Statement of the Weil Conjectures & proof for curves via the Hodge index theorem

Talk summary

- state Weil conjectures
- proof Riemann Hypothesis for curves.

Thm (Weil conjectures)

(i) X scheme of finite type over $\mathbb{F}_q$, then $\exists\ \alpha_1, \dots, \alpha_r, \beta_1, \dots \beta_s \in \overline{\mathbb{Z}}$ such that for $n \geq 1$

$$\#X(\mathbb{F}_{q^n}) = \alpha_1^n + \dots + \alpha_r^n - \beta_1^n - \dots - \beta_s^n.$$

(ii) If X is a proper smooth variety over $\mathbb{F}_q$ of dimension d,

$$\#X(\mathbb{F}_{q^n}) = \sum_{j=1}^{b_0} \alpha_{0,j}^n - \sum_{j=1}^{b_1} \alpha_{1,j}^n + \dots$$

$$+ \sum_{j=1}^{b_{2d}} \alpha_{2d,j}^{n}$$

- b_i are the <u>ℓ-adic Betti numbers</u>

  $b_i = b_{2d-i}$

- $\alpha_{i,j} \in \overline{\mathbb{Z}}$ the $\alpha_{i,*}$ are the $q^d / \alpha_{2d-i,*}$ in some order.

- <u>Riemann Hypothesis</u> $|\alpha_{ij}| = q^{i/2}$ $\forall i,j$ and all archimedean $|\ |$ on $\mathbb{Q}(\alpha_{i,j})$.

If X geometrically irreducible

$b_0 = b_{2d} = 1$

$\alpha_{0,1} = 1, \quad \alpha_{2d,1} = q^d.$

(iii) X smooth proper scheme over a finitely generate subring

$R \subseteq \mathbb{C}$, and $\mathfrak{m} \subseteq R$ is maximal ideal of R, then $R/\mathfrak{m}$ is a finite field, so $X_{R/\mathfrak{m}}$ is smooth proper over $R/\mathfrak{m}$.

$$b_i = \operatorname{rk} H^i(X(\mathbb{C}), \mathbb{Z})$$

for $i = 0, \ldots, 2d$.

Curves

If X is nice (smooth, projective, geometrically integral) curve of genus g over $\mathbb{C}$, then

$$H^0(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}$$
$$H^1(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g}$$
$$H^2(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}.$$

Analogously, if X is nice genus g curve over $\mathbb{F}_q$,

$$b_0 = 1, \quad b_1 = 2g, \quad b_2 = 1.$$

Weil conjectures: $(a_{0,1}=1,\ a_{2,1}=q)$

$$\#X(\mathbb{F}_{q^n}) = 1-(\lambda_1^n+\cdots+\lambda_{2g}^n)+q^n$$

---

where $\lambda_i \in \overline{\mathbb{Z}}$ and $\lambda_{g+i} = q/\lambda_i$

for $1 \le i \le g$, and

(RH) $|\lambda_i| = q^{1/2}$ for $1 \le i \le 2g$.

<u>Corollary</u> (Hasse-Weil bound).

X is nice genus g curve over $\mathbb{F}_q$,

$$\#X(\mathbb{F}_q) = q+1-\varepsilon$$

where $|\varepsilon| \le 2g\sqrt{q}$. //

<u>Def</u> X is scheme of finite type over $\mathbb{Z}$, define

$$\zeta_X(s) := \prod_{\substack{\text{closed} \\ p\in X}} (1-(\#k(p)^{-s}))^{-1}.$$

Converges for $re(s) \geq r$ for some r.

$\zeta(s) = \zeta_{\mathrm{Spec}\, \mathbb{Z}}(s)$.

<u>Def</u> X is scheme of finite type over $\mathbb{F}_q$,

$$Z_X(T) := \exp\left(\sum_{n\geq 1} \# X(\mathbb{F}_{q^n}) \cdot \frac{T^n}{n}\right)$$

$$\in \mathbb{Q}[[T]].$$

<u>Prop</u>. If X f. type / $\mathbb{F}_q$, then it's also f. typer over $\mathbb{Z}$, and

$$\zeta_X(s) = Z_X(q^{-s}).$$

<u>Proof</u>. $\# X(\mathbb{F}_{q^n}) = \sum_{d \mid n} d N_d$, where

N_d = number of degree d closed

points on X. $\square$

Restatement of Weil conjectures

Thm (i) X is scheme of finite type over $\mathbb{F}_q$, the $Z_X(T)$ is a rational function in $\mathbb{Q}(T)$, of the form

$$Z_X(T) = \frac{(1-\beta_1 T)\cdots(1-\beta_s T)}{(1-\alpha_1 T)\cdots(1-\alpha_r T)}$$

$\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in \overline{\mathbb{Z}}$.

