Sato–Tate groups: invariants and equidistribution[1]

Francesc Fité[2] (MIT)

Poznań-Szczecin arithmetic algebraic geometry seminar

July 15, 2021

[1] Based on joint works with K.S. Kedlaya and A.V. Sutherland; with A. Bucur and K.S. Kedlaya; and with E. Costa and A.V. Sutherland.

[2] I gratefully acknowledge support from the Simons Foundation (via grant 550033), MIT, and IAS (via grant DMS-1638352).

Layout

1. Computation of Sato–Tate group invariants in the genus 3 classification

2. Arithmetic content in Sato-Tate group invariants

Layout

1. Computation of Sato–Tate group invariants in the genus 3 classification

2. Arithmetic content in Sato-Tate group invariants

Recap from last week: the Sato–Tate group

k a number field.

A/k an abelian variety of dimension $g \geq 1$.

Attached to A, there exists an unconditionally defined compact real Lie subgroup of $\mathrm{USp}(2g)$ that is conjectured to govern the limiting distribution of:

- the number of points of the reductions of A modulo primes of k; or
- the Frobenius classes acting on the cohomology groups of A.

This group is called the Sato–Tate group of A, and is denoted $\mathrm{ST}(A)$. Recall:

- It is only well-defined up to conjugacy.
- It is not necessarily connected.
- It is sensitive to base change.

Recap from last week: classification results

Remark

There are 3 conjugacy classes of subgroups of $\mathrm{USp}(2)$ which occur as Sato–Tate groups of elliptic curves over number fields.

Theorem (F.–Kedlaya–Rotger–Sutherland; 2012)

There are 52 conjugacy classes of subgroups of $\mathrm{USp}(4)$ which occur as Sato–Tate groups of abelian surfaces over number fields.

Theorem (F.–Kedlaya–Sutherland; 2021)

There are 410 conjugacy classes of subgroups of $\mathrm{USp}(6)$ which occur as Sato–Tate groups of abelian threefolds over number fields.

Proposition

$\mathrm{ST}(A)$ determines $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$, as $\mathbb{R}$-algebra equipped with an action of G_k.

$\mathrm{ST}(A)^0$ determines $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$, as $\mathbb{R}$-algebra.

$\pi_0(\mathrm{ST}(A)) \twoheadrightarrow \mathrm{Gal}(F/k)$, where F is the endomorphism field of A.

Recap from last week: map for the $g = 3$ classification

Type	G^0	$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$	$N_{\mathrm{USp}(6)}(G^0)/G^0$	Extensions
A	$\mathrm{USp}(6)$	$\mathbb{R}$	C_1	1
B	$\mathrm{U}(3)$	$\mathbb{C}$	C_2	2
C	$\mathrm{SU}(2) \times \mathrm{USp}(4)$	$\mathbb{R} \times \mathbb{R}$	C_1	1
D	$\mathrm{U}(1) \times \mathrm{USp}(4)$	$\mathbb{C} \times \mathbb{R}$	C_2	2
E	$\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathbb{R} \times \mathbb{R} \times \mathbb{R}$	S_3	4
F	$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathbb{C} \times \mathbb{R} \times \mathbb{R}$	$C_2 \times C_2$	5
G	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{SU}(2)$	$\mathbb{R} \times \mathbb{C} \times \mathbb{C}$	D_4	5
H	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$	$\mathbb{C} \times \mathbb{C} \times \mathbb{C}$	$(C_2 \times C_2 \times C_2) \rtimes S_3$	13
I	$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$	$\mathbb{R} \times \mathrm{M}_2(\mathbb{R})$	$\mathrm{O}(2)$	10
J	$\mathrm{U}(1) \times \mathrm{SU}(2)_2$	$\mathbb{C} \times \mathrm{M}_2(\mathbb{R})$	$C_2 \times \mathrm{O}(2)$	31
K	$\mathrm{SU}(2) \times \mathrm{U}(1)_2$	$\mathbb{R} \times \mathrm{M}_2(\mathbb{C})$	$\mathrm{SO}(3) \times C_2$	32
L	$\mathrm{U}(1) \times \mathrm{U}(1)_2$	$\mathbb{C} \times \mathrm{M}_2(\mathbb{C})$	$C_2 \times \mathrm{SO}(3) \times C_2$	122
M	$\mathrm{SU}(2)_3$	$\mathrm{M}_3(\mathbb{R})$	$\mathrm{SO}(3)$	11
N	$\mathrm{U}(1)_3$	$\mathrm{M}_3(\mathbb{C})$	$\mathrm{PSU}(3) \rtimes C_2$	171

