Weil stuff

January 18, 2017

Contents

1 Introduction

These notes are a work in progress, based on a student seminar series at Stanford. The eventual goal is to understand the proof of Deligne's Weil II, as well as the theory of trace functions, without learning French.

2 Hasse bound for elliptic curves

2.1 Manin's elementary proof for characteristic not equal to 2 or 3

The exposition here follows Chahal's paper [2] extremely closely.

Theorem 1 (Hasse bound)**.** *Let $q = p^m$, p a prime other than 2, and let $a, b \in \mathbb{F}_q$ be such that $\Delta = 4a^3 + 27b^2 \neq 0$. Let*

$$N_q = \#\{(x, y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + ax + b\}$$

(note that this does not *count the point at infinity). Then*

$$|N_q - q| \leq 2\sqrt{q}.$$

Proof. We work in the function field $\mathbb{F}_q(t)$. Set $\lambda = \lambda(t) = t^3 + at + b$ throughout, and define the *twisted* curve E_λ by

$$\lambda y^2 = x^3 + ax + b.$$

The addition formulae for two points P_1, P_2 on E_λ are given by

$$x(P_1 + P_2) = \lambda\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - (x_1 + x_2)$$

if $P_1 \neq P_2$, or

$$x(2P) = \frac{(3x^2 + a)^2}{4(x^3 + ax + b)} - 2x$$

if $P_1 = P_2 = P$.

We now define a sequence of points P_n on E_λ for $n \in \mathbb{Z}$ by

$$P_n = (t^q, (t^3 + at + b)^{\frac{q-1}{2}}) + n \cdot (t, 1)$$

(that P_0 is on E_λ follows from well-known properties of Frobenius). Setting $(x_n, y_n) = P_n$ and writing $x_n = \frac{f_n}{g_n}$ with f_n, g_n relatively prime elements of $\mathbb{F}_q[t]$ whenever P_n is not the zero element of the curve E_λ (which we will denote O), we define a sequence d_n by

$$d_n = \begin{cases} \deg f_n & P_n \neq O, \\ 0 & P_n = O. \end{cases}$$

By the definition of P_0, we clearly have $d_0 = q$.

Claim: $d_{-1} = N_q + 1$. To see this, note that by the addition formula we have

$$x_{-1} = (t^3 + at + b)\left(\frac{(t^3 + at + b)^{\frac{q-1}{2}} + 1}{t^q - t}\right)^2 - (t^q + t) = \frac{t^{2q+1} + O(t^{2q})}{(t^q - t)^2}.$$

Thus, to compute the degree of f_{-1} we just need to know how many factors of the denominator cancel with factors of the numerator in the fraction

$$\frac{(t^3 + at + b)((t^3 + at + b)^{\frac{q-1}{2}} + 1)^2}{(t^q - t)^2}.$$

The denominator factors as $\prod_{\alpha \in \mathbb{F}_q}(t - \alpha)^2$, and $t - \alpha$ divides the numerator once if $\alpha^3 + a\alpha + b = 0$, and twice if $(\frac{\alpha^3 + a\alpha + b}{q}) = -1$ (here $(\frac{\alpha}{q})$ is the quadratic residue symbol for $\mathbb{F}_q$). Thus,

$$d_{-1} = 2q + 1 - \sum_{\alpha \in \mathbb{F}_q} \left(1 - (\tfrac{\alpha^3 + a\alpha + b}{q})\right) = N_q + 1.$$

Lemma: If $P_n \neq O$, then $x_n \neq 0$ and $\deg f_n > \deg g_n$.

Basic Identity: $d_{n-1} + d_{n+1} = 2d_n + 2$.

Proof of the Hasse bound given these: From the Basic Identity, we easily see that

$$d_n = n^2 - (d_{-1} - d_0 - 1)n + d_0 = n^2 - (N_q - q)n + q.$$

Let r_0, r_1 be the roots of the quadratic $n \mapsto n^2-(N_q-q)n+q$. We have $(r_0-r_1)^2 = (N_q-q)^2-4q \in \mathbb{Z}$, so if r_0, r_1 were real and distinct then their difference would be at least 1, so there would then necessarily be some n such that either $d_n < 0$ or $d_n = 0 = d_{n+1}$. Either one of these possibilities contradicts the Lemma, so we must have $(r_0 - r_1)^2 \leq 0$, or equivalently,

$$|N_q - q| \leq 2\sqrt{q}.$$

Proof of Lemma: The plan is to formally evaluate x_n, y_n at $t = \infty$ (equivalently, we are looking at the ratio of the leading term of the numerator and the leading term of the denominator), and to induct on $|n|$. Note that from $y_n^2 = \frac{x_n^3+ax_n+b}{t^3+at+b}$, we see that if $x_n|_\infty \neq \infty$ then $y_n|_\infty = 0$.

Assume that the Lemma holds for n but fails for $n+1$ (the reverse case, for $n < 0$, is handled similarly). Since

$$(x_{n+1}, -y_{n+1}) + (x_n, y_n) + (t, 1) = O,$$

the three summands on the left hand side are collinear, so

$$1 - (-y_{n+1}) = \frac{1 - y_n}{t - x_n}(t - x_{n+1}),$$

so from the assumption $\frac{x_{n+1}}{t}|_\infty = 0$, we get

$$0 = y_{n+1}|_\infty = \left(\frac{1 - y_n}{1 - \frac{x_n}{t}} \Big(1 - \frac{x_{n+1}}{t} \Big) - 1 \right) \Big|_\infty,$$

and thus

$$\frac{1 - y_n}{1 - \frac{x_n}{t}} \Big|_\infty = 1.$$

From

$$x_{n+1} = \lambda \left(\frac{1 - y_n}{t - x_n} \right)^2 - t - x_n,$$

we get

$$0 = \frac{x_{n+1}}{t} \Big|_\infty = \left(\Big(\frac{1 - y_n}{1 - \frac{x_n}{t}} \Big)^2 \Big(1 + \frac{a}{t^2} + \frac{b}{t^3} \Big) - 1 - \frac{x_n}{t} \right) \Big|_\infty = -\frac{x_n}{t} \Big|_\infty \neq 0,$$

a contradiction.

Proof of the Basic Identity: If $P_n = O$, then this is trivial. If $P_{n-1} = O$, then

$$x_{n+1} = x(2 \cdot (t,1)) = \frac{(3t^2+a)^2}{4(t^3+at+b)} - 2t = \frac{t^4 + O(t^3)}{4(t^3+at+b)},$$

and since $\Delta \neq 0$ we know that $3t^2 + a$ has no common factor with $t^3 + at + b$, so $d_{n+1} = 4$, and the identity holds in this case (as we trivially have $d_{n-1} = 0, d_n = 1$). The case $P_{n+1} = O$ is identical, so we may assume from here on that none of P_{n-1}, P_n, P_{n+1} are O.

Computing x_{n-1}, we have

$$\begin{aligned} x_{n-1} &= \lambda\Big(\frac{y_n+1}{x_n-t}\Big)^2 - (x_n+t) = \frac{\lambda(y_n+1)^2 - (x_n+t)(x_n-t)^2}{(x_n-t)^2} \\ &= \frac{x_n^3 + ax_n + b + t^3 + at + b - (x_n+t)(x_n-t)^2 + 2\lambda y_n}{(x_n-t)^2} \\ &= \frac{(x_n+t)(tx_n+a) + 2b + 2\lambda y_n}{(x_n-t)^2} \\ &= \frac{(f_n+tg_n)(tf_n+ag_n) + 2bg_n^2 + 2\lambda y_n g_n^2}{(f_n-tg_n)^2} =: \frac{R}{(f_n-tg_n)^2}, \end{aligned}$$

say. From

$$(\lambda y_n g_n^2)^2 = \lambda g_n^4(x_n^3 + ax_n + b) = \lambda g_n(f_n^3 + af_n g_n^2 + bg_n^3) \in \mathbb{F}_q[t],$$

we get $\lambda y_n g_n^2 \in \mathbb{F}_q[t]$ (by the rational root theorem), so $R \in \mathbb{F}_q[t]$. A similar calculation gives $x_{n+1} = \frac{S}{(f_n-tg_n)^2}$, where

$$S = (f_n+tg_n)(tf_n+ag_n) + 2bg_n^2 - 2\lambda y_n g_n^2.$$

Since x_{n-1} and x_{n+1} differ only in the sign of $2\lambda y_n$, we can apply the difference of squares formula to see

$$\begin{aligned} x_{n-1}x_{n+1} &= \frac{((x_n+t)(tx_n+a)+2b)^2 - 4(t^3+at+b)(x^3+ax+b)}{(x_n-t)^4} \\ &= \frac{((x^3+ax+t^3+at-(x_n+t)(x_n-t)^2)+2b)^2 - 4(t^3+at+b)(x^3+ax+b)}{(x_n-t)^4} \\ &= \frac{((x_n+t)(tx_n+a))^2 - (2t^2x_n+2ax_n)(2tx_n^2+2at) - 4b(x_n+t)(x_n-t)^2}{(x_n-t)^4} \\ &= \frac{(tx_n-a)^2 - 4b(x_n+t)}{(x_n-t)^2} \\ &= \frac{(tf_n-ag_n)^2 - 4bg_n(f_n+tg_n)}{(f_n-tg_n)^2} =: \frac{T}{(f_n-tg_n)^2} \\ &= \frac{t^2f_n^2 + O(tf_n^2)}{(f_n-tg_n)^2}. \end{aligned}$$

Noting that T has degree $2d_n + 2$ (by the last line, which implicitly used the Lemma), we just have to show that no extra cancellation occurs. Since $RS = (f_n - tg_n)^2 T$, there must exist $r, s \in \mathbb{F}_q[t]$ such that $r \mid R, s \mid S$, and $rs = (f_n - tg_n)^2$. Thus we have

$$\frac{f_{n-1}}{g_{n-1}} = \frac{R}{(f_n-tg_n)^2} = \frac{R/r}{s},$$

and similarly $\frac{f_{n+1}}{g_{n+1}} = \frac{S/s}{r}$, and of course $(R/r)(S/s) = T$. Thus we just have to show that R/r and s have no common factor, and that S/s and r have no common factor. If not, then (in either case) any irreducible common factor must divide R, S, T, and $f_n - tg_n$, so it divides

$$\begin{aligned}
\gcd(f_n - tg_n, R, S, T) &= \gcd(f_n - tg_n, 2\lambda(1+y_n)g_n^2, 2\lambda(1-y_n)g_n^2, ((t^2-a)^2 - 8bt)g_n) \\
&\mid \gcd(2\lambda(1+y_n), 2\lambda(1-y_n), (t^2-a)^2 - 8bt)\gcd(f_n - tg_n, g_n)^2 \\
&= \gcd(t^3 + at + b, t^4 - 2at^2 - 8bt + a^2) \\
&= \gcd(t^3 + at + b, 9t^4 + 6at^2 + a^2) \\
&= \gcd(t^3 + at + b, (3t^2 + a)^2) = 1,
\end{aligned}$$

(since $\Delta \neq 0$), which is a contradiction. □

What's really going on in this proof: In a follow up paper by Chahal [3], the following high level explanation of Manin's argument is given, and used to derive a similar elementary proof in characteristic 2.

Suppose we are given an elliptic curve E over a field k. By taking a quotient of the first projection map $\pi_1 : E \times E \to E$, we get a map $E \times E/(-1,-1) \to E/(-1) \cong \mathbb{P}^1$. Taking the generic fiber of this map gives $E^{\mathrm{tw}} \to \operatorname{Spec} k(t)$, where E^{tw} is a twist of E which trivializes over the degree 2 extension $k(E)/k(t)$. Thus

$$E^{\mathrm{tw}}(k(E)) \cong E(k(E)) \cong \mathrm{Mor}_k(E, E),$$

and

$$E^{\mathrm{tw}}(k(t)) \cong \{\phi \in \mathrm{Mor}_k(E, E) \mid \phi \circ (-1) = (-1) \circ \phi\}.$$

Thus the maps 1 and Frob (as well as all the other isogenies of E) correspond to $k(t)$ points on E^{tw}, and the degree of an isogeny should correspond to a naïve height of the corresponding point on E^{tw}.

2.2 Aside: binomial coefficients, Jacobi sums, and trinomial plane curves

2.2.1 Chevalley-Warning trick

How many mod-p points are there on the curve $x^m + y^n = k$? We can compute the number of points on this curve mod p by following the proof of Chevalley-Warning and seeing how badly it fails:

$$\begin{aligned}\#\{(x,y)\in\mathbb{F}_p^2 \mid x^m+y^n=k\} &\equiv \sum_{x,y\in\mathbb{F}_p} 1-(x^m+y^n-k)^{p-1}\\ &\equiv -\sum_{x,y\in\mathbb{F}_p}\sum_{a+b+c=p-1}\binom{p-1}{a,b,c}x^{am}y^{bn}(-k)^c\\ &\equiv -\sum_{a+b+c=p-1}k^c\binom{p-1-c}{a}\sum_{x,y\in\mathbb{F}_p}x^{am}y^{bn}\\ &\equiv -\sum_{\substack{a+b+c=p-1\\ a,b>0\\ p-1\mid am,bn}}k^c\binom{p-1-c}{a} \pmod p.\end{aligned}$$

Note that the number of summands depends only on m and n, and the number of summands which are not trivially congruent to ± 1 is

$$\frac{(m-1)(n-1)-(\gcd(m,n)-1)}{2},$$

which is precisely the geometric genus of the plane curve $x^m+y^n=k$ (as one can easily check with the Riemann-Hurwitz formula). A similar calculation applies to any plane curve defined by an equation involving three monomials whose exponent vectors are affinely independent.

Example 1. Applying this to the genus 1 curve $y^2=x^3+k$, we see that when $p\equiv 1 \pmod 6$ we have

$$\begin{aligned}\#\{(x,y)\in\mathbb{F}_p^2 \mid y^2=x^3+k\} &\equiv -k^{\frac{p-1}{6}}\binom{\frac{5(p-1)}{6}}{\frac{p-1}{3}}\\ &\equiv p-k^{\frac{p-1}{6}}\binom{\frac{p-1}{2}}{\frac{p-1}{3}} \pmod p.\end{aligned}$$

Suppose $p>16$, so that $p>4\sqrt{p}$. Letting w be a solution to $w^2+w+1\equiv 0 \pmod p$, and letting a be the least (in absolute value) remainder of $\binom{\frac{p-1}{2}}{\frac{p-1}{3}} \bmod p$ and b be the least (in absolute value) remainder of $w\binom{\frac{p-1}{2}}{\frac{p-1}{3}} \bmod p$, we see from the Hasse bound that $|a|,|b|,|a+b|<2\sqrt{p}$. From this we easily conclude that

$$p\mid a^2+ab+b^2=\frac{a^2+b^2+(a+b)^2}{2}<4p,$$

so a^2+ab+b^2 is either p, $2p$, or $3p$. Since the number of points on the curve $y^2=x^3+k$ is congruent to 2 modulo 3 whenever k is a quadratic residue mod p, we see that both a and b are congruent to 2 modulo 3, so we must have $a^2+ab+b^2=3p$. Similarly, since the number of points on $y^2=x^3+k$ is odd exactly when k is a cubic residue mod p, we see that a is even and b is odd. Thus, setting $A=\frac{a}{2}$ and $B=\frac{a+2b}{6}$, we have $A,B\in\mathbb{Z}$,

$$A^2+3B^2=p, \quad A\equiv 1 \pmod 3,$$

and

$$\binom{\frac{p-1}{2}}{\frac{p-1}{3}} \equiv 2A \pmod{p}.$$

Example 2. Similar reasoning applied to the curve $y^2 = x^4 + k$ (or alternatively to the curve $y^2 = x^3 - kx$) shows that if $p \equiv 1 \pmod 4$ then there are integers a, b such that

$$a^2 + b^2 = p, \quad a \equiv 1 \pmod 4,$$

and

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod{p}.$$

Remark 1. Trying the same approach with the elliptic curve $y^2 = x^3 + x + k$, we get

$$\#\{(x,y) \in \mathbb{F}_p \mid y^2 = x^3 + x + k\} \equiv - \sum_{\frac{p-1}{4} \le n \le \frac{p-1}{3}} k^{2n - \frac{p-1}{2}} \binom{\frac{p-1}{2}}{n, p-1-3n, 2n-\frac{p-1}{2}} \pmod{p}.$$

Considering the right hand side as a polynomial in k, we see that it has degree at most $\frac{p-1}{6}$ and always takes values in $(-2\sqrt{p}, 2\sqrt{p}) + p\mathbb{Z}$. Out of curiosity, I tried factoring these polynomials (in $\mathbb{F}_p[k]$) for p up to 3000, and found that they always seem to split into a product of factors of degrees $1, 2$, and 4 - can anyone explain this?

2.2.2 Jacobi sums and binomial coefficients

Definition 1. Let p be a prime and let χ be any Dirichlet character modulo p. Define the *Gauss sum* $g(\chi)$ to be

$$g(\chi) = \sum_{j=0}^{p-1} \chi(j) e^{2\pi i j/p}.$$

Proposition 1. *If χ is a nontrivial Dirichlet character mod p, then $|g(\chi)| = \sqrt{p}$ and $g(\chi)g(\overline{\chi}) = \chi(-1)p$. If χ is the real quadratic character, then $g(\chi)$ is either $\sqrt{p}$ or $i\sqrt{p}$ depending on whether p is 1 or -1 modulo 4.*

Definition 2. Let p be a prime and let χ, ψ be any two Dirichlet characters modulo p. Define the *Jacobi sum* $J(\chi, \psi)$ to be

$$J(\chi, \psi) = \sum_{j=0}^{p-1} \chi(j)\psi(1-j).$$

Proposition 2. *If χ, ψ are Dirichlet characters mod p such that $\chi\psi$ is nontrivial, then*

$$J(\chi, \psi) = \frac{g(\chi)g(\psi)}{g(\chi\psi)}.$$

Let n be a positive integer, write $\zeta_n = e^{2\pi i/n}$, and let p be a prime with $p \equiv 1 \pmod n$. From the existence of primitive roots modulo p, we see that there are $\varphi(n)$ congruence classes $z \pmod p$ with $\mathrm{ord}_p(z) = n$. Picking one of these congruence classes, we can define the prime ideal $P = (p, \zeta_n - z)$ of $\mathbb{Z}[\zeta_n]$. Note that every element of $\mathbb{Z}[\zeta_n]$ is congruent to an element of $\mathbb{Z}$ modulo P, i.e. $\mathbb{Z}[\zeta_n]/P = \mathbb{Z}/p$, and that $\mathrm{Nm}(P) = p$.