(ii) X is smooth proper dim d variety over $\mathbb{F}_q$,

$$Z_X(T) = \frac{P_1(T)\, P_3(T) \cdots P_{2d-1}(T)}{P_0(T) P_2(T)\, P_4(T) \cdots P_{2d}(T)}$$

where $P_i(T) \in \mathbb{Z}[T]$

- <u>(RH)</u> $P_i(T) = \prod_{j=1}^{b_i} (1-\alpha_{ij} T)$

with $|\alpha_{ij}| = q^{i/2}$ $\forall\ i, j$ and

any archimedean $|\ |$ on $\mathbb{Q}(\alpha_{ij})$

- Functional equation

$$Z_X\left(\frac{1}{q^d T}\right) = \pm\, q^{d\chi/2} \cdot T^{\chi} \cdot Z_X(T)$$

where $\chi := b_0 - b_1 + b_2 - \cdots + b_{2d}$

is Euler characteristic.

If X is geometrically irreducible,

$$P_0(T) = 1 - T, \quad P_{2d}(T) = 1 - q^d \cdot T.$$

(iii) same as before

Proof of RH for curves

Note

$$Z_X(T) = \prod_{\substack{\text{closed} \\ P \in X}} \frac{1}{(1 - T^{\deg P})}$$

$$= \sum_{\substack{\text{effective} \\ \text{divisors } D}} T^{\deg D}$$

Riemann-Roch $\rightsquigarrow$

$$Z_X(T) = \frac{P(T)}{(1-T)(1-qT)}$$

where $P(T) \in \mathbb{Z}[T]$ which factors as $P(T) = (1-\lambda_1 T) \cdots (1-\lambda_{2g} T)$.

Functional equation:

$$Z_X\left(\frac{1}{qT}\right) = q^{1-g} \cdot T^{2-2g} \cdot Z_X(T).$$

<u>Prop</u>. The RH stating $|\lambda_j| = q^{1/2}$ $\forall j$ is equivalent to

$$\left| \# X(\mathbb{F}_{q^n}) - 1 - q^n \right| \leq 2g \cdot q^{n/2}$$

for $n \geq 1$.

<u>Proof</u>. ($\Rightarrow$) is clear. ($\Leftarrow$)

Assume bound. Then

$$\sum_{j=1}^{2g} \frac{1}{1-\lambda_j z} = \sum_{n=0}^{\infty} \underbrace{\left(\sum_{j=1}^{2g} \lambda_j^n\right)}_{} z^n$$

since $|\#X(\mathbb{F}_{q^n}) - 1 - q^n|$

$= |\lambda_1^n + \cdots + \lambda_{2g}^n| \le 2g \cdot q^{n/2}$,

the series converges for $|z| < q^{-1/2}$.

The LHS can't have pole at z with $|z| < q^{-1/2}$, so $|\lambda_j| \le q^{1/2}$ for all j. The func. eq. $\Rightarrow$ $|\lambda_j| \ge q^{1/2}$, so $|\lambda_j| = q^{1/2}$. $\forall j$. $\square$

Let V be a smooth projective surface over an algebraically closed field.

Riemann-Roch for surfaces For D a divisor on V, let

$$h^i(D) = \dim H^i(V, \mathcal{O}(D))$$

$K = K_V$ be canonical divisor on V

$p_a = \chi(\mathcal{O}) - 1$ is arithmetic genus.

Then

$$h^0(D) - h^1(D) + \underbrace{h^0(K-D)}_{\leftarrow h^2(D)}$$

$$= p_a + 1 + \frac{1}{2}(D \cdot (D-K)).$$

Adjunction formula C curve on V,

$$\deg K_C = (K_V + C) \cdot C.$$

Lemma For a divisor D and a hyperplane section H,

$$h^0(D) > 1 \Rightarrow D \cdot H > 0.$$

Proof. Since $h^0(D) \geq 1$, we can assume D is effective and nonzero.

