.$$

Under the equivalence of categories between commutative rings and affine schemes, this corresponds to a morphism

$$\operatorname{Spec} K \to V$$

of schemes over $\operatorname{Spec} k$, where $V = \operatorname{Spec} k[x_1, \ldots, x_n]/(f_i)$ is the scheme corresponding to our variety $V = V(f_i)$ above. That is to say, the points of V with coordinates in K as first defined are in correspondence with the scheme-theoretic points $\operatorname{Hom}_{k\text{-}\mathbf{Sch}}(\operatorname{Spec} K, V)$. Similarly, if V is a projective variety embedded in $\mathbb{P}^n_k$ as the zero locus of some homogeneous polynomials, then the scheme-theoretic points $\operatorname{Hom}_{k\text{-}\mathbf{Sch}}(\operatorname{Spec} K, V)$ are in correspondence with the classical points of V defined by the same polynomials as a subvariety of $\mathbb{P}^n_K$.

1.2 Zeta Functions

Now we return to the motivation for the Weil conjectures. The classical Riemann zeta function is defined for $\Re(s) > 1$ by

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}.$$

Riemann showed that the zeta function can be analytically continued to a meromorphic function on the whole complex plane, satisfying a functional equation under the transformation $s \mapsto 1 - s$. Using the unique factorization of integers into primes, one can give an alterantive form known as the *Euler product*,

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

This connects the zeta function to prime numbers, and the analysis of the zeta function is important to number theory mainly because of its application to the distribution of primes.

If K is an algebraic number field (i.e. finite extension of $\mathbb{Q}$) with ring of integers $\mathcal{O}_K$, recall for an ideal $\mathfrak{a} \lhd \mathcal{O}_K$ the norm $N\mathfrak{a} = \#\mathcal{O}_K/\mathfrak{a}$. In this context we can rewrite the Riemann zeta function as

$$\zeta(s) = \sum_{\mathfrak{a} \lhd \mathbb{Z}} \frac{1}{(N\mathfrak{a})^s}.$$

It is simple to generalize this to an arbitrary number field:

$$\zeta_K(s) = \sum_{\mathfrak{a} \lhd \mathcal{O}_K} \frac{1}{(N\mathfrak{a})^s}.$$

As in the case of the Riemann zeta function, the zeta function of a number field extends to a meromorphic function in the complex plane, satisfies a functional equation, and admits an Euler product

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ \text{prime}}} \left(1 - \frac{1}{(N\mathfrak{p})^s}\right)^{-1}.$$

This function is useful for its application to the number theory of the field K, but also for its analogy to the Riemann zeta function.

We can generalize in the same way, summing over ideals, to function fields over finite fields (to be precise, quadratic extensions of $\mathbb{F}_q(t)$ given by adjoining the square root of a separable polynomial), with ring of integers $\mathcal{O}$ given by the integral closure of $\mathbb{F}_q[t]$. In this context also, the zeta functions admit an Euler product. There are many analogies between the integers and polynomial rings over finite fields, but the corresponding problems over finite fields often turn out to be much easier, and therefore act as a good testing ground for problems over the integers.

In the context of function fields over finite fields, every quotient of $\mathcal{O}$ is an extension of $\mathbb{F}_q$, and therefore every prime ideal has norm a power of q. We define integers $m_\mathfrak{p}$ by $N\mathfrak{p} = q^{m_\mathfrak{p}}$. Now, prime ideals $\mathfrak{p} \lhd \mathcal{O}$ with $m_\mathfrak{p} \mid n$ correspond (by quotienting) to morphisms $\mathcal{O} \to \mathbb{F}_{q^n}$, with image $\mathbb{F}_{q^{m_\mathfrak{p}}}$. Note in fact that each $\mathfrak{p}$ corresponds to $\mathfrak{m}_p$ morphisms $\mathcal{O} \to \mathbb{F}_{q^n}$, due to the Galois action on $\mathbb{F}_{q^{m_\mathfrak{p}}}$ over $\mathbb{F}_q$.

From the discussion of §1.1 we recognize morphisms $\mathcal{O} \to \mathbb{F}_{q^n}$ as points of $\operatorname{Spec}\mathcal{O}$ with coordinates in $\mathbb{F}_{q^n}$. Writing $V = \operatorname{Spec}\mathcal{O}$ and $t = q^{-s}$, we have

$$\begin{aligned}
t\frac{d}{dt}\log\zeta_V(s) &= -\frac{1}{\log q}\frac{d}{ds}\log\zeta_V(s) \\
&= -\frac{1}{\log q}\frac{d}{ds}\log\prod_{\substack{\mathfrak{p}\lhd\mathcal{O}\\ \text{prime}}}\left(1-\frac{1}{(N\mathfrak{p})^s}\right)^{-1} \\
&= \frac{1}{\log q}\sum_{\substack{\mathfrak{p}\lhd\mathcal{O}\\ \text{prime}}}\frac{d}{ds}\log\left(1-\frac{1}{(N\mathfrak{p})^s}\right) \\
&= -\frac{1}{\log q}\sum_{\substack{\mathfrak{p}\lhd\mathcal{O}\\ \text{prime}}}\frac{d}{ds}\sum_{k\geq 1}\frac{1}{k}(N\mathfrak{p})^{-ks} \\
&= \sum_{\substack{\mathfrak{p}\lhd\mathcal{O}\\ \text{prime}}}\sum_{k\geq 1}\frac{\log(N\mathfrak{p})}{\log q}(N\mathfrak{p})^{-ks} \\
&= \sum_{\substack{\mathfrak{p}\lhd\mathcal{O}\\ \text{prime}}}\sum_{k\geq 1} m_{\mathfrak{p}}q^{-km_{\mathfrak{p}}s} \\
&= \sum_{n\geq 1}\#V(\mathbb{F}_{q^n})t^n.
\end{aligned}$$

Thus we may rewrite the zeta function of V (in terms of $t = q^{-s}$) as

$$\zeta_V(t) = \exp\left[\sum_{n\geq 1}\frac{\#V(\mathbb{F}_{q^n})}{n}t^n\right]. \tag{1}$$

This expression is purely geometric, taking as input only the number of points of V over various finite fields. Thus it generalizes to any variety V over a finite field.

In fact, if X is any scheme of finite type over $\mathbb{Z}$, we can define a zeta function by

$$\zeta_X(s) = \prod_{\substack{x\in|X|\\ \text{closed}}}\frac{1}{1-(\#k(x))^{-s}} \tag{2}$$

(here $|X|$ denotes the topological space of X). This is equivalent to our previous definitions in the following way. If a point x has residue field $k(x) = \mathbb{F}_{q^{m_x}}$ then there are m_x morphisms $\operatorname{Spec}\mathbb{F}_{q^n} \to X$ with image x for any multiple n of m_x, due to the Galois action on $\mathbb{F}_{q^{m_x}}$ over $\mathbb{F}_q$. Thus if X_n denotes the set of closed points $x \in X$ with $m_x = n$, we have $\#X(\mathbb{F}_{q^n}) = \sum_{k|n} k\,\#X_k$, and by Möbius inversion $\#X_n = \frac{1}{n}\sum_{d|n}\#X(\mathbb{F}_{q^{n/d}})\mu(d)$.

$$\begin{aligned}
\log \zeta_X(s) &= \log \prod_{\substack{x \in |X| \\ \text{closed}}} \frac{1}{1 - (\#k(x))^{-s}} \\
&= - \sum_{\substack{x \in |X| \\ \text{closed}}} \log(1 - (\#k(x))^{-s}) \\
&= \sum_{\substack{x \in |X| \\ \text{closed}}} \sum_{j \geq 1} \frac{(\#k(x))^{-s})^j}{j} \\
&= \sum_{n \geq 1} \#X_n \sum_{j \geq 1} \frac{q^{-njs}}{j} \\
&= \sum_{n \geq 1} \frac{1}{n} \sum_{d|n} \#X(\mathbb{F}_{q^{n/d}}) \mu(d) \sum_{j \geq 1} \frac{q^{-njs}}{j} \\
&= \sum_{d \geq 1} \sum_{m \geq 1} \sum_{j \geq 1} \mu(d) \frac{\#X(\mathbb{F}_{q^m}) t^{mdj}}{mdj} \\
&= \sum_{m \geq 1} \sum_{\ell \geq 1} \frac{\#X(\mathbb{F}_{q^m}) t^{m\ell}}{m\ell} \sum_{d|\ell} \mu(d) \\
&= \sum_{m \geq 1} \frac{\#X(\mathbb{F}_{q^m}) t^m}{m}
\end{aligned}$$

(where as above $t = q^{-s}$, and we have used the fact that $\sum_{d|\ell} \mu(d) = \delta_{\ell,1}$).

