Character theory approach to Sato-Tate groups

Yih-Dar Shieh
Institut de Mathématiques de Marseille

Algorithmic Number Theory Symposium

September 1, 2016
I. Sato-Tate Conjecture

- Sato-Tate distributions for elliptic curves
- The Sato-Tate Conjecture for elliptic curves
- A new viewpoint: Using irreducible characters
- Higher genus

II. Character Theory

III. Explicit computation of Frobenius distributions
Frobenius Distribution

Let \( E/\mathbb{Q} \) be an elliptic curve with short Weierstrass equation

\[
y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}.
\]

Let \( p \) be a prime of good reduction of \( E \), which means \( v_p(\Delta) = 0 \), here \( \Delta = -16(4a^3 + 27b^2) \) is the discriminant of \( E \). The reduction \( \overline{E}_p \) of \( E \) module \( p \) is again an elliptic curve (over \( \mathbb{F}_p \)).

The number of \( \mathbb{F}_p \)-points on \( \overline{E}_p \) is

\[
\#\overline{E}_p(\mathbb{F}_p) = p + 1 - t_p,
\]

where \( t_p \) is the trace of Frobenius, which is an integer in the interval \([-2\sqrt{p}, 2\sqrt{p}]\).

The Sato-Tate conjecture is concerned with the limiting distribution of \( t_p/\sqrt{p} \in [-2, 2] \) as \( p \) varies over primes of good reduction.
Examples

We compute $t_p / \|p\|^{1/2}$ for $\|p\| \leq 2^{20}$ for each example curves, and plot the histogram of the probability density.

$y^2 = x^3 + x + 1, \ \mathbb{Q}$

CM: $y^2 = x^3 + 1, \ \mathbb{Q}$

CM: $y^2 = x^3 + 1, \ \mathbb{Q}(i)$

These 3 (normalized) trace distributions are in fact the trace distributions of some closed subgroups of the unitary symplectic group $USp(2) = SU(2)$. The distributions are given by the Haar measure on these subgroups.

<table>
<thead>
<tr>
<th>$G$</th>
<th>$G/G^0$</th>
<th>example curve $E$</th>
<th>$k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>U(1)</td>
<td>$C_1$</td>
<td>$y^2 = x^3 + x$</td>
<td>$\mathbb{Q}(i)$</td>
</tr>
<tr>
<td>$N(U(1))$</td>
<td>$C_2$</td>
<td>$y^2 = x^3 + x$</td>
<td>$\mathbb{Q}$</td>
</tr>
<tr>
<td>SU(2)</td>
<td>$C_1$</td>
<td>$y^2 = x^3 + x + 1$</td>
<td>$\mathbb{Q}$</td>
</tr>
</tbody>
</table>
Random variables and moments

- A compact Lie group $G$ with its Haar measure $\mu_G$ is viewed as a *probability space*.
- A character $\xi$ can be viewed as a random variable on $G$. Ex. Given an embedding $G \subseteq \text{GL}(V)$, we have an associated $\xi = \text{tr} : G \to \mathbb{C}$.
- We look the induced (probability) measure $\mu_\xi$ on $\mathbb{R}$ (or $\mathbb{C}$), which satisfies $\mu_\xi(A) = \mu(\xi^{-1}(A))$, for measurable subset $A \subseteq \mathbb{R}$. Ex. For $\text{tr} : \text{SU}(2) \to I = [-2, 2]$, $\mu_{\text{tr}} = \frac{1}{2\pi} \sqrt{4 - t^2} \, dt$, $t \in I$.
- The expectation $E[\xi]$ is $\int_{x \in G} \xi(x) \mu_G(dx)$. The $n$-th moment $M_n(\xi)$ of $\xi$ is $E[\xi^n]$. For $\text{tr}$ on $\text{SU}(2)$,

$$M_{2n}(\text{tr}) = \frac{1}{2\pi} \int_{-2}^{2} t^{2n} \sqrt{4 - t^2} \, dt = \frac{1}{n+1} \binom{2n}{n} \approx \sqrt{\frac{2}{\pi}} \frac{2^{2n}}{\sqrt{2n}}.$$
Equidistribution and the Sato-Tate Conjecture

**Definition (Equidistribution)**

Let \((X, \mu)\) be a probability space and \((x_n) \subseteq X\) be a sequence. \((x_n)\) is \textit{equidistributed with respect to} \(\mu\) if

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \xi(x_i) = \int_{X} \xi(x) \mu(dx)
\]

for all bounded continuous functions \(\xi\) on \(X\).