https://www.lmfdb.org/SatoTateGroup/

Invariants for Sato–Tate groups: Moments

Let $a_1, a_2, \ldots, a_g : \mathrm{USp}(2g) \to \mathbb{R}$ denote the characters computing the coefficients of the characteristic polynomial of a random element in $\mathrm{USp}(2g)$, that is,

$$a_1 = \mathrm{Tr}(\mathbb{C}^{2g}), \quad a_2 = \mathrm{Tr}(\wedge^2\mathbb{C}^{2g}), \quad \ldots, \quad a_g = \mathrm{Tr}(\wedge^g\mathbb{C}^{2g}),$$

where $\mathbb{C}^{2g}$ denotes the standard representation of $\mathrm{USp}(2g)$.

Let G be a closed subgroup of $\mathrm{USp}(2g)$.

For nonnegative integers $e_1, \ldots, e_g$, the moment $\mathrm{M}_{e_1,\ldots,e_g}$ of G is defined as:

- the expected value $\int_G a_1^{e_1} \cdots a_g^{e_g}$; or equivalently
- the multiplicity $\langle (\mathbb{C}^{2g})^{\otimes e_1} \otimes \cdots \otimes (\wedge^g\mathbb{C}^{2g})^{\otimes e_g}, 1\rangle$.

For a nonnegative integer m, the m-simplex of moments is the collection of $\mathrm{M}_{e_1,\ldots,e_g}$ for all tuples $(e_1, \ldots, e_g)$ with $w := e_1 + 2e_2 + \cdots + ge_g \leq m$.

LMFDB contains the 12-simplex of moments for all 410 groups in the genus 3 classification.

Examples

1) Suppose $-1 \in G$.

   If w is odd, then $\mathrm{M}_{e_1,\dots,e_g} = 0$. Indeed:

$$\int_{\gamma\in G} a_1(\gamma)^{e_1}\dots a_g(\gamma)^{e_g} = \int_{\gamma\in G} a_1(-\gamma)^{e_1}\dots a_g(-\gamma)^{e_g} = (-1)^w \int_{\gamma\in G} a_1(\gamma)^{e_1}\dots a_g(\gamma)^{e_g}.$$

2) Let $g = 1$ and $G = \mathrm{SU}(2)$.

   Character χ of G $\rightsquigarrow$ Laurent polynomial $\tilde{\chi} \in \mathbb{Z}[\alpha^{\pm 1}]$.

   (Think of α, α^{-1} as random eigenvalues of the standard representation).

   Then $\langle \chi, 1\rangle = [\alpha^0]\tilde{\chi} - [\alpha^2]\tilde{\chi}$, where $[\alpha^k]$ is the coefficient of α^k in $\tilde{\chi}$.

   (Use that the irreducible representations of $\mathrm{SU}(2)$ are $\mathrm{Sym}^n\,\mathbb{C}^2$ for $n \geq 0$, with eigenvalues $\alpha^n, \alpha^{n-2}, \dots, \alpha^{2-n}, \alpha^{-n}$).

   Hence $\mathrm{M}_{2e}(\mathrm{SU}(2))$ is

$$\langle \mathrm{Tr}((\mathbb{C}^2)^{2e}), 1\rangle = ([\alpha^0]-[\alpha^2])(\alpha+\alpha^{-1})^{2e} = \binom{2e}{e} - \binom{2e}{e-1} = \frac{1}{e+1}\binom{2e}{e}.$$

Invariants for Sato–Tate groups: character norms

Let G be a closed subgroup of $\mathrm{USp}(2g)$.