We may conjecture that these zeta functions satisfy a functional equation and a Riemann hypothesis analogous to the classical Riemann zeta function.

1.3 Cohomology

The Weil conjectures also give an analogue in finite fields of the cohomology theory of complex varieties. This arises from considering points defined over a field $\mathbb{F}_{q^n}$ as fixed points of an endomorphism, and looking for a fixed-point theorem to describe them.

If X is a scheme defined over a finite field $\mathbb{F}_q$, then the *q-power Frobenius* endomorphism π is the endomorphism of X induced on affine charts by the q-power map between coordinate rings (which is indeed a morphism in characteristic dividing q). This endomorphism is the identity on the topological space of X, but permutes the points $X(\mathbb{F}_{q^n})$ by taking q^{th} powers of the coordinates. Thus the fixed points of π acting on $X(\overline{\mathbb{F}}_q)$ are precisely the points $X(\mathbb{F}_q)$ of X with coordinates in $\mathbb{F}_q$, and similarly the fixed points of the n^{th} iteration π^n are $X(\mathbb{F}_{q^n})$.

In the setting of complex varieties, an endomorphism $f : V \to V$ induces endomorphisms $f : H^i(V) \to H^i(V)$, which in particular are linear maps. Thus we can take the trace of f acting on cohomology, and the Lefschetz trace formula states that the number of fixed points of f is equal to the alternating sum of traces $\sum_{i=0}^{2 \dim V} (-1)^i \operatorname{tr}(f; H^i(V))$ (under some hypotheses on the map f).

An optimist may then expect that there exists a cohomology theory for varieties over finite fields that admits a similar trace formula. In this case, for V a variety over $\mathbb{F}_q$, we would have a formula

$$\#V(\mathbb{F}_{q^n}) = \sum_{i=0}^{2\dim V} (-1)^i \operatorname{tr}(\pi^n; H^i(V)) = \sum_{i=0}^{2\dim V} \sum_j (-1)^i \alpha_{ij}^n, \tag{3}$$

where α_{ij} are the roots of the characteristic polynomial of $\pi : H^i(V) \to H^i(V)$.

Recalling the zeta function of a variety as in (1), an expression of the form (3) (for all n) is equivalent to

$$\begin{aligned}
\zeta_V(t) &= \exp\left[\sum_{n\geq 1} \frac{\#V(\mathbb{F}_{q^n})}{n} t^n\right] \\
&= \exp\left[\sum_{n\geq 1} \sum_{i,j} (-1)^i \frac{(\alpha_{ij}t)^n}{n}\right] \\
&= \exp\left[\sum_{i=0}^{2\dim V} (-1)^i \log(1-\alpha_{ij}t)\right] \\
&= \frac{P_1(t)\cdots P_{2\dim V-1}(t)}{P_0(t)P_2(t)\cdots P_{2\dim V}(t)}
\end{aligned}$$

where $P_i(t)$ is the characteristic polynomial of $\pi : H^i(V) \to H^i(V)$. In particular, the zeta function of V is a rational function of $t = q^{-s}$.

One might also expect other good properties of such a cohomology theory; as we shall see, the Weil conjectures state that it should satisfy a Poincaré duality, and that the cohomology of (the complex points of) a variety over a number field should be related to the cohomology of its reduction mod p.

2 The Weil Conjectures

We are now ready to see precisely how the Weil conjectures capture all of the ideas suggested above. Recall the zeta function of a variety as defined in (1).

Weil Conjectures. [7] Let V be a non-singular projective variety over $\mathbb{F}_q$. Then

1. (Rationality) The zeta function of V is rational, of the form

$$\zeta_V(t) = \frac{P_1(t)\cdots P_{2d-1}(t)}{P_0(t)P_2(t)\cdots P_{2d}(t)}, \tag{4}$$

   where d is the dimension of V, $P_0(t) = 1-t$, $P_{2d}(t) = 1-q^d t$, and each P_i is a polynomial with integer coefficients factoring over $\mathbb{C}$ as $P_i(t) = \prod_j (1-\alpha_{ij}t)$.

2. (Riemann Hypothesis) The α_{ij} above have $|\alpha_{ij}| = q^{i/2}$, or equivalently, the roots of $P_i(q^{-s})$ lie on the vertical line $\Re(s) = \frac{i}{2}$.

3. (Poincaré Duality) The zeta function of V satisfies a functional equation
$$\zeta_V(q^{-d}t^{-1}) = \pm q^{dE/2}t^E\zeta_V(t), \tag{5}$$
or equivalently
$$\zeta_V(q^{-(d-s)}) = \pm q^{E(d/2-s)}\zeta_V(q^{-s}), \tag{6}$$
where E is the Euler characteristic of V (defined as the self-intersection number of the diagonal in $V \times V$).

4. (Betti Numbers) If V is the good reduction mod p of a non-singular variety X defined over an algebraic number field, then the degree of P_i is equal to the i^{th} Betti number of the complex points of X.

As discussed in §1.3, the first statement (rationality) corresponds to a sort of cohomology trace formula; the polynomials P_i appearing in the rational function should be the characteristic polynomials of the action of Frobenius on cohomology.

The second statement is an analogue of the Riemann hypothesis, stating that the zeros and poles of the zeta function should lie on certain vertical lines in the complex plane.

The third statement is simultaneously an analogue of the functional equation satisfied by the Riemann zeta function and a statement of Poincaré duality for our hypothetical cohomology theory. The relation to the functional equation of the Riemann zeta function is plain: the zeta function should transform nicely under the flip $s \mapsto d - s$. The relation to Poicaré duality is that, supposing the rationality of the zeta function, the transformation $\zeta_V(t) \mapsto q^{-dE/2}t^{-E}\zeta_V(q^{-d}t^{-1})$ has the effect of replacing α_{ij} by q^d/α_{ij}. Satisfying the functional equation is therefore the statement that q^d/α_{ij} should be $\alpha_{2d-i,j}$ (reordering if necessary), which corresponds to a duality between $H^i(V)$ and $H^{2d-i}(V)$.

The fourth statement gives a relationship between the cohomology of a variety over a number field and the hypothetical cohomology of its reduction mod p, namely that they should have the same Betti numbers; if $P_i(t)$ is the characteristic polynomial of $\pi : H^i(V) \to H^i(V)$, then its degree is the i^{th} Betti number of V in the cohomology over finite fields.

2.1 Simple Cases

We can illustrate the Weil conjectures by explicitly computing the zeta functions of some simple smooth projective varieties.