**Theorem (Sato-Tate Conjecture - Taylor, Clozel, Harris, etc. 2006)**

Let \(E/\mathbb{Q}\) be an elliptic curve without CM. The sequence of normalized traces \(t_p/\sqrt{p} \in [-2, 2]\) is equidistributed w.r.t. \(\mu_{tr}\) from the group \(\text{SU}(2)\).

Another way to state the conjecture is: For any interval \([a, b] \subset [-2, 2]\),

\[
\lim_{N \to \infty} \frac{\# \{p \leq N \mid t_p/\sqrt{p} \in [a, b]\}}{\# \{p \leq N\}} = \int_{a}^{b} \frac{\sqrt{4-t^2}}{2\pi} dt.
\]
The moment sequence determines Sato-Tate distributions for \( g = 1 \):

<table>
<thead>
<tr>
<th>( G )</th>
<th>( G/G^0 )</th>
<th>( E )</th>
<th>( k )</th>
<th>moments ( M_{2n}(\text{tr}) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{U}(1) )</td>
<td>( C_1 )</td>
<td>( y^2 = x^3 + x )</td>
<td>( \mathbb{Q}(i) )</td>
<td>1 2 6 20 70 252 924 3432</td>
</tr>
<tr>
<td>( N(\text{U}(1)) )</td>
<td>( C_2 )</td>
<td>( y^2 = x^3 + x )</td>
<td>( \mathbb{Q} )</td>
<td>1 1 3 10 35 126 462 1716</td>
</tr>
<tr>
<td>( \text{SU}(2) )</td>
<td>( C_1 )</td>
<td>( y^2 = x^3 + x + 1 )</td>
<td>( \mathbb{Q} )</td>
<td>1 1 2 5 14 42 132 429</td>
</tr>
</tbody>
</table>

Expected vs. Sample moments: 2^{10} points for \( y^2 = x^3 + x + 1 \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>( M_{2n}(\text{tr}) )</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>14</td>
<td>42</td>
<td>132</td>
<td>429</td>
</tr>
<tr>
<td>sample moments</td>
<td>0.991</td>
<td>2.009</td>
<td>5.084</td>
<td>14.39</td>
<td>43.67</td>
<td>139.1</td>
<td>458.9</td>
</tr>
</tbody>
</table>

New idea: Use the irreducible characters of \( \text{SU}(2) \):

\[
\begin{align*}
\chi_0 &= 1 \\
\chi_3 &= \text{tr}^3 - 2 \cdot \text{tr} \\
\chi_1 &= \text{tr} \\
\chi_2 &= \text{tr}^2 - 1 \\
\chi_n &= \text{tr} \cdot \chi_{n-1} - \chi_{n-2}
\end{align*}
\]

For \( H \subseteq \text{SU}(2) \), we consider \( \langle \chi_i|_H, \chi_j|_H \rangle_H \) and use the branching rules to obtain this quantitative information.
Expected values vs. Sample means of $\langle \chi_i|_H, \chi_j|_H \rangle_H$: $2^{10}$ sample points for each example

<table>
<thead>
<tr>
<th></th>
<th>SU(2)</th>
<th>N(SO(2))</th>
<th>SO(2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00</td>
<td>0.03</td>
<td>0.01</td>
<td>1.00</td>
</tr>
<tr>
<td>0.03</td>
<td>0.99</td>
<td>0.97</td>
<td>0.01</td>
</tr>
<tr>
<td>0.00</td>
<td>0.05</td>
<td>0.03</td>
<td>0.99</td>
</tr>
<tr>
<td>0.02</td>
<td>0.02</td>
<td>1.94</td>
<td>0.00</td>
</tr>
<tr>
<td>0.03</td>
<td>0.03</td>
<td>0.94</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Goal: For higher genus, a recurrence formula for irreducible characters + the usage of these characters to the study of Sato-Tate groups.
Weil polynomial

