Seminars

Nir Elber

Fall 2025

Abstract

This semester, I will just record all seminars I go to in an uncategorized manner. I will try to record the date, the speaker, and which seminar it was to maintain some semblance of organization.

Contents

1 September 3: Arthur Representations and the Unitary Dual

This talk was given by David Vogan at MIT for the Lie groups seminar.

1.1 The Orbit Method

Given a group G, we would like to understand its unitary representations, which more or less amounts to understanding the unitary dual of G. There is a long history of trying to solve this problem for various classes of groups G, and we will focus on reductive groups, roughly speaking because it is suitable for inductive arguments. In particular, we will focus on real reductive groups.

Our story begins with the ideas of Bertram Kostant. This is the method of coadjoint orbits, which explains where one should look for representations of Lie groups. The point is that unitary representations provide operators on a Hilbert space, as do quantum mechanical systems, so one might want to undo the quantization. It turns out then that a unitary representation un-quantizes to a Hamiltonian G-space, which is a symplectic manifold with G-action (and a moment map).

> ⚠ **Idea 1.** Irreducible representations of G correspond to a quantization of covers of coadjoint orbits.

One must make precise what a quantization is, which is not known in general.

Anyway, the point is that want to construct our unitary representations geometrically (which amounts to quantizing coadjoint operators), and then we want to show that we have all them. For real reductive groups, there are not so many kinds of coadjoint orbits.

- Hyperbolic (diagonalizable with real eigenvalues): quantization is real parabolic induction. Here, parabolic induction takes unitary representations to unitary representations.

- Elliptic (diagonalizable with non-real eigenvalues): quantization is cohomological parabolic induction. Here, we take unitary representations (of some Levi subgroups) to unitary representations under some positivity requirement on the codomain.

- Nilpotent: quantization is not totally understood, though something partial was suggested by Arthur and worked out completely by other authors.

In total, here is how one can construct unitary representations using the orbit method.

1. Choose a "θ-stable" Levi subgroup $L_\theta \subseteq L_\mathbb{R}$, meaning that it is the centralizer of a compact torus.

2. Fix some unipotent representation π_θ of L_θ.

3. Twist π_θ by a positive unitary character λ of L_θ.

4. Take cohomological induction of $\pi_\theta(\lambda)$ to $\pi_\mathbb{R}(\lambda)$ on $L_\mathbb{R}$.

5. Twist further by some unitary character ν of $L_\mathbb{R}$.

6. Take real induction up to G.

There is even an explicit way to compute the infinitsemial character at the end, and it is explicit when π_θ is a "special" unipotent representation.

> **Remark 2.** One may want the infinitesimal character to be integral, but it is rarely so.

> **Example 3.** We work some of this out for $\mathrm{Sp}_{2n}(\mathbb{R})$.

Proof. Decompose $n = n_r + \cdots + n_1 + n_0$ into nonnegative integers, and we get a Levi subgroup which looks like

$$L_{\mathbb{R}} = \mathrm{GL}(n_m, \mathbb{R}) \times \cdots \times \mathrm{GL}(n_1, \mathbb{R}) \times \mathrm{Sp}(2n_0, \mathbb{R}).$$

Having lots of GLs is fairly typical for Levi subgroups, which one can see by suitably taking subgraphs of the Dynkin diagram. One then choose a compact torus suitably and writes down some $L_\theta \subseteq L_{\mathbb{R}}$. We then see that our orbit method asks for many unipotent representations of groups of smaller rank (mostly GLs or Us) and do some inductions and twisting by controlled characters. ∎

> **Remark 4.** The orbit method cannot provide a complete list of our representations, roughly speaking because of the hyperbolic step. The point is that we only allowed twisting by unitary characters, but sometimes you can twist by a non-unitary character and still end up with a unitary representation at the end due to frequent coincidences.

1.2 Arthur's Conjecture

For the rest of the talk, we will be interested in the following conjecture.

> **Conjecture 5.** Suppose G is a real reductive algebraic group and π is a unitary representation of G having integral infinitesimal character. Then π is an Arthur representation, meaning that we get it from the orbit method.

Much is known: there are no known counterexamples for classical G, nor are there any for G_2 or E_6. However, there are a few counterexamples for some exceptional groups: it fails for two representations of split F_4, at most six representations for split E_7, and at most twenty-seven representations for split E_8. (The "at most" phrase is present here because the definition of Arthur representation is difficult to calculate.)

2 Sepember 8: The Affine Chabauty Method

This talk was given by Marius Leonhardt at Boston University for the number theory seminar.

2.1 The Statement

We are interested in finding the integral solutions to curves, such as hyperelliptic curves. Fix a smooth projective curve X over $\mathbb{Q}$; after removing some finite number of "cusps" $D \subseteq X$ (which are just some closed points), we can form the affine curve Y; today, we will study the S-integral points on Y for some finite set S of primes.

> **Remark 6.** Technically, in order to make sense S-integral points, one should choose a regular model $\mathcal{X}$ of X over $\mathbb{Z}_S$, choose a closure $\mathcal{D}$ of $D \subseteq X$ in $\mathcal{X}$, and set $\mathcal{Y} := \mathcal{X} \setminus \mathcal{D}$. Then, we can speak coherently about S-integral points on $\mathcal{Y}$.

We will want a few more invariants. Choose a basepoint $P_0 \in Y(\mathbb{Q})$, and set g to be the genus of X, r to be the rank of the Jacobian, and n to be the number of geometric points in D. Note we can write $n = n_1 + 2n_2$ for the totally real and (classes) of complex points.

We are interested in making the following classical result effective.

> **Theorem 7** (Siegel)**.** If Y is hyperbolic, then $\mathcal{Y}(\mathbb{Z}_S)$ is finite.

Here is our main result.

> **Theorem 8.** Fix everything as above.
>
> (a) If
> $$r + \#S + n_1 + n_2 - \#D < g + n - 1,$$
> then $\mathcal{Y}(\mathbb{Z}_S)$ is contained in a finite computable subset of $\mathcal{Y}(\mathbb{Z}_p)$.
>
> (b) If we also have $p > 2g + n$, then $\#\mathcal{Y}(\mathbb{Z}_S)$ is bounded above by $\#\mathcal{Y}(\mathbb{F}_p) + 2g + n - 2$ multiplied by the number of reduction types.

> **Remark 9.** This result even works if the genus is 0 or 1!

> **Remark 10.** The reduction type is a piece of combinatorial data $\Sigma = (\Sigma_\ell)_\ell$ partitioning $\mathcal{Y}(\mathbb{Z}_S)$; namely, we choose the component or cusp of $\mathcal{X}_{\mathbb{F}_\ell}$ where the point reduces.

Before stating our modifications, let's recall the usual Chabauty method. Consider the following diagram.

$$
\begin{array}{ccc}
X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\
{\scriptstyle \mathrm{AJ}}\downarrow & & {\scriptstyle \mathrm{AJ}}\downarrow \quad\searrow^{\int} \\
\operatorname{Jac} X(\mathbb{Q}) & \longrightarrow & \operatorname{Jac} X(\mathbb{Q}_p) \xrightarrow[\log]{} \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^\vee
\end{array}
$$

The Jacobian has rank r, and the last cohomology group has dimension g, so $r < g$ provides a nontrivial differential ω for which $X(\mathbb{Q})$ is contained in the set of p-adic points A with $\int_{P_0}^A \omega = 0$. This last condition is computable, which is the point of the method.

2.2 How to Fix Chabauty

Let's say something about the proof of Theorem 8.

- Using logarithmic (instead of holomorphic) differentials, meaning that we allow some simple poles at D, then
$$\dim \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1(D)) = g + n - 1,$$
which exhibits the right-hand side of the inequality in (a).

- One should use generalized Jacobians to build a Jacobian J_Y of Y. For example, one definition is given by $J_Y(K)$ to be the divisors of Y_K of degree zero modulo principal divisors $\operatorname{div} f$ where $f \in K(X)^\times$ has value 1 on D. Notably, J_Y is a semiabelian variety, so it fits into a diagram
$$0 \to T_D \to J_Y \to J \to 0,$$
where T_D is some torus. This means that $J_Y(\mathbb{Q})$ has little chance of being finitely generated, so it is not enough to just write out the same Chabauty diagram as before.

- Instead, we look at $\mathbb{Z}_S$-points. Build the Chabauty diagram as follows.

$$
\begin{array}{ccc}
\mathcal{Y}(\mathbb{Z}_S) & \longrightarrow & \mathcal{Y}(\mathbb{Z}_p) \\
\downarrow & & \downarrow \\
Y(\mathbb{Q}) & \longrightarrow & Y(\mathbb{Q}_p) \\
\downarrow & & \downarrow \quad\searrow^{\int} \\
J_Y(\mathbb{Q}) & \longrightarrow & J_Y(\mathbb{Q}_p) \longrightarrow \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1(D))^\vee
\end{array}
$$

We need to show that the image of $\mathcal{Y}(\mathbb{Z}_S)$ in $J_Y(\mathbb{Q})$ is contained in a (small) finitely generated subgroup; in fact, we can get this rank down to

$$r + \#S + n_1 + n_2 - \#D,$$

from which (a) follows. From here, (b) follows by arguing as in the Chabauty−Coleman method.

