Sato–Tate groups of abelian varieties of dimension up to 3

Francesc Fité (MIT)

VaNTAGe Virtual Seminar.

7th April 2020

Layout

1. Sato–Tate conjecture for elliptic curves and equidistribution
2. Sato–Tate axioms for $g \leq 3$
3. Abelian surfaces
4. Abelian threefolds

Layout

Frobenius traces of elliptic curves

- k a number field.
- E/k an elliptic curve.
- For a prime $\mathfrak{p}$ of good reduction for E, set

$$a_{\mathfrak{p}} := N(\mathfrak{p}) + 1 - \#E(\mathbb{F}_{\mathfrak{p}})\,.$$

- For $\mathfrak{p} \nmid \ell$, we have

$$a_{\mathfrak{p}} = \mathrm{Tr}(\mathrm{Frob}_{\mathfrak{p}} \,|\, V_\ell(E))\,.$$

- By the Hasse-Weil bound, the *normalized Frobenius trace* satisfies

$$\overline{a}_{\mathfrak{p}} := \frac{a_{\mathfrak{p}}}{\sqrt{N(\mathfrak{p})}} \in [-2, 2]\,.$$

- The Sato–Tate conjecture is a prediction for the distribution of the $\overline{a}_p$ on the interval $[-2, 2]$.

Equidistribution: Basic notions

- Let X be a compact topological space and $C(X)$ be the space of continuous $\mathbb{C}$-valued functions on X.
- A measure is a continuous linear form $\mu \colon C(X) \longrightarrow \mathbb{C}$.
- Also use the notation $\int_X f\mu := \mu(f)$.
- Assume $\mu(1) = 1$ and μ positive.
- Assume given a sequence $\{x_n\}_n$ of elements in X.
- $\{x_n\}_n$ is said to be μ-equidistributed on X if

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(x_i) = \int_X f\mu \qquad \text{for every } f \in C(X)\,.$$

- Example: If $X = [0,1]$ and μ is the Lebesgue measure, then $\{x_n\}_n$ is μ-equistributed on X if and only if

$$\lim_{n\to\infty} \frac{1}{n} \#\{i \le n \,|\, x_i \in [a,b]\} = b - a \qquad \text{for every } [a,b] \subseteq X\,.$$

The Sato–Tate conjecture for elliptic curves

Sato–Tate conjecture for elliptic curves

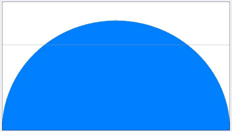
Let E be an elliptic curve defined over k. The sequence $\{\bar{a}_\mathfrak{p}\}_\mathfrak{p}$ is μ_I-equidistributed on $I = [-2, 2]$, where μ_I is of the form

1) $\dfrac{1}{2\pi}\sqrt{4 - z^2}dz$ if E does not have CM.

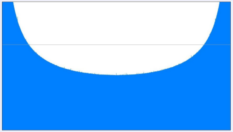
2) $\dfrac{1}{\pi}\dfrac{dz}{\sqrt{4 - z^2}}$ if E has CM by $M \subseteq k$.

3) $\dfrac{1}{2}\delta_0 + \dfrac{1}{2\pi}\dfrac{dz}{\sqrt{4 - z^2}}$ if E has CM by $M \not\subseteq k$.

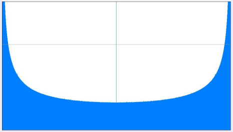
1)



2)



3)