For an abelian variety $A/\mathbb{F}_q$ of dimension $g$, its characteristic polynomial of Frobenius $P(x)$, called the Weil polynomial, is an integer polynomial of degree $2g$

$$\tilde{P}(x) = x^{2g} - \tilde{a}_1 x^{2g-1} + \tilde{a}_2 x^{2g-2} + \cdots + \tilde{a}_{2g-2} x^2 - \tilde{a}_{2g-1} x + q^g.$$ 

All of its roots have absolute value $\sqrt{q}$.

Write $\tilde{P}(x) = \prod_{i=1}^{2g} (x - \alpha_i)(x - \bar{\alpha}_i)$. The normalized Weil polynomial is

$$P(x) := \tilde{P}(\sqrt{q}x)/q^g = \prod_{i_1}^{g} (x^2 - t_i x + 1), \quad t_i = \frac{\alpha_i + \bar{\alpha}_i}{\sqrt{q}}.$$ 

$$= x^{2g} - a_1 x^{2g-1} + a_2 x^{2g-1} + \cdots + a_{2g-2} x^2 - a_{2g-1} x + 1.$$

We also consider the normalized real Weil polynomial

$$\prod_{i=1}^{g} (x - t_i) = x^g - s_1 x^{g-1} + \cdots + (-1)^g s_g.$$ 

In general, we have $s_1 = \tilde{\alpha}_1/\sqrt{q}$ and $s_2 = (\tilde{\alpha}_2 - gq)/q$.
For an abelian variety $A$ of dimension $g$ over a number field $K$, and a prime of good reduction $p$, we consider the Frobenius action $F_p$ on the Tate-module $T_\ell(A_p)$. Its normalized Weil polynomial $P_p(x)$ is the characteristic polynomial of an element in $\text{USp}(2g)$, hence the (matrix of the) normalized action $F_p/\sqrt{\|p\|}$ is conjugate to an element in $\text{USp}(2g)$.

**Key idea:** We are interested in the distribution of $F_p/\sqrt{\|p\|}$, which is the same as the study of the distribution of $P_p(x)$, or its real analogue.

The random matrix model of Katz-Sarnak predicts that, in general, the distribution of the normalized Frobenius should match the distribution of the characteristic polynomial of a random element in a compact subgroup $G$ of $\text{USp}(2g)$. This is true on average in certain families.
In general, Serre proposed a candidate for the subgroup $G$ of $\text{USp}(2g)$. This is called the "Sato-Tate group" of $A/K$.

**Generalized Sato-Tate Conjecture**

Let $G \subseteq \text{USp}(2g)$ be the Sato-Tate group of $A/K$. The distribution of normalized Weil polynomials is determined by the Haar measure of $G$.

In 2012, Fité, Kedlaya, Rotger and Sutherland proved

**Theorem (FKRS)**

Up to conjugacy, there are exactly 52 subgroups of $\text{USp}(4)$ that are Sato-Tate groups of abelian surfaces over a number field $K$. Among them, 34 Sato-Tate groups can occur for $K = \mathbb{Q}$. 
Sato-Tate groups in genus 2

They give explicitly these Sato-Tate groups. For each group $G$, they give a genus 2 curve that has $G$ as its Sato-Tate group.

For each example, they compared, using the moments of the coefficients of the characteristic polynomial, the distribution of Frobenius with the expected distribution predicted by the generalized Sato-Tate conjecture, and found they agree very closely.

We list only a few of them here.