Consider the projective line $\mathbb{P}^1$ over $\mathbb{F}_q$. Since it is 1-dimensional, its zeta function should have the form
$$\zeta_{\mathbb{P}^1}(t) = \frac{P_1(t)}{(1-t)(1-qt)}$$
for some integral polynomial $P_1(t)$. The projective line $\mathbb{P}^1$ over $\mathbb{F}_q$ has $q+1$ points, corresponding to the q points of $\mathbb{F}_q$ and the point at infinity. In the same way, the number of points defined over the extension $\mathbb{F}_{q^n}$ is $q^n + 1$. Thus we can write explicitly
$$\log \zeta_{\mathbb{P}^1}(t) = \sum_{n>0} \frac{1+q^n}{n} t^n = \sum_{n>0} \frac{1}{n} t^n + \sum_{n>0} \frac{1}{n} (qt)^n = -\log(1-t) - \log(1-qt).$$

Exponentiating gives

$$\zeta_{\mathbb{P}^1}(t) = \frac{1}{(1-t)(1-qt)}.$$

We see that the zeta function of $\mathbb{P}^1$ is a rational function of the desired form (with $P_1(t) = 1$). The Riemann hypothesis is trivial, and it is a simple computation to verify the functional equation

$$\zeta_{\mathbb{P}^1}(q^{-1}t^{-1}) = qt^2\zeta_{\mathbb{P}^1}(t)$$

(note that the Euler characteristic of $\mathbb{P}^1$ is 2). Furthermore, $\mathbb{P}^1_{\mathbb{F}_p}$ is indeed the (good) reduction mod p of the projective line over a(ny) number field. The Betti numbers of the complex variety $\mathbb{P}^1_{\mathbb{C}}$, i.e. the sphere, are $1, 0, 1$, which coincide with the degrees of P_0, P_1, P_2 in the above zeta function.

Another more complicated example that can still be computed by hands is the Grassmannian $\mathrm{Gr}(2,4)$ over $\mathbb{F}_q$, parametrizing 2-dimensional linear subspaces of $\mathbb{F}_q^4$. A 2-dimensional linear subspace of $\mathbb{F}_q^4$ is determined by a pair v, w of linearly independent vectors. There are $q^4 - 1$ non-zero vectors in $\mathbb{F}_q^4$, and $q^4 - q$ vectors linearly independent from a chosen vector, for a total of $(q^4-1)(q^4-q)$ such pairs. However, two pairs v, w and v', w' determine the same plane precisely when there is an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2 \mathbb{F}_q$ such that $v' = av + bw$, $w' = cv + dw$. Such elements consist of two linearly independent vectors (columns) in $\mathbb{F}_q^2$, and in the same way as above there are $(q^2-1)(q^2-q)$ of these. The stabilizer of a pair v, w in $\mathrm{GL}_2 \mathbb{F}_q$ is trivial, so the number of 2-dimensional subspaces of $\mathbb{F}_q^4$, i.e. the number of points of $\mathrm{Gr}(2,4)$ defined over $\mathbb{F}_q$, is the quotient

$$\frac{(q^4-1)(q^4-q)}{(q^2-1)(q^2-q)} = 1 + q + 2q^2 + q^3 + q^4.$$

The same argument shows that the number of points of $\mathrm{Gr}(2,4)$ defined over $\mathbb{F}_{q^n}$ is

$$\frac{(q^{4n}-1)(q^{4n}-q^n)}{(q^{2n}-1)(q^{2n}-q^n)} = 1 + q^n + 2q^{2n} + q^{3n} + q^{4n}.$$

As in the case of $\mathbb{P}^1$, we can now write the log of the zeta function of $\mathrm{Gr}(2,4)$ as

$$\begin{aligned}\log \zeta_{\mathrm{Gr}(2,4)}(t) &= \sum_{n>0} \frac{1}{n} t^n + \sum_{n>0} \frac{1}{n}(qt)^n + 2\sum_{n>0} \frac{1}{n}(q^2t)^n + \sum_{n>0} \frac{1}{n}(q^3t)^n + \sum_{n>0} \frac{1}{n}(q^4t)^n \\ &= -\log(1-t) - \log(1-qt) - 2\log(1-q^2t) - \log(1-q^3t) - \log(1-q^4t),\end{aligned}$$

and exponentiating,

$$\zeta_{\mathrm{Gr}(2,4)}(t) = \frac{1}{(1-t)(1-qt)(1-q^2t)^2(1-q^3t)(1-q^4t)}.$$

This is indeed a rational function of the desired form, noting that the dimension of $\mathrm{Gr}(j,n)$ is $j(n-j)$, so that $\dim \mathrm{Gr}(2,4) = 4$. The Riemann hypothesis is evident (indeed $\alpha_{ij} = q^{i/2}$ for all i, j), and it is simple to verify the functional equation

$$\zeta_{\mathrm{Gr}(2,4)}(q^{-4}t^{-1}) = q^{12}t^6\zeta_{\mathrm{Gr}(2,4)}(t).$$

It can be verified that the Betti numbers of the complex Grassmannian $\mathrm{Gr}(2,4)$ are

$$1, 0, 1, 0, 2, 0, 1, 0, 1$$

and its Euler characteristic 6, in agreement with the properties of its zeta function.

3 Abelian Varieties

In this section we give the basic properties of abelian varieties, and develop the theory that will be necessary in §4. For the general theory of abelian varieties we follow [5].

Fix a field k. An *abelian variety* A over k is a complete connected variety with a compatible group structure, in the sense that the maps

$$m : A \times A \to A$$

given by the group operation and

$$\cdot^{-1} : A \to A$$

given by inversion are regular maps (i.e. morphisms of varieties), and there is an identity element $0 \in A(k)$. In particular, multiplication (or translation) by a group element $A \xrightarrow{\cdot x} A$ is regular. It will develop that abelian varieties are abelian, so we will denote the identity by 0 and the group operation additively.

It follows easily from the definition that abelian varieties are smooth and irreducible. Recall that the smooth points of a variety form a non-empty open subset. Any point of an abelian variety can be translated to a smooth point, and translation is an isomorphism, so every point is smooth. Now a smooth point cannot be contained in more than one irreducible component of a variety, so irreducible components do not intersect, and the connectedness hypothesis implies irreducibility.

The properties of completeness and irreducibility are tight constraints on the behavior of varieties. The following theorem is an example of this.

Theorem 1 ([5], Theorem 1.1)**.** *If V, W, U are varieties over k, V is complete, $V \times W$ geometrically irreducible, and $\alpha : V \times W \to U$ a regular map such that*

$$\alpha(V \times \{w_0\}) = \{u_0\} = \alpha(\{v_0\} \times W)$$

for some $v_0 \in V(k)$, $w_0 \in W(k)$, and $u_0 \in U(k)$, then α is constant.

The additional feature of a group structure makes abelian varieties extremely rigid objects. In fact the above theorem, together with the group structure, is enough to prove some interesting properties of abelian varieties.

Proposition 2 ([5], Corollay 1.2)**.** *Any regular map $\phi : A \to B$ of abelian varieties can be decomposed as a group homomorphism $A \to B$ followed by a translation $B \to B$.*

Proof. After composing with a translation $B \to B$, we may assume that ϕ sends the identity element 0_A of A to the identity element 0_B of B. The regular map

$$\begin{aligned} \tilde{\phi} : A \times A &\to B \\ (a, a') &\mapsto \phi(a + a') - \phi(a) - \phi(a') \end{aligned}$$

then satisfies $\tilde{\phi}(\{0_A\} \times A) = \{0_B\} = \tilde{\phi}(A \times \{0_A\})$, so we may apply Theorem 1 to conclude that $\tilde{\phi}(A \times A) = \{0_B\}$. This implies that ϕ is a morphism of groups. □

Proposition 3 ([5], Corollary 1.4)**.** *The group structure of an abelian variety is abelian.*

Proof. If A is an abelian variety, by definition the map $\cdot^{-1} : A \to A$ given by inversion is regular. Furthermore it preserves the identity $0 \in A$, so by Proposition 2 we conclude that inversion is a group homomorphism. This implies that the group structure is abelian. □

We also have the following strong result regarding maps from smooth varieties to abelian varieties.