Dominant weights of $\mathrm{USp}(2g) \leftrightsquigarrow$ partitions of integers≥ 0 of length g.

For a partition $\lambda : \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_g$, let χ_λ denote the irreducible character of $\mathrm{USp}(2g)$ with highest weight λ.

For a partition λ, the character norm N_λ of G is:

- the expected value $\int_G (\chi_\lambda|_G)^2$; or equivalently
- the multiplicity of the trivial representation in $(\chi_\lambda|_G)^2$.

For a nonnegative integer m, the *m*-diagonal of character norms is the collection of N_λ for all subpartitions λ of the rectangular partition $m \overset{g}{\leq \cdots \leq} m$.

LMFDB contains the 3-diagonal of character norms for all 410 groups in the genus 3 classification.

The m-diagonal of character norms was introduced by Kohel–Shieh. They suggested it should distinguish Sato–Tate groups more efficiently (and verified it for $g = 2$).

Invariants for Sato–Tate groups: point densities

Lemma

Let G be a closed subgroup of $\mathrm{USp}(6)$. Suppose that:

- G satisfies the rationality condition and contains -1.
- For some $i \in \{1,2,3\}$ and some connected component C, the function $a_i : G \to \mathbb{R}$ is identically equal to the constant function $t \in \mathbb{R}$.

Then $t = 0$ if $i \in \{1,3\}$, and $t \in \{-1,0,1,2,3\}$ if $i = 2$.

The matrix of point densities associated to G is

$$Z(G) = \begin{bmatrix} 1 & z_2 & z_2^{-1} & z_2^0 & z_2^1 & z_2^2 & z_2^3 \\ z_1 & z_{12} & z_{12}^{-1} & z_{12}^0 & z_{12}^1 & z_{12}^2 & z_{12}^3 \\ z_3 & z_{23} & z_{23}^{-1} & z_{23}^0 & z_{23}^1 & z_{23}^2 & z_{23}^3 \\ z_{13} & z_{123} & z_{123}^{-1} & z_{123}^0 & z_{123}^1 & z_{123}^2 & z_{123}^3 \end{bmatrix}.$$

where, for example, the proportion of connected components of G on which:

- a_1 and a_2 are constant is denoted by z_{12}.
- a_1 is constant and a_2 is constant and equal to 2 is denoted by z_{12}^2.

The result of a computation

Theorem (F.–Kedlaya–Sutherland)

i) The 410 groups in the genus 3 classification give rise to 409 distinct distributions of charpolys.

The groups $J(C(3,3))$, $J_s(C(3,3))$ share the same distribution of charpolys, but have nonisomorphic component groups.

ii) The 409 distinct distributions are distinguished by either:

- the 3-diagonal of character norms (20 terms of size at most 10^5); or
- the 14-simplex of moments (147 terms of size sometimes exceeding 10^8).

iii) The 410 groups are distinguished by the data including:

- the group of connected components;
- the matrix of point densities; and
- the character norms $\mathrm{N}_{(1,1,0)}, \mathrm{N}_{(1,1,1)}, \mathrm{N}_{(2,0,0)}$.

Computation of averages: the connected case I

Let $G \subseteq \mathrm{USp}(6)$ be one of the 14 connected Sato–Tate groups.

$\mathrm{USp}(6)$	$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathrm{SU}(2) \times \mathrm{U}(1)_2$
$\mathrm{U}(3)$	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{SU}(2)$	$\mathrm{U}(1) \times \mathrm{U}(1)_2$
$\mathrm{SU}(2) \times \mathrm{USp}(4)$	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$	$\mathrm{SU}(2)_3$
$\mathrm{U}(1) \times \mathrm{USp}(4)$	$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$	$\mathrm{U}(1)_3$
$\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathrm{U}(1) \times \mathrm{SU}(2)_2$	

Goal: Compute $\langle \chi, 1 \rangle$ for χ a character of G.