- It remains to prove the bound on the rank, which is done using arithmetic intersection theory. Inspired by something with p-adic heights, we may take mod-ℓ intersections of points in $J_Y(\mathbb{Q})$ with reductions of the cusps, and one can compute that $\mathcal{Y}(\mathbb{Z}_S)$ has controlled image.

3   September 9th: Singularities of Secant Varieties

The (pre-)talk was given by Debaditya Raychaudhury at the Harvard−MIT algebraic geometry seminar, and it takes up the first two subsections; it was titled "The Hodge Filtration on Local Cohomology." The rest is from the main talk.

3.1   Properties of Local Cohomology

Fix a subvariety Z of a smooth variety X over $\mathbb{C}$. Then one has local cohomology sheaves $\mathcal{H}_Z^\bullet(-)$, which are understod as the derived functors of $\mathrm{H}_Z^0(-)$, which is the sheaf of sections supported on Z.

> **Example 11.** Locally, we can make everything affine, so say $X = \operatorname{Spec} R$ and $Z = \operatorname{Spec} R/I$. Then $H_I^0(R)$ consists of the $r \in R$ for which $I^k r = 0$ for some k large enough.

We would like to compute these sheaves.

One way is geometric. With $U := X \setminus Z$, we let $j \colon U \hookrightarrow X$ be the inclusion. Then there is an exact sequence

$$0 \to \mathcal{O}_X \to j_* \mathcal{O}_U \to \mathcal{H}^1(\mathcal{O}_X) \to 0$$

and $\mathrm{R}^{q-1} j_* \mathcal{O}_U \cong \mathcal{H}_Z^q(\mathcal{O}_X)$ for $q \geq 2$.

> **Example 12.** Continuing with the affine situation, suppose further that $I = (f)$. Then we get an exact sequence
>
> $$0 \to R \to R_f \to \mathrm{H}_{(f)}^1(R) \to 0,$$
>
> so we can compute $\mathrm{H}_{(f)}^1(R)$ via some Čech complex. In general, with $I = (f_1, \ldots, f_s)$, one builds the Čech complex
>
> $$0 \to R \to \bigoplus_{i_1} R_{f_{i_1}} \to \bigoplus_{i_1 \leq i_2} R_{f_{i_1} f_{i_2}} \to \cdots$$
>
> to compute the cohomology $\mathrm{H}_I^q(R)$; here, the differential maps are the usual ones for the Čech complex. For example, if $q > s$, then $\mathrm{H}_I^q(R) = 0$ automatically!

Thus, we see that $\mathcal{H}_Z^q(\mathcal{O}_X)$ vanishes for q not so large: it vanishes as soon as q is larger than the number of local defining equations. We are now allowed to make the following definition.

> **Definition 13.** We define the *local cohomological dimension* $\operatorname{lcd}(X, Z)$ to be the maximum q such that $\mathcal{H}_Z^q(\mathcal{O}_X)$ is nonzero.

> **Remark 14.** It turns out that the minimal q such that $\mathcal{H}_Z^q(\mathcal{O}_X)$ is equal to the codimension of $Z \subseteq X$, which can be seen by a computation on affines.

> **Remark 15.** As discussed above, if $Z \subseteq X$ is a local complete intersection, then $\mathrm{lcd}(Z, X)$ will equal the codimension.

Thus, we see that the local cohomological dimension does a reasonable job keeping track of singularities.

> **Notation 16.** We define $\mathrm{lcdef}(Z) := \mathrm{lcd}(X, Z) - \mathrm{codim}_X(Z)$

> **Remark 17.** This quantity does not depend on Z! One way to see this is to show that $\mathrm{lcdef}(Z)$ is the maximum j for which
> $$\mathcal{H}^j(\mathbb{Q}_Z^H[\dim Z]) \neq 0,$$
> which is more manifestly independent of X. Here, $\mathbb{Q}_X^H$ is the Hodge module.

3.2   The Hodge Filtration

It turns out that $\mathcal{H}_Z^q(\mathcal{O}_X)$ has the structure of aa filtered $\mathcal{D}_X$-module, where $\mathcal{D}_X$ is defined as the (dual) differential ring, given on affines U by

$$\mathcal{D}_X(U) := \bigoplus_{\alpha \in \mathbb{N}^n} \mathcal{O}_X(U)\partial^\alpha,$$

where $\partial^\alpha = \partial_1^{\alpha_1} \cdots \partial_n^{\alpha_n}$; here ∂_i is dual to dx_i. Approximately speaking, this arises because $\mathcal{H}_Z^q(\mathcal{O}_X)$ is the underling $\mathcal{D}$-module for the filtered module $\mathcal{H}^q(i_* i^! \mathbb{Q}_X^H[z])$, where $i \colon Z \hookrightarrow X$ is the inclusion.

We would like to compute the Hodge filtration $F_\bullet \mathcal{H}_Z^q(\mathcal{O}_X)$. Suppose we have a "resolution of singularities" $f \colon Y \to X$ fitting into a pullback square

$$\begin{array}{ccc} Y \setminus E & \longrightarrow & Y \\ \| & & \downarrow{\scriptstyle f} \\ U & \longrightarrow & X \end{array}$$

where $Z := f^{-1}(Z)$ is some simple normal crossings divisor. Namely, one uses the complex

$$0 \to f^* \mathcal{D}_X \to \Omega_Y^1(\log E) \otimes f^* \mathcal{D}_X \to \cdots \to \omega_Y(E) \otimes f^* \mathcal{D}_X \to 0.$$

Roughly speaking, one hits this with F_{k-n} and computes the image of some cohomology of this complex.

Here is the sort of thing that one can prove.

> **Theorem 18.** Suppose $q \geq 1$ and $\mathcal{H}_Z^k(\mathcal{O}_X) = 0$ for $k > q$. Then $F_\bullet \mathcal{H}_Z^q(\mathcal{O}_X)$ is generated at level ℓ if and only if $\mathrm{R}^{q-1+i} f_* \Omega_Y^{n-i}(\log E) = 0$.

We end this talk by defining one more invariant.

> **Definition 19.** We say that $c(Z) \geq k$ if and only if $F_p \mathcal{H}_Z^q(\mathcal{O}_X) = 0$ for all $p \leq k$ and $q > \mathrm{codim}_X(Z)$.

Roughly speaking, this is expected to "cohomologically" generalize local complete intersections.

> **Theorem 20.** One has $c(Z) \geq k$ if and only if $\mathrm{depth}\, \Omega_Z^p \geq \dim Z - p$ for all $p \leq k$.

> **Theorem 21.** One has that $\dim Z - \mathrm{lcdef}(Z)$ is the minimal value of $\mathrm{depth}\, \Omega_Z^k + k$.

3.3   The Secant Variety

Given an ample line bundle $\mathcal{L}$ on a smooth variety X of dimension n, we get an embedding $X \hookrightarrow \mathrm{H}^0(\mathcal{L})$. Then we define the secant variety Σ as the closure of the line spanned by any pair $x_1, x_2 \in X$.

> **Remark 22.** With $\dim X = n$, we expect $\dim \Sigma = 2n + 1$: each point has n degrees of freedom, and then the line adds another degree of freedom.

> **Example 23.** If X is $\mathbb{P}^1$ embedded in $\mathbb{P}^2$ (via $\mathcal{O}(2)$), then $\Sigma = \mathbb{P}^2$, which is smaller than expected.

> **Example 24.** If X is $\mathbb{P}^2$ embedded in $\mathbb{P}^3$ (via $\mathcal{O}(3)$), then $\dim \Sigma = 3$.

The moral is that Σ only achieves the expected dimension for sufficiently positive line bundles.

> **Proposition 25.** Suppose that $\mathcal{L}$ is 3-very ample (which we won't define), then $\dim \Sigma = 2n + 1$, and the singular locus of Σ is precisely X unless Σ is the whole space.

Thus, we will focus on our secant varieties arising from 3-very ample line bundles.
    With more positivity, we get more.

> **Theorem 26** (Ullery–Chou–Song)**.** If $\mathcal{L} = \mathcal{K}_X + (2n + 2)\mathcal{A} + \mathcal{B}$ where $\mathcal{A}$ is very ample, and $\mathcal{B}$ is nef, then Σ is normal, has DB singularities, is Cohen–Macaulay (CM), weakly rational, and thus has rational singularities if and only if $\mathrm{H}^i(\mathcal{O}_X) = 0$ for all $i > 0$.

To improve this result, one needs to know something about $\mathbb{Q}_\Sigma^H[2n + 1]$, where the H adds emphasizes that it is a Hodge module.

3.4   Mixed Hodge Modules

Let's quickly say something about mixed Hodge modules. Suppose Z is a smooth variety.

> **Definition 27.** A *Hodge module* M is the data of a left $\mathcal{D}_Z$-module M along with a Hodge filtration $F_\bullet M$ on M, satisfying some conditions, together with a $\mathbb{Q}$-perverse sheaf K and isomorphism $\alpha \colon K \otimes_\mathbb{Q} \mathbb{C} \to \mathrm{DR}_Z(M)$, where $\mathrm{DR}_Z(M)$ is the de Rham complex of M.