Definition 3. Let P be a prime ideal of $\mathbb{Z}[\zeta_n]$ which does not divide n, and let a be any element of $\mathbb{Z}[\zeta_n]$. Define the nth *power residue symbol* of a on P by

$$\left(\frac{a}{P}\right)_n \equiv a^{\frac{\mathrm{Nm}(P)-1}{n}} \pmod{P}$$

and

$$\left(\frac{a}{P}\right)_n \in \{0, 1, \zeta_n, \zeta_n^2, ..., \zeta_n^{n-1}\}.$$

Theorem 2 (Theorem 5.1 of [6])**.** *Let n, p, P be as above, so $p \equiv 1 \pmod{n}$ and P is a prime ideal of $\mathbb{Z}[\zeta_n]$ lying over p. Let χ_n be the Dirichlet character mod p defined by $\chi_n(a) = (\frac{a}{P})_n$. Then for any $0 < k, l < n$ we have*

$$\binom{\frac{k(p-1)}{n}}{\frac{l(p-1)}{n}} \equiv (-1)^{\frac{l(p-1)}{n}+1} J(\chi_n^k, \chi_n^{n-l}) \pmod{P}.$$

Proof. From $\chi_n(a) \equiv a^{\frac{p-1}{n}} \pmod{P}$, we have

$$\begin{aligned}
J(\chi_n^{n-l}, \chi_n^k) &= \sum_{j=0}^{p-1} \chi_n(j)^{n-l} \chi_n(1-j)^k \\
&\equiv \sum_{j=0}^{p-1} j^{p-1-\frac{l(p-1)}{n}} (1-j)^{\frac{k(p-1)}{n}} \\
&= \sum_{j=0}^{p-1} j^{p-1-\frac{l(p-1)}{n}} \sum_m \binom{\frac{k(p-1)}{n}}{m} (-j)^m \\
&= \sum_m (-1)^m \binom{\frac{k(p-1)}{n}}{m} \sum_{j=0}^{p-1} j^{p-1+m-\frac{l(p-1)}{n}} \\
&\equiv -(-1)^{\frac{l(p-1)}{n}} \binom{\frac{k(p-1)}{n}}{\frac{l(p-1)}{n}} \pmod{P}.
\end{aligned}$$

□

Example 3. Take $n = 4$, and let p be a prime which is 1 (mod 4). Writing $p = a^2 + b^2$ with $a \equiv 1 \pmod{4}$, let $P = (a + bi)$. Define the Dirichlet character χ_4 by $\chi_4(k) = (\frac{k}{a+bi})_4$, and let $\chi_2 = \chi_4^2$ be the quadratic character mod p. Then

$$J(\chi_2, \chi_4) \equiv -\binom{\frac{p-1}{4}}{\frac{p-1}{2}} = 0 \pmod{P}$$

and

$$\overline{J(\chi_2, \chi_4)} = J(\chi_2, \chi_4^3) \equiv (-1)^{\frac{p-1}{4}+1} \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod{P},$$

so

$$\mathrm{Tr}(J(\chi_2, \chi_4)) \equiv (-1)^{\frac{p-1}{4}+1} \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod{p}.$$

From $|J(\chi_2,\chi_4)| = \sqrt{p}$ and $(a+bi) \mid J(\chi_2,\chi_4)$, we see that $J(\chi_2,\chi_4) = i^k(a+bi)$ for some k. By computing $J(\chi_2,\chi_4)$ modulo 4, one can show that in fact we have

$$J(\chi_2,\chi_4) = (-1)^{\frac{p-1}{4}+1}(a+bi),$$

giving us a second proof of the congruence

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod{p}.$$

3 Weil's argument for diagonal hypersurfaces

This section follows Weil's paper [8]. Let q be a power of a prime p. Let $a_0, ..., a_r \in \mathbb{F}_q^\times$ and let $n_0, ..., n_r \in \mathbb{N}^+$. We want to count

$$N = \#\{(x_0, ..., x_r) \in \mathbb{F}_q^{r+1} \mid a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0\}.$$

Set $d_i = \gcd(n_i, q-1)$.

The plan is to use Fourier analysis, so the first step is to pick additive and multiplicative characters.

Definition 4. Define $\psi_q : \mathbb{F}_q \to \mathbb{C}^\times$ by

$$\psi_q(a) = e^{\frac{2\pi i \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}{p}}.$$

Proposition 3. *The character ψ_q is not identically equal to 1, and every additive character of $\mathbb{F}_q$ can be written as $a \mapsto \psi_q(ca)$ for some $c \in \mathbb{F}_q$.*

Proof. This follows immediately from Artin's theorem on the linear independence of characters. □

Definition 5. Fix once and for all an injective multiplicative map $\phi : \overline{\mathbb{F}}_q^\times \to \mathbb{C}^\times$. For $\alpha \in \mathbb{Q}/\mathbb{Z}$ and $n \in \mathbb{N}$ such that $(q^n-1)\alpha \equiv 0 \pmod 1$, define $\chi_{\alpha,n} : \mathbb{F}_{q^n}^\times \to \mathbb{C}^\times$ by

$$\chi_{\alpha,n}(x) = \phi(x)^{(q^n-1)\alpha}.$$

Extend this to $\mathbb{F}_{q^n}$ by

$$\chi_{\alpha,n}(0) = \begin{cases} 0 & \alpha \not\equiv 0 \pmod 1, \\ 1 & \alpha \equiv 0 \pmod 1, \end{cases}$$

and set $\chi_\alpha = \chi_{\alpha,1}$.

Proposition 4. *If $(q-1)\alpha \equiv 0 \pmod 1$, then $\chi_{\alpha,n}(x) = \chi_\alpha(\operatorname{Nm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$.*

Proof.

$$\chi_{\alpha,n}(x) = \phi(x)^{(q^n-1)\alpha} = (\phi(x)^{(q-1)\alpha})^{q^{n-1}+\cdots+1} = \chi_\alpha(x^{q^{n-1}+\cdots+1}) = \chi_\alpha(\operatorname{Nm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)). \qquad \square$$

Proposition 5. *If $d = \gcd(n, q-1)$ and $u \in \mathbb{F}_q$ then number of $x \in \mathbb{F}_q$ such that $x^n = u$ is $\sum_{d\alpha \equiv 0 \pmod 1} \chi_\alpha(u)$.*

From this we see that

$$\begin{aligned} N &= \sum_{\substack{\alpha=(\alpha_0,\dots,\alpha_r)\\ d_i\alpha_i\equiv 0 \pmod 1}} \sum_{\substack{u=(u_0,\dots,u_r)\\ \sum a_iu_i=0}} \chi_{\alpha_0}(u_0)\cdots\chi_{\alpha_r}(u_r) \\ &= q^r + \sum_{\substack{\alpha=(\alpha_0,\dots,\alpha_r)\\ 0<\alpha_i<1\\ d_i\alpha_i\equiv 0 \pmod 1}} \chi_{\alpha_0}(a_0^{-1})\cdots\chi_{\alpha_r}(a_r^{-1}) \sum_{u_0+\cdots+u_r=0} \chi_{\alpha_0}(u_0)\cdots\chi_{\alpha_r}(u_r), \end{aligned}$$

where the second equality follows from the fact that the inner sum is 0 if some but not all of the α_i are 0 (mod 1). For $0 < \alpha_0 < 1$, we can simplify the inner sum further by restricting to $u_0 \neq 0$ and setting $u_i = u_0v_i$:

$$\begin{aligned} \sum_{u_0+\cdots+u_r} \chi_{\alpha_0}(u_0)\cdots\chi_{\alpha_r}(u_r) &= \sum_{u_0\neq 0} \chi_{\alpha_0+\cdots+\alpha_r}(u_0) \sum_{1+v_1+\cdots+v_r=0} \chi_{\alpha_1}(v_1)\cdots\chi_{\alpha_r}(v_r) \\ &= \begin{cases} 0 & \alpha_0+\cdots+\alpha_r \not\equiv 0 \pmod 1, \\ (q-1)\sum_{1+v_1+\cdots+v_r=0} \chi_{\alpha_1}(v_1)\cdots\chi_{\alpha_r}(v_r) & \alpha_0+\cdots+\alpha_r \equiv 0 \pmod 1. \end{cases} \end{aligned}$$

Definition 6. For $\alpha = (\alpha_0, ..., \alpha_r)$ with $\alpha_0 + \cdots + \alpha_r \equiv 0 \pmod 1$, define the *Jacobi sum* $j(\alpha)$ by

$$\begin{aligned} j(\alpha) &= \frac{1}{q-1} \sum_{u_0+\cdots+u_r} \chi_{\alpha_0}(u_0)\cdots\chi_{\alpha_r}(u_r) \\ &= \sum_{1+v_1+\cdots+v_r=0} \chi_{\alpha_1}(v_1)\cdots\chi_{\alpha_r}(v_r). \end{aligned}$$

In terms of the Jacobi sums, we have

$$N = q^r + (q-1) \sum_{\substack{\alpha_0+\cdots+\alpha_i\equiv 0 \pmod 1\\ d_i\alpha_i\equiv 0 \pmod 1\\ 0<\alpha_i<1}} \chi_{\alpha_0}(a_0^{-1})\cdots\chi_{\alpha_r}(a_r^{-1}) j(\alpha).$$

Note that the number of summands is bounded by a constant which depends only on r and $d_0, ..., d_r$. In order to evaluate the Jacobi sums, we will use Gauss sums.

Definition 7. If $\chi : \mathbb{F}_q \to \mathbb{C}$ is a multiplicative character, then the *Gauss sum* $g(\chi)$ is

$$g(\chi) = \sum_{x\in\mathbb{F}_q} \chi(x)\psi_q(x).$$

Proposition 6. *If $\chi \neq \chi_0$ then $|g(\chi)| = \sqrt{q}$, $g(\chi)g(\overline{\chi}) = \chi(-1)q$, and $g(\chi_0) = 0$. For $\chi \neq \chi_0$, we have*

$$\chi(t) = \frac{g(\chi)}{q} \sum_{x\in\mathbb{F}_q} \overline{\chi}(x)\overline{\psi}_q(tx).$$

Proof. The first statement is easy. For the second, note that for any $t \neq 0$ we have

$$\frac{q}{g(\chi)} = \overline{g}(\chi) = \overline{\chi}(t) \sum_{x\in\mathbb{F}_q} \overline{\chi}(x)\overline{\psi}_q(tx). \qquad \square$$

Proposition 7. *If $\alpha = (\alpha_0, ..., \alpha_r)$ with $\alpha_0 + \cdots + \alpha_r \equiv 0 \pmod 1$, then*

$$j(\alpha) = \frac{g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r})}{q}$$

and $|j(\alpha)| = q^{\frac{r-1}{2}}$.

Proof. Expanding out each $\chi_{\alpha_i}(u_i)$ in the definition of $j(\alpha)$, we get

$$(q-1)j(\alpha) = \frac{g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r})}{q^{r+1}} \sum_{x_0,\ldots,x_r} \overline{\chi}_{\alpha_0}(x_0) \cdots \overline{\chi}_{\alpha_r}(x_r) \sum_{u_0+\cdots+u_r=0} \overline{\psi}_q(x_0u_0 + \cdots + x_ru_r),$$

and the inner sum is 0 unless $x_0 = \cdots = x_r$, in which case it is q^r. □

Next we want to understand how N changes when we replace $\mathbb{F}_q$ with $\mathbb{F}_{q^\nu}$. The main difficulty is understanding what happens to Gauss sums.

Theorem 3 (Davenport, Hasse)**.** *If $(q-1)\alpha \equiv 0 \pmod 1$, then $-g(\chi_{\alpha,\nu}) = (-g(\chi_\alpha))^\nu$.*

Proof. For $F(x) = x^n + c_1x^{n-1} + \cdots + c_n \in \mathbb{F}_q[x]$ monic, set

$$\lambda_\alpha(F) = \chi_\alpha(c_n)\psi_q(c_1).$$

Note that $\lambda_\alpha(F_1F_2) = \lambda_\alpha(F_1)\lambda_\alpha(F_2)$, so by unique factorization for polynomials in $\mathbb{F}_q[x]$ we have

$$\sum_{F \in \mathbb{F}_q[x] \text{ monic}} \lambda_\alpha(F)T^{\deg F} = \prod_{P \in \mathbb{F}_q[x] \text{ irred.}} (1 - \lambda_\alpha(P)T^{\deg P})^{-1},$$

and the left hand side is easily seen to be equal to $1 + g(\chi_\alpha)T$. Defining $\lambda_{\alpha,\nu}$ for functions in $\mathbb{F}_{q^\nu}[x]$ similarly, we have

$$1 + g(\chi_{\alpha,\nu})T = \prod_{P' \in \mathbb{F}_{q^\nu}[x] \text{ irred.}} (1 - \lambda_{\alpha,\nu}(P')T^{\deg P'})^{-1}.$$

Suppose that $P(x) = x^n + bx^{n-1} + \cdots + a$ is irreducible in $\mathbb{F}_q[x]$ and $P'(x) = x^{n'} + b'x^{n'-1} + \cdots + a'$ is an irreducible factor of $P(x)$ in $\mathbb{F}_{q^\nu}[x]$. Then by Galois theory we have $n' = \frac{n}{(n,\nu)}$ and

$$\begin{aligned}
\lambda_{\alpha,\nu}(P') &= \chi_{\alpha,\nu}(a')\psi_{q^\nu}(b') \\
&= \chi_\alpha(\mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(a'))\psi_q(\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(b')) \\
&= \chi_\alpha\big(a^{\frac{\nu}{(n,\nu)}}\big)\psi_q\big(\tfrac{\nu}{(n,\nu)}b\big) \\
&= \lambda_\alpha(P)^{\frac{\nu}{(n,\nu)}}.
\end{aligned}$$

Thus we have

$$\begin{aligned}
\prod_{P'|P} (1 - \lambda_{\alpha,\nu}(P')T^{\nu \deg P'})^{-1} &= (1 - \lambda_\alpha(P)T^{\frac{n\nu}{(n,\nu)}})^{-(n,\nu)} \\
&= \prod_{a=0}^{\nu-1} (1 - \lambda_\alpha(P)(e^{\frac{2\pi i a}{\nu}}T)^n)^{-1},
\end{aligned}$$

so

$$\begin{aligned}1+g(\chi_{\alpha,\nu})T^\nu &= \prod_{a=0}^{\nu-1}\prod_{P\in\mathbb{F}_q[x]\text{ irred.}}(1-\lambda_\alpha(P)(e^{\frac{2\pi ia}{\nu}}T)^{\deg P})^{-1}\\ &= \prod_{a=0}^{\nu-1}(1+g(\chi_\alpha)e^{\frac{2\pi ia}{\nu}}T)\\ &= 1-(-g(\chi_\alpha))^\nu T^\nu.\end{aligned}$$

□

Now we restrict to the special case $n_0=\cdots=n_r=n$, and set

$$\overline{N}_\nu = \#\{[x_0:\cdots:x_r]\in\mathbb{P}^r_{\mathbb{F}_{q^\nu}} \mid a_0x_0^n+\cdots+a_rx_r^n=0\}.$$

From the formula we derived for N, we have

$$\overline{N}_\nu = \frac{N_\nu}{q^\nu-1} = q^{(r-1)\nu}+\cdots+q^\nu+1+\sum_{\substack{\alpha_0+\cdots+\alpha_r\equiv 0 \pmod 1\\ (n,q^\nu-1)\alpha_i\equiv 0 \pmod 1\\ 0<\alpha_i<1}}\overline{\chi}_{\alpha_0,\nu}(a_0)\cdots\overline{\chi}_{\alpha_r,\nu}(a_r)j_\nu(\alpha).$$

We want to compute the generating function $\exp(\sum_{\nu\geq 1}\overline{N}_\nu\frac{T^\nu}{\nu})$ (this is the zeta function of the diagonal hypersurface in $\mathbb{P}^r$ given by $a_0x_0^n+\cdots+a_rx_r^n=0$). Setting

$$\mu(\alpha)=\min\{\mu\mid(q^\mu-1)\alpha\equiv\vec{0}\pmod 1\},$$

we have

$$\exp\left(\sum_{\nu\geq 1}\overline{N}_\nu\frac{T^\nu}{\nu}\right)=\frac{1}{(1-T)(1-qT)\cdots(1-q^{r-1}T)}\prod_{\substack{\alpha_0+\cdots+\alpha_r\equiv 0 \pmod 1\\ (n,q^\nu-1)\alpha_i\equiv 0 \pmod 1\\ 0<\alpha_i<1}}(1-C(\alpha)T^{\mu(\alpha)})^{\frac{(-1)^r}{\mu(\alpha)}},$$

where

$$C(\alpha)=(-1)^{r+1}\overline{\chi}_{\alpha_0,\mu(\alpha)}(a_0)\cdots\overline{\chi}_{\alpha_r,\mu(\alpha)}(a_r)j_{\mu(\alpha)}(\alpha),$$

and $|C(\alpha)|=q^{\frac{(r-1)\mu(\alpha)}{2}}$. Furthermore, we have $C(q\alpha)=C(\alpha)$ since $a_i^q=a_i$, $\mu(q\alpha)=\mu(\alpha)$, and $j_{\mu(\alpha)}(q\alpha)=j_{\mu(\alpha)}(\alpha)$, so by grouping the terms in the product corresponding to $\alpha,q\alpha,...,q^{\mu(\alpha)-1}\alpha$ we see that in fact the zeta function of our diagonal hypersurface is a rational function of T.

Furthermore, either the last product or its inverse is a polynomial with integer coefficients (since $j(\alpha)$, being a sum of roots of unity, is always an algebraic integer), and the degree of this polynomial is the number of tuples $(\alpha_0,...,\alpha_r)$ such that $0<\alpha_i<1$ for all i, each α_i has denominator dividing n and coprime to p, and $\alpha_0+\cdots+\alpha_r\equiv 0 \pmod 1$. Since α_0 is determined by $\alpha_1,...,\alpha_r$, we see that the number of such tuples is

$$(n-1)^r-((n-1)^{r-1}-\cdots)=\frac{(n-1)((n-1)^r-(-1)^r)}{n}$$

if n is relatively prime to p.

4 Ho Chung's notes on rationality of the zeta function for curves

4.1 Introduction

So one goal of the seminar is to perhaps give bounds of sum of trace functions on a variety.

4.1.1 Some examples of what we care about

Example 4 (Gauss sum for Dirichlet characters mod p). We want to understand the size of

$$\tau(\chi) = \sum_{a \in \mathbb{A}^1(\mathbb{F}_p)} \chi(a) e\left(\frac{a}{p}\right)$$

for a non-trivial multiplicative character $\chi : \mathbb{F}_p^* \to \mathbb{C}$, extending to domain $\mathbb{F}_p$ by zero.

This is a classical Gauss sum, where it is known that $|g(\chi)| = \sqrt{p}$.

Example 5 (Kloosterman sums). We want to understand the size of

$$S(a, b; p) = \sum_{x \in (\mathbb{A}^1 - 0)(\mathbb{F}_p)} e\left(\frac{ax + b\overline{x}}{p}\right)$$

for $a, b \in \mathbb{F}_p^*$. Here $\overline{x}$ means multiplicative inverse of $x \mod p$.

Here Weil bound says that

$$|S(a, b; p)| \leq 2\sqrt{p}$$

so we do attain square-root cancellation.

Example 6 (Hasse-Weil). We want to understand the size of

$$|\#E(\mathbb{F}_p) - p - 1|$$

for an elliptic curve $E : y^2 = f(x)$ with $f(x) = x^3 + ax + b$ over $\mathbb{F}_p$.

Note that the number of solutions of $x^2 \equiv a \mod p$ equals $1 + \left(\frac{a}{p}\right)$. Thus, after first subtracting off the point at infinity,

$$|\#E(\mathbb{F}_p) - p - 1| = \left| \sum_{x \in \mathbb{A}^1(\mathbb{F}_p)} \left(1 + \left(\frac{x^3 + ax + b}{p}\right) - p\right) \right| = \left| \sum_{x \in \mathbb{A}^1(\mathbb{F}_p)} \left(\frac{x^3 + ax + b}{p}\right) \right|$$

Here Hasse-Weil bound says that

$$|\#E(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}$$

It can be considered a square-root cancellation type result for the functions $\chi(f(x))$ where χ is the Legendre symbol/non-trivial quadratic character for $\mathbb{F}_p^*$.

4.1.2 The general setup

The most general set up here would be

- Let $k = \mathbb{F}_q$ be a finite field Consider any separated scheme X/k of finite type, any constructible $\mathbb{Q}_l$-sheaf $\mathcal{F}$ on X, any finite extension E/k. For any $x \in X(E)$, denote

$$\mathrm{Frob}_{E,x}(\mathcal{F})$$

  the action of geometric Frobenius $\mathrm{Frob}_E \in \mathrm{Gal}(\overline{E}/E)$ on the pullback $\mathcal{F}$ to $\mathrm{Spec}(E)$ by the point $x \in X(E)$ viewed as a map $\mathrm{Spec}(E) \to X$. Write

$$t_{\mathcal{F}}(E, x) = \mathrm{Tr}(\mathrm{Frob}_{E,x} \,|\mathcal{F})$$

  In other words, $t_{\mathcal{F}}(E, x)$ is the trace of Frob_E action on the stalk $\mathcal{F}_x$. A simplified but good enough case would be X/k is quasi-projective, $\mathcal{F}$ is locally constant (synonym: lisse) sheaf on X.