We can also assume that $H = V \cap H'$

H' intersects D properly. Then

$$D \cap H = D \cap H' \neq \emptyset,$$

$\Rightarrow D \cdot H > 0.$ $\square$

Thm (Hodge Index theorem). For a divisor D, hyperplane section H,

$$D \cdot H = 0 \Rightarrow D \cdot D \leq 0.$$

Proof.

Fact: Suppose $h^0(D) > 0$, $\exists f \neq 0$ such that $D + (f) \geq 0$. Then for any D'

$$h^0(D + D') = h^0(D + (f) + D')$$

$\geq h^0(D')$.

Contrapositive: $D.D > 0 \Rightarrow D.H \neq 0$.

STS $D.D > 0 \Rightarrow h^0(mD) > 1$

for some $m \in \mathbb{Z}$, because

$$D \cdot H = \frac{1}{m}(mD \cdot H) \neq 0$$

by the lemma $mD \cdot H > 0$.

Suppose $D.D > 0$, by Riemann-Roch

$$h^0(mD) + h^0(K - mD)$$
$$\geq \underbrace{\frac{D.D}{2}}_{>0} m^2 - \frac{D.K}{2} m + p_a + 1.$$

Thus for any $m_0 \geq 1$ we can find $m > 0$ such that

$$h^0(mD) + h^0(K - mD) \geq m_0 + 1$$

$$h^0(-mD) + h^0(K+mD) \geq m_0 + 1.$$

Suppose for contradiction that

$$h^0(mD),\ h^0(-mD) \leq 1$$

Then $h^0(K-mD),\ h^0(K+mD) \geq m_0$.

By Fact

$$h^0(2K) = h^0(K-mD+K+mD)$$

$$\geq h^0(K-mD)$$

$$\geq m_0 \qquad \forall m_0.$$

This impossible. $\square$

<u>Corollary</u> (of Hodge Index).

If D is divisor on V, such that $D^2 > 0$, and $D' \cdot D = 0$, then $(D')^2 \leq 0$.

<u>Proof</u>. Suppose <u>$D^2 > 0, D'^2 > 0$</u>,

$D' \cdot D = 0$. Consider

$$0 \to H^{\perp} \to \mathrm{Pic}(V) \xrightarrow{\cdot H} \mathbb{Z}.$$

subgroup $\mathbb{Z}D + \mathbb{Z}D' \subseteq \mathrm{Pic}(V)$

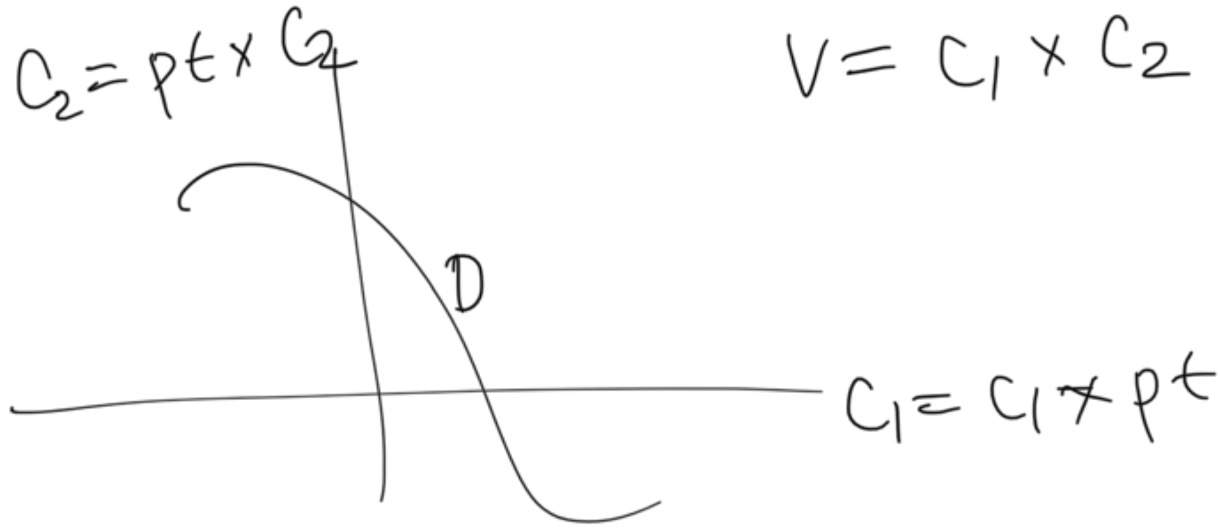
$$\cong \mathbb{Z}^2$$

can't inject into $\mathbb{Z}$, so there's some $mD + nD' \in H^{\perp}$. Hodge index thm $\Rightarrow (mD + nD')^2 \leq 0$.