<table>
<thead>
<tr>
<th>$G$</th>
<th>$G/G^0$</th>
<th>example curve $E$</th>
<th>$K$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$SO(2)^2$</td>
<td>$C_1$</td>
<td>$y^2 = x^6 + 3x^4 + x^2 - 1$</td>
<td>$\mathbb{Q}(i, \sqrt{2})$</td>
</tr>
<tr>
<td>$SU(2)^2$</td>
<td>$C_1$</td>
<td>$y^2 = x^6 + x^2 + 1$</td>
<td>$\mathbb{Q}$</td>
</tr>
<tr>
<td>$N(SU(2)^2)$</td>
<td>$C_2$</td>
<td>$y^2 = x^6 + x^5 + x - 1$</td>
<td>$\mathbb{Q}$</td>
</tr>
<tr>
<td>$USp(4)$</td>
<td>$C_1$</td>
<td>$y^2 = x^5 - x + 1$</td>
<td>$\mathbb{Q}$</td>
</tr>
</tbody>
</table>
II. Character Theory

- Character Theory: $\text{USp}(2g)$
- Brauer-Klimyk formula
- Algorithm for computing irreducible characters
Notation

- **$G$:** Compact Lie group
  \[ \text{USp}(2g) = \{ g \in \text{GL}_{2g}(\mathbb{C}) \mid g \cdot J \cdot g^t = J, \ g \cdot \overline{g}^t = I_g \}, \ J = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}. \]

- A maximal torus $T$ of $G$: Its elements are
  \[ u = \begin{pmatrix} U & 0 \\ 0 & U^{-1} \end{pmatrix}, \text{ where } U = \begin{pmatrix} u_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & u_g \end{pmatrix}, u_i \in \mathbb{C}, |u_i| = 1. \]

- **Weight**: irreducible character of $T$. $\lambda : T \to \mathbb{C}, \ \lambda(u) = u_1^{k_1} u_2^{k_2} \ldots u_g^{k_g}$ for $(k_1, k_2, \ldots, k_g) \in \mathbb{Z}^g$. They form a lattice $\Lambda$.

- **Dominant weights**: $\lambda$ with $(k_1, k_2, \ldots, k_g) \in \mathbb{N}^g$, $k_1 \geq k_2 \geq \ldots \geq k_g$.

- **Fundamental dominant weights**: $\varpi_1, \varpi_2, \ldots, \varpi_g$, corresponding to $(1, 0, \ldots, 0), (1, 1, 0, \ldots, 0), \ldots, (1, 1, \ldots, 1)$. 

Irreducible characters of $\text{USp}(2g) + \text{Brauer-Klimyk formula}$

- The theory of the highest weight applied to $G = \text{USp}(2g)$ gives:
  \[
  \{\text{Irreducible characters } \chi \text{ of } G\} \xleftarrow{1-1} \Lambda_+ = \{\text{Dominant weights } \lambda \text{ of } G\}
  \]
- Using the basis $\varpi = \{\varpi_1, \ldots, \varpi_g\}$, $\lambda \in \Lambda_+$ iff $[\lambda]_{\varpi} = (n_1, \ldots, n_g) \in \mathbb{N}_g^g$.
  
  Let $W$ be the Weyl group $W := N(T)/T$ of $G$ and $\rho = \sum_{i=1}^{g} \varpi_i$.

**Theorem (Brauer-Klimyk Formula) \(\sim\) Recursive way to compute $\chi_\lambda$**

Given $\mu, \lambda \in \Lambda_+$. We want to compute $\chi_\mu \chi_\lambda$.

- Decompose $\chi_\mu$ into weights: $\chi_\mu = \sum \nu m_\nu \nu$.
- For each $\nu$:
  - Find $w_\nu \in W$ such that $\eta_\nu := w_\nu (\lambda + \nu + \rho) \in \Lambda_+$.
  - If $\eta_\nu \in \partial(\Lambda_+)$, define $\xi(\nu) = 0$, otherwise,
  - $w$ is unique, $\eta_\nu - \rho \in \Lambda_+$, and define $\xi(\nu) = (-1)^{\det(w_\nu)} \chi(\eta_\nu - \rho)$.
- Then $\chi_\mu \chi_\lambda = \sum \nu m_\nu \xi(\nu)$.
We apply the Brauer-Klimyk formula and design an algorithm.