- We have a version of Lefschetz trace formula here:

$$\sum_{x \in X(E)} t_{\mathcal{F}}(E, x) = \sum_i (-1)^i \,\mathrm{Tr}\left(\mathrm{Frob}_E \,|H^i_c(X \otimes_k \overline{k}, \mathcal{F}\right)$$

- Deligne's work (seems to be mainly Weil II, Theorem 3.3.1) buys us something of the sort
  - There are generally hard Lefschetz type result on cohomology; and in special cases concentration of cohomology results, that roughly says most of the cohomology groups (say, all but the middle one) vanish.
  - The dimension of the nonvanishing cohomology group can be written down.
  - Purity result - The cohomology groups are mixed with some weight in general; pure with some weight in nice cases. A cohomology group being pure of weight n means that all eigenvalues of Frob_k acting on this cohomology has complex absolute value $|k|^{n/2}$, once you fixed the isomorphism between $\overline{\mathbb{Q}_l} \cong \mathbb{C}$.

  Triangle inequality then gives us square cancellation we look for.

- Fouvry, Kowalski, Michel et al's work seems to focus on the case X being a dense open subset of $\mathbb{P}^1$, and $E = k$ so far.

What is the most general setup here; how to unify the multiplicative characters and the additive

What is constructible sheaf, local system,...

4.2 Zeta function for varieties over $\mathbb{F}_q$

It does not hurt to replace all the "scheme of finite type" below with "quasi-projective variety"

Execution of this plan for the three examples

Extremely sketchy END

4.2.1 Two definitions of zeta function

Lemma 1. *Let X be a scheme of finite type over $\mathbb{F}_q$. Then*

$$\#X(\mathbb{F}_{q^n}) \leq O\left(q^{n\cdot \dim X}\right) \text{ as } n \to \infty$$

Proof. Without loss of generality, assume that X is affine and integral. Then the result follows from Noether normalization. □

Definition 8 (Local zeta function)**.** Let X be a scheme of finite type over $\mathbb{F}_q$. Define the local zeta function to be

$$Z\left(X/\mathbb{F}_q, T\right) = \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n})\frac{T^n}{n}\right) \in \mathbb{Q}[\![T]\!]$$

Say a word on what $X(\mathbb{F}_{q^n})$ is, closed point etc for analytic number theorist in audience

Remark 2. The previous lemma implies that $Z(X, q^{-s})$ converges to a holomorphic function on $\Re s > \dim X$.

Example 7 ($\mathbb{A}^0 = Spec(\mathbb{F}_q)$). For each n there is only one point for $\mathbb{A}^0(\mathbb{F}_{q^n})$, which is already rational over $\overline{\mathbb{F}_q}$. Thus the zeta function is

$$Z(\mathbb{A}^0/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n}\right) = exp\left(-\log(1-T)\right) = \frac{1}{1-T} \in \mathbb{Z}[\![T]\!]$$

which corresponds to the Euler factor of $\zeta(s)$ once we substitute $T = p^{-s}$. In general, the Euler factor of Dedekind zeta function can be obtained in the same way.

Example 8 ($\mathbb{A}^k$). Clearly $\#\mathbb{A}^k(\mathbb{F}_{q^n}) = (q^n)^k = q^{kn}$. Thus the zeta function is

$$Z(\mathbb{A}^k/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} q^{kn}\frac{T^n}{n}\right) = exp\left(-\log(1-q^kT)\right) = \frac{1}{1-q^kT} \in \mathbb{Z}[\![T]\!]$$

Example 9 ($\mathbb{P}^k$). Clearly

$$\#\mathbb{P}^k(\mathbb{F}_{q^n}) = (q^n)^k + (q^n)^{k-1} + \cdots + 1$$

Thus the zeta function is

$$Z(\mathbb{P}^k/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty}(q^{kn} + \cdots + 1)\frac{T^n}{n}\right) = exp\left(-\sum_{i=0}^{k}\log(1-q^iT)\right) = \prod_{i=1}^{k}\frac{1}{1-q^iT} \in \mathbb{Z}[\![T]\!]$$

Here is another way of writing down the local zeta function.

Proposition 8. *Let X be a quasi-projective variety $\mathbb{F}_q$. For each closed point x we define $deg(x)$ to be the degree of the extension $k_{X,x}/\mathbb{F}_q$. Then*

$$Z(X/\mathbb{F}_q, T) = \prod_{x\in|X|}\left(1 - T^{deg(x)}\right)^{-1}$$

We ignore convergence issues as we are merely considering formal power series.

Proof. When we count $\#X(\mathbb{F}_{q^n})$, separate the counting for each $x \in |X|$ and use the fact that a closed point $x \in |X|$ will show up in $X(\mathbb{F}_{q^n})$ if and only if $deg(x)|n$. □

Corollary 1. *We actually have* $Z(X/\mathbb{F}_q, T) \in \mathbb{Z}[\![T]\!]$.

Remark 3. Note also that

$$Z(X/\mathbb{F}_q, q^{-s}) = \prod_{x \in |X|} \left(1 - |k_{X,x}|^{-s}\right)^{-1}$$

This can be used as a definition of (global) zeta function for scheme of finite type over $\mathbb{Z}$. In this set up the above proposition may be regarded as the analogue (in the local case) of Euler product factorization for Riemann zeta function.

Proposition 9 (Properties of local zeta functions)**.**

- *If* $C \hookrightarrow X$ *is a closed subscheme,* $U = X - C$ *an open subscheme of* X*, then*

$$Z(X, T) = Z(C, T)Z(U, T)$$

- *If* X *is reduced,* $X = X_1 \cup X_2$ *is a union of two closed subschemes, and* $X_1 \cap X_2$ *is equipped with reduced induced subscheme structure, then*

$$Z(X, T) = \frac{Z(X_1, T)Z(X_2, T)}{Z(X_1 \cap X_2, T)}$$

These two properties are useful in doing reduction arguments. For example, to prove rationality of zeta function, these properties reduce it to the case where X *is affine and integral, which is birational to an irreducible hypersurface in* $\mathbb{A}_{\mathbb{F}_{q^n}}$*.*

- *If* X *is defined over* $\mathbb{F}_q$*, then*

$$Z(X \times_{\mathbb{F}_q} \mathbb{F}_{q^r}, T^r) = \prod_{i=1}^{r} Z(X, \xi_r^i T)$$

where ξ_r *is a primitive* r*-th root of unity.*

4.2.2 Statement of Weil conjectures

The properties of this local zeta function was conjectured by Weil and proved by Deligne.

Theorem 4 (Deligne)**.** *For a smooth, projective, geometrically irreducible variety* $X/\mathbb{F}_q$ *we have,*

(Rationality) $Z(X/\mathbb{F}_q, T)$ *is a rational function in* T*. If* $\dim X = n$ *we can write it as*

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

where each $P_i(T)$ *has integral coefficients with leading coefficient 1.*

Functional equation) *Define* $\chi = \chi(X) = \sum_i (-1)^i deg(P_i)$. *We have*

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

Here the root number ϵ *is defined as follows.*

$$\epsilon = \begin{cases} (-1)^\chi & \text{if } n \text{ is odd} \\ (-1)^\chi & \text{if } n \text{ is even and ground field } \mathbb{F}_q \text{ is large enough} \end{cases}$$

FIX: What is the exact root number

iemann Hypothesis) *We can pin down* $P_0(T) = 1 - T$ *and* $P_{2n}(T) = 1 - q^{2n}T$. *For* $1 \leq i \leq 2n-1$,

$$P_i(T) = \prod_j (1 - \alpha_i(j)T)$$

with $|\alpha_i(j)| = q^{i/2}$ *for every archimedean place of* $\mathbb{Q}(\alpha_i(j)) \hookrightarrow \mathbb{C}$.

4.3 The case of curves

In this section, we will show rationality/functional equation of the zeta function via Riemann-Roch. For the Riemann hypothesis, there is also an elementary approach due to Bombieri-Stepanov.

4.3.1 Divisors on curves

Let $k = \mathbb{F}_q$ and X/k be a smooth, projective, geometrically irreducible curve. We use $\overline{X} = X_{\overline{k}}$ to denote its base change to $\overline{k}$.

- A divisor
$$D = \sum_{x \in |X|} n_x \cdot x$$
is a formal finite linear combination of closed points of X, with integer coefficients n_x. An effective divisor is one where each $n_x \geq 0$ - we use the notation $D \geq 0$ to denote effectiveness.
- $\mathrm{Div}(X)$ is the set of divisors.
- The degree of a divisor $D = \sum_{x \in |X|} n_x \cdot x$ is
$$\deg(D) := \sum_{x \in |X|} n_x \cdot \deg(x)$$
- Let $k(X)$ be the field of rational functions of X over k. For $f \in k(X)$, we can define the order of zeros/poles of f at each closed point. (Smoothness gives you a local uniformizer at each closed point). Denote the order of f at closed point x by $ord_x(f)$. We can then define the principal divisors
$$\mathrm{div}(f) = \sum_{x \in |X|} ord_x(f) x$$
Since X is projective, $\deg(\mathrm{div}(f)) = 0$ for all $f \in k(X)$.

4.3.2 Picard group

- We define an equivalence relation on divisors: $D \sim D'$ iff $D = D' + \mathrm{div}(f)$ for some $f \in k(X)$. The Picard group is then defined as

$$\mathrm{Pic}(X) = \mathrm{Div}(X)/\sim$$

- Degree map descends so we can define

$$\mathrm{Pic}(X) = \mathrm{Div}(X)/\sim \xrightarrow{deg} \mathbb{Z}$$

  Define $\mathrm{Pic}^0(X)$ to be the kernel of this map.

4.3.3 Section of line bundles

- For any divisor D on X, define

$$L(D) = \{f \in k(X) : \mathrm{div}(f) + D \geq 0\}$$

  which is a k-vector space. We also use $l(D)$ to denote the dimension of $l(D)$ as a k-vector space. Clearly $l(D) \geq 0$. It is also finite - this can be considered part of Riemann-Roch.

- Note that

$$\deg(\mathrm{div}(f) + D) = \deg(\mathrm{div}(f)) + \deg(D) = \deg(D)$$

  So if $\deg(D) < 0$, so that some coefficients of D is negative, $L(D) = \emptyset$ and $l(D) = 0$.

4.3.4 Riemann-Roch

Theorem 5 (Riemann-Roch + Serre Duality)**.** *There is a canonical divisor K on X such that for any divisor D on X, we have*

$$l(D) - l(K - D) = \deg(D) + 1 - g$$

where $g := l(K)$.

Corollary 2.

- $\deg(K) = 2g - 2$.
- $l(D) \leq \deg(D) + 1 - g$ *for all divisor D (Riemann's inequality), and thus is finite.*
- *If $n > 2g - 2$, then $l(D) = \deg(D) + 1 - g$.*

Corollary 3. *Implications on Picard group:*

- *For $n > 2g - 2$, each equivalence class in $\mathrm{Div}(n)/\sim$ has a representative by effective divisor. This follows from Riemann Roch.*
- $\mathrm{Pic}^0(X)$ *is finite. Note that from lemma 2.1, for fixed n there are finitely many effective divisors of degree $\leq n$. Last bullet point then implies that $\mathrm{Div}(n)/\sim$ is finite for all n large. But these are all cosets for $\mathrm{Pic}^0(X)$, hence $\mathrm{Pic}^0(X)$ is also finite.*

4.3.5 Rationality of zeta function of curves

Let X_0/k be a smooth, projective, geometrically irreducible curve over k. We saw that the zeta function is

$$\begin{aligned} Z(X,T) &= \prod_{x\in|X|}\left(1-T^{\deg(x)}\right)^{-1} \\ &= \prod_{x\in|X|}\left(1+T^{\deg(x)}+T^{2\deg(x)}+\cdots\right) \\ &= \sum_{D\geq 0} T^{\deg(D)} \\ &= \sum_{n=0}^{\infty} T^n \ \#\{\text{effective divisors of degree } n\} \qquad (\star) \end{aligned}$$

The constant term is the number of effective divisors of degree 0, which is 1.

Suppose that the degree map of Picard group maps onto $d\mathbb{Z}$, and let $\mathfrak{a}$ be a divisor of degree d. Then,

- If $d|n$, we see that $\mathrm{Div}(n)/\sim$ are cosets of $\mathrm{Pic}^0(X)$. In particular,

$$|\,\mathrm{Div}(n)/\sim\,| = |\,\mathrm{Pic}^0(X)|$$

- If $d\nmid n$, $\mathrm{Div}(n)/\sim$ is empty.

We will eventually show that $d=1$, but for now, $(\star)$is

$$\sum_{\substack{n=0\\ d|n}}^{\infty} T^n \ \#\{\text{effective divisors of degree } n\}$$

Any direct proof of this?

Note that for $n > 2g-2$ (and $d|n$), the degree n effective divisors surjects onto $\mathrm{Div}(n)/\sim$ (by our second bullet point in last section.) This means that

$$\begin{aligned} \#\{\text{effective divisors of degree } n\} &= \sum_{D\in\mathrm{Div}(n)/\sim} \#\{\text{effective divisors of degree } n \text{ equivalent to } D\} \\ &= \sum_{D\in\mathrm{Div}(n)/\sim} |\mathbb{P}(L(D))| \\ &= \sum_{D\in\mathrm{Div}(n)/\sim} \frac{q^{l(D)}-1}{q-1} \end{aligned}$$

Note also that $l(D) = n+1-g$ since $n > 2g-2$, and that $|\mathrm{Div}(n)/\sim| = |\,\mathrm{Pic}^0(X)|$

$$= |\,\mathrm{Pic}^0(X)|\frac{q^{n+1-g}-1}{q-1}$$

Therefore the $n > 2g-2$ part in $(\star)$ is

$$\sum_{\substack{n=2g-2+d \\ d|n}}^{\infty} T^n |\operatorname{Pic}^0(X)| \frac{q^{n+1-g}-1}{q-1} = \frac{|\operatorname{Pic}^0(X)|}{q-1} \left(\sum_{\substack{n=2g-2+d \\ d|n}}^{\infty} q^{n+1-g} T^n - \sum_{\substack{n=2g-2+d \\ d|n}}^{\infty} T^n \right)$$
$$= \frac{|\operatorname{Pic}^0(X)|}{q-1} \left(q^{1-g} \frac{(qT)^{2g-2+d}}{1-(qT)^d} - \frac{T^{2g-2+d}}{1-T^d} \right)$$

and is of the shape

$$\frac{\text{Polynomial in } T^d}{(1-T^d)(1-(qT)^d)}$$

For the $0 \leq n \leq 2g-2$ part of $(\star)$, it is clearly a polynomial in T^d of degree at most $\frac{2g-2}{d}$. In particular, we get that

$$Z(X,T) = \frac{\text{Polynomial in } T^d}{(1-T^d)(1-(qT)^d)}$$

where the polynomial in numerator has degree at most $\frac{2g-2}{d} + 2$. Notice that $Z(X,T)$ is a rational function in T^d.

We now seek more refined information about d and the numerator of $Z(X,T)$.

Claim 1. $d = 1$.

Proof. If ξ_d is a primitive d-th root of unity, recall that

$$Z(X \times_{\mathbb{F}_q} \mathbb{F}_{q^d}, T^d) = \prod_{i=1}^{d} Z(X, \xi_d^i T) = Z(X,T)^d$$

where the last equality is because $Z(X,T)$ is rational function in T^d as we have shown.

Now same proof (of rationality of zeta) shows that $Z(X \times_{\mathbb{F}_q} \mathbb{F}_{q^d}, T)$ has a pole of order 1 at $T = 1$, so same is true for $Z(X \times_{\mathbb{F}_q} \mathbb{F}_{q^d}, T^d) = Z(X,T)^d$. But this is impossible unless $d = 1$. □

So far we saw that

$$Z(X,T) = \frac{\text{Polynomial in } T}{(1-T)(1-qT)}$$

with degree of numerator at most $2g$. We now show that it is exactly $2g$.

- Contribution from $n \geq 2g-1$ term to $Z(X,T)$ is of the shape:

$$\frac{|\operatorname{Pic}^0(X)|}{q-1} \left(q^g \frac{T^{2g-1}}{1-qT} - \frac{T^{2g-1}}{1-T} \right) = \frac{|\operatorname{Pic}^0(X_0)|}{q-1} \cdot \frac{(q-q^g)T^{2g} + (q^g-1)T^{2g-1}}{(1-qT)(1-T)}$$

- Contribution from $n \leq 2g-2$ term to $Z(X,T)$ is of the shape

$$T^{2g-2} \#\{\text{effective divisors of degree } 2g-2\} = T^{2g-2} \sum_{\substack{D \in \operatorname{Div}(2g-2)/\sim \\ D \text{ effective}}} \frac{q^{l(D)}-1}{q-1}$$

- For $D \in \mathrm{Div}(2g-2)/\sim$,
  - if $D \sim K$, then $l(D) = l(K) = g$.
  - If $D \not\sim K$, then $l(D) = g - 1$. This is by Riemann-Roch, and note that as $K - D$ is a divisor of degree 0 that is not equivalent to 0, we must have $l(K - D) = 0$.
- This would imply that after we clear the fraction, the leading term in the numerator of $Z(X, T)$ will not be cancelled.

Thus we conclude that

Theorem 6 (Rationality of zeta function)**.** *For a smooth, projective, geometrically irreducible curve X over $\mathbb{F}_q$, we have*

$$Z(X, T) = \frac{P_1(T)}{(1-T)(1-qT)}$$

where $P_1(T) \in \mathbb{Z}[T]$ is of degree $2g$.

We mention that functional equation can be argued in a bare-hand way along this line, while Riemann Hypothesis would be more involved.

4.4 Dwork's proof for rationality of zeta function for quasi-projective variety over $\mathbb{F}_q$

4.5 References

General background of zeta function for varieties over $\mathbb{F}_p$

[1] Nick Katz, *Lecture Notes at Princeton 1973-1974*

[2] Sam Raskin, *UChicago REU 07 notes*

[3] Mustata, *Zeta Functions in Algebraic Geometry*

Weil II

[1] Nick Katz, *Four Lectures on Weil II*

[2] Michel, *Diophantine Consequences of Deligne's Weil II Main Theorem*, `http://wiki.epfl.ch/quantumchaos2013/documents/PhMichel_SeminarTamas.pdf`

Dwork's proof of rationality

[1] Terry Tao, *Blog post on Dwork's proof*, `https://terrytao.wordpress.com/2014/05/13/dworks-proof-of-rationality-of-the-zeta-function-over-finite-fields/`

5 Weil bound for curves

5.1 Bombieri-Stepanov

Given a smooth proper curve X over $\mathbb{F}_q$, our strategy is to count the $\mathbb{F}_q$ points of X by finding the points of $\overline{X} = X \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ whose coordinates are unchanged by raising them to the qth power. Algebraically, we are looking for fixed points of frobenius. Since there are several versions of frobenius, we'll give a concrete description of the two versions of frobenius we will be using and how they are different.

Relative frobenius is defined as $F_q = (\text{frobenius on } X) \times (\text{identity on } \overline{\mathbb{F}}_q)$, while absolute frobenius just raises everything to the pth power. What this really means, with an example:

"If $(x, y) \in \overline{X}$ satisfies $x^q = \sqrt{2}$, then $(x', y') = F_q((x, y))$ satisfies $x' = \sqrt{2}$" vs "If $(x, y) \in \overline{X}$ satisfies $x^p = \sqrt{2}^p$, then $(x', y') = (x^p, y^p)$ satisfies $x' = \sqrt{2}$."