For later convenience: we allow χ be a virtual character of G, that is, a linear combination of irreducible characters of G with *complex* coefficients.

Let r be the rank of G.

Let $u_1, \overline{u}_1, \dots, u_r, \overline{u}_r$ be independent eigenvalues of a random element in G.

Then χ gives rise to:

$$\tilde{\chi} \in \mathbb{C}[u_1^{\pm 1}, \dots, u_r^{\pm 1}] .$$

Computation of averages: the connected case II

Suppose that $G = G_1 \times G_2$, where:

- $G_1 = \mathrm{U}(1)$ or $\mathrm{SU}(2)$.
- We assume the eigenvalues of G_1 are $u_1, \overline{u}_1$.

$$\langle \chi, 1 \rangle = \langle \psi, 1 \rangle, \text{ where } \psi : G_2 \to \mathbb{C} \text{ is assoc. to } \begin{cases} [u_1^0]\tilde{\chi} & \text{if } G_1 = \mathrm{U}(1) \\ [u_1^0]\tilde{\chi} - [u_1^2]\tilde{\chi} & \text{if } G_1 = \mathrm{SU}(2) \end{cases}$$

This reduces the problem to consider $G \in \{\mathrm{USp}(4), \mathrm{SU}(3), \mathrm{USp}(6)\}$.

These groups being *connected* and *semisimple*, we can use Weyl's theory of highest weights. To recover $\langle \chi, 1 \rangle$, successively apply:

- Identify the highest dominant weight λ in χ.
- Compute the irreducible character χ_λ associated to λ.
- If $\chi_\lambda = 1$, then return $\dim(\chi)$. Otherwise, start over with $\chi - \chi_\lambda$.

Computation of averages: the Weyl character formula

Let $\lambda = (\lambda_1, \ldots, \lambda_r)$ be a dominant weight.

χ_λ can be computed via the Weyl character formula.

Let W denote the Weyl group of G. Set:

$$D_\lambda := \sum_{w \in W} \mathrm{sign}(w) u_1^{w(\lambda)_1} \cdots u_r^{w(\lambda)_r} \in \mathbb{Z}[u_1^{\pm 1}, \ldots, u_r^{\pm 1}] \,.$$

Then the Weyl character formula establishes

$$\tilde{\chi}_\lambda = \frac{D_{\lambda+\rho}}{D_\rho} \in \mathbb{Z}[u_1^{\pm 1}, \ldots, u_r^{\pm 1}] \,.$$

Here ρ is the half-sum of the positive roots of G.

Computation of averages: groups of central type

Let $G \subseteq \mathrm{USp}(6)$ be a Sato–Tate group (not necessarily connected).

Let χ be a character of $\mathrm{USp}(6)$ (like for example $a_1^{e_1} a_2^{e_2} a_3^{e_3}$).

In order to compute $\int_G \chi$, it suffices to compute:

Goal: Compute $\int_C \chi$ for every connected component C of G.

We say that G is of central type if G can be written as $\langle G^0, H\rangle$ for some finite group H such that, for each $h \in H$, the map

$$G^0 \to \mathbb{R}[T]\,, \qquad \gamma \mapsto \det(1 - \gamma h T)$$

is a class function. If G is of central type, then for all $h \in H$, the map

$$G^0 \to \mathbb{C}\,, \qquad \gamma \mapsto \chi(\gamma h)$$

is a virtual character of G^0. If $C = G^0 h$, then

$$\int_{\gamma \in C} \chi(\gamma) = \int_{\gamma \in G^0 h} \chi(\gamma) = \int_{\gamma \in G^0} \chi(\gamma h)$$

can be computed as in the connected case.

Computation of averages: exceptional groups

Proposition

If G is distinct from $N(\mathrm{U}(3)),\ E_t,\ E_s,\ E_{s,t},\ F_t,\ F_{at},\ F_{a,t}$, then G is of central type.