Equidistribution: Compact groups

- Let G be a compact group and $X = \mathrm{Conj}(G)$.
- $C(X)$ space of $\mathbb{C}$-valued continuous *class functions* on G.
- Let μ_G be the Haar measure of G and let $\mu_X = \pi_*(\mu_{\mathrm{G}})$, where

$$\pi\colon\; G \longrightarrow X = \mathrm{Conj}(G)\,.$$

- Example $G = \mathrm{SU}(2) := \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}) \mid a\overline{a} + b\overline{b} = 1 \right\}$.
  - $\pi\colon\; \mathrm{SU}(2) \to X \simeq [0,\pi]$ sends a matrix with eigenvalues $e^{i\theta}, e^{-i\theta}$ to θ.
  - For $f \in C(X)$, we have $\mu_X(f) = \int_X f\mu_X = \frac{2}{\pi}\int_0^\pi f(\theta)\sin^2\theta d\theta$.
- Example $G = \mathrm{U}(1) := \left\{ \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} : \theta \in \mathbb{R}/2\pi\mathbb{Z} \right\} \simeq X$.
  - For $f \in C(X)$, we have $\mu_X(f) = \frac{1}{2\pi}\int_0^{2\pi} f(\theta)d\theta$.

The Sato–Tate conjecture for abelian varieties

- Let A/k be an abelian variety of dimension $g \geq 1$.
- Consider the ℓ-adic representation attached to A

$$\varrho_\ell \colon G_k \to \mathrm{Aut}(V_\ell(A))\,.$$

Sato–Tate conjecture for abelian varieties (Serre; mid 1990's)

There exist:

- a compact subgroup $G \subseteq \mathrm{USp}(2g)$;
- For each prime $\mathfrak{p}$ of good reduction for A, an $x_\mathfrak{p} \in \mathrm{Conj(G)}$ s.t.

$$\mathrm{Charpoly}(x_\mathfrak{p}) = \mathrm{Charpoly}\left(\frac{\varrho_\ell(\mathrm{Frob}_\mathfrak{p})}{\sqrt{N(\mathfrak{p})}}\right)\,;$$

such that the sequence $\{x_\mathfrak{p}\}_\mathfrak{p}$ is equidistributed on $X = \mathrm{Conj}(G)$ w.r.t the push forward of the Haar measure of G.

- Moreover, Serre constructs a candidate $\mathrm{ST}(A)$ for G. For $g \leq 3$, Banaszak and Kedlaya define it purely in terms of endomorphisms.

Equidistribution: Moments

- Example: For an elliptic curve E, there are three options for $\mathsf{ST}(E)$:
  - $\mathsf{SU}(2)$ if E does not have CM.
  - $\mathsf{U}(1)$ if E has CM by $M \subseteq k$.
  - $N_{\mathsf{SU}(2)}(\mathsf{U}(1)) = \left\langle \mathsf{U}(1), \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$ if E has CM by $M \not\subseteq k$.
- Note that the map

$$\mathrm{Conj}(\mathsf{ST}(A)) \to \mathrm{Conj}(\mathsf{USp}(2g)), \qquad x \mapsto \mathrm{Charpoly}(x)$$

  is in general not injective.
- The distribution of the "Charpolys" is captured by the *moments*.
- Let $G \subseteq \mathsf{USp}(2g)$ be a compact subgroup. $X = \mathrm{Conj}(G)$.
- Let χ denote the character of the tautological rep. $G \to \mathsf{GL}_{2g}(\mathbb{C})$.
- For integers $n_1, \ldots, n_g \geq 0$, define the moment

$$\mathrm{M}_{n_1,\ldots,n_g}(G) = \int_G \chi^{n_1} \cdot (\wedge^2\chi)^{n_2} \cdot \cdots \cdot (\wedge^g\chi)^{n_g} \mu_G \, .$$

Equidistribution: Moments of SU(2)

- Note that:

$$\mathrm{M}_{n_1,\dots,n_g}(G) = \langle \mathbf{1}, \chi^{n_1} \cdot (\wedge^2\chi)^{n_2} \cdot \dots \cdot (\wedge^g\chi)^{n_g} \rangle \in \mathbb{Z}_{\geq 0}.$$

- Example: $G = \mathrm{SU}(2)$.
  The irreducible characters of SU(2) are

$$\chi_n(\theta) = \mathrm{Sym}^n(\chi)(\theta) = e^{-n\theta i} + e^{(2-n)\theta i} \cdots + e^{(n-2)\theta i} + e^{n\theta i}\,, \quad n \geq 0\,.$$