Here, the de Rham complex is M tensored with

$$\mathcal{O}_Z \to \Omega_Z^1 \to \cdots \to \omega_Z.$$

We remark that once we take graded pieces with respect to F, we get an object in $D^b(\mathrm{Coh}(Z))$.

> **Remark 28.** There is a derived category $D^b(\mathrm{MHM}(Z))$, even when Z fails to be singular, and it admits the six functors. Thus, we may define
> $$\mathbb{Q}_Z^H := p^*\mathbb{Q}_{\mathrm{pt}}^H,$$
> where $p \colon Z \to \mathrm{pt}$ is the constant map.

3.5   Main Result

For our application, we need a log resolution of X. Let $X^{[2]}$ be the Hilbert scheme of lines on X. Then there is a tautological $\Phi \subseteq X^{[2]} \times X$ of pairs (ξ, x) where $x \in \xi$. (Equivalently, Φ is the blow up of $X \times X$ along the

diagonal.) Let $\theta\colon \Phi \to X^{[2]}$ and $q\colon \Phi \to X$ be the projections, so we may define $\mathcal{E} \coloneqq \theta_* q^* \mathcal{L}$. It turns out that $\mathrm{H}^0(\mathcal{E}) = \mathrm{H}^0(\mathcal{L})$, and it turns out that $\mathbb{P}\mathcal{E}$ projects onto Σ. We are now able to draw the following diagram.

$$
\begin{array}{ccccc}
\mathrm{Bl}_{\{x\}} X & \lhook\joinrel\longrightarrow & \Phi & \longrightarrow & \mathbb{P}\mathcal{E} \\
\downarrow & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle t} \\
\{x\} & \lhook\joinrel\longrightarrow & X & \longrightarrow \Sigma & \longrightarrow \mathbb{P}\mathrm{H}^0(\mathcal{L})
\end{array}
$$

The squares are all pullback squares.

Here is our main theorem. Recall that there is a complex $\underline{\Omega}^p_Z$ given by

$$
\mathrm{gr}_{-p} \mathrm{DR}(\mathbb{Q}^H_Z[\dim Z])[p - \dim Z].
$$

> **Theorem 29.** Suppose $\mathcal{L}$ is sufficiently positive.
>
> (a) $\underline{\Omega}^p_\Sigma \cong \Omega^{[p]}_Z$ for all $0 \leq p \leq k$ is equivalent to $\mathrm{H}^i(\mathcal{O}_X)$ for all $1 \leq p \leq k$. In particular, this implies that $\underline{\Omega}^p_\Sigma$ is a sheaf.
>
> (b) $\mathcal{E}xt^i(\Omega^{2n}_\Sigma, \omega^\bullet_\Sigma[-2n - 2]) = 0$ for all $i \geq 1$ if and only if $X \cong \mathbb{P}^1$.
>
> (c) If $\mathcal{L}$ is 3-very ample, and $\Sigma \neq \mathbb{P}^n$, then
>
> $$
> \mathrm{lcdef}(\Sigma) = \begin{cases} n - 1 & \text{if } n \geq 2 \text{ and } \mathrm{H}^1(\mathcal{O}_X) \neq 0, \\ n - 2 & \text{if } n \geq 2 \text{ and } \mathrm{H}^1(\mathcal{O}_X) = 0, \\ 0 & \text{if } n = 1. \end{cases}
> $$

The speaker then did some intricate calculation to prove a partial result of (c), that $\mathrm{lcdef}(\Sigma) \leq n - 1$.

> **Remark 30.** There are other theorems with more calculations of these invariants of secant varieties. For example, under the hypothesis of (c) above, the defect
>
> $$
> \sigma(Z) \coloneqq \dim_\mathbb{Q} \frac{\mathrm{WeilDiv}_\mathbb{Q}(Z)}{\mathrm{CarDiv}_\mathbb{Q}(Z)}
> $$
>
> is finite if and only if $\mathrm{H}^1(\mathcal{O}_X) = 0$, and it is zero if and only if X is $\mathbb{P}^1$.

4   September 10: Unipotent Representations: Changing q to $-q$

This talk was given by George Lusztig at MIT for the Lie groups seminar.

4.1   A Special Basis

For today, G is a split, connected reductive group over $k = \mathbb{F}_q$. Each Weyl element $w \in W$ produces a subvariety X_w of the flag variety $\mathcal{B} \times \mathcal{B}$ (where $\mathcal{B}$ is made of all the Borel subgroups) consisting of the pairs (B, FB) for $w \in \mathcal{O}_w$. It turns out that a unipotent representation of $G(k)$ appears in the cohomology of X_w if and only if it appears in the Euler characteristic.

These unipotent representations have been classified as follows: as the Weyl group W has its irreducible representations in canonical bijection with the conjugacy classes, the unipotent representations also have a classification according to these conjugacy classes. To explain how this bijection works, we give each c a finite group Γ_c, then the unipotent representations are parameterized by pairs (g, ρ) (up to conjugacy) where $g \in \Gamma_c$ and ρ is an irreducible representation of $Z(g)$. We let $M(\Gamma_c)$ be this collection of pairs. For a pair m, we may write ξ_m for the corresponding unipotent representation.

Here is the sort of thing that we are able to prove.

Theorem 31. There is an ordered basis of $\mathbb{C}[M(\Gamma_c)]$ where all the matrices relating the elements are upper-triangular with 1s on the diagonal and otherwise positive entries; in fact, these entries are natural always except for a single c in the case of E_8, in which case the entry is in $\mathbb{Z}[\zeta_5]$.

Remark 32. It turns out that there is a canonical pairing on $\mathbb{C}[M(\Gamma_c)]$ (which is akin to a nonabelian Fourier transform), and the basis of the theorem makes this pairing be represented by a matrix with nonnegative rational entries always except for one exception.

4.2   Negating Dimensions

It turns out that the dimensions of the unipotent representations ξ_m are polynomials in q, and we will write $D(\xi_m)$ for this dimension. We will assume that the long Weyl element is central. By tabulating these dimensions, one can show that there is an involution $(\cdot)'$ on the unipotent representations so that

$$D(\xi')(q) = \pm D(\xi)(-q).$$

However, this involution is not uniquely determined by this property.

Let's try to exhibit this involution. It turns out that $M(\Gamma_c)$ can be viewed as the set of irreducible objects in the tensor category of Γ_c-equivariant vector bundles. Then one can do something categorical.

5   September 11: Statements of the Weil Conjectures

This talk was given by Ari Krishna and Sophie Zhu at MIT for the STAGE seminar.

5.1   Some History

For today, X will be a smooth proper variety over a finite field $\mathbb{F}_q$. Let's give a statement of the Weil conjectures in the spirit of counting points.

Conjecture 33 (Weil)**.** Fix a finite field $\mathbb{F}_q$.

(a) Fix a scheme X of finite type over a field $\mathbb{F}_q$. Then there are algebraic integers $\{\alpha_1, \ldots, \alpha_r\}$ and $\{\beta_1, \ldots, \beta_s\}$ such that

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

for all $n \geq 0$.

(b) Rationality: suppose further that X is proper of equidimension d. Then we can arrange these algebraic integers as

$$\#X(\mathbb{F}_{q^n}) = \sum_{i=0}^{2d} (-1)^i \left(\sum_{j=0}^{b_i} \alpha_{ij}^n \right).$$

(c) Poincaré duality: with X proper, the multi-sets $\{\alpha_{2d-i,j} : 1 \leq j \leq b_i\}$ and $\{q^d/\alpha_{ij} : 1 \leq j \leq b_i\}$ agree.

(d) Riemann hypothesis: with X proper, $|\alpha_{ij}| = q^{i/2}$ for all i and j.

(e) Betti numbers: with X proper, if X admits an integral model $\mathcal{X}$ over some subring $R \subseteq \mathbb{C}$, then b_i is the ith Betti number of $\mathcal{X}(\mathbb{C})$.

The history of these conjectures is long and fraught.

- In the 1930s, Artin, Hasse, and Schmidt proved everything but the Riemann hypothesis for curves, and they proved the Riemann hypothesis for curves of genus at most 1.

- In 1948, Weil proved the Weil conjectures for curves of any genus. This arose by combining two observations: first, counting $\#X(\mathbb{F}_{q^n})$ should equal the number of fixed points of F^n, and second, these counts could be understood in terms of intersection theory with the graph of the Frobenius.

- In 1949, Weil proved the Riemann hypothesis for other varieties, namely certain Fermat varieties. At this point, the conjectures were finally stated.

- In the 1950s, Grothendieck and many others developed the theory of étale cohomology. By rather formal arguments, this proves everyting but the Riemann hypothesis.

- In 1974, Deligne finishes his first proof of the Weil conjectures.

- In 1980, Deligne strengthens his proof of the Weil conjectures.

5.2 ζ-Functions

The Weil conjectures admit an important reformulation in terms of ζ-functions. Let's begin with the classical ζ-function.