Remark

The computation of the averages $\int_C \chi$ for the 6 exceptional groups of type E or F can be done via elementary adhoc methods.

When G is $N(\mathrm{U}(3))$, then use first that in order to compute $\langle 1, \chi|_G\rangle$ it suffices to compute $\langle 1, \chi_\lambda|_G\rangle$ for all irreducible characters χ_λ. Then apply the following

Lemma Let λ denote the partition $a \geq b \geq c$. Then:

i) $\langle 1, \chi_\lambda|_{\mathrm{U}(3)}\rangle = 1$ if a, b, c are all even, and it is 0 otherwise.

ii) $\langle 1, \chi_\lambda|_{N(\mathrm{U}(3))}\rangle = 1$ if a, b, c are all even and $a + b + c \equiv 0 \pmod 4$, and it is 0 otherwise.

Remark

In principle, it should be possible to compute $\int_G \chi$ via the Kostant character formula, which extends the Weyl character formula to disconnected groups.

Layout

Arithmetic-geometric information from moments

Let A be an abelian variety defined over k.

Proposition (Costa-F.-Sutherland, Zywina)

Suppose that the Mumford–Tate conjecture holds for A. Then:

i) $\int_{\mathrm{ST}(A)} a_1^2 = \mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(A))\,,$

ii) $\int_{\mathrm{ST}(A)} a_2 = \mathrm{rk}_{\mathbb{Z}}(\mathrm{NS}(A))\,,$

iii) $\int_{\mathrm{ST}(A)^0} a_{2r} = \dim_{\mathbb{Q}}(\mathcal{H}^r(A))\,,$

where $\mathcal{H}^r(A)$ are the Hodge classes of A in degree $1 \leq r \leq g$, that is,

$$\mathcal{H}^r(A) = H^{2r}(A(\mathbb{C}), \mathbb{Q}) \cap H^{r,r}(A)\,.$$

Here $H^{r,r}(A)$ is the space appearing in the Hodge decomposition

$$H^{2r}(A(\mathbb{C}), C) = \bigoplus_{p+q=2r} H^{p,q}(A)\,.$$

Choose a prime ℓ. Let

$$\varrho_\ell : G_k \to \mathrm{Aut}(V_\ell(A))$$

be the ℓ-adic representation attached to A

Let G_ℓ denote the Zariski closure of the image of ϱ_ℓ.

By work of Banaszak–Kedlaya and Cantoral Farfán–Commelin, the assumption of the Mumford–Tate conjecture exhibits $\mathrm{ST}(A)$ as a compact form of $G_\ell \times_\iota \mathbb{C}$ independent of the choice of ℓ and $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$.

Let V denote the standard representation of $\mathrm{ST}(A)$.

Proof of i)

$$\int_{\mathrm{ST}(A)} a_1^2 = \dim_{\mathbb{C}}(V^{\otimes 2})^{\mathrm{ST}(A)} = \dim_{\mathbb{Q}_\ell}(V_\ell(A) \otimes V_\ell(A)(1))^{G_\ell} =$$

$$= \dim_{\mathbb{Q}_\ell}(V_\ell(A) \otimes V_\ell(A)^\vee)^{G_\ell} = \dim_{\mathbb{Q}_\ell} \mathrm{End}_{G_k}(V_\ell(A)) = \mathrm{rk}_{\mathbb{Z}} \mathrm{End}(A)\,.$$

Proof of iii)

$$\int_{\mathrm{ST}(A)^0} a_{2r} = \dim_{\mathbb{C}}(\wedge^{2r} V)^{\mathrm{ST}(A)^0} = \dim_{\mathbb{Q}}(\wedge^{2r} H^1(A(\mathbb{C}), \mathbb{Q}))^{\mathrm{MT}(A)} =$$

$$= \dim_{\mathbb{Q}}(H^{2r}(A(\mathbb{C}), \mathbb{Q}))^{\mathrm{MT}(A)} = \dim_{\mathbb{Q}} \mathcal{H}^r(A)\,.$$