Theorem 4 ([5], Theorem 3.2)**.** *A rational map $V \dashrightarrow A$ from a smooth variety to an abelian variety is in fact regular.*

In particular, this shows that every rational map of abelian varieties is in fact a regular map, and birational maps of abelian varieties are isomorphisms.

Much can be said about abelian varieties because of the large amount of structure that they carry. However, rather few varieties are abelian varieties. This is mitigated by the fact that abelian varieties can be naturally associated to arbitrary varieties, and these connections allow us to use abelian varieties in our study of general varieties. Indeed, after proving the Riemann hypothesis for abelian varieties, we proceed to prove the Riemann hypothesis for curves and for cubic threefolds by reducing these problems to problems about abelian varieties.

An important method of constructing abelian varieties is the *Jacobian* variety of a curve. If C is a curve, its Jacobian is $J(C) = \mathrm{Pic}^0(C)$, the group of degree 0 line bundles on C up to isomorphism (with group operation the tensor product). The Jacobian receives a rational map from its curve $C \to J(C)$, and satisfies the universal property that any rational map $C \to A$ from C to an abelian variety factors uniquely into the rational map $C \to J(C)$ followed by a regular map $J(C) \to A$.

This universal property defines the *Albanese* variety of a general variety. That is, for any variety V there exists an abelian variety $A(V)$ receiving a rational map $V \to A(V)$, and such that any rational map $V \to B$ to an abelian variety factors as $V \to A(V)$ followed by a regular map $A(V) \to B$. The universal property shows that $A(V)$ is unique up to isomorphism. Note in particular that for a curve, the Jacobian and Albanese varieties coincide.

Note also that birational varieties have the same Albanese variety, for a birational map $V \dashrightarrow V'$ induces a birational map $A(V) \dashrightarrow A(V')$, and birational maps of abelian varieties are isomorphisms. For example, a curve and its normalization have the same Jacobian variety.

3.1 Endomorphism Algebras & Tate Modules

For A, B abelian varieties, let $\mathrm{Hom}(A, B)$ be the abelian group of morphisms $A \to B$ (under pointwise addition), and $\mathrm{End}\, A = \mathrm{Hom}(A, A)$ the ring of endomorphisms (with multiplication given by function composition). We define $\mathrm{Hom}^0(A, B) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}(A, B)$ and $\mathrm{End}^0 A = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}\, A$.

The composition form $\mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$ extends uniquely to a $\mathbb{Q}$-bilinear form $\mathrm{Hom}^0(A, B) \times \mathrm{Hom}^0(B, C) \to \mathrm{Hom}^0(A, C)$. In this way we can define composition of elements of Hom^0, and obtain a category whose elements are abelian varieties and whose morphisms are elements of Hom^0. In this category isogenies are isomorphisms, because every isogeny $\phi : A \to B$ has a dual isogeny $\phi^* : B \to A$ such that $\phi^* \phi = n\,\mathrm{id}$, and $n\,\mathrm{id}$ is invertible after tensoring with $\mathbb{Q}$. Thus for $\phi : A \to B$ an isogeny, we denote by ϕ^{-1} its inverse in $\mathrm{Hom}^0(B, A)$.

The structure of the endomorphism algebra of an abelian variety can be described in a fairly precise way.

Theorem 5 ([6], IV)**.** *If A is an abelian variety, then $\mathrm{End}^0 A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$, where the D_i are division algebras over $\mathbb{Q}$ and $M_{n_i}(D_i)$ denotes the ring of $n_i \times n_i$ matrices with coefficients in D_i.*

However, it is useful to introduce an auxiliary object which encodes much of the information of morphisms of abelian varieties. If A is an abelian variety over k and ℓ a prime different from the characteristic of k, denote by $A[\ell^n](k^s)$ the ℓ^n-torsion subgroup of the k^s-points of A (where k^s is a separable closure of k). Define the *ℓ-adic Tate module* of A to be

$$T_\ell A = \varprojlim_n A[\ell^n](k^s) \cong \mathrm{Hom}_{\mathbf{Ab}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(k^s)_{\mathrm{tors}}). \tag{7}$$

If $\dim A = g$, the group $A[\ell^n](k^s)$ has precisely $\ell^{n \cdot 2g}$ elements, and $T_\ell A \cong \mathbb{Z}_\ell^{2g}$ as $\mathbb{Z}_\ell$-modules.

A morphism $A \to B$ of abelian varieties over k induces a morphism of groups $A(k^s) \to B(k^s)$ which restricts to a morphism $A(k^s)_{\mathrm{tors}} \to B(k^s)_{\mathrm{tors}}$, and this induces a morphism $\mathrm{Hom}_{\mathbf{Ab}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(k^s)_{\mathrm{tors}}) \to \mathrm{Hom}_{\mathbf{Ab}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, B(k^s)_{\mathrm{tors}})$. That is, for abelian varieties A, B, there is a natural map

$$\mathrm{Hom}(A, B) \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B). \tag{8}$$

The significance of the Tate module is that passing to the Tate module remembers much of the information about the original abelian variety, as demonstrated by the following theorem.

Theorem 6. *Let A be an abelian variety over a finite field k with separable closure k^s, and let ℓ be a prime different from the characteristic of k. Then the natural map*

$$\mathrm{End}(A \times_k k^s) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell A)$$

is injective and $\mathrm{Gal}(k^s/k)$-equivariant.

Thus we may study an endomorphism of A by transporting it to an endomorphism of the Tate module, which as observed above is a free $\mathbb{Z}_\ell$-module and therefore perhaps a simpler environment. In particular, the degree of an isogeny $A \to A$ corresponds to the determinant of the corresponding endomorphism of $T_\ell A$, and the trace and characteristic polynomial of an isogeny $A \to A$ as defined in the next section coincide with the trace and characteristic polynomial of the corresponding endomorphism of $T_\ell A$.

3.2 The Riemann Hypothesis for Abelian Varieties

The *degree* of a surjective morphism $\alpha : A \to B$ of abelian varieties, denoted $\nu(\alpha)$, is the degree of the induced extension of function fields $k(B) \to k(A)$. If the characteristic of the ground field does not divide $\nu(\alpha)$, or more generally if α is separable (i.e. the extension $k(B) \to k(A)$ is separable), then $\nu(\alpha)$ is preciesly the order of the kernel of α.

Proposition 7 ([4], IV Theorem 6)**.** *Let $\alpha_1, \ldots, \alpha_r : A \to B$ be morphisms of abelian varieties of the same dimension g. Then $\nu(m_1\alpha_1 + \cdots + m_r\alpha_r)$, as a function on integers m_i, is a homogeneous polynomial of degree $2g$ with rational coefficients.*

Because of the Proposition, we have for $\alpha \in \operatorname{End} A$ a *characteristic polynomial* P_α, defined by

$$P_\alpha(n) = \nu(\alpha - n \operatorname{id}) \tag{9}$$

for all integers n (with $\operatorname{id} \in \operatorname{End} A$ the identity). As in the case of matrices, we define the *trace* $\operatorname{tr}(\alpha)$ of an endomorphism to be (the negative of) the second-highest coefficient of the characteristic polynomial, or equivalently the sum of the roots of the characteristic polynomial (or *characteristic roots*).