> **Definition 34.** The *Riemann ζ-function* $\zeta(s)$ is defined as the analytic continuation of the series
> $$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

The Riemann ζ-function admits the following properties.

- Euler product: one can write $\zeta(s)$ as a product
$$\zeta(s) = \prod_{\text{prime } p} \frac{1}{1-p^{-s}}.$$

- Continuation: there is a meromorphic continuation to the plane, and it has only a simple pole at $s = 1$.

- Functional equation: upon completing the ζ-function as
$$\xi(s) := (s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}+1\right)\zeta(s),$$
we have the functional equation $\xi(s) = \xi(1-s)$.

- Riemann hypothesis: it is expected that the only zeroes of ζ occur at the negative integer integers and along $\{s \in \mathbb{C} : \operatorname{Re} s = 1/2\}$.

This generalizes as follows.

> **Definition 35.** Fix a scheme X of finite type over $\mathbb{Z}$. Then we define the *arithmetic ζ-function* $\zeta_X(s)$ as
> $$\zeta_X(s) := \prod_{\text{closed } \mathfrak{p} \in X} \frac{1}{1 - \#\kappa(\mathfrak{p})^{-s}}.$$

> **Example 36.** The Euler product implies that $\zeta(s) = \zeta_{\operatorname{Spec} \mathbb{Z}}(s)$.

In order to relate this to point-counts, we produce the following definition.

Definition 37. Fix a scheme X of finite type over $\mathbb{F}_q$. Then we define

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

Remark 38. A direct calculation shows that $Z_X(q^{-s}) = \zeta_X(s)$.

We are now able to rewrite the Weil conjectures.

Conjecture 39 (Weil)**.** Fix a finite field $\mathbb{F}_q$.

(a) Fix a scheme X of finite type over $\mathbb{F}_q$. There are algebraic integers $\{\alpha_1,\ldots,\alpha_r\}$ and $\{\beta_1,\ldots,\beta_s\}$ such that
$$Z_X(T)\frac{(1-\beta_1 T)\cdots(1-\beta_s T)}{(1-\alpha_1 T)\cdots(1-\alpha_r T)}$$
for some algebraic integers $\alpha_\bullet$s and $\beta_\bullet$s.

(b) Rationality: let X be a smooth proper variety over $\mathbb{F}_q$ of equidimension d. Then Z_X admits a factorization as
$$\frac{P_1(T)\cdots P_{2d-1}(T)}{P_0(T)\cdots P_{2d}(T)},$$
where $P_i \in 1 + T\mathbb{Z}[T]$ for each T.

(c) Functional equation: with X proper, we have $Z_X(1/q^d T) = \pm q^{d\chi/2}T^\chi Z_X(T)$, where $\pm$ is some sign, and χ is the Euler characteristic.

(d) Riemann hypothesis: with X proper, we have $|\alpha_{ij}| = q^{i/2}$ for all i.

(e) Betti numbers: with X proper, if X admits an integral model $\mathcal{X}$ over some subring $R \subseteq \mathbb{C}$, then $\deg P_i$ is the ith Betti number of $\mathcal{X}(\mathbb{C})$.

These statements are shown to be equivalent by expanding out the definition of Z_X and taking logarithms.

5.3   Proof for Curves

We prove many of the Weil conjectures for curves. By keeping track of completions, we may as well assume that X is smooth and proper. Let's start with rationality.

Proposition 40. Fix a smooth proper curve X over $\mathbb{F}_q$. Then $Z_X(T)$ is a rational function of T.

Proof. The point is to write $Z_X(T)$ out in terms of divisors, which will allow us to use Riemann–Roch. Recall $Z_X(T)$ is the product
$$Z_X(T) = \prod_{\text{closed } p\in X} \left(1 - T^{\deg p}\right)^{-1},$$
which then expands out into the sum
$$Z_X(T) = \sum_{\substack{D\in\text{Div }X \\ D\geq 0}} T^{\deg D},$$
where $D \geq 0$ means that D is effective. There are now two cases: if $\deg D \leq 2g - 2$, we will handle this separately. Otherwise, when $\deg D \geq 2g - 2$, then Riemann–Roch implies that the number of effective divisors with this degree is $\left(q^{d-g+1} - 1\right)/(q - 1)$. (Namely, Riemann–Roch allows one to compute the dimension of

the space of effective divisors with given degree; this is a finite vector space over $\mathbb{F}_q$, so we can now compute its size!) This finishes the proof upon rewriting this out as a geometric series. ∎

> **Remark 41.** By inputting more effort, one can use this proof to prove the functional equation. If one is careful, then one can achieve an expansion
>
> $$Z_X(T) = \frac{f(T)}{(1-T)(1-qT)}$$
>
> for some polynomial $f(T)$ of degree $2g$ with integral coefficients. Note that this includes the Betti numbers conjecture!

We now turn to the Riemann hypothesis, which of course is the hard part. This will depend on the following size bound.

> **Theorem 42** (Hasse−Weil)**.** Fix a smooth proper curve C over a finite field $\mathbb{F}_q$. Then
>
> $$|\#C(\mathbb{F}_q) - (q+1)| \le 2g\sqrt{q}.$$

Let's explain why this produces the Riemann hypothesis. Because we already have an expression

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

we may factor $f(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$, and we note that we are trying to show $|\alpha_i| = \sqrt{q}$ for all i. By the functional equation, it is enough to show merely that $|\alpha_i| \le \sqrt{q}$ for all i. Now, by definition of $Z_X(T)$, we see that

$$\sum_{n\ge 1} \#C(\mathbb{F}_{q^n})T^n = \frac{d}{dT}\log Z_X(T),$$

which can be computed directly to be

$$\sum_{n\ge 1} \#C(\mathbb{F}_{q^n})T^n = \sum_{i=1}^{2g}\left(\frac{-\alpha_i}{1-\alpha_i T} + \frac{1}{1-T} + \frac{1}{1-qT}\right),$$

which after expanding out the geometric series becomes

$$\sum_{n\ge 1} \#C(\mathbb{F}_{q^n})T^n = \sum_{n\ge 1}\left(q^n + 1 - \sum_{i=1}^{2g}\alpha_i^n\right).$$

Thus, the Hasse−Weil bound shows that

$$\left|\sum_{i=1}^{2g}\alpha_i^n\right| \le 2g\sqrt{q^n}.$$

Now, if $|\alpha_i| > \sqrt{q}$ for any i, then we can send $i \to \infty$ to achieve a contradiction because the left-hand side is too large.

5.4   Intersection Theory on a Surface

We will want to know something about intersection theory on a surface. We're in a talk, so we're allowed to just state the result we want.

Theorem 43. Fix a smooth projective surface X over an algebraically closed field k. Then there is a unique integral symmetric bilinear pairing $(\cdot, \cdot)$ on $\mathrm{Div}\, X$ such that any two transverse curves $C, C' \subseteq X$ have

$$(C, C') = \#(C \cap C').$$

There are many ways to the pairing (C, C'). The most geometric is to show that one can always wiggle one of the curves to make the intersection transverse.

   For our bound, we need the following geometric input.

Theorem 44 (Hodge index)**.** Fix a smooth projective surface X over an algebraically closed field k. Further, fix an ample line bundle H in $\mathrm{Div}\, X$. If we are given a divisor D on X which is not linearly equivalent to 0 while $D \cdot H = 0$, then $D \cdot D < 0$.

Proof. We will prove this in steps.

1. Suppose instead that $D \cdot H > 0$ and $D^2 > 0$. Then we claim mD is linearly equivalent to an effective divisor for sufficiently large m. Well, beacuse $D \cdot H > 0$, $(K_X - mD) \cdot H < 0$ for m sufficiently large, so $K_X - mD$ cannot be effective. Thus, $\mathrm{H}^0(K_X - mD) = 0$, so $\mathrm{H}^2(mD) = 0$ by Serre duality. However, by Riemann–Roch for surfaces, one has

$$h^0(mD) = h^1(mD) + \frac{1}{2}mD \cdot (mD - K_X) + \chi(\mathcal{O}_X),$$

   which becomes positive for m large enough.

2. Now, suppose for the sake of contradiction that $D^2 > 0$. Then we can take $H' := D + nH$ to be ample for n large enough, from which we find $D \cdot H' = D^2 > 0$, so the lemma implies that mD is effective for m large enough, which contradicts having $D \cdot H = 0$.

3. Lastly, suppose for the sake of contradiction that $D^2 = 0$. Because $D \cdot H = 0$, we can find an effective divisor E such that $D \cdot E \neq 0$ while $E \cdot H = 0$. Now, consider $D' := nD + E$. One can calculate $(D')^2 > 0$ while $D' \cdot H = 0$, so we reduce to the previous step. ∎

To apply this, we will want to understand ample divisors.

Theorem 45. Fix a divisor D on X. Then D is ample if and only if $D^2 > 0$ and $D \cdot C > 0$ for all irreducible curves C on X.

Here is how this is applied.