  The even moments are:

$$\begin{aligned} \mathrm{M}_{2n}(\mathrm{SU}(2)) &= \langle \mathbf{1}, \chi^{2n} \rangle \\ &= \langle \mathbf{1}, \chi_{2n} + \left(\binom{2n}{1} - 1\right)\chi_{2n-1} + \dots + \left(\binom{2n}{n} - \binom{2n}{n-1}\right)\mathbf{1} \rangle \\ &= \binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n} = n\text{-th Catalan number.} \end{aligned}$$

- The odd moments are 0.

Layout

Sato–Tate axioms

- From now on, let A be an abelian variety of dimension $g \leq 3$.
- Banaszak and Kedlaya show that $G = \mathrm{ST}(A)$ satisfies then:

Hodge condition (ST1)

There is a homomorphism $\theta\colon \mathrm{U}(1) \to G^0$ such that $\theta(u)$ has eigenvalues u and $\overline{u}$ each with multiplicity g. The image of such a θ is called a *Hodge circle*. Moreover, the Hodge circles generate a dense subgroup of G^0.

(Expected in general; known if the Mumford–Tate conjecture holds for A).

Rationality condition (ST2)

For every connected component $H \subseteq G$ and for every irreducible character $\chi\colon \mathrm{GL}_{2g}(\mathbb{C}) \to \mathbb{C}$:

$$\int_H \chi(h)\mu_{\mathrm{G}} \in \mathbb{Z}\,,$$

where μ_G is normalized so that $\mu_G(1) = [G : G^0]$.

(Expected in general).

Sato–Tate axioms

Lefschetz condition (ST3)

Write $E := \{\alpha \in \mathrm{M}_{2g}(\mathbb{C}) \,|\, g\alpha g^{-1} = \alpha \text{ for all } g \in G^0\}$. Then

$$\{\gamma \in \mathrm{USp}(2g) | \gamma\alpha\gamma^{-1} = \alpha \text{ for all } \alpha \in E\} = G^0 \,.$$

Serre condition (ST4)

Let F/k be the minimal extension such that $\mathrm{End}(A_F) \simeq \mathrm{End}(A_{\overline{\mathbb{Q}}})$. We call F the endomorphism field of A. Then

$$G/G^0 \simeq \mathrm{Gal}(F/k) \,.$$

- None of (ST3) and (ST4) are expected in general. In particular, Mumford has constructed examples of abelian fourthfolds A with

$$\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z} \qquad \text{and} \qquad G^0 \subsetneq \mathrm{USp}(8) \,.$$

- Up to conjugacy, 3 subgroups of USp(2) satisfy the ST axioms.

Layout

Sato–Tate groups of abelian surfaces

- Define the *Galois endomorphism type* of an abelian variety A/k as the isomorphism class of the $\mathbb{R}$-algebra

$$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{R} \quad \text{equipped with the action of } \mathrm{Gal}(F/k).$$

- Example: There are three Galois types of elliptic curves. They are $\mathbb{R}$, $\mathbb{C}$ (both equipped with the trivial action), and $\mathbb{C}$ equipped with the action of complex conjugation.

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

- Up to conjugacy, 52 subgroups of $\mathrm{USp}(4)$ satisfy the ST axioms. All of them occur as ST groups of abelian surfaces over number fields.
- 34 of them occur as ST groups of abelian surfaces over $\mathbb{Q}$.
- The ST group and the GET of an abelian surface determine each other uniquely.

Comments on the classification

(ST1) allows 6 possibilities for $G^0 \subseteq \mathrm{USp}(4)$ ((ST3) is redundant for $g = 2$).