Consider $\alpha = \pi^n$ the q^n-power Frobenius endomorphism of A. The fixed points of π^n, which is the same as the kernel of $\pi^n - 1$, are precisely the points of A defined over $\mathbb{F}_{q^n}$. Now $\pi^n - 1$ is a separable isogeny, so we have

$$\#A(\mathbb{F}_{q^n}) = \nu(\pi^n - 1) = P_{\pi^n}(1). \tag{10}$$

This is our motivation for examining the characteristic polynomial of an endomorphism. In particular, for the Riemann hypothesis we are interested in the absolute values of roots of the characteristic polynomial. Before doing this another definition is necessary.

Let $\mathscr{L}$ be a line bundle on A, i.e. an element of the dual abelian variety $A^\vee = \operatorname{Pic}^0 A$. Denoting translation by x on A by t_x, the line bundle $\mathscr{L}$ induces an isogeny

$$\begin{aligned} \lambda_{\mathscr{L}} : A &\to A^\vee \\ x &\mapsto \mathscr{L} \otimes t_x^* \mathscr{L}^{-1}. \end{aligned} \tag{11}$$

This in turn induces an endomorphism, called the *Rosati involution*

$$\begin{aligned} {}' : \operatorname{End}^0(A) &\to \operatorname{End}^0(A) \\ \alpha &\mapsto \alpha' = \lambda_{\mathscr{L}}^{-1} \alpha^\vee \lambda_{\mathscr{L}} \end{aligned} \tag{12}$$

where $\alpha^\vee : A^\vee \to A^\vee$ is the dual morphism to α (not to be confused with the dual isogeny denoted by * above).

The following proposition gives us access to the absolute values of the characteristic roots of an endomorphism.

Proposition 8 ([6], IV)**.** *Let A be an abelian variety of dimension g, $'$ the Rosati involution on End^0 A defined by some ample line bundle, and $\alpha \in \mathrm{End}\, A$ such that $\alpha'\alpha = n\,\mathrm{id}$ for some $n \in \mathbb{Z}$. Let $\omega_1, \ldots, \omega_{2g}$ be the roots of the characteristic polynomial of α. Then $|\omega_i|^2 = n$ for all i, and the map $\omega_i \mapsto n/\omega_i$ is a permutation of the roots ω_i.*

We can apply the Proposition to the Frobenius endomorphism on account of the following lemma.

Lemma 9 ([6], IV)**.** *Let A be an abelian variety, $'$ the Rosati involution on End^0 A defined by some ample line bundle, and $\pi : A \to A$ the q-power Frobenius endomorphism. Then $\pi'\pi = q\,\mathrm{id}$.*

Combining Lemma 9 and Proposition 8, we conclude that the roots $\omega_1, \ldots, \omega_{2g}$ of the characteristic polynomial $P_{\pi^n}(t)$ have absolute value $|\omega_i| = q^{1/2}$. By Equation (10),

$$\#A(\mathbb{F}_{q^n}) = \prod_{i=1}^{2g}(1-\omega_i) = \sum_{|\mathbf{a}|=0}^{2g}(-1)^{|\mathbf{a}|}\omega^{\mathbf{a}}, \tag{13}$$

where $\mathbf{a} = (a_1, \ldots, a_{2g})$ is a multi-index and $\omega^{\mathbf{a}} = \omega_1^{a_1} \cdots \omega_{2g}^{a_{2g}}$. Clearly $|\omega^{\mathbf{a}}| = q^{|\mathbf{a}|/2}$, and thus we conclude the Riemann hypothesis for abelian varieties.

3.3 The Riemann Hypothesis for Curves

We prove the Riemann hypothesis for curves by relating them to abelian varieties, and using the above results on abelian varieties. This section largely follows [4, VI §3].

For X and Y irreducible subvarieties of a variety (which intersect properly, i.e. $\mathrm{codim}\, X \cap Y = \mathrm{codim}\, X + \mathrm{codim}\, Y$), recall the intersection product

$$X \cdot Y = \sum \mu(X, Y; Z_i) Z_i,$$

where Z_i are the irreducible components of the intersection $X \cap Y$ and $\mu(X, Y; Z_i)$ is the intersection multiplicity of X and Y at Z_i. We can extend the intersection product to irreducible subvarieties not intersecting properly by considering rational equivalence classes (and choosing representatives which intersect properly), and we can extend further to formal linear combinations of irreducible subvarieties (i.e. algebraic cycles) by linearity. Thus we obtain an intersection product on the group of algebraic cycles (up to rational equivalence) on a variety.

If $\sum n_i P_i$ is a linear combination of points, i.e. a 0-cycle, then we define its *degree* to be $\sum n_i$.

We consider intersection theory of divisors on $C \times C$, for C a curve. Since the dimension and codimension of a divisor in $C \times C$ are both 1, the intersection of two divisors

will be a collection of points, i.e. a 0-cycle, and we can ask for its degree. For X a divisor on $C \times C$ and Δ the diagonal, define

$$\sigma(X) = d(X) + d'(X) - I(X \cdot \Delta), \tag{14}$$

where $d(X)$ is the degree of $X \cdot (P \times C)$, $d'(X)$ is the degree of $X \cdot (C \times P)$ (here P is any point on C), and $I(X \cdot \Delta)$ is the degree of $X \cdot \Delta$.

Let us consider the interpretation of these definitions. The idea is that the graph of an endomorphism $C \to C$ is a divisor on $C \times C$, and a general divisor on $C \times C$ can be thought of similarly. The quantity $d(X)$ is a measure of "multi-valued-ness", as the intersection $X \cap (P \times C)$ consists of points in the target (right-hand) C, corresponding to a single point of the source (left-hand) C. The quantity $d'(X)$ is an analogue of "degree" of an endomorphism, as the intersection $X \cap (C \times P)$ consists of points in the source C corresponding to a single point in the target C.

The quantity $I(X \cdot \Delta)$ is an analogue of "number of fixed points" of an endomorphism. Indeed, if $X = \Gamma_f$ is the graph of a function $f : C \to C$ then the points of intersection of $X \cap \Delta$ correspond precisely to the fixed points of f, and if this intersection is transverse then $I(X \cdot \Delta)$ is equal to the number of fixed points of f.

The essential relation between a curve and its Jacobian is as follows.

Theorem 10 ([4], VI Theorem 6)**.** *Let C be a smooth complete curve with Jacobian J, X a divisor on $C \times C$, and $\tau : J \to J$ the endomorphism induced by X. Then $\sigma(X) = \mathrm{tr}(\tau)$.*

Now let $\pi^n : C \to C$ be the q^n-power Frobenius endomorphism, and $X = \Gamma_{\pi^n}$ its graph. The induced endomorphism $\tau : J \to J$ is the q^n-power Frobenius endomorphism on J, so applying Theorem 10 we have $\sigma(\Gamma_{\pi^n}) = \mathrm{tr}(\pi^n; J)$.