$\square$

Castelnuovo-Severi inequality

$V = C_1 \times C_2$



D is some divisor on V

$C_1 \cdot C_1 = C_2 \cdot C_2 = 0$

$C_1 \cdot C_2 = 1$.

Let $d_1 = D \cdot C_1$, $d_2 = D \cdot C_2$.

Thm. If D divisor on V,

$$D^2 \le 2 d_1 d_2 .$$

Proof. Apply corollary

$$(C_1 + C_2)^2 = 2 > 0$$

$$(D - d_1 C_2 - d_2 C_1) \cdot (C_1 + C_2) = 0$$

So

$$(D - d_1 C_2 - d_2 C_1)^2 \le 0 .$$

$$\Rightarrow D^2 \le 2 d_1 d_2 .$$

$\square$

Def. Equivalence defect of D

$$\operatorname{def}(D) := 2 d_1 d_2 - D^2 \ge 0 .$$

Cor. For D, D' divisors on V,

we have

$$|D \cdot D' - d_1 d_2' - d_2 d'| \le \left(\operatorname{def}(D)\operatorname{def}(D')\right)^{\frac{1}{2}}.$$

<u>Proof</u>. $\operatorname{def}(mD + nD') \geq 0$

for any $m, n \in \mathbb{Z}$.

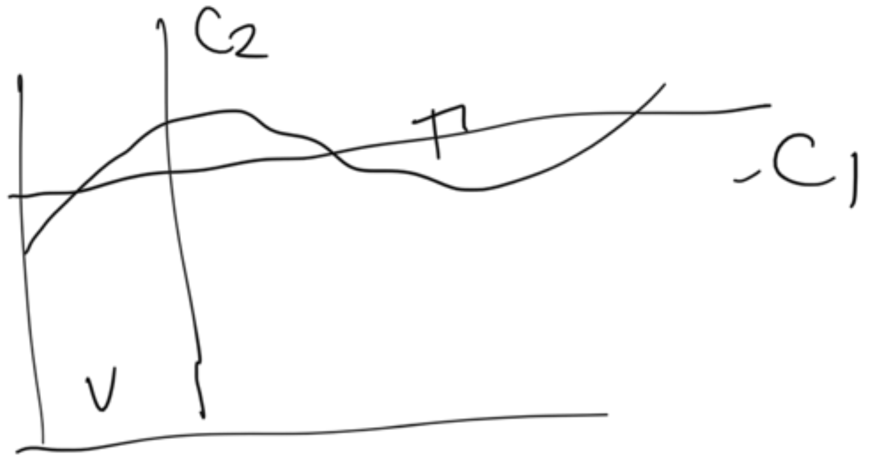
Expand:

$$m^2 \cdot \operatorname{def}(D) - 2mn(D \cdot D' - d_1 d_2' - d_2 d_1') + n^2 \operatorname{def}(D') \geq 0.$$

This means discriminant $b^2 - 4ac \leq 0$.

$\Rightarrow$ inequality. $\square$

<u>Ex</u>. $f: C_1 \to C_2$ nonconstant morphism, suppose C_i genus g_i.



Γ = graph of f.

$d_1 = \deg f$, $d_2 = 1$.

<u>Adjunction</u> formula $\Rightarrow$

$$\deg K_\Gamma = (K_V + \Gamma)\cdot\Gamma,$$

Since $K_V = K_{C_1} \times C_2 + C_1 \times K_{C_2}$,

$$2g_1 - 2 = \Gamma^2 + (2g_1 - 2)\cdot 1 + (2g_2 - 2)\cdot \deg f.$$

$$\Rightarrow \quad \mathrm{def}(\Gamma) = 2g_2 \cdot \deg(f). \quad //$$

Proof of RH for curves

Let X be projective smooth curve

over $\mathbb{F}_q$ of genus g.

Let $X' = X \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$.

Let $\pi : X' \to X'$ be frobenius endomorphism of X'. Let Γ be its graph. Let $\Delta \subseteq X' \times X'$ be diagonal.

$$\deg \pi = q$$
$$\deg(id) = 1.$$

Example $\Rightarrow$

$$\operatorname{def}(\Delta) = 2g \quad , \operatorname{def}(\Gamma) = 2g \cdot q.$$

Then by corollary ($b^2 \leq 4ac$)

$$|\Delta \cdot \Gamma - 1 - q| \leq 2g\sqrt{q}.$$

since $\Delta \cdot \Gamma = \# X(\mathbb{F}_q)$, done $\square$.