So absolute frobenius doesn't do anything interesting other than change multiplicites of roots by multiples of p, while relative frobenius changes the coordinates of $\overline{\mathbb{F}}_q$-points of $\overline{X}$. Thus, we want to count fixed points of *relative* frobenius.

One of the main tricks in the proof of the Riemann hypothesis is based on the following Lemma, which, when combined with the rationality of the zeta function, turns asymptotic bounds with poor implicit constants into more precise bounds.

Lemma 2. *If $\alpha_1, ..., \alpha_n \in \mathbb{C}$ and $c \in \mathbb{R}^+$ are such that $\Re(\sum_{i=1}^n \alpha_i^k) = O(c^k)$, then for all i we have $|\alpha_i| \leq c$.*

Proof. Either one can apply the Pigeonhole Principle several times to show that there exist arbitrarily large integers k such that for all i, $\arg(\alpha_i) \cdot k$ is very close to an element of $2\pi\mathbb{Z}$, or alternatively one can look at the radius of convergence of the power series $\sum_{k\geq 0}(\sum_{i=1}^n \alpha_i^k)z^k = \sum_{i=1}^n \frac{1}{1-\alpha_i z}$. □

Main Idea: Suppose $Y/\mathbb{P}^1$ is Galois, that is, that $\mathbb{F}_q(Y)/\mathbb{F}_q(\mathbb{P}^1)$ is a Galois extension of fields, of degree d (so $d = |\operatorname{Gal}(Y/\mathbb{P}^1)|$). Since Y is proper and of dimension 1, every element of $g \in \operatorname{Gal}(Y/\mathbb{P}^1)$ gives a well defined regular function $g : Y \to Y$ which is defined over $\mathbb{F}_q$ (a priori, we only knew that g was a rational function). All but finitely many points $x \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ have exactly d preimages in $Y(\overline{\mathbb{F}}_q)$, and these d preimages will be permuted by $\operatorname{Gal}(Y/\mathbb{P}^1)$ (the points with less than d preimages are the "ramification points", and the number of ramification points is bounded by $2d + 2g - 2$, where g is the genus of Y). If $x \in \mathbb{P}^1(\mathbb{F}_q)$ and $y \mapsto x$ is unramified, then there exists a unique $g \in \operatorname{Gal}(Y/\mathbb{P}^1)$ such that $g(y) = F_q(y)$ (since y and $F_q(y)$ are both preimages of $x = F_q(x)$). Thus, we have

$$1 + q = |\mathbb{P}^1(\mathbb{F}_q)| = \frac{1}{|\operatorname{Gal}(Y/\mathbb{P}^1)|} \sum_{g \in \operatorname{Gal}} |\operatorname{Fix}(g^{-1} \circ F_q \text{ on } \overline{Y})| + O(2d + 2g - 2).$$

Although this is good enough for our purposes, we can actually get rid of the error term. We use the following group theoretic fact: if a group acts on a set, then the expected number of fixed points of a random element of the group is equal to the number of orbits of the action. We know that away from a finite collection of points $x \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$, the group $\operatorname{Gal}(Y/\mathbb{P}^1)$ acts transitively on the preimages of x, and the set of points x such that the action on the preimages of x is *not* transitive is easily seen to be open, so it must be empty. Thus, the number of orbits of the action of $\operatorname{Gal}(Y/\mathbb{P}^1)$

on the set of preimages of any $x \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ is always 1, so

$$1 + q = \frac{1}{|\operatorname{Gal}(Y/\mathbb{P}^1)|} \sum_{g \in \operatorname{Gal}} |\operatorname{Fix}(g^{-1} \circ F_q \text{ on } \overline{Y})|.$$

The upshot of all this is that if we can get good upper bounds on $|\operatorname{Fix}(g^{-1} \circ F_q \text{ on } \overline{Y})|$ for any $g \in \operatorname{Gal}(Y/\mathbb{P}^1)$, then we can get decent lower bounds on the same quantity by applying the upper bounds to $|\operatorname{Fix}(h^{-1} \circ F_q \text{ on } \overline{Y})|$ for $h \neq g$ (the error terms will get multiplied by $|\operatorname{Gal}| - 1$ in the process).

For general $X/\mathbb{P}^1$, we let Y be the Galois closure of X over $\mathbb{P}^1$. Let $G = \operatorname{Gal}(Y/\mathbb{P}^1)$, and let $H = \operatorname{Gal}(Y/X)$. Then a similar argument to the above gives us the formula

$$|X(\mathbb{F}_q)| = \frac{1}{|H|} \sum_{h \in H} |\operatorname{Fix}(h^{-1} \circ F_q \text{ on } \overline{Y})|.$$

Then good upper and lower bounds for $|\operatorname{Fix}(h^{-1} \circ F_q \text{ on } \overline{Y})|$ give us good upper and lower bounds for $|X(\mathbb{F}_q)|$.

Theorem 7 (Bombieri-Stepanov)**.** *Suppose X is a proper smooth curve over $\mathbb{F}_q$ of genus g, and let $g \in \operatorname{Aut}(X/\mathbb{F}_q)$. Set $\varphi = g^{-1} \circ F_q$. Assume that $q = p^\alpha$, with α even, and that $q > (g+1)^4$. Then*

$$|\operatorname{Fix}(\varphi \text{ on } \overline{X})| \leq 1 + q + (2g+1)\sqrt{q}.$$

Proof. The general strategy is to show that there is a nonzero function of low degree which vanishes at every fixed point of φ, and we will produce such a function by doing a dimension count, using the fact that the collection of pth powers of functions forms a vector space. Suppose there is some $x_0 \in \operatorname{Fix}(\varphi)$ (if there is no such x_0 then we are done). We will treat x_0 as the "point at infinity" on X, study functions on X which only have poles at x_0, and measure the degree of such a function by the order of its pole at x_0. Formally, we set

$$L_m = \Gamma(\overline{X}, \mathcal{O}_{\overline{X}}(m x_0)) \subseteq \overline{\mathbb{F}}_q(X),$$

so L_m is the collection of functions of degree at most m which only have poles at x_0, and we let $l_m = \dim L_m$. Recall that Riemann-Roch implies that

$$m + 1 - g \leq l_m \leq m + 1,$$

and that $l_m = m + 1 - g$ if $m > 2g - 2$. We'll also set

$$L_m^\varphi = \{f \circ \varphi \mid f \in L_m\}, L_l^{p^\mu} = \{f^{p^\mu} \mid f \in L_l\},$$

the images of L_m and L_l under composition with φ and powers of absolute frobenius, respectively. Since g is an automorphism and F_q has order q, we have

$$L_m \xrightarrow[\approx]{\varphi} L_m^\varphi \hookrightarrow \Gamma(\overline{X}, \mathcal{O}_{\overline{X}}(mqx_0)) = L_{mq}, \quad L_l \xrightarrow[\approx]{p^\mu} L_l^{p^\mu} \subseteq L_{lp^\mu}.$$

Lemma 3. *If $lp^\mu < q$, then $L_l^{p^\mu} \otimes_{\overline{\mathbb{F}}_q} L_m^\varphi \to L_{lp^\mu + mq}$ is injective.*

Proof. Look at the Laurent expansion at x_0. □

Corollary 4. *If $lp^\mu < q$, there exists a well-defined map $\delta : L_l^{p^\mu} \cdot L_m^{\varphi} \to L_l^{p^\mu} \cdot L_m \subseteq L_{m+lp^\mu}$, given by*

$$\delta : \sum_i g_i^{p^\mu} \cdot (f_i \circ \varphi) \mapsto \sum_i g_i^{p^\mu} f_i.$$

If $l_m l_l > l_{m+lp^\mu}$, then $\ker \delta \neq 0$.

Suppose that $lp^\mu < q, l_m l_l > l_{m+lp^\mu}$, and let $f = \sum_i g_i^{p^\mu} \cdot (f_i \circ \varphi) \neq 0$ be in the kernel of δ. From $lp^\mu < q$, we see that f is a p^μth power, and for $x \in \operatorname{Fix}(\varphi), x \neq x_0$, we have

$$f(x) = \sum_i g_i(x)^{p^\mu} f_i(\varphi(x)) = \sum_i g_i(x)^{p^\mu} f_i(x) = 0,$$

so

$$p^\mu(|\operatorname{Fix}(\varphi)| - 1) \leq \#\text{zeroes of } f \leq lp^\mu + mq,$$

since every root of f occurs with multiplicity at least p^μ. Dividing by p^μ, this becomes

$$|\operatorname{Fix}(\varphi)| \leq l + m\frac{q}{p^\mu} + 1.$$

Now we just need to choose values of l, m, μ in order to get a good bound. We take $p^\mu = \sqrt{q}, m = \sqrt{q} + 2g, l = g + 1 + \lfloor \frac{g}{g+1}\sqrt{q} \rfloor$:

- $lp^\mu < q$ is the same as $l < \sqrt{q}$, which follows from $g + 1 < \frac{\sqrt{q}}{g+1}$.
- To check that $l_l l_m > l_{m+lp^\mu}$, note that $l_l \geq l+1-g, l_m \geq m+1-g$, and $l_{m+lp^\mu} = m+lp^\mu+1-g$, so we just need to check that $(l-g)(m+1-g) > lp^\mu = l\sqrt{q}$, or equivalently $l(m+1-q-\sqrt{q}) > g(m+1-g)$. Simplifying, this becomes $l(g+1) > g(\sqrt{q}+g+1)$, or $l > \frac{g}{g+1}\sqrt{q} + g$.
- Finally, we get

$$\begin{aligned} |\operatorname{Fix}(\varphi)| &\leq g + 1 + \lfloor \frac{g}{g+1}\sqrt{q} \rfloor + \sqrt{q}(\sqrt{q} + 2g) + 1 \\ &\leq q + (2g+1)\sqrt{q} + 1 - (\tfrac{\sqrt{q}}{g+1} - (g+1)). \end{aligned}$$

□

5.2 Improvements to the Weil bound

This section follows Schoof's exposition [7]. Recall that for a proper smooth curve $X/\mathbb{F}_q$ of genus g, the zeta function attached to X is rational, of the form

$$Z(X,T) = \frac{P_X(T)}{(1-T)(1-qT)},$$

where $P_X(T)$ has integral coefficients and constant term 1, and $Z(X,T)$ satisfies the functional equation

$$Z\Big(X, \frac{1}{qT}\Big) = q^{1-g}T^{2-2g}Z(X,T).$$

Thus the leading coefficient of $P_X(T)$ is q^g, and

$$P_X(T) = \prod_{i=1}^{2g}(1 - \alpha_i T)$$

for some algebraic integers α_i. From the functional equation, we see that for factor $1-\alpha_i T$ of $P_X(T)$ there must be a corresponding factor $1-\frac{q}{\alpha_i}T$ with the same multiplicity. Together with the fact that there are an even number of α_is and that their product is q^g, we see that we can arrange the α_is such that $\alpha_{g+i}=\frac{q}{\alpha_i}$ for $i=1,...,g$. The Riemann Hypothesis for X (proved in the last subsection) then gives us $|\alpha_i|=\sqrt{q}$, so $\alpha_{g+i}=\overline{\alpha}_i$. This gives us the following **explicit formula**, valid for all $d\in\mathbb{N}$:

$$|X(\mathbb{F}_{q^d})|=q^d+1-\sum_{i=1}^{g}(\alpha_i^d+\overline{\alpha}_i^d),$$

where each α_i is an algebraic integer such that the absolute value of any conjugate of α_i is $\sqrt{q}$.

Theorem 8 (Hasse-Weil-Serre)**.** $|X(\mathbb{F}_q)|\leq q+1+\lfloor 2\sqrt{q}\rfloor g$.

Proof. Set $x_i=\lfloor 2\sqrt{q}\rfloor+1+\alpha_i+\overline{\alpha}_i$. Then each x_i is a totally positive algebraic integer, so $\prod_{i=1}^{g}x_i\geq 1$, and then by the AM-GM inequality we have $\sum_{i=1}^{g}x_i\geq g$. □

When the genus is very large compared to q, strange things start to happen. In this case, the lower bound on the number of points becomes trivial, and the upper bound becomes much smaller than expected. The following bound becomes better than the Weil bound once $g\geq\frac{q-\sqrt{q}}{2}$.

Theorem 9 (Ihara)**.** $|X(\mathbb{F}_q)|\leq q+1+\Big(\sqrt{2q+\frac{1}{4}+\frac{q^2-q}{g}}-\frac{1}{2}\Big)g$.

Proof. Set $t_i=\alpha_i+\overline{\alpha}_i$. Then by the explicit formula,

$$|X(\mathbb{F}_q)|\leq|X(\mathbb{F}_{q^2})|=q^2+1-\sum_{i=1}^{g}(\alpha_i^2+\overline{\alpha}_i^2)=q^2+1+2qg-\sum_{i=1}^{g}t_i^2,$$

and by the Cauchy-Schwarz inequality the right hand side is

$$\leq q^2+1+2qg-\frac{1}{g}\Big(\sum_{i=1}^{g}t_i\Big)^2=q^2+1+2qg-\frac{1}{g}\Big(|X(\mathbb{F}_q)|-q-1\Big)^2.$$

Rearranging and multiplying by g, we have

$$\Big(|X(\mathbb{F}_q)|-q-1\Big)^2+g\Big(|X(\mathbb{F}_q)|-q-1\Big)\leq(q^2-q)g+2qg^2,$$

and completing the square finishes the proof. □

Oeserlé Method: Set $\omega_i=\frac{\alpha_i}{\sqrt{q}}$, so $|\omega_i|=1$. Then from the explicit formula, we get

$$|X(\mathbb{F}_q)|q^{-\frac{d}{2}}\leq|X(\mathbb{F}_{q^d})|q^{-\frac{d}{2}}=q^{\frac{d}{2}}+q^{-\frac{d}{2}}-\sum_{i=1}^{g}(\omega_i^d+\overline{\omega}_i^d).$$

Multiplying these inequalites by nonnegative constants $c_1,c_2,...$ and adding them together, we get

$$|X(\mathbb{F}_q)|\lambda(q^{-\frac{d}{2}})\leq\lambda(q^{\frac{d}{2}})+\lambda(q^{-\frac{d}{2}})-\sum_{i=1}^{g}(\lambda(\omega_i)+\lambda(\overline{\omega}_i)),$$

where

$$\lambda(t) = \sum_{d=1}^{\infty} c_d t^d.$$

Letting $f(t) = 1 + \lambda(t) + \lambda(\frac{1}{t})$, we see that as long as the c_ds are chosen such that $f(t) \geq 0$ for all t with $|t| = 1$, then we have

$$|X(\mathbb{F}_q)|\lambda(q^{-\frac{d}{2}}) \leq \lambda(q^{\frac{d}{2}}) + \lambda(q^{-\frac{d}{2}}) + g.$$

Theorem 10 (Drinfeld-Vlădut)**.** $\limsup_{g\to\infty} \frac{|X(\mathbb{F}_q)|}{g} \leq \sqrt{q} - 1$*, that is,* $|X(\mathbb{F}_q)| \leq (\sqrt{q} - 1)g + o(g)$ *when q is fixed and g goes to infinity.*

Proof. We want to apply Oesterlé's method with the c_ds as large as possible, in order to maximize $\lambda(q^{-\frac{d}{2}})$. From

$$1 - c_d = \frac{1}{\pi}\int_0^{2\pi} f(e^{i\theta})(1 - \cos(n\theta))d\theta \geq 0,$$

we see that each c_d is ≤ 1. If we take

$$f(t) = \frac{1}{N+1}(1 + t + \cdots + t^N)(1 + t^{-1} + \cdots + t^{-N}),$$

then we see that $f(t) \geq 0$ whenever $|t| = 1$, and $f(t) = 1 + \sum_{d=1}^{N} \frac{N+1-d}{N+1}(t^d + t^{-d})$ gives $c_d = \frac{N+1-d}{N+1} \geq 0$ for $1 \leq d \leq N$. Taking N to ∞, each c_d tends to 1 from below, and

$$\lim_{N\to\infty} \lambda(q^{-\frac{1}{2}}) = q^{-\frac{1}{2}} + q^{-1} + q^{-\frac{3}{2}} + \cdots = \frac{1}{\sqrt{q} - 1}.$$ □

6 Dwork's proof of rationality of the zeta function

In this section we follow Dwork's paper [5].

6.1 Motivation

Recall the Chevalley-Warning trick:

$$\#\{(x, y) \in \mathbb{F}_p^2 \mid f(x, y) = 0\} \equiv \sum_{x,y\in\mathbb{Z}/p} (1 - f(x, y)^{p-1}) \pmod{p},$$

$$\sum_{x\in\mathbb{Z}/p} x^i \equiv \begin{cases} 0 & (p-1) \nmid i \text{ or } i = 0, \\ -1 & (p-1) \mid i, i > 0 \end{cases} \pmod{p}.$$

Together with a crude bound on the number of points, this congruence was often enough to give us an exact point count. We would like to generalize this approach in order to compute zeta functions, so we have to generalize in two different directions at once:

- we need to find a way to count points in $\mathbb{F}_{p^s}$, $s > 1$, and
- we need to find a way to get pount counts modulo p^k, $k > 1$.

Towards the second bullet point, we are lead to wonder what the value of

$$\sum_{x=0}^{p-1} x^i \pmod{p^2}$$

is. While this is a hard question, if we instead look at the sum

$$\sum_{x=0}^{p-1} (x^p)^i \pmod{p^2}$$

it becomes much easier! Generalizing this observation, we see that we want to work with Teichmüller lifts, which are given by

$$[x] = \lim_{n\to\infty} x^{p^n},$$

where the limit is taken p-adically (if x is an integral element of $\overline{\mathbb{Q}}_p$ or $\mathbb{C}_p$, then the limit should be taken over the net of positive integers ordered by divisibility). Teichmüller lifts are always either 0 or roots of unity, we have $[xy] = [x][y]$, and $x \equiv [x] \pmod{p}$ whenever $|x|_p = 1$. Because of that last point, we can think of Techmüller lifts as a function from $\overline{\mathbb{F}}_p$ to $\overline{\mathbb{Z}}_p$.

Now for the first bullet point: how will we get point counts in $\mathbb{F}_{p^s}$? The strategy is to use either additive or multiplicative characters (Dwork tried both approaches: multiplicative characters almost worked, while additive characters worked perfectly). We will need to have certain compatibilities between our characters for different powers of p. Recall that for complex characters, we made the definitions

$$\psi_q(a) = e^{\frac{2\pi i \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}{p}}, \quad \chi_q(a) = \chi(\operatorname{Nm}_{\mathbb{F}_p}^{\mathbb{F}_q}(a)),$$

giving

$$\psi_q(a) = \psi(a + a^p + \cdots + a^{p^{s-1}}) \quad \text{“} = \psi(a)\psi(a^p)\cdots\psi(a^{p^{s-1}})\text{”}.$$

Dwork's idea is to find a p-adic power series $\theta(x)$ such that for $x \in \mathbb{F}_{p^s}$ we have

$$\zeta_p^{\operatorname{Tr}(x)} = \theta([x])\theta([x]^p)\cdots\theta([x]^{p^{s-1}}),$$

where ζ_p is a primitive pth root of unity in $\overline{\mathbb{Q}}_p$. Then we can evaluate sums of additive characters at points in $\mathbb{F}_{p^s}$ by turning them into sums of power series evaluated at (p^s-1)th roots of unity in $\mathbb{C}_p$.