Since Γ_{π^n} is the graph of a function, $d(\Gamma_{\pi^n}) = 1$; also π^n has degree q^n, so $d'(\Gamma_{\pi^n}) = q^n$. Since the derivative of π^n is zero, Γ_{π^n} intersects the diagonal Δ transversely, and $I(\Gamma_{\pi^n} \cdot \Delta)$ is the number of fixed points of π^n on C, i.e. the number of points of C defined over $\mathbb{F}_{q^n}$. We can write this number as

$$\#C(\mathbb{F}_{q^n}) = I(\Gamma_{\pi^n} \cdot \Delta) = d(\Gamma_{\pi^n}) + d'(\Gamma_{\pi^n}) - \sigma(\Gamma_{\pi^n}) = 1 + q^n - \mathrm{tr}(\pi^n; J). \tag{15}$$

Now applying the results of §3.2, we see

$$\#C(\mathbb{F}_{q^n}) = 1 + q^n - \sum_{i=1}^{2g} \omega_i^n \tag{16}$$

where $\omega_1, \ldots, \omega_{2g}$ are the roots of the characteristic polynomial of $\pi^n \in \mathrm{End}^0 J$; in particular, $|\omega_i| = q^{1/2}$. This implies that the zeta function of C satisfies the Riemann Hypothesis.

4 The Riemann Hypothesis for Cubic Threefolds

In [1], Bombieri and Swinnerton-Dyer prove the Riemann hypothesis for cubic threefolds in $\mathbb{P}^4$ over a finite field. The idea, as in the case of curves, is to relate the point count

on a cubic threefold to the trace of a Frobenius endomorphism on an abelian variety. However, the connection to abelian varieties is not so straightforward as in the case of curves. Indeed, both clever geometric constructions and hard work with abelian varieties must be employed in order to establish the connection. In this section we describe the geometric constructions of [1] in detail, and indicate how the above results on curves and abelian varieties enter in to complete the proof.

4.1 Schemes of j-Planes

One of the key geometric objects used in the proof is the variety parametrizing lines contained in the cubic threefold. In this section we consider general geometric constructions of this type.

The projective space $\mathbb{P}^n$ parametrizes lines through the origin (i.e. 1-dimensional linear subspaces) in affine space $\mathbb{A}^{n+1}$. Similarly, the Grassmannian $\mathrm{Gr}(j,n)$ parametrizes the set of j-dimensional linear subspaces of $\mathbb{A}^n$. Since points of $\mathbb{P}^n$ are lines of $\mathbb{A}^{n+1}$, the j-dimensional projective subspaces of $\mathbb{P}^n$ are precisely $(j+1)$-dimensional linear subspaces of $\mathbb{A}^{n+1}$. Thus $\mathrm{Gr}(j+1,n+1)$ parametrizes j-dimensional projective subspaces of $\mathbb{P}^n$. For brevity we will refer to a j-dimensional projective subspace of $\mathbb{P}^n$ as a *j-plane*, and we will write $\mathrm{Pl}(j,n) = \mathrm{Gr}(j+1,n+1)$ for the variety of j-planes in $\mathbb{P}^n$.

In addition to parametrizing j-planes in $\mathbb{P}^n$, it will prove useful to parametrize j-planes in $\mathbb{P}^n$ containing a chosen k-plane. This is straightforward: j-planes in $\mathbb{P}^n$ containing a chosen k-plane correspond to $(j+1)$-dimensional subspaces of $\mathbb{A}^{n+1}$ containing the corresponding $(k+1)$-dimensional subspace, which in turn correspond (via the quotient by this $(k+1)$-dimensional subspace) to $(j-k)$-dimensional subspaces of $\mathbb{A}^{n-k}$. Thus j-planes in $\mathbb{P}^n$ containing a chosen k-plane are parametrized by $\mathrm{Gr}(j-k,n-k)$. In particular, the set of 2-planes in $\mathbb{P}^n$ containing a chosen line is $\mathrm{Gr}(1,n-1) \cong \mathbb{P}^{n-2}$.

When working with j-planes in projective space, a very useful object is the universal j-plane

$$Q(j,n) = \{(H,x) \mid x \in H\} \subset \mathrm{Pl}(j,n) \times \mathbb{P}^n.$$

It is equipped with projections $\pi_1 : Q(j,n) \to \mathrm{Pl}(j,n)$ and $\pi_2 : Q(j,n) \to \mathbb{P}^n$ by restricting the projections of the product. Note that the fiber over a point $H \in \mathrm{Pl}(j,n)$ in the projection $Q(j,n) \to \mathrm{Pl}(j,n)$ is precisely H itself, as a subset of $\mathbb{P}^n$.

For a variety V and natural number j, we define a *scheme of j-planes in V* to be a closed subscheme $X \subset \mathrm{Pl}(j,n)$ such that $\pi_1^{-1}(X) \subset \mathrm{Pl}(j,n) \times V$. Note that a scheme of j-planes is projective, as a closed subscheme of the projective variety $Q(j,n) \subset \mathrm{Pl}(j,n) \times \mathbb{P}^n$.

Just as $Q(j,n)$ is the universal j-plane in $\mathbb{P}^n$, we would like to define a universal j-plane in any projective scheme embedded in $\mathbb{P}^n$. We can do this in the following way.

Proposition 11. *Let $V \subset \mathbb{P}^n$ be a closed subvariety, and $\Lambda_j(V) \subset \mathrm{Pl}(j,n)$ the set of points $w \in \mathrm{Pl}(j,n)$ for which the corresponding j-plane H_w is contained in V. Then $\Lambda_j(V)$ is closed in $\mathrm{Pl}(j,n)$.*

Proof. Consider $Q(j,n) \subset \mathrm{Pl}(j,n) \times \mathbb{P}^n$ and let

$$\pi_2 : Q(j,n) \to \mathbb{P}^n$$

be projection onto the second factor. By continuity

$$\pi_2^{-1}(V) = \{(H, x) : x \in H \cap V\}$$

is closed in $Q(j,n)$. Let's call this $Q_V = \pi_2^{-1}(V)$, and give it the natural reduced subscheme structure.

Consider the morphism $Q_V \to V$ given by projection onto the second factor (regarding Q_V as a subscheme of $\mathrm{Pl}(j,n) \times V$). The fiber of this map over a point $x \in V$ is simply the set of j-planes in $\mathbb{P}^n$ containing x, which (from the discussion above) is isomorphic to $\mathrm{Pl}(j-1, n-1)$. Since the target V is irreducible and the fibers $\mathrm{Pl}(j-1,n-1)$ are irreducible of uniform dimension, the domain Q_V is irreducible as well. Thus Q_V is a variety, and in fact a projective variety, because it is a closed subvariety of the projective variety $Q(j,n)$.

Now consider

$$\pi_1 : Q_V \to \mathrm{Pl}(j,n),$$

the restriction of the projection from $Q(j,n)$ onto the first factor. The fiber of this map over $H \in \mathrm{Pl}(j,n)$ is $H \cap V$. Since π_1 is a projective morphism and therefore proper, the fiber dimension

$$\begin{aligned} d : \mathrm{Pl}(j,n) &\to \mathbb{N} \\ H &\mapsto \dim \pi_1^{-1}(H) = \dim H \cap V \end{aligned}$$

is upper-semicontinuous, i.e. for any $k \in \mathbb{N}$ the set

$$d_k = \{H \in \mathrm{Pl}(j,n) : d(H) \geq k\}$$

is closed in $\mathrm{Pl}(j,n)$.

To complete the proof we observe that d_j is precisely $\Lambda_j(V)$. By definition d_j is the set of $H \in \mathrm{Pl}(j,n)$ for which $\dim H \cap V \geq j$, but since $\dim H = j$ this is the same as $\dim H \cap V = j$. The intersection $H \cap V$ is a closed subset of the irreducible variety H, so $\dim H \cap V = \dim H (= j)$ if and only if $H \cap V = H$, and this is equivalent to $H \subset V$. $\square$

Thus for any closed subvariety $V \subset \mathbb{P}^n$ we obtain a maximal (reduced) scheme of j-planes by equipping $\Lambda_j(V)$ with the natural reduced subscheme structure. Note that by taking the reduced scheme structure we are destroying some subtlety; in general a maximal scheme of j-planes in a closed subscheme of $\mathbb{P}^n$ need not be reduced.