G^0	$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$	$N_{\mathrm{USp}(4)}(G^0)/G^0$	$\#\mathcal{A}$
$\mathrm{USp}(4)$	$\mathbb{R}$	C_1	1
$\mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathbb{R} \times \mathbb{R}$	C_2	2
$\mathrm{SU}(2) \times \mathrm{U}(1)$	$\mathbb{R} \times \mathbb{C}$	C_2	2
$\mathrm{U}(1) \times \mathrm{U}(1)$	$\mathbb{C} \times \mathbb{C}$	D_4	8
$\mathrm{SU}(2)_2$	$\mathrm{M}_2(\mathbb{R})$	$O(2)$	10
$\mathrm{U}(1)_2$	$\mathrm{M}_2(\mathbb{C})$	$SO(3) \times C_2$	32
			55

- $\mathcal{A}$ = set of finite subgroups of $N_{\mathrm{USp}(4)}(G^0)/G^0$ for which (ST2) is satisfied.
- 3 of the groups in the case $G^0 = \mathrm{U}(1) \times \mathrm{U}(1)$ do not satisfy (ST4):
  - A is $\overline{\mathbb{Q}}$-isogenous to a product of abelian varieties A_i with CM by M_i.
  - $G/G^0 \simeq \mathrm{Gal}(F/k) \simeq \prod \mathrm{Gal}(kM_i^*/k) \subseteq C_2 \times C_2, C_4$.

Additional facts

Remark

As G runs over the 52 groups, $\{\mathrm{M}_{i,j}(G)\}_{i,j}$ attains 52 values:
Distinct groups yield distinct distributions of charpolys.

Corollary

The degree of the endomorphism field of an abelian surface over a number field divides 48.

(this refines previous results by Silverberg).

Theorem (Johansson, N. Taylor; 2014-19)

For $g = 2$ and $k = \mathbb{Q}$, the ST conjecture holds for 33 of the 34 possible ST groups.

Layout

Sato–Tate groups for $g = 3$

Theorem(F.-Kedlaya-Sutherland; 2019)

Up to conjugacy, 410 subgroups of USp(6) satisfy the ST axioms. All of them of them occur as Sato–Tate groups of abelian threefolds over number fields.

Corollary

The degree of the endomorphism field $[F : \mathbb{Q}]$ of an abelian threefold over a number field divides 192, 336, or 432.

- This refines a previous result of Guralnick and Kedlaya, which asserts

$$[F : \mathbb{Q}] \mid 2^6 \cdot 3^3 \cdot 7 = \mathrm{Lcm}(192, 336, 432)\,.$$

Classification: identity components

(ST1) and (ST3) allow 14 possibilities for $G^0 \subseteq \mathrm{USp}(6)$:

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

Notations:

- For $d \in \{1, 3\}$:

$$\mathrm{U}(d) = \left\{ \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix} \,|\, u \in \mathrm{U}(d)^{\mathrm{Std}} \right\}$$

- For $d \in \{2, 3\}$ and $H \in \{\mathrm{SU}(2), \mathrm{U}(1)\}$:

$$H_d = \{\mathrm{diag}(u, \overset{d}{\ldots}, u) \,|\, u \in H\}$$

- Note in particular that

$$\mathrm{SU}(2) \times \mathrm{U}(1)_2 \simeq \mathrm{U}(1) \times \mathrm{SU}(2)_2 \,.$$