6.2 Combining p-adic congruences with inequalities

Knowing point counts of varieties modulo powers of p is great, but how will we eventually use this to prove that $Z(V,T)$ is rational? Recall that a power series is a rational function if and only if its coefficients eventually satisfy some linear recurrence relation. Thus, our strategy is as follows:

- We know that $Z(V,T)$ is a power series with integer coefficients.
- Trivial bounds on the point counts show that $Z(V,T)$ has a nontrivial radius of convergence, so its coefficients are not too big.
- Since the coefficients are small, if they satisfy a recurrence modulo large enough powers of p, then they actually satisfy that recurrence over the integers.

To make this last bullet point precise, we have the following Lemma, from Chapter 13 of [1].

Lemma 4. *Suppose that $f(x) = \sum_{i \geq 0} f_i x^i$ is a power series with coefficients in some field. Then f is a rational function if and only if there exists some $l \geq 0$ such that for all sufficiently large n, we have*

$$\det \begin{pmatrix} f_n & f_{n+1} & \cdots & f_{n+l} \\ f_{n+1} & f_{n+2} & \cdots & f_{n+l+1} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n+l} & f_{n+l+1} & \cdots & f_{n+2l} \end{pmatrix} = 0.$$

Proof. Let $F(n, l)$ be the determinant corresponding to n and l, so that $F(n, 0) = f_n$ and $F(n, 1) = f_n f_{n+2} - f_{n+1}^2$, etc.

Suppose first that $f(x)$ is rational, with $f(x) = \frac{p(x)}{q(x)}$, $q(x) = q_l x^l + \cdots + q_1 x + 1$. Then since $f(x)q(x) = p(x)$, we see that

$$f_{k+l} = -q_1 f_{k+l-1} - \cdots - q_l f_k$$

for all $k > \deg p$. Plugging in $k = n, n+1, ..., n+l$, we see that the rigtmost column of the matrix corresponding to n and l is a linear combination of the remaining columns, so the determinant is 0 for all $n > \deg p$.

Now suppose that $l \geq 0$ is chosen to be minimal such that $F(n, l) = 0$ for all sufficiently large n. If $l = 0$ then f is a polynomial and we are done. Using the determinant identity (for a proof of this identity, see [1]: apparently it is a special case of "Jacobi's Theorem on the minors of the adjugate")

$$F(n, l-1)F(n+2, l-1) - F(n+1, l-1)^2 = F(n, l)F(n+2, l-2),$$

we see that for n sufficiently large we have $F(n, l-1)F(n+2, l-1) = F(n+1, l-1)^2$, so the sequence $F(n, l-1)$ is eventually a geometric progression, and so by the minimality of l we must have $F(n, l-1) \neq 0$ for all sufficiently large n.

Thus, for n sufficiently large the matrix corresponding to n and l has rank exactly l (and the first l columns are independent), so there is a unique tuple $q_{1,n}, ..., q_{l,n}$ such that

$$f_{k+l} + q_{1,n} f_{k+l-1} + \cdots + q_{l,n} f_k = 0$$

for $k = n, ..., n+l$. Comparing this system of equations for n and $n+1$, and using the fact that the last l rows of the matrix corresponding to n and l are the same as the first l rows of the matrix corresponding to $n+1$ and l and that these rows are independent, we see that in fact the $q_{i,n}$ are independent of n, so we can write $q_{i,n} = q_i$. Setting $q(x) = q_l x^l + \cdots + q_1 x + 1$, we see that $f(x)q(x)$ is a polynomial $p(x)$, so $f(x) = \frac{p(x)}{q(x)}$ is a rational function, and we are done. □

Recall that a power series $f(x)$ is *meromorphic in a disc of radius R* if and only if there exists a nonzero polynomial $p(x)$ such that the power series $f(x)p(x)$ converges everywhere in the disc of radius R. We also say that a power series is *meromorphic* if it can be written as a ratio of two entire functions, i.e. two power series which converge everywhere. These definitions are compatible since every entire function has only finitely many roots inside any disc. We can make entirely analogous definitions for p-adic meromorphic functions, and this time the compatibility between the definitions relies on a result known as the Weierstrass preparation theorem:

Proposition 10 (Weierstrass preparation theorem)**.** *Let $f(x) = \sum_i f_i x^i \in \mathbb{C}_p[\![x]\!]$ with $|f_n|_p \to 0$. Let N be defined by $|f_N|_p = \max |f_n|_p$ and $|f_N|_p > |f_n|_p$ for all $n > N$. Then there is a polynomial $g(x) = g_0 + \cdots + g_N x^N \in \mathbb{C}_p[x]$ and a power series $h(x) = 1 + h_1 x + \cdots \in \mathbb{C}_p[\![x]\!]$ with $|h_n|_p \to 0$ such that $f(x) = g(x)h(x)$, $|g_N|_p = \max |g_n|_p$, and $|h_n|_p < 1$ for $n > 0$.*

The proof of the Weierstrass preparation theorem is similar to the proof of Hensel's lemma: first you find a solution that works modulo a small power of p, and then show that you can modify it to make it work modulo larger powers of p (for this last step, you use the division lemma for polynomials).

Theorem 11 (Borel, Dwork)**.** *Let $f(x) \in \mathbb{Z}[\![x]\!]$ be meromorphic in a disc of radius R_∞, and p-adically meromorphic in a disc of radius R_p. If $R_p R_\infty > 1$, then f is a rational function.*

Proof. Let $g_\infty \in \mathbb{C}[x], g_p \in \mathbb{C}_p[x]$ be polynomials with constant term 1 such that $h_\infty(x) = g_\infty(x)f(x)$ converges in a disc of radius R_∞ and $h_p(x) = g_p(x)f(x)$ converges p-adically in a disc of radius R_p (note that even though f had integral coefficients, g_∞ and g_p might have transcendental coefficients). For $v = p, \infty$ define $t_v, T_v > 0$ such that $T_v R_v > 1$, $T_p T_\infty < 1$, and such that t_∞ is more than the inverse of the radius of convergence of f and t_p is more than the inverse of the p-adic radius of convergence of f, so that $|f_n|_v \ll t_v^n$ and $|h_n|_v \ll T_v^n$. Suppose also that both g_∞, g_p have degree bounded by m.

Since $T_p T_\infty < 1$, by choosing l sufficiently large we can ensure that

$$(t_p t_\infty)^m (T_p T_\infty)^{l+1-m} < 1.$$

Fix such an l with $l \geq m$, and let $F(n, l)$ be the determinant

$$\det \begin{pmatrix} f_n & f_{n+1} & \cdots & f_{n+l} \\ f_{n+1} & f_{n+2} & \cdots & f_{n+l+1} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n+l} & f_{n+l+1} & \cdots & f_{n+2l} \end{pmatrix}$$

considered in the earlier lemma. Then we can replace the fs in the rows after the mth row with the corresponding hs without changing the determinant, by using the recurrences implied by $h(x) = f(x)g(x)$. This gives us the bounds

$$|F(n, l)| \ll (t_\infty^n)^m (T_\infty^n)^{l+1-m}$$

and

$$|F(n, l)|_p \ll (t_p^n)^m (T_p^n)^{l+1-m},$$

where the implied constants depend on l, t_v, T_v, and on the implied constants in the bounds $|f_n|_v \ll t_v^n$ and $|h_n|_v \ll T_v^n$. Combining these, we get

$$|F(n, l)||F(n, l)|_p \ll ((t_p t_\infty)^m (T_p T_\infty)^{l+1-m})^n,$$

and for n sufficiently large the right hand side goes to 0. Since $F(n, l)$ is an integer, the only way to have $|F(n, l)||F(n, l)|_p < 1$ is to have $F(n, l) = 0$. Thus for all sufficiently large n, we have $F(n, l) = 0$, and so $f(x)$ must be a rational function (with denominator of degree at most l). □

Dwork's strategy for proving the rationality of $Z(V, T)$ is now to show that $Z(V, T)$ extends to a p-adic meromorphic function on all of $\mathbb{C}_p$, so we will be able to take R_p as large as we like in the previous theorem.

6.3 Summing over roots of unity

We will need to have convenient formulas for sums of the form

$$\sum_{x_1,\ldots,x_n \in \mathbb{F}_{q^s}^\times} F([x_1],\ldots,[x_n])F([x_1]^q,\ldots,[x_n]^q)\cdots F([x_1]^{q^{s-1}},\ldots,[x_n]^{q^{s-1}}),$$

where F is a power series in n variables, say $F(\vec{x}) = \sum_{\vec{u}} F_{\vec{u}}\vec{x}^{\vec{u}} \in \mathbb{C}_p[\![x]\!]$, with radius of convergence strictly greater than 1.

Since summing over (q^s-1)th roots of unity picks out the monomials with coefficients divisible by (q^s-1), it's almost natural to define the operator ψ by

$$\psi(\vec{x}^{\vec{u}}) = \begin{cases} \vec{x}^{\frac{\vec{u}}{q}} & q \mid \vec{u}, \\ 0 & q \nmid \vec{u}, \end{cases}$$

which one might call the "left inverse of Frobenius" (it seems at first that powers of ψ will always be "off by one" from what we really want, but this will actually work out nicely later on). What we really care about is not ψ, but the operator $\psi \circ F$, which acts on $\mathbb{C}_p[\![x]\!]$ as follows: first you multiply by F, then you apply ψ to the result of that multiplication. The (infinite) matrix M of this action is given by

$$M_{\vec{u},\vec{v}} = \text{coefficient of } \vec{x}^{\vec{u}} \text{ in } \psi(\vec{x}^{\vec{v}}F(\vec{x})) = F_{q\vec{u}-\vec{v}}.$$

Example 10. If we take $p = 2$ and $F(x) = \frac{1}{1-2x} = 1 + 2x + 4x^2 + \cdots$, then we get

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \cdots \\ 4 & 2 & 1 & 0 & 0 & \cdots \\ 16 & 8 & 4 & 2 & 1 & \cdots \\ 64 & 32 & 16 & 8 & 4 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Note that modulo p^n, F is congruent to a polynomial, so M is eventually strictly upper triangular, and therefore $\operatorname{Tr} M^s$ and $\det(1-tM)$ make sense modulo p^n. We will also write $\operatorname{Tr}(\psi \circ F)^s$ and $\det(1-t(\psi\circ F))$ for these two quantities.

Lemma 5. *If $F(\vec{x}) = \sum_{\vec{u}} F_{\vec{u}}\vec{x}^{\vec{u}} \in \mathbb{C}_p[\![x]\!]$ has coefficients going to 0, then for all $s \geq 1$ we have*

$$(q^s-1)^n \operatorname{Tr}(\psi\circ F)^s = \sum_{\vec{x}\in\mu_{q^s-1}^n} F(\vec{x})F(\vec{x}^q)\cdots F(\vec{x}^{q^{s-1}}),$$

where μ_{q^s-1} is the set of (q^s-1)th roots of unity in $\mathbb{C}_p$.

Proof. Since $(\psi\circ F)^s = \psi^s \circ (F(\vec{x})F(\vec{x}^q)\cdots F(\vec{x}^{q^{s-1}}))$, it's enough to prove it for $s = 1$. When $s = 1$ we see that the trace of $\psi \circ F$ is the sum over $\vec{u}$ of $F_{q\vec{u}-\vec{u}} = F_{(q-1)\vec{u}}$, and each of monomial $\vec{x}^{(q-1)\vec{u}}$ contributes $(q-1)^n$ to the sum on the right. □

For the next lemma, we define the *weight* of a vector $\vec{u}$, written $\operatorname{wt}(\vec{u})$, to be the sum of the coefficients of $\vec{u}$. Thus, if $\vec{u}$ is an exponent vector, then $\operatorname{wt}(\vec{u})$ is the total degree.

Lemma 6. *If there is a constant $c > 0$ such that $v_p(F_{\vec{u}}) \geq cwt(\vec{u})$ for all $\vec{u} \in \mathbb{N}^n$, then if $M_{\vec{u},\vec{v}} = F_{q\vec{u}-\vec{v}}$ is the matrix of $\psi \circ F$, we have the power series identity*

$$\exp\left(\sum_{s=1}^{\infty} \frac{t^s \operatorname{Tr} M^s}{s}\right) = \frac{1}{\det(1-tM)}$$

and $\det(1-tM)$ is entire.

Proof. The identity follows from the corresponding fact for finite dimensional matrices by considering both sides modulo powers of p and the fact that modulo any power of p, M is eventually strictly upper triangular.

Now write $\det(1-tM) = \sum_{m\geq 0} d_m t^m$. By the definition of the determinant in terms of sums of products over permutations, we have

$$\begin{aligned} v_p(d_m) &\geq \min_{\{\vec{u}_1,\ldots,\vec{u}_m\}=\{\vec{v}_1,\ldots,\vec{v}_m\}} \sum_i v_p(F_{q\vec{u}_i-\vec{v}_i}) \\ &\geq c \min_{\{\vec{u}_1,\ldots,\vec{u}_m\}} (\mathrm{wt}(\vec{u}_1)+\cdots+\mathrm{wt}(\vec{u}_m))(q-1) \\ &\gg m^{1+\frac{1}{n}}, \end{aligned}$$

where the last inequality follows from the fact that the number of vectors in $\mathbb{N}^n$ of total weight less than $\frac{1}{2}m^{\frac{1}{n}}$ is at most $\frac{1}{2}m$ for m sufficiently large. Thus p-adic absolute values of the coefficients d_m of $\det(1-tM)$ go to zero faster than any r^m with $r > 0$, so $\det(1-tM)$ is entire. □

6.4 The additive character as a power series

We need to construct a power series $\theta(x) \in \mathbb{Z}_p[\![x]\!]$ such that

- if $x \in \mathbb{F}_{p^s}$, then
$$\zeta_p^{\mathrm{Tr}(x)} = \prod_{i=0}^{s-1} \theta([x]^{p^i}),$$
where ζ_p is a primitive pth root of unity in $\mathbb{C}_p$, and
- $\theta(x) = \sum_{m\geq 0} \beta_m x^m$ with $v_p(\beta_m) \gg m$.

Let's fix some notation for talking about elements of $\mathbb{C}_p$ such as ζ_p while making as few "choices" as possible. Start by taking your favorite quadratic nonresidue $\alpha \in \mathbb{F}_p^\times \backslash (\mathbb{F}_p^\times)^2$ for $p \neq 2$ (for instance, maybe your favorite is just the least quadratic nonresidue modulo p), and choose a square root $\sqrt{a}$ in $\mathbb{F}_{p^2}$ (this time the choice doesn't really matter). Set $\pi = [\sqrt{\alpha}]p^{\frac{1}{p-1}}$, and if $p = 2$ set $\pi = -2$, so that

$$\pi^{p-1} = -p.$$

Then we choose ζ_p to be the primitive pth root of unity satisfying

$$\zeta_p \equiv 1 + \pi + \frac{\pi^2}{2} + \cdots + \frac{\pi^{p-1}}{(p-1)!} \pmod{\pi p}.$$

(Try working out more terms of the expansion of ζ_p in powers of π yourself! It's fun.)

Define a power series $E(x)$, called the *Artin-Hasse exponential*, by

$$E(x) = \exp\Big(\sum_{j\geq 0} \frac{x^{p^j}}{p^j}\Big)$$

for $|x|_p < \frac{1}{p^{\frac{1}{p-1}}}$ (although we will soon show that the power series for $E(x)$ converges for all x with $|x|_p < 1$, the equality above will no longer be valid for x with $|x|_p \geq \frac{1}{p^{\frac{1}{p-1}}}$ - this subtlety has several counterintuitive consequences). Since

$$\frac{E(x)^p}{E(x^p)} = \exp(px) \in 1 + px\mathbb{Z}_p[\![x]\!],$$

we have $E(x) \in \mathbb{Z}_p[\![x]\!]$ by the following easy result:

Lemma 7 (Dwork's Lemma)**.** *If $f(x) = 1 + f_1 x + \cdots \in \mathbb{Q}_p[\![x]\!]$, then $f(x) \in \mathbb{Z}_p[\![x]\!]$ if and only if $\frac{f(x)^p}{f(x^p)} \in 1 + px\mathbb{Z}_p[x]$.*

In the power series identity

$$E(x)^p = \exp\Big(p\sum_{j\geq 0} \frac{x^{p^j}}{p^j}\Big),$$

both sides converge for $|x|_p < 1$, so this identity is valid for all such x.

Let $\eta \in \mathbb{Z}_p[\pi]$ be the unique solution to $E(\eta) = \zeta_p$. One can easily check from the power series expansion of $E(x)$ and the displayed identity above that η exists and is unique, and that we have

$$\eta \equiv \pi \pmod{\pi p^{p-1}}.$$

Finally, define $\theta(x)$ by

$$\theta(x) = E(\eta x).$$

Note that since $E(x) \in \mathbb{Z}_p[\![x]\!]$ and $v_p(\eta) = \frac{1}{p-1}$, if we write $\theta(x) = \sum_{m\geq 0} \beta_m x^m$ then we have $v_p(\beta_m) \geq \frac{m}{p-1}$.

Lemma 8. *For $x \in \mathbb{F}_{p^s}$, we have*

$$\zeta_p^{\mathrm{Tr}(x)} = \prod_{i=0}^{s-1} \theta([x]^{p^i}).$$

Proof. First we check that the right hand side is a pth root of unity:

$$\Big(\prod_{i=0}^{s-1} \theta([x]^{p^i})\Big)^p = \exp\Big(p\sum_{i=0}^{s-1}\sum_{j\geq 0} \frac{[x]^{p^{i+j}}\eta^{p^j}}{p^j}\Big),$$

and since $[x]^{p^s} = [x]$, we can rewrite the right hand side as

$$\exp\Big(p\sum_{i=0}^{s-1}[x]^{p^i}\sum_{j\geq 0} \frac{\eta^{p^j}}{p^j}\Big).$$

Now, we have $\sum_{i=0}^{s-1}[x]^{p^i} \in \mathbb{Z}_p$ since it is preserved by frobenius and is an integral element of an unramified extension of $\mathbb{Q}_p$, so we can write it as the limit of a sequence of elements of $\mathbb{N}^+$. Since for any element $n \in \mathbb{N}^+$ we have

$$\exp\Big(pn\sum_{j\geq 0}\frac{\eta^{p^j}}{p^j}\Big) = E(\eta)^{pn} = \zeta_p^{pn} = 1,$$

we see that $\prod_{i=0}^{s-1}\theta([x]^{p^i})$ is a pth root of unity. In order to figure out which pth root of unity it is, we just have to compute it modulo π^2:

$$\prod_{i=0}^{s-1}\theta([x]^{p^i}) \equiv \prod_{i=0}^{s-1}(1+\pi[x]^{p^i}) \equiv 1+\pi\,\mathrm{Tr}(x) \equiv \zeta_p^{\mathrm{Tr}(x)} \pmod{\pi^2}. \qquad \square$$

For general q, we define $\theta_q(x)$ by

$$\theta_q(x) = \theta(x)\theta(x^p)\cdots\theta(x^{\frac{q}{p}}).$$

It turns out that there is actually more than one power series $\theta(x)$ with the properties given above. Dwork's original construction from [5] was the much more complicated:

$$(1+(\zeta_p-1))^x\prod_{j\geq 1}(1+(\zeta_p-1)^{p^j})^{\frac{x^{p^j}-x^{p^{j-1}}}{p^j}},$$

where $(1+y)^x$ was defined to be the binomial series $1+xy+\frac{x(x-1)}{2}y+\cdots$ (proving that this infinite product has a large radius of convergence involved a two-variable version of Dwork's Lemma). Another power series which works is given by $\exp(\pi(x-x^p))$ (is this the same as $\theta(x)$?).