It is difficult to compute the dimension of $\Lambda_j(V)$ for an arbitrary variety, but possible to give simple heuristic estimates in some cases. Say $V = V(f) \subset \mathbb{P}^n$ for a homogeneous polynomial $f \in k[x_0, \ldots, x_n]$ of degree d, i.e. a hypersurface of degree d. Lines in $\mathbb{P}^n$ are parametrized by $\mathrm{Pl}(1,n) = \mathrm{Gr}(2, n+1)$, whose dimension is $2(n+1-2) = 2n-2$. We can parametrize an open subvariety by $\mathbb{A}^{2n-2}$, with coordinates $(a_{k,\ell})_{\substack{1 \leq k \leq n-1 \\ 0 \leq \ell \leq 1}}$, by sending $(a_{k,\ell})$ to the projective line

$$\begin{aligned} \mathbb{P}^1 &\to \mathbb{P}^n \\ [s,t] &\mapsto [s, t, a_{1,0}s + a_{1,1}t, \ldots, a_{n-1,0}s + a_{n-1,1}t]. \end{aligned}$$

A line in this open subset of $\mathrm{Pl}(1,n)$ lies on $V(f)$ precisely when the polynomial

$$f(s,t,a_{1,1}s+a_{1,2}t,\ldots,a_{n-1,1}s+a_{n-1,2}t)$$

is identically zero. The above polynomial is homogeneous of degree d in s,t, so equating the coefficients of $s^d, s^{d-1}t,\ldots,t^d$ to zero we obtain $d+1$ polynomial equations in the $a_{k,\ell}$ whose vanishing defines the intersection of $V(f)$ with our open subset. If these equations are independent in an appropriate sense, then the dimension of this intersection will be $(2n-2)-(d+1) = 2n-d-3$. Thus if $V \subset \mathbb{P}^n$ is a hypersurface of degree d, we generally expect $\dim \Lambda_1(V) = 2n-d-3$.

Similarly, j-planes in $\mathbb{P}^n$ are parametrized by $\mathrm{Pl}(j,n) = \mathrm{Gr}(j+1,n+1)$, whose dimension is $(j+1)(n-j)$. Using a similar parametrization and the fact that there are $\binom{j+d}{d}$ monomials of degree d in $j+1$ variables, we expect

$$\dim \Lambda_j(V(f)) = \max\left[(j+1)(n-j) - \binom{j+d}{d}, 0\right]$$

for $V(f) \subset \mathbb{P}^n$ a hypersurface of degree d. In general this is a lower bound for the dimension of $\Lambda_j(V(f))$.

4.2 Geometric Constructions

We now return to the setting of [1]. Let $V \subset \mathbb{P}^4$ be a smooth cubic hypersurface defined over $\mathbb{F}_q$, and $X = \Lambda_1(V)$ the variety of lines in V. The goal of our geometric constructions is this: rather than counting the points of V all at once, we produce a rational map from V to the projective plane, and count the points on each fiber. The points on non-degenerate fibers can be counted rather simply, and the point count on degenerate fibers can expressed in terms of point counts on curves, about which much is known.

In order to carry out our constructions, we choose a point $u \in X$ corresponding to a line $L_u \subset V$. Despite its importance for the argument, this point is essentially auxiliary information, and the choice of point is unimportant.

As in §4.1, the set of 2-planes in $\mathbb{P}^4$ containing L_u is parametrized by a projective plane, which we denote $\mathbb{P}^2_u$. For each point $v \in V$ off of L_u, there is a unique 2-plane in $\mathbb{P}^4$ spanned by v and L_u. In this way we obtain a rational map $p_u : V \dashrightarrow \mathbb{P}^2_u$, defined on the complement of L_u, sending a point $v \in V$ to the plane defined by v and L_u.

We want to describe the fibers of this rational map. First note that the number of fibers is the number of points of $\mathbb{P}^2_u$ over $\mathbb{F}_q$, which is q^2+q+1. To describe the fibers themselves we describe the intersections of planes in $\mathbb{P}^2_u$ with V, which is not precisely the same, but can easily be adjusted to obtain the desired result.

Now, let $P_w \in \mathbb{P}^4$ be a plane corresponding to a point $w \in \mathbb{P}^2_u$. Since V has degree 3, by Bézout's theorem $V \cap P_w$ will have degree 3. Also, as long as $P_w \not\subset V$, we have $\dim V \cap P_w = \dim V + \dim P_w - \dim \mathbb{P}^4 = 3+2-4 = 1$. Since P_w and V both contain the line L_u, it must be an irreducible component, i.e. $V \cap P_w = L_u \cup Q_w$ for some conic Q_w.

We can count the points of V over $\mathbb{F}_q$ by counting the points on these conics. Indeed, each point of V not on L_u lies on a unique plane P_w through L_u, and thus lies on a unique

conic Q_w. Each point x on L_u lies on a conic Q_w precisely when the plane P_w is tangent to V at x, i.e. P_w is contained in the tangent plane to V at x. Since V is smooth its tangent spaces are all 3-dimensional, so by the argument in §4.1, the 2-planes contained in the tangent space at x and containing L_u are parametrized by a projective line $\mathbb{P}^1$. This implies that each of the $q+1$ points of L_u lies on $q+1$ conics Q_w, and is therefore counted q times too many if we take all points on the conics Q_w. Writing ν_q for "number of points defined over $\mathbb{F}_q$", we have shown

$$\nu_q(V) = \sum_{w \in \mathbb{P}^2_u} \nu_q(Q_w) - q(q+1). \tag{17}$$

Now we examine the number of points on the conics Q_w. There are four forms the conics Q_w can take:

1. a non-singular conic, defined over $\mathbb{F}_q$;
2. a pair of distinct lines, defined over $\mathbb{F}_q$;
3. a double line, defined over $\mathbb{F}_q$; or
4. a pair of distinct lines, defined over a quadratic extension of $\mathbb{F}_q$.

In the non-degenerate case 1, the conic Q_w (being isomorphic to $\mathbb{P}^1$) has precisely $q+1$ points defined over $\mathbb{F}_q$. In case 2, Q_w has $2q+1$ points defined over $\mathbb{F}_q$, for each line making up Q_w has $q+1$ points, and the two lines intersect in precisely one point (on account of being distinct and both lying on the plane P_w). In case 3, being a single line, Q_w has $q+1$ points defined over $\mathbb{F}_q$. Finally, in case 4, Q_w has a single point defined over $\mathbb{F}_q$, at the intersection of the two lines defined over a quadratic extensions of $\mathbb{F}_q$.

Note that in each degenerate case, the number of points of Q_w over $\mathbb{F}_q$ is one plus q times the number of lines defined over $\mathbb{F}_q$ making up Q_w. Thus if we let F be the number of degenerate conics Q_w, and G the total number of lines contained in these degenerate conics, then the number of points collectively on the degenerate conics is

$$F + qG.$$

Recalling that there are q^2+q+1 conics Q_w (corresponding to points of $\mathbb{P}^2_u$) and $q+1$ points on each non-degenerate conic, the total number of points on all conics is

$$\sum_{w \in \mathbb{P}^2_u} \nu_q(Q_w) = (q^2+q+1-F)(q+1) + F + qG. \tag{18}$$

Combining (17) and (18), we find

$$\nu_q(V) = \frac{q^4-1}{q-1} + q(G-F). \tag{19}$$

The key idea of the geometric constructions is that the number F of degenerate conics and the number G of lines on them can be expressed as point counts on curves. This essentially reduces our problem about cubic threefolds to a problem about curves, where much more is known.