Classification: From G^0 to G

G^0	$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$	$N_{\mathrm{USp}(6)}(G^0)/G^0$	$\#\mathcal{A}$
$\mathrm{USp}(6)$	$\mathbb{R}$	C_1	1
$\mathrm{U}(3)$	$\mathbb{C}$	C_2	2
$\mathrm{SU}(2) \times \mathrm{USp}(4)$	$\mathbb{R} \times \mathbb{R}$	C_1	1
$\mathrm{U}(1) \times \mathrm{USp}(4)$	$\mathbb{C} \times \mathbb{R}$	C_2	2
$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathbb{C} \times \mathbb{R} \times \mathbb{R}$	$C_2 \times C_2$	5
$\mathrm{SU}(2) \times \mathrm{U}(1) \times \mathrm{U}(1)$	$\mathbb{R} \times \mathbb{C} \times \mathbb{C}$	D_4	8
$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$	$\mathbb{R} \times \mathrm{M}_2(\mathbb{R})$	$O(2)$	10
$\mathrm{SU}(2) \times \mathrm{U}(1)_2$	$\mathbb{R} \times \mathrm{M}_2(\mathbb{C})$	$SO(3) \times C_2$	32
$\mathrm{U}(1) \times \mathrm{SU}(2)_2$	$\mathbb{C} \times \mathrm{M}_2(\mathbb{R})$	$C_2 \times O(2)$	31
$\mathrm{U}(1) \times \mathrm{U}(1)_2$	$\mathbb{C} \times \mathrm{M}_2(\mathbb{C})$	$C_2 \times \mathrm{SO}(3) \times C_2$	122
$\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathbb{R} \times \mathbb{R} \times \mathbb{R}$	S_3	4
$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$	$\mathbb{C} \times \mathbb{C} \times \mathbb{C}$	$(C_2 \times C_2 \times C_2) \rtimes S_3$	33
$\mathrm{SU}(2)_3$	$\mathrm{M}_3(\mathbb{R})$	$\mathrm{SO}(3)$	11
$\mathrm{U}(1)_3$	$\mathrm{M}_3(\mathbb{C})$	$\mathrm{PSU}(3) \rtimes C_2$	171

$\mathcal{A}$ = set of finite subgroups of $N_{\mathrm{USp}(6)}(G^0)/G^0$ for which (ST2) is satisfied.

Classification: The 23 spurious groups and invariants

- For $G^0 = \mathrm{SU}(2) \times \mathrm{U}(1) \times \mathrm{U}(1)$:
  As in the case $g = 2$, only 5 of 8 groups in $\mathcal{A}$ satisfy (ST4).
- For $G^0 = \mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$:
  Only 13 of the 33 subgroups in $\mathcal{A}$ satisfy (ST4). Indeed:
  - A is isogenous to a product of abelian varieties A_i with CM by M_i.
  - $G/G^0 \simeq \mathrm{Gal}(F/k) \simeq \prod \mathrm{Gal}(kM_i^*/k) \subseteq C_2 \times C_2 \times C_2, C_2 \times C_4, C_6$.
- This leaves 433-20-3=410 groups, of which 33 are maximal (w.r.t finite inclusions).
- As G runs over the 410 groups, the sequence $\{\mathrm{M}_{i,j,k}(G)\}_{i,j,k}$ attains 409 values. It only conflates a pair of groups G_1, G_2, for which however

$$G_1/G_1^0 \simeq \langle 54, 5\rangle \not\simeq \langle 54, 8\rangle \simeq G_2/G_2^0\,.$$

- Any possible order of G/G^0 divides 192, 336, or 432.

Realization

- It suffices to realize the 33 maximal groups (for prescribed G^0). Finite index subgroups are realized by base change.
- For 8 of the 14 possibilities for G^0, the maximal groups are of the form $G \simeq G_1 \times G_2$ where G_1 and G_2 are realizable in dimensions 1 and 2. This accounts for 13 maximal groups.
- USp(6): generic case. Eg.: $y^2 = x^7 - x + 1/\mathbb{Q}$.
- $N(\mathrm{U}(3))$: Picard curves. Eg.: $y^3 = x^4 + x + 1/\mathbb{Q}$.
- $G^0 = \mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$ (1. max. group): $\mathrm{Res}^L_{\mathbb{Q}}(E)$, where $L/\mathbb{Q}$ a non-normal cubic and E/L e.c. which is not a $\mathbb{Q}$-curve.
- $G^0 = \mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$ (3 max. groups): Products of CM abelian varieties.
- $G^0 = \mathrm{SU}(2)_3$ (2 max. groups): Twists of cubes of non CM e.c.
- $G^0 = \mathrm{U}(1)_3$ (12 max. groups): Twists of cubes of CM elliptic curves.