Theorem 46. Let $X = C \times C'$ where C and C' are smooth projective curves. Set $\ell := C \times \mathrm{pt}$ and $m := \{\mathrm{pt}\} \times C'$. Then for any divisor D, we have

$$D^2 \leq 2(D \cdot \ell)(D \cdot m).$$

Proof. As a lemma, we claim that if H is ample, then

$$\left(D^2\right) \cdot \left(H^2\right) \leq (D \cdot H)^2.$$

For this, one uses the Hodge index theorem on $E := \left(H^2\right) D - (H \cdot D)H$, from which one can calculate $E^2 < 0$. Thus, as long as $D \neq 0$, we get $\left(D^2\right)\left(H^2\right) - (D \cdot H)^2 < 0$; in all cases, we get the inequality.

   Now, by Theorem 45, the divisor $H := \ell + m$ is ample. Applying the above argument with D' defined as

$$D' = \left(H^2\right)\left(E^2\right) D - \left(E^2\right)(D \cdot H)H - \left(H^2\right)(D \cdot E)E$$

where $E := \ell - m$. ∎

We are now ready to prove the Hasse–Weil bound. We will do intersection theory on the surface $X := C \times C$. Let $\Delta \subseteq X$ be the diagonal, and let $\Gamma \subseteq X$ be the graph. Then $\#C(\mathbb{F}_q) = (\Delta \cdot \Gamma)$, which is what we want to bound. Here are our steps.

1. We claim $\Delta^2 = (2 - 2g)$. By the adjunction formula (note $\Delta \cong C$), we see

$$2g - 2 = \Delta^2 + \Delta \cdot K_X.$$

   However, one can expand out K_X as $\mathrm{pr}_1^* C + \mathrm{pr}_2^* C$, which each have intersection number $2g - 2$ with Δ by using the adjunction formula, so the result follows.

2. We claim $\Gamma^2 = q(2 - 2g)$. By the adjunction formula (note $\Gamma \cong C$), we see

$$2g - 2 = \Gamma^2 + \Gamma \cdot K_X.$$

   After doing the same expansion of K_X, one calculates that $\Gamma \cdot \mathrm{pr}_1^* K_C = q(2g-2)$ and $\Gamma \cdot \mathrm{pr}_2^* K_C = 2g-2$ by using the adjunction formula.

3. We now apply Theorem 46 to $X = C \times C$. Take large integers r and s, and set $D := r\Gamma + s\Delta$. Then $D \cdot \ell = rq + s$ and $D \cdot m = r + s$. From Theorem 46, one calculates that

$$|N - (q+1)| \leq g\left(\frac{rg}{s} + \frac{s}{r}\right),$$

   so the result follows by sending $\frac{r}{s} \to \frac{1}{\sqrt{q}}$.

6 September 15: Rational Points on $X_0(N)^*$ for N Non-Squarefree

This talk was given by Sachi Haschimoto at Boston University of the Boston University number theory seminar. We are discussing joint work with Timo Keller and Samuel Le Fourn.

6.1 Overview

The motivation for our results arises from the following theorem of Mazur.

Theorem 47. Fix a prime p, and let E be an elliptic curve over $\mathbb{Q}$ with (potential) complex multiplication. If E admits a rational isogeny of degree p, then

$$p \in \{2, 3, 5, 7, 13, 37\}.$$

This is proved by classifying the points on certain modular curves.

Definition 48. Fix a positive integer N. Then there is an affine curve $Y_0(N)$ defined over $\mathbb{Q}$ such that $Y_0(N)(K)$ is in bijection with the $\overline{K}$-isomorphism classes of pairs (E, C_N), where E is an elliptic curve over K, and $C_N \subseteq E(K)$ is a cyclic subgroup of order N. We let $X_0(N)$ be the completion, and we set $J_0(N) := \mathrm{Jac}\, X_0(N)$.

Thus, we see that Theorem 47 is equivalent to saying that $Y_0(p)(\mathbb{Q})$ only has CM points except when p is among the listed exceptions: simply take any such elliptic curve E with rational isogeny φ of degree p, and we can produce the pair $(E, \ker \varphi) \in Y_0(p)(\mathbb{Q})$. Equivalently, we may say that $X_0(p)(\mathbb{Q})$ only has CM points or cusps.

Definition 49 (trivial)**.** A modular curve $X_0(N)$ is *trivial* if and only if $X_0(N)(\mathbb{Q})$ only has cusps and CM points.

Remark 50. The exceptional p have $X_0(p) \cong \mathbb{P}^1_{\mathbb{Q}}$ (and therefore must have many points) except for $p = 37$. When $p = 37$, it turns out that $X_0(37)$ is genus 2 and hence hyperelliptic, and one finds that the hyperelliptic involution produces the non-CM, non-cuspidal points.

For this talk, we are interested in certain quotients of $X_0(N)$ rather than $X_0(N)$ itself.

Definition 51 (Atkin−Lehner involution)**.** Fix a positive integer N and a divisor $Q \mid N$ with $\gcd(Q, N/Q) = 1$. Then we define the *Atkin−Lehner involution* $w_Q \colon X_0(N) \to X_0(N)$ by

$$w_Q((E, C_N)) := \left(\frac{E}{C_N[Q]}, \frac{C_N + E[Q]}{C_N[Q]} \right)$$

One can check that this definition is smooth and therefore extends from $Y_0(N)$ to $X_0(N)$. One can also check that $w_Q^2 = \mathrm{id}$.

Remark 52. We see that w_Q also extends to $J_0(N)$ by pullback, and it still has $w_Q^2 = \mathrm{id}$. To relate to modular forms, we note that $S_2(\Gamma_0(N))$ is the cotangent space of $0 \in J_0(N)$, from which it follows that w_Q also acts on $S_2(\Gamma_0(N))$. But $S_2(\Gamma_0(N))$ is just some finite-dimensional complex vector space, so we end up with some linear algebra.

Notation 53. We define $X_0(N)^*$ as the quotient of $X_0(N)$ by all the Atkin−Lehner involutions.

Remark 54. It turns out that rational points of $X_0(N)^*$ (minus cusps) correspond to elliptic curves which are isogenous to all their Galois conjugates, where the isogenies have degree dividing by N.

Here is what is currently known, which is due to many people.

Theorem 55. Fix a positive integer N. If N is a prime-power, and the genus of $X_0(N)^*$ is positive, then all rational points of $X_0(N)^*(\mathbb{Q})$ are trivial, except when $N = 5^3$, in which case there is only one interesting point.

Remark 56. The hardest part of the theorem covers the cases $N \in \{125, 169\}$, where the rank of the Jacobian equals the genus, so one has to work harder to make something like the Chabauty−Coleman method work.

Here is what is expected

Conjecture 57 (Elkies)**.** For N large enough, all rational points on $X_0(N)^*(\mathbb{Q})$ are either CM points or cusps.

6.2 Formal Immersion Method

We will be interested in the following morphisms.

Definition 58 (formal immersion)**.** Fix locally Noetherian schemes X and Y. A map $f \colon X \to Y$ is a *formal immersion* at some point $x \in X$ if and only if it induces an isomorphism of residue fields and is injective on tangent spaces.

Here is how these are used.

> **Theorem 59** (Mazur)**.** Fix a morphism $f\colon X_0(N) \to A$ of schemes over $\mathbb{Z}$, where A is an abelian scheme over $\mathbb{Z}$ of rank 0. Suppose that f is a formal immersion at ∞, where $f(\infty) = 0$. Then any $(E, C_N) \in X_0(N)(\mathbb{Q})$ has E with potentially good reduction at all primes $p > 2$.

The point is that we have upgraded rationality of E to some integrality. Indeed, an equivalent statement is that $j(E) \in \mathbb{Z}[1/2]$.

Sketch. Suppose not. Then E becomes a cusp at some prime p, so by using Atkin−Lehner involutions, one can move E to become ∞ at p. Now, $f((E, C_N)) \in A(\mathbb{Q})$ is torsion because $A(\mathbb{Q})$ is torsion, so because torsion reduces $(\mathrm{mod}\ p)$ injectively, we see that $f((E, C_N)) \equiv f(\infty) \equiv 0 \pmod{p}$ and therefore $f(x) = f(\infty) = 0$. But then our tangent spaces will fail to be injective. ∎

> **Remark 60.** If N is squarefree, then the simple factors of $J_0(N)^*$ over $\mathbb{Q}$ are all expected to have positive rank (by the Birch−Swinnerton-Dyer conjecture), so one does not expect Theorem 59 to be particularly helpful.

Here is what we are able to prove.

> **Theorem 61.** Fix $N \geq 1$ which is not 99 or 147 but is not squarefree and not a prime-power. For any $P \in Y_0(N)^*(\mathbb{Q})$, choose a lift (E, C_N) to $Y_0(N)(K)$ for some number field K. Then
> $$(8 \cdot 3 \cdot 25 \cdot 49 \cdot 31)^N j(E) \in \mathcal{O}_K.$$
> In fact, if $p^2 \mid N$ for some $p \notin \{2, 3, 5, 7, 13\}$, then $j(E) \in \mathcal{O}_K$.

> **Remark 62.** The $N \in \{99, 147\}$ cases have positive rank, so we do not have hope for an integrality statement.

> **Remark 63.** The exponent N is more or less sharp. The 31 is never expected to appear.

Our method proof, following Mazur, uses the following.