6.5 Counting points on hypersurfaces

Let V be the affine hypersurface given by

$$V = \{(x_1,...,x_n) \in \mathbb{A}^n_{\mathbb{F}_q} \mid f(x_1,...,x_n) = 0, x_1\cdots x_n \neq 0\},$$

and let $N_s = |V(\mathbb{F}_{q^s})|$. Our goal is to compute

$$Z(V,T) = \exp\Big(\sum_{s\geq 1}\frac{T^sN^s}{s}\Big).$$

We have

$$q^sN_s = \sum_{\vec{x}\in(\mathbb{F}_{q^s}^\times)^n}\sum_{x_0\in\mathbb{F}_{q^s}}\zeta_p^{\mathrm{Tr}(x_0f(\vec{x}))} = (q^s-1)^n + \sum_{(x_0,\vec{x})\in(\mathbb{F}_{q^s}^\times)^{n+1}}\zeta_p^{\mathrm{Tr}(x_0f(\vec{x}))}.$$

Suppose that $x_0f(\vec{x}) = \sum_{\vec{u}\in\mathbb{N}^{n+1}}a_{\vec{u}}(x_0,\vec{x})^{\vec{u}}$, then since $[a_{\vec{u}}]^{q^i} = [a_{\vec{u}}]$ for all i (since $a_{\vec{u}} \in \mathbb{F}_q$), we have

$$q^sN_s = (q^s-1)^n + \sum_{\vec{x}\in(\mathbb{F}_{q^s}^\times)^{n+1}}\prod_{\vec{u}}\prod_{i=0}^{s-1}\theta_q([a_{\vec{u}}][\vec{x}^{\vec{u}}]^{q^i}).$$

Set $F(\vec{x}) = \prod_{\vec{u}} \theta_q([a_{\vec{u}}]\vec{x}^{\vec{u}})$. If we write $F(\vec{x}) = \sum_{\vec{u}} F_{\vec{u}}\vec{x}^{\vec{u}}$, ten from the definition of θ_q we see that

$$v_p(F_{\vec{u}}) \geq \frac{\mathrm{wt}(\vec{u})}{q-1}.$$

Thus we have

$$\begin{aligned} q^s N_s &= (q^s-1)^n + \sum_{\vec{x}\in\mu_{q^s-1}^{n+1}} \prod_{i=0}^{s-1} F(\vec{x}^{q^i}) \\ &= (q^s-1)^n + (q^s-1)^{n+1} \operatorname{Tr}(\psi\circ F)^s, \end{aligned}$$

and this gives us

$$Z(V,T) = \exp\left(\sum_{s\geq 1} \frac{T^s(q^s-1)^n(1+(q^s-1)\operatorname{Tr}(\psi\circ F)^s)}{q^s s}\right).$$

Defining an operator δ by $h(t)^\delta = \frac{h(t)}{h(qt)}$, we can simplify the above to

$$\begin{aligned} Z(V,qT) &= \exp\left(\sum_{s\geq 1}\frac{T^s}{s}\right)^{(-\delta)^n} \exp\left(\sum_{s\geq 1}\frac{T^s\operatorname{Tr}(\psi\circ F)^s}{s}\right)^{(-\delta)^{n+1}} \\ &= (1-t)^{-(-\delta)^n} \det(1-t(\psi\circ F))^{-(-\delta)^{n+1}}, \end{aligned}$$

and this is p-adically meromorphic since $\det(1-t(\psi\circ F))$ is entire (which followed from the fact that F had radius of convergence strictly greater than 1).

6.6 General varieties

In the previous section, we completed the proof of the fact that every affine hypersurface has a rational zeta function. Now note that if V_1, V_2 are hypersurfaces, then $V_1 \cup V_2$ is *also* a hypersurface, so

$$Z(V_1\cap V_2, T) = \frac{Z(V_1,T)Z(V_2,T)}{Z(V_1\cup V_2,T)}$$

is also a rational function. Generalizing this in the obvious way, we see that if $V_1, ..., V_k$ are affine hypersurfaces, then $Z(V_1\cap\cdots\cap V_k, T)$ is a rational function. Since every closed affine variety is an intersection of finitely many hypersurfaces, this proves rationality for closed affine varieties. Since every affine variety can be written as the difference of two closed affine varieties, this shows that every affine variety has a rational zeta function.

Finally, since every variety V has an open cover $U_1\cup\cdots\cup U_k$ such that all the intersections $U_{i_1}\cap\cdots\cap U_{i_j}$ with $1\leq i_1<\cdots<i_j\leq k$ are affine, an inclusion-exclusion argument lets us write the zeta function for V in terms of the zeta functions of such intersections, so the zeta function of V is also rational.

7 Tony Feng's Notes on Deligne's "La Conjecture de Weil. I"

7.1 Introduction

7.1.1 Weil's conjectures

Let X_0 be a smooth projective variety of dimension n over $\mathbf{F}_q$.

Definition 9. The *zeta function* of X_0 is

$$\zeta(X_0, s) := \prod_{x \in X_0} \left(1 - \frac{1}{q_x^s}\right)^{-1}.$$

This is in obvious analogy to the Riemann zeta function, but it will be more convenient for us to work with the function

$$Z(X_0, t) = \prod_{x \in X_0} \left(1 - t^{-\deg x}\right)^{-1}.$$

We clearly have

$$\zeta(X_0, s) = Z(X_0, q^s).$$

Now we can state Weil's conjectures.

Conjecture 12 (Weil)**.**

1. *$Z(X_0, t)$ is a rational function of t, i.e $Z(X_0, t) \in \mathbf{Q}(t)$, with factorization of the form*

$$Z(X_0, t) = \frac{P_1(t) \dots P_{2n-1}(t)}{P_0(t) \dots P_{2n}(t)}.$$

2. *$Z(X_0, t)$ satisfies a functional equation.*

3. *The roots of $P_i(X_0, t)$ have absolute value $q^{-i/2}$.*

7.1.2 Cohomological formulation

Weil envisioned these conjectures as a consequence of an appropriate cohomology theory for $X := (X_0)_{\overline{\mathbf{F}}_q}$ which would behave analogously to singular cohomology. In particular, (1) should follow from a "Lefschetz trace formula" in $\overline{X}$, with $X(\mathbf{F}_q)$ interpreted as the "fixed points" of Frobenius. The functional equation predicted in (2) should follow from Poincaré duality. The condition (3) is an analogue of Riemann's hypothesis.

This hypothetical cohomology theory was eventually constructed by Grothendieck, and is now called étale cohomology. The purpose of these notes is to explain the main ideas going into the proof of the proof of (3) in its étale cohomological formulation:

> The eigenvalues of Frobenius on $\mathrm{H}^i_{\text{ét}}(X; \mathbf{Q}_\ell)$ are algebraic over $\mathbf{Q}$, with magnitude $q^{i/2}$ under every complex embedding.

Everything here comes from Deligne's article [4], but I have reorganized the presentation, and focused on the simplest cases in order to highlight the key ideas.

7.1.3 Overview of the proof

By simple reductions, one quickly reduces to checking the eigenvalues of Frobenius on the *middle*-dimensional cohomology. To analyze this, one chooses a Lefschetz pencil $f\colon X \to \mathbf{P}^1$, which always exists after possibly blowing up X (and it is easy to see that blowing up doesn't affect the problem).

The idea is then to study the cohomology of $R^n f_* \mathbf{Q}_\ell$ on $\mathbf{P}^1$. This sheaf will be a local system on a dense open subset of $\mathbf{P}^1$, for general reasons of constructibility of proper pushforwards. There are three main ingredients in the argument.

1. A "big image" result on monodromy for a Lefschetz pencil.
2. A rationality result, showing that a certain characteristic polynomial has coefficients $\mathbf{Q}$ (being a priori in $\overline{\mathbf{Q}}_\ell$). This is achieved by an extremely clever "gcd argument", which is quintessentially Deligne.
3. A very clever analytic estimate, finally establishing the desired bound (in view of the previous two ingredients). This is inspired by the Rankin-Selberg method.

We will actually present (3) first, even though it relies on the first two points, because it is the crux of the argument. Then we will go back and indicate how to verify (1) and (2).

7.2 Étale cohomology

The P_i in Weil's conjecture are essentially characteristic polynomials of Frobenius acting on étale cohomology. The intuition to keep in mind is that étale cohomology with coefficients in a *constant* (torsion) sheaf (or more generally, a torsion local system) behaves "like singular cohomology". As we will shortly see, the familiar fundamental results of classical singular cohomology, once phrased invariantly enough, become theorems in étale cohomology.

Remark 13. For *quasi-coherent* sheaves, étale cohomology coincides with coherent cohomology. These won't come up in our discussion.

7.2.1 The orientation sheaf

Here's an example of what I mean. It's commonly said that complex manifolds are canonically oriented, but from an algebraic perspective that's not quite true - you have to choose an orientation for $\mathbb{C}$. This amounts to a choice of $\pm i$, which can be thought of as a choice of embedding of $\mathbf{Q}/\mathbf{Z}$ into the roots of unity.

We're going to be talking about $\mathbf{Q}_\ell$, the ℓ-adic numbers. The orientation sheaf for $\mathbf{Q}_\ell$ involves a choice of the ℓ-power roots of unity. Such a choice is equivalent to a choice of trivialization

$$\varprojlim \mu_{\ell^n} \simeq \varprojlim \mathbf{Z}/\ell^n \simeq \mathbf{Z}_\ell.$$

In any case $\mathbf{Z}_\ell$ acts on $\varprojlim \mu_{\ell^n}$, and we define

$$\mathbf{Q}_\ell(1) = \mathbf{Q}_\ell \otimes_{\mathbf{Z}_\ell} \varprojlim \mu_{\ell^n}.$$

For any n, we define $\mathbf{Q}_\ell(n) = \mathbf{Q}_\ell(1)^{\otimes n}$. For negative n, this is defined by

$$\mathbf{Q}_\ell(n) := \mathbf{Q}_\ell(-n)^\vee.$$

Remark 14. For varieties over finite fields, you can think of this in the following way. $\mathbf{Q}_\ell(n)$ is a $\mathbf{Q}_\ell$-vector space with a natural action of $\mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$, where Frobenius acts as multiplication by q. However, my Frobenius F will always be the *geometric* Frobenius $x \mapsto x^{q^{-1}}$, which acts as multiplication by q^{-1}.

7.2.2 Properties of étale cohomology

Let X be a smooth variety of pure dimension n over an algebraically closed field. (In terms of earlier notation, think $X = (X_0)_{\overline{\mathbf{F}}_q}$.)

1. (*Fundamental class*) There is a fundamental class

$$\mathrm{Tr}\colon \mathrm{H}_c^{2n}(X, \mathbf{Q}_\ell(n)) \xrightarrow{\sim} \mathbf{Q}_\ell.$$

   Equivalently, you can think of this as $\mathrm{Tr}\colon \mathrm{H}_c^{2n}(X, \mathbf{Q}) \xrightarrow{\sim} \mathbf{Q}_\ell(-n)$.

2. (*Cohomological dimension*) X has cohomological dimension $2n$:

$$\mathrm{H}^i(X, \mathbf{Q}_\ell) = 0 \text{ if } i > 2n.$$

3. (*Poincaré duality*) There is a cup product

$$\mathrm{H}^i(X, \mathbf{Q}_\ell) \otimes \mathrm{H}_c^{2n-i}(X, \mathbf{Q}_\ell) \to \mathrm{H}_c^{2n}(X, \mathbf{Q}_\ell) \xrightarrow{\sim} \mathbf{Q}_\ell(-n).$$

   which induces a perfect pairing.

4. (*Lefschetz trace formula*) There's a Lefschetz trace formula

$$\mathrm{Fix}(F) = \#X(\mathbf{F}_q) = \sum_i (-1)^i \,\mathrm{Tr}(F, \mathrm{H}_c^i(X, \mathbf{Q}_\ell)).$$

Everything generalizes to a version with coefficients in a more general local system. It may not be clear how to do that for the last one now, but it should become clear later.

7.2.3 Rationality of the zeta function

Because it will actually be important for us later, we derive the rationality of the zeta function from the above properties. Consider

$$\begin{aligned} t\frac{d}{dt}\log Z(X,t) &= t\frac{d}{dt}\sum_x -\log(1 - t^{-\deg x}) \\ &= t\frac{d}{dt}\sum_{n\geq 1}\frac{x t^{-n\deg x}}{n} \\ &= \sum_{n\geq 1} t^{-n} \sum_{\deg x \mid n} \deg x \end{aligned}$$

Observe that $\sum \deg x \mid n = \#X(\mathbf{F}_{q^n})$, since points of X can be thought of as orbits in $\#X(\mathbf{F}_{q^n})$, of size equal to the their degree. Substituting in the Lefschetz trace formula, we find that this is

$$\sum_{n\geq 1} t^{-n} \sum_i (-1)^i \operatorname{Tr}(F, \mathrm{H}^i_c(X, \mathbf{Q}_\ell) = \sum_i (-1)^i \sum_{n\geq 1} \operatorname{Tr}(F^n, \mathrm{H}^i_c(X, \mathbf{Q}_\ell).$$

Now, recall that for an operator F on a vector space V,

$$t\frac{d}{dt} \log \det(1 - tF, V)^{-1} = \sum_{n\geq 1} \operatorname{Tr}(F^n) t^n.$$

Proof: write $\det(1 - tF) = \prod(1 - t\alpha_i)$, so that this becomes

$$t\frac{d}{dt} \sum_n \sum_i \frac{\alpha_i^n t^n}{n} = \sum_n t^n \sum_i \alpha_i^n.$$

So that tells us that

$$\sum_i (-1)^i \sum_{n\geq 1} \operatorname{Tr}(F^n, \mathrm{H}^i_c(X, \mathbf{Q}_\ell)) = t\frac{d}{dt} \log \det(1 - Ft, \mathrm{H}^i_c(X, \mathbf{Q}_\ell))^{-1}.$$

Substituting this above, we obtain

$$\prod_x (1 - t^{-\deg x}) = \prod_i \det(1 - Ft, \mathrm{H}^i_c(X, \mathbf{Q}_\ell))^{(-1)^{i+1}}.$$

The right hand side predicts the polynomials appearing in Weil's conjectures.

7.3 Some reductions

Let X_0 be a smooth proper variety of dimension n over $\mathbf{F}_q$, and set $X = (X_0)_{\overline{\mathbf{F}}_q}$. Let $RH(\mathrm{H}^i(X))$ denote the statement that

> the eigevalues of F^* on $\mathrm{H}^i(X, \mathbf{Q}_\ell)$ are algebraic with absolute value $q^{i/2}$ under all complex embeddings.

We would like to prove $RH(\mathrm{H}^i(X))$ for $0 \leq i \leq 2n$.

7.3.1 Formalities

If we have an embedding

$$\mathrm{H}^i(X) \hookrightarrow \mathrm{H}^i(X')$$

then $RH(\mathrm{H}^i(X')) \implies RH(\mathrm{H}^i(X))$.

Example 15. If $X' \to X$ the blowup along a closed subvariety $Z \subset X$, then we get such an embedding. We will use the special case where Z is the section by a codimension-2 plane.

If we have a surjection

$$\mathrm{H}^i(X'') \to \mathrm{H}^i(X)$$

then $RH(\mathrm{H}^i(X')) \implies RH(\mathrm{H}^i(X))$.

7.3.2 Poincaré duality

Thanks to the perfect pairing

$$\mathrm{H}^i(X, \mathbf{Q}_\ell) \times \mathrm{H}^{n-i}(X, \mathbf{Q}_\ell) \to \mathbf{Q}_\ell(-n)$$

furnished by Poincaré duality, we automatically know that the $P_i(T) = T^{???} P_{2n-i}(q^n/T)$. In particular, if α is an eigenvalue for F^* on $\mathrm{H}^i(X, \mathbf{Q}_\ell)$ then q^n/α is an eigenvalue for F^* on $\mathrm{H}^i(X, \mathbf{Q}_\ell)$. Therefore,

$$RH(\mathrm{H}^i) \implies RH(\mathrm{H}^{n-i}).$$

The upshot is that it suffices to prove $RH(\mathrm{H}^i)$ for $i = 0, \ldots, n$.

7.3.3 Weak Lefschetz

Let $Y \subset X$ be a general (smooth) hyperplane section. (Since we're over a finite field, this might not exist a priori. But a smooth *hypersurface* section always exists, so we're okay after passing to some large Veronese embedding first.)

Theorem 16 (Lefschetz Hyperplane)**.** *The restriction map* $\mathrm{H}^i(X) \to \mathrm{H}^i(Y)$ *is an isomorphism for* $i < n-1$ *and an injection for* $i = n-1$.

This will be useful for an inductive proof of the theorem. By the preceding reductions, we get for free that the we only need to worry about the *middle* dimension.

7.4 Cohomology of Lefschetz pencils

7.4.1 Introduction to Lefschetz pencils

Most of what we can do for general varieties is bootstrapped from curves, so it is natural to adopt an inductive approach. We've already seen that a hyperplane section of X captures "most" of its cohomology (everything except the middle). To get the rest we'll put X in the"cookie cutter" to get many hyperplane sections. By induction we "know" the cohomology of the hyperplane sections, and then the task is to assemble them together.

A *pencil* of hyperplanes is the set of hyperplanes passing through some codimension-2 plane A, which we call the *axis* of the pencil. This set has a natural structure of a $\mathbf{P}^1$. We have a natural rational map $X \dashrightarrow \mathbf{P}^1$ sending x to the hyperplane spanned by x and A. This is defined away from $A \cap X$. The fibers of this map are points which lie in a common hyperplane through A, i.e. hyperplane sections of X.

We can resolve the indeterminacy of the map by blowing up at the locus $A \cap X$, giving an honest fibration

$$\widetilde{X} \to \mathbf{P}^1.$$

Furthermore,

$$\mathrm{H}^i(X) \hookrightarrow \mathrm{H}^i(\widetilde{X}) = \mathrm{H}^i(X) \oplus \mathrm{H}^{i-2}(X \cap A)(-1)$$

(the last equality by the Thom isomorphism theorem), so by one of reductions it suffices to prove $RH(\mathrm{H}^i(\widetilde{X}))$.

There's an additional technical point in the definition of Lefschetz pencil. The map $\widetilde{X} \to \mathbf{P}^1$ is not smooth, since hyperplane sections can be singular (exactly when the hyperplane becomes

tangent to X). I'll want to choose A generally, so that these singularities are as mild as possible, i.e. simple points. You can think of this as asking that the function $f\colon \widetilde{X} \to \mathbf{P}^1$ be a "morse function". A *Lefschetz pencil* is by definition a fibration $\widetilde{X} \to \mathbf{P}^1$, with singularities as mild as possible. As more precise definition will be given when it is needed, in §7.6.

7.4.2 Monodromy and the spectral sequence

We're going to try to "fit together" the cohomologies of the different hyperplane sections and see what they tell us about the cohomology of the whole thing. This is an obvious setting for a spectral sequence.

$$E_2^{iq} = \mathrm{H}^i(\mathbf{P}^1, R^q f_* \mathbf{Q}_\ell) \implies \mathrm{H}^{i+q}(X, \mathbf{Q}_\ell).$$

Now, since $\mathbf{P}^1$ is a curve we have that $\mathrm{H}^i(\mathbf{P}^1, R^q f_* \mathbf{Q}_\ell)$ vanishes for $i > 2$. Therefore, there are only three groups that we need to worry about, corresponding to $(i, q) = (0, n), (1, n-1)$, and $(2, n-2)$. However, it is clear that in order to analyze them we need to understand the sheaves $R^q f_* \mathbf{Q}_\ell$.

The basic intuition to keep in mind that is that the "constructible sheaf" $R^q f_* \mathbf{Q}_\ell$ is assembled together from its stalks $(R^q f_* \mathbf{Q}_\ell)_u = \mathrm{H}^q(X_u, \mathbf{Q}_\ell)$ using monodromy. Let me explain.

Let $j\colon U \hookrightarrow \mathbf{P}^1$ be the inclusion of the open set where f is smooth. Over U, $R^q f_* \mathbf{Q}_\ell$ restricts to a local system. This means that it is a locally constant $\mathbf{Q}_\ell$ sheaf for the étale topology (with some finiteness assumptions). There is a monodromy action of $\pi_1(U, u)$ on the fibers which determines the local system - in fact, a $\mathbf{Q}_\ell$-local system is equivalent to the data of a finite-dimensional $\mathbf{Q}_\ell$-representation of $\pi_1(U, u)$.