**Algorithm 1** Compute Irreducible Characters of $\text{USp}(2g)$ in $\mathbb{Z}[\chi_1, \ldots, \chi_g]$

1. **def** $\text{Chi}(x)$ # $\chi_{\lambda}$ for $[\lambda]_\omega = x \in \mathbb{Z}^g_{\geq 0}$
2. **if** $x \notin \mathbb{N}^g$ :
   - **return** 0 # $\lambda$ should be dominant
3. **if** $\sigma(x) = 0$ :
   - **return** 1 # $x = (0, \ldots, 0)$
4. **if** $\sigma(x) = 1$ :
   - **return** the symbol $\chi_l$ # Recursive computing
5. **if** $\sigma(x) = e_l$ :
   - **return** $\text{Chi}(x - e_l) \text{Chi}(e_l) - \tilde{\chi}$
6. **Find** $1 \leq l \leq g$ such that $x_l \geq 1$
7. **Set** $\tilde{\chi} = \sum_{\nu \neq \omega} (-1)^{\text{det}(w)} m(\nu) \text{Chi}([w(\lambda + \rho + \nu) - \rho]_{\omega})$

I implemented this algorithm in Sage. For $g = 10$ and $d = 5$, it computes the first 3002 irreducible characters of $\text{USp}(20)$ with $\sigma(x) \leq 5$ in 780 seconds ($\approx 0.26$ s per irreducible character).

- $\sigma(x) = \sum_{i=1}^{g} x_i$, $x = (x_1, \ldots, x_g)$.
- We can also compute $\chi$ in the ring $\mathbb{Z}[s_1, \ldots, s_g]$. This requires the knowledge of the relations between the fundamental irreducible characters $\chi_i$ and $s_1, \ldots, s_g$.
- The size of $W$ is $2^g g!$. But we only need a set of generators, which is of size $g$, and we can find $w \in W$ quickly.
- The efficiency of this algorithm is best reflected in the computation for all $\chi_{\lambda}$ with $\sigma(x) \leq d$. 

$\sigma(x) = \sum_{i=1}^{g} x_i$, $x = (x_1, \ldots, x_g)$.
For $g = 2$ and $g = 3$, we have

<table>
<thead>
<tr>
<th>$\lambda$</th>
<th>$\chi_i$</th>
<th>$\chi_\lambda$ in terms of $s_i$</th>
<th>$a_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0)</td>
<td>$\chi_0$</td>
<td>$s_0$</td>
<td>$a_0$</td>
</tr>
<tr>
<td>(1, 0)</td>
<td>$\chi_1$</td>
<td>$s_1$</td>
<td>$a_1$</td>
</tr>
<tr>
<td>(0, 1)</td>
<td>$\chi_2$</td>
<td>$s_2 + 1$</td>
<td>$a_2 - 1$</td>
</tr>
<tr>
<td>(2, 0)</td>
<td>$\chi_1^2 - \chi_2 - 1$</td>
<td>$s_2^2 - s_2^2 + 2s_2 - 2$</td>
<td>$a_1^2 - a_2$</td>
</tr>
<tr>
<td>(1, 1)</td>
<td>$\chi_1 \chi_2 - \chi_1$</td>
<td>$s_1 s_2$</td>
<td>$a_1 a_2 - 2a_1$</td>
</tr>
<tr>
<td>(0, 2)</td>
<td>$\chi_2^2 - \chi_1^2 + \chi_2$</td>
<td>$s_2^3 - 2s_1 s_2 - 3s_1$</td>
<td>$a_2^2 - a_1^2 - a_2$</td>
</tr>
<tr>
<td>(3, 0)</td>
<td>$\chi_1^3 - 2\chi_1 \chi_2 - \chi_1$</td>
<td>$s_1^2 s_2 - s_2^3 - 3s_2 - 1$</td>
<td>$a_1^3 - 2a_1 a_2 + a_1$</td>
</tr>
<tr>
<td>(2, 1)</td>
<td>$\chi_1^2 \chi_2 - \chi_1^2 - \chi_2 + 1$</td>
<td>$s_1^2 s_2^2 - s_2^3 - 3s_2 - 1$</td>
<td>$a_1^2 a_2 - a_2^2 - 2a_1^2 + a_2 + 1$</td>
</tr>
<tr>
<td>(1, 2)</td>
<td>$\chi_1 \chi_2^2 - \chi_2^3 + \chi_1$</td>
<td>$s_1^2 s_2^2 + 2s_1 s_2 + 2s_1$</td>
<td>$a_1 a_2^2 - a_1^3 - 2a_1 a_2 + 2a_1$</td>
</tr>
<tr>
<td>(0, 3)</td>
<td>$\chi_2^3 - 2\chi_1 \chi_2^2 + 2\chi_2^2 + \chi_1^2 - 1$</td>
<td>$s_2^3 - 2s_1^2 s_2 + 3s_1^2 s_2 + s_2^3 + 7s_2 + 2$</td>
<td>$a_2^3 - 2a_1^2 a_2 - a_2^2 + 3a_1^2 - a_2$</td>
</tr>
</tbody>
</table>