> **Theorem 64** (Mazur)**.** If $p \notin \{2, 3, 5, 7, 13\}$, then $J_0(p)^- := J_0(p)/(1 + w_p)$ has a rank zero quotient.

The exceptions arise because $\dim J_0(p) = 0$, so there is no way to find such a quotient. These rank zero abelian varieties are good enough for our purposes most of the time, but we have also proven the following.

> **Theorem 65.** Fix distinct primes p and q with $p \in \{2, 3, 5, 7, 13\}$ and $q > 23$. Then $J_0(pq)^{-p,+q} := J_0(pq)/(1 + w_p, 1 - w_q)$ has a rank 0 quotient.

This is proven using some analytic techniques showing that some L-functions vanish. Now, the point of the proof of the main theorem is to do some reduction of levels to construct formal immersions to abelian varieties of rank 0.

7 September 16: Higher Siegel−Weil Formula for Unitary Groups

This talk was given by Mikayel Mkrtchyan at MIT for the MIT number theory seminar.

7.1 The Kudla Program

Let's start by recalling the classical formulation of the Siegel−Weil formula. An approximate statement is that an Eisenstein series $E(g, s_0)$ is approximately equal to a period $\int_{[H]} \theta(g, h) \, dh$ for some θ-function θ. This was proved for a dual pair (G, H) of reductive groups over a global field F in the case where $(G, H) = (\mathrm{U}(2n), \mathrm{U}(n))$.

The Kudla program geometrizes this into a statement that $E(g, s_0)$ should be equal to the degree of some 0-cycle on a Shimura variety. There is also an arithmetic Siegel−Weil formula, which describes the derivative of the Eisenstein series as the degree of a 0-cycle on the integral model(!) of a Shimura variety.

For this talk, we will be working over function fields. As such, we go ahead and fix a morphism $X' \to X$ of smooth curves over a finite field $k := \mathbb{F}_q$, and we will assume that $X' \to X$ is an étale double cover, where $\sigma \colon X' \to X'$ is the automorphism. We also set $F := k(X)$ and $F' := k(X')$.

With the above motivation in mind, we are now ready to set some notation. Let's describe the automorphic side of our Siegel−Weil formula.

Definition 66 (Siegel−Eisenstein series)**.** Fix the group $G := \mathrm{U}(n, n)$ over a global field, and let $P \subseteq G$ be a parabolic subgroup. Consider the induction

$$\mathrm{Ind}_{P(\mathbb{A})}^{G(\mathbb{A})} \left(\chi \, |\mathrm{det}|^{s + n/2} \right),$$

where χ is some auxiliary character, and $s \in \mathbb{C}$. To produce an automorphic form, we may choose some $\varphi(g, s)$ in this induction satisfying $\varphi(1, s) = 1$, and then we define our Eisenstein series as

$$E(g, s) := \sum_{\gamma \in P(F) \backslash G(F)} \varphi(\gamma g, s).$$

We may normalize this to $\widetilde{E}(g, s)$ via some silent process.

Remark 67. The Eisenstein series $E(g, s)$ admits a Fourier decomposition, indexed by Hermitian $n \times n$ matrices $T \in \mathrm{Herm}_n(F)$. These can alternatively be parameterized by pairs $(\mathcal{E}, a)$ where $\mathcal{E}$ is a vector bundle of rank n, and $a \colon \mathcal{E} \to \sigma^* \mathcal{E}^\vee$ is some map.

We now turn to the geometric side. Instead of Shimura varieties, we are able to use shtukas.

Definition 68. A $\mathrm{U}(n)$-*bundle* on X' is a pair $(\mathcal{F}, h)$ of a rank-n vector bundle on X' and some isomorphism $h \colon \mathcal{F} \to \sigma^* \mathcal{F}$. We let $\mathrm{Bun}_{\mathrm{U}(n)}$ denote the relevant moduli space.

Definition 69. We define the *Hecke modification* $\mathrm{HK}_{\mathrm{U}(n)}^1$ as the collection of tuples $(x, \mathcal{F}_0, \mathcal{F}_1, f_{1/2}, \iota_0, \iota_1)$ where $x \in X'$, $\mathcal{F}_0$ and $\mathcal{F}_1$ are $\mathrm{U}(n)$-bundles, and $\iota_0 \colon \mathcal{F}_{1/2} \to \mathcal{F}_0$ and $\iota_1 \colon \mathcal{F}_{1/2} \to \mathcal{F}_1$ are some maps respeecting the unitary structure.

Remark 70. It turns out that the canonical map $\mathrm{HK}_{\mathrm{U}(n)}^1 \to X' \times \mathrm{Bun}_{\mathrm{U}(n)}$ onto the first two coordinates is a $\mathbb{P}^{n-1}$-bundle.

Definition 71. We define $\mathrm{Sht}_{\mathrm{U}(n)}^r$ as the moduli space of chains of r Hecke modifications

$$\mathcal{F}_0 \to \mathcal{F}_1 \to \cdots \to \mathcal{F}_r,$$

where $\mathcal{F}_r$ is isomorphic to the Frobenius twist of $\mathcal{F}_0$. This is a Deligne−Mumford stack.

17

Remark 72. It turns out that $\dim \mathrm{Sht}^r_{\mathrm{U}(n)} = rn$ for even r and vanishes for odd r. (One should modify the definition slightly to get interesting statements when r is odd.)

With our analogue of Shimura varieties in hand, we are able to define our special cycles.

Definition 73. Fix a pair $(\mathcal{E}, a)$ of a vector bundle $\mathcal{E}$ of rank m and a map $a \colon \mathcal{E} \to \sigma^* \mathcal{E}^\vee$. Then we define the special cycle $Z^r_{\mathcal{E}}(a) \to \mathrm{Sht}^r_{\mathrm{U}(n)}$ to parameterize the data of an r-shtuka

$$\mathcal{F}_0 \to \mathcal{F}_1 \to \cdots \to \mathcal{F}_r$$

equipped with commuting maps $\mathcal{E} \to \mathcal{F}_0$ which commute with our Frobenius twists and pullbacks by σ.

Remark 74. The map $Z^r_{\mathcal{E}}(a) \to \mathrm{Sht}^r_{\mathrm{U}(n)}$ is finite, so we are more or less producing a cycle.

Remark 75. If a in the pair $(\mathcal{E}, a)$ is an isomorphism, then $\mathcal{Z}^r_{\mathcal{E}}(a) \cong \mathrm{Sht}^r_{\mathrm{U}(n-\mathrm{rank}\,\mathcal{E})}$.

Remark 76. The expected dimension of $Z^r_{\mathcal{E}}(a)$ is $r(n - \mathrm{rank}\,\mathcal{E})$.

We are now raedy to state our main theorem.

Theorem 77. Fix the following data.

- A pair $(\widetilde{\mathcal{E}}, \widetilde{a})$, where $\mathrm{rank}\,\widetilde{E} = n$ with $\mathrm{rank}\,\mathrm{im}\,\widetilde{a} = n-1$. Then $Z^r_{\widetilde{\mathcal{E}}}(\widetilde{a})$ is proper, and the degree of the corresponding cycle equals

$$\partial^r_{s=0} \left(\widetilde{E}_{(\widetilde{E}, \widetilde{a})(s)} \right)$$

up to some explicit constant.

8   September 18th: The Étale Site

This talk was given by Yutong Chen for the STAGE seminar at MIT.

8.1   Étale Morphisms

We will be interested in étale morphisms today. Intuitively, they are supposed to be the algebro-geometric version of a covering space in topology. Here is the easiest definition.

Definition 78 (étale)**.** A morphism $f \colon X \to S$ of schemes is *étale* if and only if it is locally of finite presentation, flat, and unramified.

While locally of finite presentation and flatness are fairly common notions, we should define what it means for a morphism to be unramified. We will define this in steps.

Definition 79 (unramified)**.** Fix an extension $A \subseteq B$ of discrete valuation rings with uniformizers π_A and π_B, respectively. Then $A \subseteq B$ is *unramified* if and only if $(\pi_B) = \pi_A \cdot B$ and the extension of residue fields is separable.

Definition 80 (unramified). Fix a map $f: A \subseteq B$ of local rings. Then f is *unramified* if and only if $f(\mathfrak{m}_A) = \mathfrak{m}_B$ and the field extension

$$A/\mathfrak{m}_A \to B/\mathfrak{m}_B$$

is separable.

Definition 81 (unramified). Fix a morphism $f: X \to S$ of schemes. Then f is *unramified* if and only if the local maps

$$\mathcal{O}_{S,f(x)} \to \mathcal{O}_{X,x}$$

are unramified for all $x \in X$.

Example 82. Open and closed immersions are unramified.

Non-Example 83. Consider the squaring map $\mathbb{A}^1_k \to \mathbb{A}^1_k$ given by the ring map $k[t] \to k[t^2]$ defined by $t \mapsto t^2$. Then this map is not ramified at 0. Indeed, this map is locally given by

$$k[t^2]_{(t^2)} \to k[t]_{(t)},$$

but the maximal ideal fails to go to the maximal ideal.

There are many ways to think about étale morphisms.