Recall that the conics Q_w are defined by $V \cap P_w = L_u \cup Q_w$ for P_w a plane through L_u corresponding to a point $w \in \mathbb{P}^2_u$. A line in Q_w is a line in V contained in P_w and different from L_u, which therefore intersects L_u. Conversely, if a line in V intersects L_u, then the two of then span a plane P_w through L_u, and thus the line lies in a conic Q_w. Thus the lines contained in the degenerate conics (whose number is G) are precisely the subset of X, the variety of lines of V, consisting of lines intersecting L_u. In fact this subset is a curve in X, which we call C_u. The number of lines contained in degenerate conics is $G = \nu_q(C_u)$.

Now let Q_w be a degenerate conic containing a line L corresponding to a point of C_u. Since Q_w has degree 2 it must contain another line L' corresponding to another point of C_u (or Q_w may be a double line in which case $L' = L$). The assignment $L \mapsto L'$ defines an involution j_u on C_u, and the quotient parametrizes conics Q_w containing a line, i.e. degenerate conics. We can realize the quotient C_u/j_u as a curve in $\mathbb{P}^2_u$, which we call Γ_u. The number of degenerate conics is now $F = \nu_q(\Gamma_u)$.

Combining the previous paragraphs with (19) we find

$$\nu_q(V) = \frac{q^4 - 1}{q - 1} + q(\nu_q(C_u) - \nu_q(\Gamma_u)),$$

and replacing q by q^n throughout, we arrive at the key equation

$$\nu_{q^n}(V) = \frac{q^{4n} - 1}{q^n - 1} + q^n(\nu_{q^n}(C_u) - \nu_{q^n}(\Gamma_u)). \tag{20}$$

This is very nearly the reduction we want, except that the curves C_u, Γ_u may not be smooth. Fortunately we may replace them by their normalizations with no effect on the difference in number of points between them. Thus

$$\nu_{q^n}(V) = \frac{q^{4n} - 1}{q^n - 1} + q^n(\nu_{q^n}(\tilde{C}_u) - \nu_{q^n}(\tilde{\Gamma}_u)). \tag{21}$$

We have achieved the goal of the geometric constructions, expressing the number of points on V in terms of the number of points on a pair of smooth projective curves.

4.3 Completion of the Proof

Since $\tilde{C}_u$ and $\tilde{\Gamma}_u$ are smooth projective curves, we can conclude the Riemann hypothesis for cubic threefolds from Equation (21) by invoking the Riemann hypothesis for curves. This would show that the term $q^n(\tilde{C}_u) - \nu_{q^n}(\tilde{\Gamma}_u)$ is a sum of n^{th} powers of algebraic numbers with norm $q^{3/2}$, so that $\#V(\mathbb{F}_{q^n})$ is the sum of n^{th} powers of algebraic numbers with norm equal to a half-integer power of q. However, we can give a formula not depending on the auxiliary point u in the following way.

From (15) we see $\#\tilde{C}_u(\mathbb{F}_{q^n}) = 1 + q^n - \operatorname{tr}(\pi^n; J(C_u))$ and $\#\tilde{\Gamma}_u(\mathbb{F}_{q^n}) = 1 + q^n - \operatorname{tr}(\pi^n; J(\Gamma_u))$ (recall that a curve and its normalization have the same Jacobian). Substituting these expressions into (21) gives

$$\nu_{q^n}(V) = \frac{q^{4n} - 1}{q^n - 1} + q^n(\operatorname{tr}(\pi^n; J(\Gamma_u)) - \operatorname{tr}(\pi^n; J(C_u))). \tag{22}$$

The essential facts about abelian varieties needed to remove the point u are the following.

Proposition 12 ([4]). *If abelian varieties A, B over a finite field k are isogenous over k, then they have the same number of points defined over k.*

This implies that their respective Frobenius endomorphisms have the same trace.

Theorem 13 ([1], Lemma 9). *If u is a point of X with C_u geometrically irreducible, then there is a sequence*

$$0 \to J(\Gamma_u) \to J(C_u) \to A(X) \to 0$$

defined over $k(u)$ which is exact up to isogeny.

Combining Proposition 12 and Theorem 13, we conclude

$$\operatorname{tr}(\pi^n; A(X)) = \operatorname{tr}(\pi^n; J(C_u)) - \operatorname{tr}(\pi^n; J(\Gamma_u)),$$

and thus

$$\nu_{q^n}(V) = \frac{q^{4n}-1}{q^n-1} - q^n(\operatorname{tr}(\pi^n; A(X))). \tag{23}$$

This formula eliminates the dependence on our auxiliary variable u.

Observe, however, that Theorem 13 requires the curve C_u to be geometrically irreducible, and such a point u is only guaranteed to exist (i.e. be defined) over a sufficiently large field extension. Thus (23) only holds a priori for sufficiently large n. However, Dwork [3] proved that a hypersurface of odd degree d in $\mathbb{P}^n$ such as our cubic threefold V has zeta function of the form

$$\zeta_V(t) = P(t)^{(-1)^n} \prod_{i=0}^{n-1} (1-q^i t)^{-1}, \tag{24}$$

where $P(t)$ is a polynomial of degree $\frac{(d-1)^{n+1}+(-1)^{n+1}(d-1)}{d}$. In the present case of course $n = 4$ and $d = 3$. The factor $\prod_{i=0}^{n-1}(1-q^i t)^{-1}$ corresponds to the summand $\frac{q^{4n}-1}{q^n-1}$ in (23), so we find

$$q^n \operatorname{tr}(\pi^n; A(X)) = \sum_{i=1}^{10} \omega_i^n$$

where $\omega_1, \ldots, \omega_{10}$ are the $10 = \frac{(d-1)^{n+1}+(-1)^{n+1}(d-1)}{d}$ roots of $P(t)$ as in (24). From the discussion of §3.2 we know that $\operatorname{tr}(\pi^n; A(X)) = \sum_{i=1}^{2g} \eta_i^n$ where $g = \dim A(X)$ and η_i are the roots of the characteristic polynomial of π as an endomorphism of $A(X)$. Furthermore, Lemma 5 of [1] states $\dim X = 5$, so that we have

$$\sum_{i=1}^{10} (q\eta_i)^n = \sum_{i=1}^{10} \omega_i^n$$

for sufficiently large n. But sufficiently large n is enough to prove this equation for all n, so we conclude that the roots ω_i of $P(t)$ are equal to $q\eta_i$, and thus (23) holds for all n, as desired.

Acknowledgement

I would like to thank Professor Hansen for his excellent mentorship during my time working on this thesis.

References

[1] E. Bombieri and H. P. F. Swinnerton-Dyer. On the local zeta function of a cubic threefold. *Ann. Scuola Norm. Sup. Pisa (3)*, 21:1–29, 1967.

[2] J. A. Dieudonné. On the history of the weil conjectures. *The Mathematical Intelligencer*, 10, 1975. Reprinted in *Étale cohomology and the Weil conjecture*, volume 13 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)* Springer-Verlag, Berlin, 1988.

[3] Bernard Dwork. On the zeta function of a hypersurface. *Inst. Hautes Études Sci. Publ. Math.*, (12):5–68, 1962.

[4] Serge Lang. *Abelian varieties*. Interscience Tracts in Pure and Applied Mathematics. No. 7. Interscience Publishers, Inc., New York; Interscience Publishers Ltd., London, 1959.

[5] James S. Milne. Abelian varieties (v2.00), 2008.

[6] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970.

[7] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.