Equidistibution

Generalized Sato-Tate conjecture

For every prime $\mathfrak{p}$ of good reduction for A, there exists a conjugacy class $x_\mathfrak{p}$ of $\mathrm{ST}(A)$, with the property that

$$\det(1 - x_\mathfrak{p} T) = \det(1 - \varrho_\ell(\mathrm{Frob}_\mathfrak{p})\,\mathrm{Nm}(\mathfrak{p})^{-1/2} T)\,,$$

such that the sequence $\{x_\mathfrak{p}\}_\mathfrak{p}$ is equidistributed on the set of conjugacy classes of $\mathrm{ST}(A)$ with respect to the Haar measure.

A proof paradigm via L-functions

For an irreducible representation ϱ of $\mathrm{ST}(A)$, define

$$L(A, \varrho, s) = \prod_{\mathfrak{p}} \det(1 - \varrho(x_\mathfrak{p})\,\mathrm{Nm}(\mathfrak{p})^{-s})^{-1}\,, \qquad \text{for } \Re(s) > 1\,.$$

Serre shows that, if for every nontrivial ϱ, the L-function $L(A, \varrho, s)$ extends to a neighborhood of $\Re(s) \geq 1$ and does not vanish on $\Re(s) = 1$, then the Sato-Tate conjecture holds.

Trace equidistribution

Set

$$a_\mathfrak{p} := \mathrm{Tr}(\varrho_\ell(\mathrm{Frob}_\mathfrak{p}))\,, \qquad \overline{a}_\mathfrak{p} := a_\mathfrak{p} / \mathrm{Nm}(\mathfrak{p})^{1/2}\,.$$

Let μ denote the push forward of the Haar measure of $\mathrm{ST}(A)$ on the interval $[-2g, 2g]$ via the trace map.

Trace Sato-Tate conjecture

The sequence $\{\overline{a}_\mathfrak{p}\}_\mathfrak{p}$ is equidistributed on $[-2g, 2g]$ wrt to μ.

Equivalently, for every $I \subseteq [-2g, 2g]$, we have

$$\#\{\mathfrak{p} : \mathrm{Nm}(\mathfrak{p}) \leq x, \overline{a}_\mathfrak{p} \in I\} = \mu(I)\mathrm{Li}(x) + o\left(\frac{x}{\log(x)}\right) \qquad \text{as } x \to \infty.$$

Effective trace Sato-Tate conjecture

There exists $\epsilon > 0$ such that, for every $I \subseteq [-2g, 2g]$, we have

$$\#\{\mathfrak{p} : \mathrm{Nm}(\mathfrak{p}) \leq x, \overline{a}_\mathfrak{p} \in I\} = \mu(I)\mathrm{Li}(x) + O\left(x^{1-\epsilon+o(1)}\right) \qquad \text{as } x \to \infty.$$

An efective version

Theorem (Bucur-F.-Kedlaya)

Suppose that $L(A,\varrho,s)$ extends to a meromorphic function on $\mathbb{C}$, with only simple poles at $s=1$ and $s=0$ if ϱ is trivial, and analytic otherwise.

Suppose that if $L(A,\varrho,s)=0$, with $0\leq\Re(s)\leq 1$, then $\Re(s)=1/2$.

Then, for every $I\subseteq[-2g,2g]$, we have

$$\#\{\mathfrak{p}:\mathrm{Nm}(\mathfrak{p})\leq x, \overline{a}_{\mathfrak{p}}\in I\}=\mu(I)\mathrm{Li}(x)+O\left(x^{1-\epsilon+o(1)}\right)\qquad \text{as } x\to\infty,$$

with

$$\epsilon=\frac{1}{2(q+\varphi)}\,,$$

where q is the rank of $\mathrm{ST}(A)$ and φ is the number of positive roots of the semisimple part of $\mathrm{ST}(A)$.