Definition 84 (étale). A morphism $f: X \to S$ is *étale* if and only if it is smooth of relative dimension 0.

Here is one version of smoothness which is fairly hands-on.

Definition 85 (smooth). Fix a morphism $f: X \to S$. Given $x \in X$, we say that f is *smooth* at x if and only if the morphism locally looks like

$$\operatorname{Spec} \frac{A[t_1, \ldots, t_n]}{(g_{r+1}, \ldots, g_n)} \to \operatorname{Spec} A$$

and the corresponding Jacobian matrix has full rank $n - r$. We may also say that f is smooth of *relative dimension r* in this situation.

Of course, there are also many ways to define smoothness. Here is another useful criterion.

Proposition 86. Fix a flat morphism $f: X \to S$ of irreducible varieties over a field k, and set $r := \dim X - \dim S$. Then f is smooth of relative dimension r if and only if $\Omega_{X/S}$ is locally free of rank r.

Here are a few more ways to work with the yoga of étale morphisms.

Proposition 87. Fix a ring A, an extension $B = A[t]/(p)$ where $p \in A[t]$ is monic, and a localization $C = B\left[q^{-1}\right]$ for some q. If $p'(t) \in C^\times$, then the natural map $\operatorname{Spec} C \to \operatorname{Spec} A$.

We will not prove this (all of these proofs are horribly annoying), but we will content ourselves with an example.

Example 88. Fix $A := k[x]$ and $B := k[x,y]/\left(y^2 - x(x-1)(x+1)\right)$. Then $\operatorname{Spec} B \to \operatorname{Spec} A$ is basically the projection from an elliptic curve to the affine line, so we expect to have some ramification at $(0,0)$, $(1,0)$, and $(-1,0)$. Accordingly, if we localize out by $x^3 - x$, then we see that the map $\operatorname{Spec} C \to \operatorname{Spec} A$ is successfully étale, which can be checked because the derivative of $p(y) = y^2 - \left(x^3 - x\right)$ is in $C^\times$.

Remark 89. It turns out that all étale morphisms can locally be factored like Proposition 87.

Proposition 90. Fix a smooth morphism $f\colon X \to S$ of relative dimension r at a point $x \in X$. Further, fix some local functions $g_1, \ldots, g_r \in \mathcal{O}_{X,x}$. Then the following are equivalent.

(i) The elements $dg_1, \ldots, dg_r$ form a local basis for $\Omega_{X/S} \otimes k(x)$.

(ii) The elements $g_1, \ldots, g_r$ extend to an open neighborhood U of x such that $(g_1, \ldots, g_r)\colon U \to \mathbb{A}_S^r$ is étale.

Remark 91. Property (i) is relatively easy to satisfy, so we know that such functions surely exist.

Remark 92. The point of (ii) is that f now factors as

$$X \supseteq U \to \mathbb{A}_S^r \to S,$$

where the map $U \to \mathbb{A}_S^r$ is étale. Thus, smooth morphisms are "just" projections up to an étale map.

8.2   The Fundamental Group

Continuing with our intuition that étale morphisms are covering spaces, we now try to define a fundamental group. It is difficult to make sense of paths in algebraic geometry, so instead we will use covering spaces. Here is the construction that we will try to generalize.

Example 93. For a nice topological space X (e.g., a manifold) with a basepoint $x \in X$, then there is a natural "fiber" functor

$$\mathrm{Fib}_x\colon \mathrm{Cover}(X) \to \mathrm{Set}$$

from the category of covering spaces of X to sets given by sending $p\colon Y \to X$ to the fiber $p^{-1}(\{x\})$. By a path-lifting argument, one shows that

$$\pi_1(X, x) = \mathrm{Aut}(\mathrm{Fib}_x).$$

(In particular, path-lifting desribes an action of $\pi_1(X, x)$ on all fibers in a compatible way.) We remark that this allows us to upgrade the fiber functor into an equivalence

$$\mathrm{Fib}_x\colon \mathrm{Cover}(X) \to \mathrm{Set}(\pi_1(X, x)).$$

Remark 94. Topology is aided by the existence of a universal cover. For example, one has a universal cover of S^1 given by $\mathbb{R} \twoheadrightarrow S^1$, but this covering space fails to be finite; similarly, the universal cover of $\mathbb{C}^\times$ is the exponential map $\exp\colon \mathbb{C} \twoheadrightarrow \mathbb{C}^\times$, which is not algebraic. Algebra is going to have some trouble producing coverings which are not finite (or algebraic), so we will have to content ourselves with some finite quotients.

Accordingly, we find that we are contenting ourselves to work with finite covering spaces, which amounts to working with finite étale covers.

Definition 95 (étale fundamental group). Fix a scheme X and a geometric point $\overline{x} \hookrightarrow X$, and consider the corresponding category $\mathrm{Fin\acute{E}t}(X)$ of finite étale covers of X. Then we define the *étale fundamental group* $\pi_1(X, \overline{x})$ to be the automorphism group of the fiber functor

$$\mathrm{Fib}_x \colon \mathrm{Fin\acute{E}t}(X) \to \mathrm{Set}$$

given by sending the cover $p \colon Y \to X$ to the covering to the fiber $Y \times_p \overline{x}$.

Remark 96. As in the topological case, one finds that Fib_x upgrades to an equivalence

$$\mathrm{Fib}_x \colon \mathrm{Fin\acute{E}t}(X) \to \mathrm{Set}(\pi_1(X, \overline{x})).$$

As a sanity check, we note the following comparison theorem.

Theorem 97. Fix an irreducible variety X over $\mathbb{C}$. Then $Y \mapsto Y(\mathbb{C})$ upgrades to an equivalence of categories between the finite étale covers of X and the finite covers of $X(\mathbb{C})$.

Example 98. Consider $X = \mathbb{C}\left[x, x^{-1}\right]$ so that $X(\mathbb{C}) = \mathbb{C}^\times$. Then we see that $\pi_1^{\text{ét}}(X, \overline{1})$ will be $\widehat{\mathbb{Z}}$ because it is the colimit of the automorphism groups of the finite covers of $\mathbb{C}^\times$.

But now that we can do algebraic geometry, we can add in some arithmetic information.

Example 99. Consider the point $X = \mathrm{Spec}\, k$ and an algebraic closure $\overline{x} = \mathrm{Spec}\, \overline{k}$. Then a finite étale cover $Y \to X$ will be a finite disjoint union of points. To describe our category, we are allowed to work with just the connected covers of X, which amounts to making Y a point, so we may write $Y = \mathrm{Spec}\, L$. In order for the map $Y \to X$ to be an étale cover, it is equivalent to ask for the induced field extension $k \subseteq L$ to be finite and separable. The fiber of such an L is given by

$$(Y \times \overline{x})(\overline{k}) = \mathrm{Spec}(L \otimes \overline{k})(\overline{k}) = \mathrm{Hom}_k(L, \overline{k}).$$

Thus, $\mathrm{F\acute{E}t}(X)$ amounts to the category of finite separable extensions of k, and it is not hard to see that the automorphism group is simply $\mathrm{Gal}(\overline{k}/k)$.

8.3   Grothendieck Topologies

The point of a Grothendieck topology is to recognize that what makes a topology important is not its open sets but instead the notion of covers. Thus, to specify a Grothendieck topology, we will try to specify the covers and make do with that.

Definition 100 (Grothendieck topology). Fix a category $\mathcal{C}$ closed under finite products. A *Grothendieck topology* on $\mathcal{C}$ is a collection of families $\mathcal{T}$ of the form $\{f_i \colon U_i \to U\}_i$ and satisfying the following.

(a) Isomorphisms: the family $\mathcal{T}$ contains all isomorphisms.

(b) Refinement: given a covering $\{U_i \to U\}_i$ in $\mathcal{T}$ and some coverings $\{V_{ij} \to U_i\}_j$, then the composite $\{V_{ij} \to U_i \to U\}_{i,j}$ continues to be in $\mathcal{T}$.

(c) Pullback: given a covering $\{U_i \to U\}_i$ in $\mathcal{T}$ and some object V with a map $V \to U$, then the pullback $\{U_i \times_U V \to V\}_i$ is in $\mathcal{T}$.

In this situation, the pair $(\mathcal{C}, \mathcal{T})$ is a site.

Here is the motivating example.

Example 101 (Zariski site)**.** If X is a topological space, then we can let $\mathcal{C}$ be the category of open sets in X with morphisms given by inclusion. We can endow $\mathcal{C}$ with the structure of a Grothendieck topology by letting the covers simply be the open covers. If X is a scheme, then this site is called the Zariski site.

Here is the site for today.

Definition 102 (small étale site)**.** Fix a scheme X, and consider the category $\text{Ét}(X)$ of all étale covers of X. Then we endow $\text{Ét}(X)$ with the structure of a Grothendieck topology by saying that a collection of morphisms $\{U_i \to U\}_i$ is a covering if and only if $\bigsqcup_i U_i \to U$ is surjective. This is called the *(small) étale site* and is denoted $X_{\text{ét}}$.

Remark 103. It turns out that a morphism of étale covers of X is automatically étale. This can be proven using the usual techniques of cancellation.