The key is to understand this monodromy action. Its precise nature will be elaborated upon later, but for now it's enough to emphasize that *the monodromy is only non-trivial on the middle-dimensional groups* $\mathrm{H}^{n-1}(X_{\text{ét}}, \mathbf{Q}_\ell)$. In other words, the local systems $R^i f_* \mathbf{Q}_\ell|_U$ are *trivial* except when $i = n - 1$. This fact will be part of the "Picard-Lefschetz" formula for the monodromy to be discussed in the future.

Armed with this knowledge, we can immediately dispose of a couple terms of the spectral sequence. One of them was

$$\mathrm{H}^0(\mathbf{P}^1, R^n f_*(X_u, \mathbf{Q}_\ell) = (\mathrm{H}^n(X_u, \mathbf{Q}_\ell))^{\pi_1} = \mathrm{H}^n(X_u, \mathbf{Q}_\ell).$$

Now, the result follows from induction on the dimension of X.

Remark 17. Actually, it turns out that we need to induct on *even* dimension (for reasons having to do with the Picard-Lefschetz description of monodromy). We can address this issue by taking another hyperplane section of X_u.

The other term $\mathrm{H}^2(\mathbf{P}^1, R^{n-2} f_* \mathbf{Q}_\ell)$ is basically dual to the one just discussed.

Remark 18. There is a difference between $\mathrm{H}^i(U, R^n f_* \mathbf{Q}_\ell)$ and $\mathrm{H}^i(\mathbf{P}^1, R^n f_* \mathbf{Q}_\ell)$, and it will typically happen that $R^n f_* \mathbf{Q}_\ell$ is not a local system, while its restriction to U is a local system. But that's not really an issue, because for any $\mathcal{F}$ on X we have a short exact sequence

$$0 \to j_!(\mathcal{F}|_U) \to \mathcal{F} \to (\text{sum of skyscrapers}) \to 0.$$

which induces a surjection

$$\mathrm{H}^1_c(U, \mathcal{F}) \to \mathrm{H}^1(\mathbf{P}^1, j_* \mathcal{F}) \to 0.$$

Therefore, for our purposes is really is enough to consider the restriction to U.

The last case $\mathrm{H}^1(\mathbf{P}^1, R^{n-1}f_*\mathbf{Q}_\ell)$ is the most subtle. For now we'll just say that there is a short exact sequence

$$0 \to j_*\mathcal{E} \to R^{n-1}f_*\mathbf{Q}_\ell \to (\text{constant sheaf}) \to 0 \tag{1}$$

with $\mathcal{E}$ a sheaf on U, so it suffices to analyze $\mathrm{H}^1(U, \mathcal{E})$ (since H^1 of $\mathbf{P}^1$ with values in a constant sheaf vanishes). The local system $\mathcal{E}$ contains the "vanishing cycles", which are the cohomology classes that vanish in restriction to some special (singular) fiber. The monodromy action is unipotent, and acts by deforming the cohomology by vanishing cycles, so acts trivially on the quotient sheaf (explaining why it is constant).

We will elaborate on this monodromy theory later, but for present purposes it is only to know the following formal facts:

- The monodromy action preserves the subsheaf $\mathcal{E}$.
- The sheaves $\mathcal{E}^\perp$ (orthogonal for the Poincaré pairing) and $R^{n-1}f_*\mathbf{Q}_\ell/\mathcal{E}$ are constant.

7.5 The Fundamental Estimate

7.5.1 Theorem on weights

We are now going to jump into Deligne's estimate on the eigenvalues of Frobenius, *assuming* various auxiliary facts which we have to go back and justifiy later.

We were considering a Lefschetz fibration

$$f\colon X \to \mathbf{P}^1$$

which was smooth over $U \subset \mathbf{P}^1$. This situation is over the algebraic closure $\overline{\mathbf{F}}_q$, but we can assume that everything is defined over $\mathbf{F}_q$, i.e. that the above situation is the base change of

$$f_0\colon X_0 \to \mathbf{P}^1_0$$

which is smooth over $U_0 \subset \mathbf{P}^1$, with everything defined over $\mathbf{F}_q$.

Definition 10. A local system $\mathcal{F}_0$ on X_0 is said to have *weight* β if for all $x \in |X_0|$, the (geometric) Frobenius F_x^* acting on $\mathcal{F}_x$ has eigenvalues which are algebraic with absolute value $q_x^{\beta/2}$ under every complex embedding.

Example 19. In particular, $\mathbf{Q}_\ell(r)$ has weight $-2r$.

Theorem 20. *Suppose $\mathcal{E}_0$ is a sheaf on U_0 satisfying the following conditions:*

1. *$\mathcal{E}_0$ is equipped with an alternating, non-degenerate bilinear form*

$$\psi\colon \mathcal{E}_0 \otimes \mathcal{E}_0 \to \mathbf{Q}_\ell(-\beta).$$

2. *The image of $\pi_1(U, u)$ in $\mathrm{GL}(\mathcal{E}_u)$ is an open subgroup of $\mathrm{Sp}(\mathcal{E}_u, \psi_u)$.*
3. *For all $x \in U_0$, the polynomial $\det(1 - F_x t, \mathcal{E}_0)$ has rational coefficients.*

Then $\mathcal{E}_0$ has weight β.

Remark 21. One can imagine that $\mathcal{E}_0$ is essentially sheaf of vanishing cycles as in (1). (Then $\beta = n-1$.) This is not quite how the argument goes, because we don't know a priori that the restriction of the symplectic form to $\mathcal{E}$ is non-degenerate. (This is true, but only by deduction a posteriori.) This can be easily rectified by considering the filtration by the *constant* sheaf $\mathcal{E} \cap \mathcal{E}^{\perp}$.

The inspiration from the following argument is said to come from ideas of Rankin attacking the Ramanujan conjecture (one of the consequences of Deligne's work).

Recall that

$$t\frac{d}{dt}\log\det(1-F_x t, \mathcal{E}_0) = \sum_{n\geq 1}\mathrm{Tr}(F_x^n)t^n.$$

In particular, since $\mathrm{Tr}(F_x, \bigotimes^{2k}\mathcal{E}_0) = \mathrm{Tr}(F_x, \mathcal{E}_0)^{2k}$ we have that $t\frac{d}{dt}\log\det(1-F_x t, \mathcal{E}_0)$ has positive rational coefficients (the positivity would make no sense without knowing that they were rational!). Therefore, the same holds for

$$\det(1-F_x t, \otimes^{2k}\mathcal{E}_0).$$

Now,

$$Z(U, \otimes^{2k}\mathcal{E}_0, t) = \prod_u \det(1-F_u t, \otimes^{2u}\mathcal{E}_0).$$

The key point is that a product of power series with *positive* coefficients has radius of convergence at most that of any of its factors, since the radius of convergence can be measured by the size of the coefficients of the power series, which *can only increase* by multiplying by a power series with positive coefficients. (If we did not know that the coefficients were positive, then there could be "cancellation of poles" among the factors.)

Now let's consider the Grothendieck-Lefschetz formula for the zeta function:

$$Z(U, \otimes^{2k}\mathcal{E}_0, t) = \frac{P_1(t)}{P_0(t)P_2(t)}.$$

Here $P_0(t) = \det(1-F^* t, \mathrm{H}^0_c(U,\mathcal{E}))$. But a local system on an affine variety has no compactly supported global sections, so $P_0(t) = 1$. What about H^2_c? By duality,

$$\mathrm{H}^2_c(\mathcal{E}_0) \simeq \mathrm{H}^0(\mathcal{E}_0^{\vee})^{\vee}(-1) = ((\mathcal{E}_u^{\vee})^{\pi_1})^{\vee} = (\mathcal{E}_u)_{\pi_1}(-1)$$

Now, since $\pi_1(U,u)$ is open in $\mathrm{Sp}(\mathcal{E}_u)$ it has the same Lie algebra. This is where we use the "big image" assumption! The coinvariants of representation of $\mathrm{Sp}(\mathcal{E}_u)$ coincide with coinvariants for its Lie algebra, so it is equivalent to understand the coinvariants ofr $\mathrm{Sp}(\mathcal{E}_u)$ on $\pi_1(U,u)$. Then $\mathcal{E}_u$ is just the "standard representation" of the symplectic group. This become a classical question about the coinvariants of tensor powers of the standard representation. It is a theorem that the ring of invariants is generated by the tensor symbols $[x,y]$ corresponding to the symplectic form, and so we find that

$$\left(\otimes^{2k}\mathcal{E}_u\right)_{\pi_1} \simeq \bigoplus_{\mathcal{P}'}\mathbf{Q}_\ell(-k\beta)$$

where $\mathcal{P}'$ is a set of partitions of $[1,2k]$ into pairs, corresponding to $[x_i,x_j]$.

The upshot is that $\mathrm{H}^2_c(U, \otimes^{2k}\mathcal{E}) \simeq Q_\ell(-k\beta-1)^N$ for some N. So

$$Z(U_0, \otimes^{2k}\mathcal{E}, t) = \frac{P_1}{(1-q^{k\beta+1}t)^N}.$$

In particular, the only pole is at $t = q^{-k\beta-1}$. Since there are no poles of $Z(U_0, \otimes^{2k}\mathcal{E}, t)$ with $|t| \leq q^{-k\beta-1}$, there are no poles of $\det(1 - F_x t, \otimes^{2k}\mathcal{E}_0)^{-1}$ with $|t| \leq q^{-k\beta-1}$. In other words, there are no zeros of $\det(1 - F_x t, \otimes^{2k}\mathcal{E}_0)$ with absolute value less than $q^{-k\beta-1}$. The zeros are the inverses of the eigenvalues of Frobenius raised to $2k$, so for any such zero α we must have

$$|\alpha|^{-2k} \geq q^{-k\beta-1}.$$

Rearranging we get

$$|\alpha| \leq q^{\frac{\beta}{2}+\frac{1}{2k}}.$$

Now we just take $2k \to \infty$ to get the desired upper bound. By Poincaré duality q^β/α is also an eigenvalue, so

$$|q^\beta/\alpha| \leq q^{\beta/2}$$

implies the opposite inequality.

7.5.2 Calculation of Frobenius eigenvalues

We now indicate how to complete the calculation of Frobenius eigenvalues. The induction is actually a little subtler than we suggested before, because of the way one needs to use the tensor power trick. The reason is that at some point we need to replace X by a large cartesian power, so we cannot induct on the dimension all at once. Instead, we prove a certain estimate by induction, and then go back and refine it using the tensor power trick.

The statement to be proved by induction is:

> Let $X_0/\mathbf{F}_q$ be a smooth projective variety of even dimension d. Every eigenvalues α of F^* on $\mathrm{H}^d_c(X, \mathbf{Q}_\ell)$ is algebraic and has absolute value
>
> $$q^{\frac{d}{2}-\frac{1}{2}} \leq |\alpha| \leq q^{\frac{d}{2}+\frac{1}{2}}. \tag{2}$$

The induction we started will establish this. Then, by considering X^k for large k (the tensor powe trick) and using the Künneth formula, one refines this inequality to the desired equality.

So it remains to establish the bound (2) for the eigenvalues of Frobenius on $\mathrm{H}^1_c(\mathbf{P}^1, \mathcal{E}_0)$, where now we take $\mathcal{E}_0$ to be the sheaf of vanishing cycles as in (1). The zeta function is

$$\prod_u \det(1 - F_u^* t, \mathcal{E}_u)^{-1} = Z(U, \mathcal{E}_0, t) = P_1(t). \tag{3}$$

The zeros of $P_1(t)$ are the inverses of the Frobenius eigenvalues. Now, this is manifestly an ℓ-adic polynomial, but also a power series with *rational* coefficients by our assumptions, hence a rational polynomial. This shows that the eigenvalues are rational.

We want to control the zeros of $P_1(t)$, which are the zeros of $Z(U, \mathcal{E}_0, t)$. We would like to say that by the Euler product (3), the zeros of $P_1(t)$ occur at the zeros of $\prod_u \det(1 - F_u^* t, \mathcal{E}_u)^{-1}$. The zeros of this product occur at zeros of the individual factors, but there are none!

The issue is that the product expansion (3) only holds for small t. It is valid where it converges, so what we would like is for it to converge for $|t| < q^{-\beta/2}$. In fact it just barely fails; it only converges for $|t| < q^{-\beta/2-1}$. By the tensor power trick and Poincaré duality, we can upgrade this bound to the desired equality.

We have $\det(1 - F_u^* t, \mathcal{E}_u) = \prod(1 - \alpha_{i,u} t)$. Therefore, it suffices to analyze when

$$\sum_{i,u} \alpha_{i,u} t$$

converges. We know that $|\alpha_{i,u}| = q^{\beta \deg u/2}$, so we can regroup the sum as

$$\sum_u \sum_n q^{n\beta/2} \# U(\mathbf{F}_{q^n}) t^n.$$

What is $\# U(\mathbf{F}_{q^n})$? Well U is off from $\mathbf{A}^1$ by just a finite set of points, so $\# U(\mathbf{F}_{q^n}) \leq \mathbf{A}^1(\mathbf{F}_{q^n}) = q^n$. So the conclusion is that the sum is

$$\sum_n q^{n(1+\beta/2)} t^n$$

and thus converges for $|t| < q^{-(1+\beta/2)}$.

We're almost done. We proved that $\mathrm{H}^1(U, \mathcal{E}_0)$ has eigenvalues of magnitude

$$q^{\beta/2-1} \leq |\alpha|.$$

By Poincaré duality, we can conclude for free that

$$q^{\beta/2-1} \leq |\alpha| \leq q^{\beta/2+1}.$$

This is what precisely the estimate (2) that we wanted.

7.6 Monodromy theory of Lefschetz pencils

We now want to go back and substantiate some of the claims about Lefschetz pencils that we used. The setup of interest is that we have a fibration

$$f \colon X \to \mathbf{P}^1$$

such that

1. X is non-singular of dimension $n + 1$
2. f is proper,
3. f has non-degenerate critical points, i.e. the only singular points of the singular fibers are simple double points.

The third condition is essentially that of being a "morse function".

In such a situation, f will be smooth outside a finite set of points $S \subset \mathbf{P}^1$. If U is the open complement, then $R^i f_* \mathbf{Q}_\ell$ will be a loca system on U, and we want to understand the monodromy action of $\pi_1(U, u)$ on $(R^i f_* \mathbf{Q}_\ell)_u = \mathrm{H}^i(f^{-1}(u), \mathbf{Q}_\ell)$.

7.6.1 Existence of Lefschetz pencils

This situation arose from taking a pencil of hyperplane sections of a smooth projective $X \subset \mathbf{P}^N$ along an axis A, and blowing up along $A \cap X$. Why does a pencil of the desired form exist? The picture is clarified by looking at the *dual variety* $X^\vee \subset (\mathbf{P}^N)^\vee$. The points of $(\mathbf{P}^N)^\vee$ are the hyperplanes of $\mathbf{P}^N$, and $X^\vee$ is the subset of hyperplane tangent to some point of X. In other words, it is the image of the incidence correspondence

$$\Sigma = \{(x, H) \subset X \times (\mathbf{P}^N)^\vee \mid H \supset T_x X\}. \tag{4}$$

By dimension counting, Σ has dimension $\dim X + (N - \dim X - 1) = N - 1$, so $X^\vee$ has dimension at most $N - 1$. A pencil of hyperplanes is the same as a literal pencil $\mathbf{P}^1 \subset (\mathbf{P}^N)^\vee$ (linearly embedded). It turns out that if it avoids the singular locus and intersects $X^\vee$ transversely, then it will be a Lefschetz pencil. This is a local calculation which we leave as an exercise to the reader.

7.6.2 The local theory

Let's consider the classical case first: suppose we have a map $f\colon X^{n+1} \to D$ where is an open unit disc in $\mathbb{C}$, which is smooth outside 0 and such that $X_0 := f^{-1}(0)$ has a double point.

It turns out (but is not obvious) that X deformation retracts to X_0, so we have an isomorphism

$$\mathrm{H}^i(X_0, \mathbb{C}) \simeq \mathrm{H}^i(X, \mathbb{C}).$$

On the other hand, if t denotes some generic non-zero point of D then we have a restriction map

$$\mathrm{H}^i(X_0, \mathbb{C}) \simeq \mathrm{H}^i(X, \mathbb{C}) \to \mathrm{H}^i(X_t, \mathbb{C}).$$

The image consists of the "monodromy invariants" under the monodromy action of $\pi_1(D^*, t) \simeq \mathbf{Z}$ on $\mathrm{H}^i(X_t, \mathbb{C})$. Let γ be a generator of $\pi_1(D^*, t)$.

Definition 11. We define the *vanishing subspace* to be $\mathrm{H}^n(X_0, \mathbb{C})^\perp \subset \mathrm{H}^n(X_t, \mathbb{C})$ under the pairing induced by Poincaré duality.The elements of $\mathrm{H}^n(X_0, \mathbb{C})^\perp$ will be referred to as *vanishing cycles*.

Here are the essential facts:

- The vanishing subspace is a line, with generator denoted δ.
- γ acts trivially on $\mathrm{H}^i(X_t, \mathbb{C})$ for $i \neq n$.
- For $x \in \mathrm{H}^n(X_t, \mathbb{C})$, γ acts by $x \mapsto x \pm (x, \delta)\delta$.

Remark 22. The $\pm$ depends on n mod 4.

It is straightforward to write down the algebro-geometric analogue. We replace D by the spectrum of a (strictly henselian) DVR, with special point s and generic point η, so we have maps

$$\mathrm{H}^i(X_s, \mathbf{Q}_\ell) \simeq \mathrm{H}^i(X, \mathbf{Q}_\ell) \to \mathrm{H}^i(X_{\overline{\eta}}, \mathbf{Q}_\ell).$$

Now the possibilities are a little complicated. First, they depend on whether n is odd or even. Fortunately we're only going to discuss the even case, so we can ignore that. It is also possible that there is no vanishing cycle, i.e. $\delta = 0$, which makes things easier (no monodromy means everything is a local system). The interesting case is the one where

$$\gamma(x) = x + (x, \delta)\delta \tag{5}$$

so this is the one we're going to discuss.

7.6.3 The global theory

We have a Lefschetz pencil

$$f\colon X \to \mathbf{P}^1.$$

This is smooth outside a finite set S. We choose a baseopint $u \notin S$. For each $s \in S$, we get a vanishing cycle δ_s, and a loop γ_s such that for $x \in \mathrm{H}^n(X_u := f^{-1}(u), \mathbf{Q}_\ell)$

$$\gamma_s(x) = x \pm (x, \delta_s)\delta_s.$$

Definition 12. We define the subspace of (global) *vanishing cycles* $E \subset \mathrm{H}^n(X_u)$ to be the span $\langle \delta_s \colon s \in S \rangle$.

Proposition 11. *The space E is stable under the monodromy action, and its orthogonal complement (for the Poincaré pairing) $E^\perp$ is the monodromy invariants.*

This obvious from the nature of the Picard-Lefschetz formula. Therefore, we rename $E = E/E^\perp$ and forget that $E^\perp$ exists.

Theorem 23. *The vanishing cycles δ_s are conjugate under the monodromy action.*

Proof. We give an argument in the classical case, i.e. for varieties over $\mathbb{C}$, and implicitly invoking an equivalence between the étale and analytic settings. (This is also what Deligne does.)