Flatness

Def. A module B over a commutative ring A is flat if the functor $- \otimes_A B$ is exact.

Ex.

(i) free modules, vectors spaces

(ii) A module over a DVR or Dedekind domain is flat iff it is torsion free.

(iii) localizations $S^{-1}A$ of A are flat.

Def. A morphism $f: X \to Y$ of schemes is flat at $x \in X$ if $\mathcal{O}_{X,x}$ is a flat $\mathcal{O}_{Y,f(x)}$-module, and f is flat if it's flat at every $x \in X$.

Def. $f: X \to Y$ is faithfully flat if it's flat and surjective.

Def. For a topological space X its dimension $\dim X$ is the supremum of nonnegative n such that $\exists$ a chain

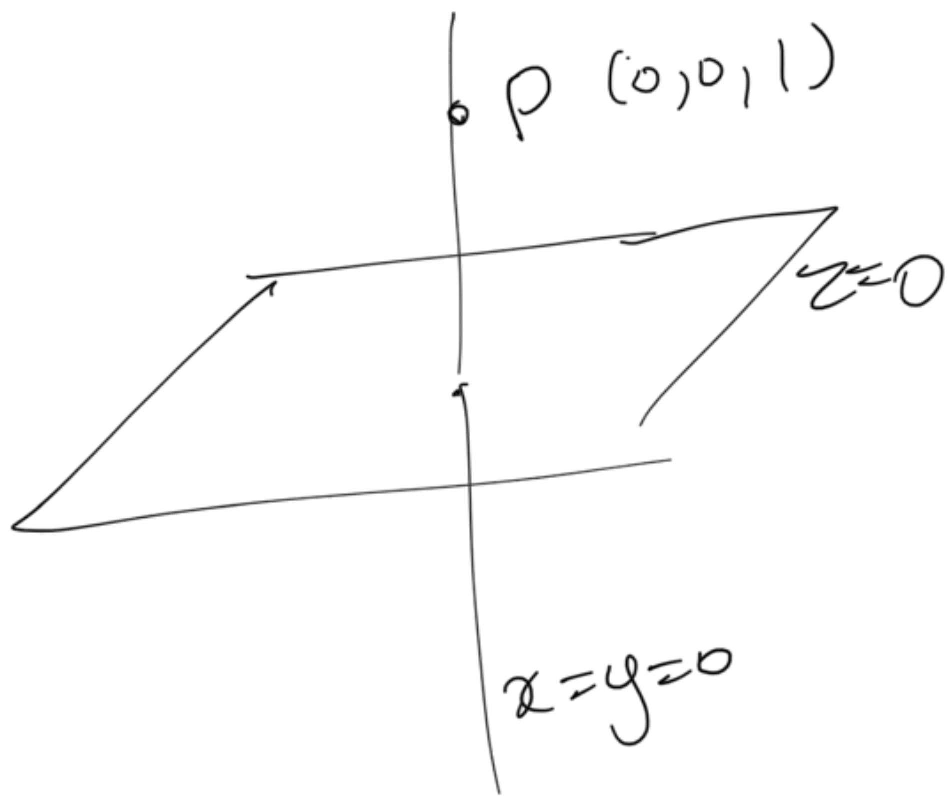
$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n \subseteq X$$

of irreducible closed subsets of X.
And for $x \in X$, dimension of X at x

$$\dim_x X := \inf \{ \dim U : x \in U \overset{\text{open}}{\subseteq} X \}$$

Note that $\dim X = -\infty$ iff $X = \emptyset$.

Ex $X \subseteq \mathbb{A}^3_k$



$\dim X = 2$, $\dim_p X = 1$.

Thm Let X be a scheme that is locally of finite type over k. Let $x \in X$, then

$$\dim_x X = \dim \mathcal{O}_{X,x} + \operatorname{trdeg}(k(x)/k).$$

Property of flat morphisms:

Def. Let $f : X \to S$ is a continuous map of top'l spaces, and $x \in X$. The relative dimension of X over S at x

$$\dim_x f := \dim_x f^{-1}(f(x)).$$

Prop If $f : X \to S$ is a flat k-morphism of irreducible k-varieties, then

$$\dim_x f = \dim X - \dim S,$$

is independent of X. //