Remark 104. By replacing the word étale with other adjectives, we also have an fppf site and fpqc site. We note that the Zariski site has the same definition where étale is replaced with open embeddings.

As usual, once we have an object, we want some morphisms.

Definition 105 (continuous)**.** A *continuous* map $F\colon (\mathcal{C}', \mathcal{T}') \to (\mathcal{C}, \mathcal{T})$ is the data of a functor $F\colon \mathcal{C} \to \mathcal{C}'$ satisfying the following.

   (a) For any covering $\{U_i \to U\}_i$ in $\mathcal{T}$, we require that $\{FU_i \to FU\}_i$ to be in $\mathcal{T}'$.

   (b) Given a covering $\{U_i \to U\}_i$ in $\mathcal{T}$ and a map $V \to U$, then we require that $F(V \times_U U_i) \to FV \times_{FU} FU_i$ to be an isomorphism.

Remark 106. If $f\colon X' \to X$ is a continuous map of topological spaces, then taking the pre-image induces a functor of the categories of open sets, and one can see directly that taking the pre-image produces a continuous map of the Grothendieck topologies.

Remark 107. For any scheme X, there is a continuous map between the étale site

$$X_{\text{fpqc}} \to X_{\text{fppf}} \to X_{\text{ét}} \to X_{\text{Zar}}.$$

The point of having a notion of topology is that it lets us do sheaf theory.

Definition 108. Fix a Grothendieck topology on a category $\mathcal{C}$. Then a presheaf $\mathcal{F}\colon \mathcal{C}^{\text{op}} \to \text{Ab}$ is a *sheaf* if and only if the usual exact sequence

$$\mathcal{F}(U) \to \prod_i \mathcal{F}(U_i) \to \prod_{i,j} \mathcal{F}(U_i \times_U U_j)$$

is exact for all covers $\{U_i \to U\}_i$.

Example 109. A sheaf on the Zariski site is the usual notion of sheaf in scheme theory.

Remark 110. Because open embeddings are already étale, fppf, and fpqc, we see that a sheaf on any of these sites must be a Zariksi sheaf as well.

Remark 111. Because the sites we care about are closed under arbitrary coproduct, it is enough to check it on coverings which look like $U' \to U$, though of course one cannot require either U' or U to be connected.

We have yet to construct any sheaves! Here is the usual way to do so.

Definition 112. Fix a scheme X. For any Zariski quasicoherent sheaf $\mathcal{F}$ on X, we define the étale presheaf $\mathcal{F}^{\text{ét}}$ on $X_{\text{ét}}$ by sending the cover $p \colon U \to X$ to

$$\mathcal{F}_{\text{ét}}(U) \coloneqq \operatorname{Hom}(p^*\mathcal{O}_X, p^*\mathcal{F}).$$

Remark 113. It turns out that this construction produces a sheaf. Something similar works for the fppf sites and fpqc sites. Let's explain this for the fpqc site. Indeed, fix a fpqc morphism $p \colon S' \to S$, so we set $S' \coloneqq S' \times_S S'$ with projection $q \colon S'' \to S$, and we need to check that the usual sequence

$$\mathcal{F}_{\text{fpqc}}(S) \to \mathcal{F}_{\text{fpqc}}(S') \to \mathcal{F}_{\text{fpqc}}(S'')$$

is exact. Accordingly, we see that we may as well replace $\mathcal{F}$ with the pullback to S (so that $X = S$), and we have left to check that

$$\operatorname{Hom}(\mathcal{O}_S, \mathcal{F}) \to \operatorname{Hom}(\mathcal{O}_{S'}, p^*\mathcal{F}) \to \operatorname{Hom}(\mathcal{O}_{S''}, q^*\mathcal{F})$$

is exact. Exactness now follows from some notion of descent.

The last remark we should make about sheaves on a site is that we can do sheafification.

Definition 114 (sheafification)**.** Fix a site $\mathcal{C}$. Then there is a left adjoint to the forgetful functor $\operatorname{Sh}(\mathcal{C}) \to \operatorname{PSh}(\mathcal{C})$, which we call sheafification.

9   September 22nd: Uniform Boundedness over Function Fields

This talk was given by Jit Wu Yap at Boston University for the Boston University number theory seminar.

9.1   The Main Theorems

For today, we will work over a function field $K \coloneqq \mathbb{C}(B)$, where B is a smooth projective curve over $\mathbb{C}$. We are interested in abelian varieties with semistable reduction.

Definition 115 (semistable reduction)**.** Fix an abelian variety A over K. We say that A has *semistable reduction* if and only if there is a semiabelian scheme G over B such that $G_K \cong A$.

Here are two theorems.

Theorem 116. Fix an integer g. Then there is an integer N only depending on g and the genus of B such that all g-dimensional abelian varieties A over K of semistable reduction has

$$\operatorname{ord}(x) \leq N$$

for all $x \in A(K)_{\text{tors}}$.

> **Remark 117.** Intuitively, this is a result on the boundedness of torsion, analogous to Maur's theorem for $g = 1$ over $K = \mathbb{Q}$. There is a long history of such results. In the 1990s, results were achieved for $g = 1$ over a number field. For $g \geq 2$, Silverberg showed the result when A has complex multiplication. Cadoret–Tamagawa's results were used as an input to Bakkar–Tsiermann showing this for $g \geq 2$ when A has real multiplication in 2018.

> **Theorem 118.** Fix an integer g. Then there is a positive constant c depending only on g and the genus of B such that all g-dimensional abelian varieties A of semistable reduction, then the Néron–Tate height of any $x \in A(K)$ for which $\overline{\mathbb{Z}x} = A$ is bounded below by $ch_{\text{Fal}}(A)$.

The Faltings height and the Weil height machine work just fine for function fields over $\mathbb{C}$. For example, one can define the Faltings height as the usual Weil height of the point $A \in \mathcal{A}^*_{g,3}$ against some canonically defined ample line bundle.

> **Remark 119.** This is referred to as a "Lang–Silverman" result because it was conjectured by them. In the case of $g = 1$, this was shown by Hindry–Silverman in 1988.

> **Remark 120.** The methods are largely arithmetic. The fact that we are working over $\mathbb{C}$ is used only once in the proof: we use Faltings's Arakelov inequality, which asserts that there is a positive constant c depending only on $g = \dim A$ for which
>
> $$h_{\text{Fal}}(A) \leq c \left(|S| + g(B) + 1 \right),$$
>
> where S is the set of places of bad reduction of A. Accordingly, if this inequality is true over number fields K (which is known as a higher-dimensional Szpiro conjecture), then Theorems 116 and 118 hold. However, Szpiro's conjecture is known to be hard: just in $g = 1$, it is known to imply the abc conjecture.

9.2 Some Ideas

Here is the main idea for the results.

1. If $x \in A(K)$, then the Arakelov inequality is able to place constraints on $x \in A(K_v)$ for many places v.

2. However, K-points of small Néron–Tate height will equidistribute. Here is a formal statement for elliptic curves: given ascending collections $F_n \subseteq A(\overline{K})$ of Galois-invariant points, then it is known that

$$\frac{1}{\#F_n} \sum_{x \in F_n} \delta_x \to \mu,$$

for some suitably defined Haar measure μ. Thus, we cannot expeect to have too many points in $A(K)$ of small Néron–Tate height.

Here are a couple of tools.

1. Over $\mathbb{C}$, there is a notion of "transfinite diameter" of a sequence of points $\{x_1, \ldots, x_n\}$ defined as

$$\frac{1}{n^2} \sum_{i \neq j} -\log |x_i - x_j|.$$

This turns out to measure how close a given set of points are to a large-degree hypersurface.

2. It turns out that abelian varieties over local fields satisfies "degeneration by ultrafilters." Roughly speaking, given a countable collection $\{K_n\}_n$ of complete, algebraically closed field, nonarchimedean

fields, and g-dimensional principally polarized abelian varieties A_n over K_n, then there is a "limit" A_ω over some complete, algebraically closed, nonarchimedean field K_ω for any ultrafilter ω on $\mathbb{N}$. Roughly speaking, one fixes a compactification $\overline{X}$ of $X := \mathcal{A}_{g,3}$. Then define $\lambda_{\partial X}(A)$ to be $-\log$ of the distance of A to $\partial\overline{X}$. Then we may define

$$A^\varepsilon := \left\{ (x_n)_n \in \prod_{n=1}^{\infty} K_n : |x_n|^{1/\lambda_{\partial X}(A_n)} \text{ is bounded} \right\}.$$

It now turns out that there is a morphism $\operatorname{Spec} A^\varepsilon \to \mathcal{A}_{g,3}$ making the diagram

$$
\begin{array}{ccc}
\operatorname{Spec} A^\varepsilon & \longrightarrow & \mathcal{A}_{g,3} \\
{\scriptstyle \operatorname{pr}_n} \downarrow & \nearrow {\scriptstyle A_n} & \\
\operatorname{Spec} K_n & &
\end{array}
$$

commute. Of course, one can certainly induce a map to $\overline{X}$, so the difficulty is showing that we do not end up in the boundary in the limit.

25