Consider the incidence correspondence $\Sigma \subset X \times \mathbf{P}^\vee$ from (4). Let $D \subset \mathbf{P}^\vee$ be the hyperplanes cutting out the Lefschetz pencil. Then $S = D \cap X^\vee$ is precisely the set of points where the Lefschetz pencil is not smooth, and we want to show that the vanishing cycles are all conjugate by $\pi_1(D - S, u)$. By the Lefchetz Hyperplane Theorem, for a general choice of D we have

$$\pi_1(D - S, u) \twoheadrightarrow \pi_1(\mathbf{P}^\vee - X, u).$$

Therefore, it suffices to show that the vanishing cycles are conjugate under $\pi_1(\mathbf{P}^\vee - X, u)$. To do this, we will argue that there is an element in $\pi_1(\mathbf{P}^\vee - X, u)$ taking γ_s to $\gamma_{s'}$. Indeed, we can just draw a loop in $\mathbf{P}^\vee - X$ that follows γ_s until it is very close to s, then moves to s' and winds once around it, and then returns along its original path. □

7.6.4 Proof of "big image"

Corollary 5. *The representation of $\pi_1(U, u)$ on E is irreducible.*

Proof. Note that $\gamma_s x = x \pm (x, \delta_s)\delta_s$. Take some non-zero $x \in F$. Then $(x, \delta_s) \neq 0$ for some s, so

$$\gamma_s x - x = \pm(x, \delta_s)\delta_s.$$

Therefore, $\delta_s \in F$. But since the δ_s are all conjugate, they must then all lie in F. □

Theorem 24. *The image of $\rho\colon \pi_1(U, u) \to \mathrm{Sp}(E)$ is open.*

Proof. The image is some compact ℓ-adic Lie group. It suffices to show that its Lie algebra $\mathfrak{L}$ is open.

Note that the $\mathfrak{L}$ is generated by automorphisms of the form

$$d(x \mapsto x \mp (x, \delta_s)\delta_s) = (x \mapsto \pm(x, \delta_s)\delta_s).$$

In slightly more generality, we claim that if V is any irreducible representation of $\mathfrak{L}$, equipped with an invariant non-degenerate symplectic form $(\cdot,\cdot)$, and such that $\mathfrak{L}$ is generated by endomorphisms of the form $x \mapsto \psi(x,\delta)\delta$, then $\mathfrak{L} = \mathrm{Sp}(V,\psi)$.

For any $\delta \in V$, define $N(\delta) \in \mathrm{End}(V)$ by

$$N(\delta)(x) = \psi(x,\delta)\delta.$$

We know that $\mathcal{L}$ is generated by elements of this form. We're going to try to argue that $N(\delta)$ for *every* δ is in $\mathcal{L}$. This at least produces many elements of $\mathcal{L}$, and we leave it as an exercise to verify that they are enough to generate $\mathfrak{sp}(V,\psi)$.

Let W be the set of $\delta \in V$ such that $N(\delta) \in \mathcal{L}$. We know at least that this is non-empty, and we want to show that it is very big. We're going to do that by arguing that it is an invariant subrepresentation of V. Note that at present, is it not even clearly a subspace! However, it is at least obviously closed under scaling.

Since $N(\delta)$ is nilpotent, the endomorphism $\exp(N(\delta))$ makes sense. We want to show that $\exp(N(\delta))$ preserves W for any $\delta \in W$. It will be enough to show that $\exp(\lambda N(\delta))$ preserves ψ and $\mathcal{L}$, since W is defined in terms of these. These statements are familiar (at least by analogy) from classical Lie theory:

- $N(\delta)$ preserves ψ, in the sense that

  $$\psi(N(\delta)x, y) + \psi(x, N(\delta)y) = 0.$$

  This is just what it means for $\mathcal{L} \subset \mathfrak{sp}(V,\psi)$.

- Notice that since $N(\delta)$ has square 0, the automorphism $\exp(N(\delta))$ makes sense. We claim that $\mathrm{Ad}\exp(N(\delta))$ preserves $\mathcal{L}$. You should think of this as analogous to "$\mathrm{Ad}\, G$ preserves $\mathfrak{g}$", and crank out the calculation if you aren't convinced. (I have done it!)

Now comes an important calculation. For a scalar $\lambda \in \mathbf{Q}_\ell$, we have

$$\exp(\lambda N(\delta'))\delta'' = \delta'' + \lambda\psi(\delta'',\delta')\delta'.$$

This implies that if δ' and δ'' are in W, and $\psi(\delta'',\delta') \neq 0$, then the whole subspace spanned by δ' and δ'' is in W. This almost shows that W is a subspace, but not quite. We know that W is closed under sums of *non-orthogonal* vectors.

What we *can* conclude is that W is the union of its maximal linear subspaces, which must furthermore be pairwise mutually orthogonal. Suppose there is more than one such, say W' and W''. Since neither can be stable under $\mathcal{L}$, by the irreducibility of V, some $N(\delta) \in \mathcal{L}$ doesn't preserve W', say $N(\delta)$ takes $w' \in W'$ out of W'. Then $N(\delta)w'$ is orthogonal to w'. But the image of $N(\delta)$ is the line spanned by δ, so $N(\delta)w' = 0$, a contradiction.

□

7.7 The rationality theorem

Finally we are going to justify the rationality assumption of Theorem 20.

7.7.1 Setup

Let's recall the setup. We have a Lefschetz pencil

$$f\colon X \to \mathbf{P}^1$$

smooth over an open subscheme $U \subset \mathbf{P}^1$ which is the complement of S. We have a local system $\mathcal{E} \subset R^n f_* \mathbf{Q}_\ell|_U$ on U consisting of the "vanishing cycles", where $\dim X = n+1$. The cup product on the cohomology of the fibers of f induces a pairing

$$\psi\colon R^n f_* \mathbf{Q}_\ell \otimes R^n f_* \mathbf{Q}_\ell \to \mathbf{Q}_\ell(-n).$$

The vanishing cycles are preserved by monodromy, and the pairing restricts to one on $\mathcal{E}$, which is non-degenerate on

$$\psi\colon \mathcal{E}/(\mathcal{E} \cap \mathcal{E}^\perp) \otimes \mathcal{E}/(\mathcal{E} \cap \mathcal{E}^\perp) \to \mathbf{Q}_\ell(-n).$$

Lastly, this whole situation is defined over a finite field $\mathbf{F}_q$, and we denote by $X_0, U_0, S_0, \mathcal{E}_0$, etc. the corresponding objects over $\mathbf{F}_q$. What we want to prove is:

Theorem 25. *For all $u \in |U_0|$, the polynomial $\det(1 - F_u^* t, \mathcal{E}_0/(\mathcal{E}_0 \cap \mathcal{E}_0^\perp))$ has rational coefficients.*

We are going to argue as follows. We know that the zeta function of X_u is rational, and this zeta function is

$$Z(X_u, t) = \prod_{i=0}^{2n} \det(1 - F_u^* t, R^i f_{0*} \mathbf{Q}_\ell)^{(-1)^{i+1}}.$$

This can be compared to the polynomial in question. The filtrations

$$0 \to \mathcal{E}_0 \to R^n f_{0*} \mathbf{Q}_\ell \to R^n f_{0*} \mathbf{Q}_\ell / \mathcal{E}_0 \to 0$$

and

$$0 \to \mathcal{E}_0 \cap \mathcal{E}_0^\perp \to \mathcal{E}_0 \to \mathcal{E}_0/(\mathcal{E}_0 \cap \mathcal{E}_0^\perp) \to 0$$

cut up $R^n f_{0*} \mathbf{Q}_\ell$ into $\mathcal{E}_0$ and pieces which are *constant* on U_0. This gives a factorization

$$Z(X_u, t) = Z_s(t) \cdot Z_b(t)$$

where Z_s contains the factors corresponding to the local systems with **s**mall small monodromy, and Z_b contains the factors corresponding to $\mathcal{E}_0/(\mathcal{E}_0 \cap \mathcal{E}_0^\perp)$ (b for "big monodromy"). More precisely,

$$\begin{aligned} Z_s(t) = \det(1 - F_u^* t, \mathcal{E}_0 \cap \mathcal{E}_0^\perp)^{(-1)^{n+1}} &\times \det(1 - F_u^* t, R^n f_{0*} \mathbf{Q}_\ell / \mathcal{E}_0)^{(-1)^{n+1}} \\ &\times \prod_{i \neq n} \det(1 - F_u^* t, R^i f_* \mathbf{Q}_\ell)^{(-1)^{i+1}}. \end{aligned}$$

and

$$Z_b(t) = \det(1 - F_u^* t, \mathcal{E}_0/(\mathcal{E}_0 \cap \mathcal{E}_0^\perp)).$$

Of course, $Z_b(t)$ is the term that we are interested in showing has rational coefficients. We know that $Z(X_u, t) \in \mathbf{Q}(t)$, so it suffices to show that $Z_s(t) \in \mathbf{Q}(t)$.

Now, the local systems appearing in $Z_s(t)$ are not quite constant, but they are constant after base change to $\overline{\mathbf{F}}_q$. It is worth recording an observation about this situation:

Lemma 26. *Let $\mathcal{G}_0$ be a $\mathbf{Q}_\ell$-local system on $\epsilon\colon U_0 \to \mathbf{F}_q$ whose base change to U is constant. Then there are units $\alpha_i \in \mathbf{Q}_\ell$ such that for all $x \in |U_0|$, we have*

$$\det(1 - F_u^* t, \mathcal{G}_0) = \prod_i (1 - \alpha_i^{\deg x} t).$$

Proof. Indeed, the hypothesis implies that $\mathcal{G}_0$ is pulled back from a sheaf G_0 on $\operatorname{Spec} \mathbf{F}_q$, namely $G_0 := \epsilon_* \mathcal{G}_0$ (since the hypothesis says that $\epsilon^* \epsilon_* \mathcal{G}_0 \to \mathcal{G}_0$ is an isomorphism after base change to $\overline{\mathbf{F}}_q$).

Then F_u acts as $\mathrm{Frob}^{-\deg u}$, and we can take α_i as in

$$\det(1 - Ft, G_0) = \prod_i (1 - \alpha_i t).$$

□

Let $\mathcal{F}_0 = \mathcal{E}_0/(\mathcal{E}_0 \cap \mathcal{E}_0^\perp)$. Applying the Lemma to the product $Z = Z_s \cdot Z_f$, we find that

$$Z(X_u, t) = \frac{\prod_i (1 - \alpha_i^{\deg u} t)}{\prod_j (1 - \beta_j^{\deg u} t)} \cdot \det(1 - F_u^* t, \mathcal{F}_0).$$

Since the left side is in $\mathbf{Q}(t)$, so is the right side. To complete the proof, we will argue that the α_i and β_j lie in $\mathbf{Q}$.

7.7.2 Overview of the proof

The strategy for proving rationality of α_i, β_j is as follows. First, we may assume that there are no coincidences between the α_i and β_j, since we can just delete them in pairs. We will try to show that the *family* of functions in $\mathbf{Q}_\ell(t)$

$$P_u(t) = \frac{\prod_i (1 - \alpha_i^{\deg u} t)}{\prod_j (1 - \beta_j^{\deg u} t)} \cdot \det(1 - F_u^* t, \mathcal{F}_0)$$

varying with u, allows us to reconstruct the α_i and β_j. Since every member of this family is rational, this will show that the α_i and β_j are rational.

For example, we will try to characterize $\prod (1 - \beta_j^{\deg u} t)$ as being the denominator of $P_u(t)$. The difficulty is that the factors coming from $\det(1 - F_u^* t, \mathcal{F}_0)$ might "accidentally" cancel some of the $(1 - \beta_j^{\deg u} t)$. The key point is that this can only happen to a very limited extent, because $\mathcal{F}_0$ has big monodromy (by Theorem 24): this suggests that F_u^* behaves like a "random" element of $\mathrm{Sp}((\mathcal{F}_0)_u)$, as u varies. In particular, the eigenvalues of a random family of elements $\{F_u\}$ will behave very differently from the family of eigenvalues $\{\beta_j^{\deg u}\}$.

The fundamental technical lemma, which makes the preceding intuition precise, is the following.

Proposition 12. *Let $(\gamma_i)_{1 \le i \le P}$ and $(\delta_j)_{1 \le j \le Q}$ be two families of numbers in $\overline{\mathbf{Q}}_\ell$. Assume that $\gamma_i \neq \delta_j$ for any i, j. Then there is a finite exceptional set K of integers $\neq 1$, and an exceptional set L of density 0 in $|U_0|$, such that for $u \in |U_0|$ with $k \nmid \deg u$ for all $k \in K$ and $u \notin L$, the denominator of*

$$\frac{\prod_i (1 - \gamma_i^{\deg u} t)}{\prod_j (1 - \delta_j^{\deg u} t)} \det(1 - F_u^* t, \mathcal{F}_0)$$

written irreducibly is exactly $\prod_j (1 - \delta_j^{\deg u} t)$.

In the next subsection we will complete the proof of rationality *assuming* Proposition 12. Then we will go back and verify Proposition 12.

7.7.3 Proof of Theorem 25

As discussed, Proposition 12 gives an *intrinsic characterization* of the set $\{(\beta_j^{\deg u})_j\}_u$ in terms of the family $\{P_u(t)\}_u$, which we know to have rational coefficients. A slightly subtle point is to show that this actually pins down $\{\beta_j\}$, which is the content of the following Lemma. Once we know that, it will show that $\beta_j \in \mathbf{Q}$.

Lemma 27. *Let K be any finite set of integers not containing 1 and $(\delta_j)_{1\leq j\leq Q}, (\epsilon_j)_{1\leq j\leq Q}$ two families of elements of a field. If for all sufficiently large n not divisible by the members of K we have $\{\delta_j^n\} = \{\epsilon_j^n\}$ then $\{\delta_j\} = \{\epsilon_j\}$.*

Proof. By induction, it suffices to show that $\delta_Q = \epsilon_j$ for some j. Consider the set of exponents n for which we have

$$\delta_Q^n = \epsilon_j^n.$$

This equality is clearly closed under addition and subtraction, hence forms an *ideal* of $\mathbf{Z}$, necessarily of the form (n_j). If none of these ideals (as j varies) is the unit ideal, then we can find an arbitrarily large integer which is not divisible by any n_j or member of K. But hypothesis tells us that such an integer lies in some (n_j), which is a contradiction. □

We next try to give an intrinsic characterization of the α_i.

Proposition 13. *Let $(\gamma_i)_{1\leq i\leq P}$ and $(\delta_j)_{1\leq j\leq Q}$ be two families of numbers in $\overline{\mathbf{Q}}_\ell$. Set*

$$R(t) = \prod_i (1-\gamma_i t)$$
$$S(t) = \prod_j (1-\delta_j t).$$

Suppose that for all $u \in |U_0|$ we have the divisibility

$$\prod_i (1-\delta_j^{\deg u} t) \mid \left[\prod_i (1-\gamma_i^{\deg u} t)\det(1-F_u^* t, \mathcal{F}_0)\right].$$

Then $S(t) \mid R(t)$.

Once this is established, it provides the following "recognition principle" for the α_i. Consider the family (varying with u)

$$\prod_i (1-\alpha_i^{\deg u} t)\det(1-F_u^* t, \mathcal{F}_0) \in \mathbf{Q}[t].$$

Consider the collection of ($\delta_j \in \mathbf{Q}_\ell$), possibly with multiplicities, such that for all u

$$\prod_j (1-\delta_j^{\deg u} t) \mid \left[\prod_i (1-\alpha_i^{\deg u} t)\det(1-F_u^* t, \mathcal{F}_0)\right].$$

Proposition 13 tells us that each $\prod_j (1-\delta_j t)$ divides a unique maximal such polynomial, which must then be equal to $\prod_i (1-\alpha_i t)$.

Proof of Proposition 13. Apply Proposition 12 to the family of polynomials

$$\frac{\prod_i(1-\gamma_i^{\deg u}t)}{\prod_j(1-\delta_j^{\deg u}t)}\det(1-F_u^*t,\mathcal{F}_0).$$

By hypothesis the denominator is usually 1, so $S(T) \mid R(T)$. □

7.7.4 Proof of Proposition 12

For a geometric point $\overline{u}$ of U_0, *arithmetic fundamental group* $\pi_1(U_0,\overline{u})$ admits a surjection onto $\mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$ whose kernel is the *geometric fundamental group* $\pi_1(U,\overline{u})$:

$$0 \to \pi_1(U,\overline{u}) \to \pi_1(U_0,\overline{u}) \to \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q) \to 0.$$

The monodromy action of $\pi_1(U_0,\overline{u})$ on $\mathcal{F}_{\overline{u}}$ defines a representation

$$\rho\colon \pi_1(U_0,\overline{u}) \to \mathrm{GSp}(\mathcal{F}_{\overline{u}})$$

which restricts to the previous considered monodromy representation on the geometric fundamental group:

$$\pi_1(U,\overline{u}) \to \mathrm{Sp}(\mathcal{F}_{\overline{u}}).$$

Let μ be the homothety character of $\mathrm{GSp}(\mathcal{F}_{\overline{u}})$. Then we know that the product of projection to $\widehat{\mathbf{Z}}$ and ρ takes $\pi_1(U_0,\overline{u})$ into the subgroup

$$H \subset \widehat{\mathbf{Z}} \times \mathrm{GSp}(\mathcal{F}_{\overline{u}})$$

of (n,g) such that

$$q^n = \mu(g).$$

Let

$$\rho_1\colon \pi_1(U_0,\overline{u}) \to H$$

denote this representation, and let H_1 be the image of ρ_1.

Lemma 28. *The image* H_1 *of* ρ_1 *is open in* H*.*

Proof. We know that H_1 surjects onto $\widehat{\mathbf{Z}}$, and by Theorem 24 the image of the geometric monodromy subgroup in $\mathrm{Sp}(\mathcal{F}_{\overline{u}})$ is open. □

Lemma 29. *For any* $\delta \in \overline{\mathbf{Q}}_\ell$*, the set* Z *of* $(n,g) \in \mathrm{H}_1$ *such that* δ^n *is an eigenvalue of* g *is closed of measure* 0*.*

Proof. The closedness is obvious. Fix $n \in \widehat{\mathbf{Z}}$, and let $\mathrm{GSp}(\mathcal{F}_{\overline{u}})_n$ denote the subset of g such that $\mu(g) = q^n$. This is a torsor for $\mathrm{Sp}(\mathcal{F}_{\overline{u}})$. It is easily verified that $Z_n := Z \cap \mathrm{GSp}(\mathcal{F}_{\overline{u}})_n$ is the points of a closed algebraic subvariety, which is necessarily of density 0. Thus, we have verified that "fiberwise over $\widehat{\mathbf{Z}}$ the subset Z has density 0. The result then follows from Fubini's Theorem. □

Finally we can complete the proof of Proposition 12. For each i and j, the set of exponents n such that

$$\gamma_i^n = \delta_j^n$$

is obviously closed under addition and multiplication, hence forms an ideal in $\mathbf{Z}$ of the form (n_{ij}). By hypothesis, $n_{ij} \neq 1$. Take K to be the union of the n_{ij}. By the preceding lemma and Cebotarev's density theorem, the set of $u \in |U_0|$ such that $\delta_j^{\deg u}$ is an eigenvalue of F_u is of density 0. □

References

[1] J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.

[2] Jasbir S. Chahal. Manin's proof of the Hasse inequality revisited. *Nieuw Arch. Wisk. (4)*, 13(2):219–232, 1995.

[3] Jasbir S. Chahal, Afzal Soomro, and Jaap Top. A supplement to Manin's proof of the Hasse inequality. *Rocky Mountain J. Math.*, 44(5):1457–1470, 2014.

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

[5] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.*, 82:631–648, 1960.

[6] Richard H. Hudson and Kenneth S. Williams. Binomial coefficients and Jacobi sums. *Trans. Amer. Math. Soc.*, 281(2):431–505, 1984.

[7] René Schoof. *Algebraic curves and coding theory*. Dipartamento di matematica. Università degli studi di Trento, 1990.

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