$g = 2$

<table>
<thead>
<tr>
<th>$\lambda$</th>
<th>$\chi_i$</th>
<th>$\chi_\lambda$ in terms of $s_i$</th>
<th>$a_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0, 0)</td>
<td>$\chi_0$</td>
<td>$s_0$</td>
<td>$a_0$</td>
</tr>
<tr>
<td>(1, 0, 0)</td>
<td>$\chi_1$</td>
<td>$s_1$</td>
<td>$a_1$</td>
</tr>
<tr>
<td>(0, 1, 0)</td>
<td>$\chi_2$</td>
<td>$s_2 + 2$</td>
<td>$a_2 - 1$</td>
</tr>
<tr>
<td>(0, 0, 1)</td>
<td>$\chi_3$</td>
<td>$s_3 + s_1$</td>
<td>$a_3 - a_1$</td>
</tr>
<tr>
<td>(2, 0, 0)</td>
<td>$\chi_1^2 - \chi_2 - 1$</td>
<td>$s_1 s_2 - s_2 - 3$</td>
<td>$a_1^2 - a_2$</td>
</tr>
<tr>
<td>(1, 1, 0)</td>
<td>$\chi_1 \chi_2 - \chi_3 - \chi_1$</td>
<td>$s_1 s_2 - s_3$</td>
<td>$a_1 a_2 - a_1 - a_3$</td>
</tr>
<tr>
<td>(1, 0, 1)</td>
<td>$\chi_1 \chi_3 - \chi_2$</td>
<td>$s_1^2 s_2 + s_2^2 - s_2 - 2$</td>
<td>$a_1^2 a_3 - a_2 + 1$</td>
</tr>
<tr>
<td>(0, 2, 0)</td>
<td>$\chi_2^2 - \chi_1 \chi_3 - \chi_1^2 + \chi_2$</td>
<td>$s_2^2 - s_1 s_3 - 2s_1 + 5s_2 + 6$</td>
<td>$a_2^2 - a_1 a_3 - a_2$</td>
</tr>
<tr>
<td>(0, 1, 1)</td>
<td>$\chi_2 \chi_3 - \chi_1 \chi_2 + \chi_3$</td>
<td>$s_2 s_3 + 3s_3 + s_1$</td>
<td>$a_2 a_3 - 2a_1 a_2 + a_1$</td>
</tr>
<tr>
<td>(0, 0, 2)</td>
<td>$\chi_3^2 - \chi_2^2 + \chi_1 \chi_3$</td>
<td>$s_3^2 - s_2^2 + 3s_1 s_3 + 2s_1^2 - 4s_2 - 4$</td>
<td>$a_3^2 - a_2^2 - a_1 a_3 + 2a_2 - 1$</td>
</tr>
</tbody>
</table>

$g = 3$
III. Explicit computation of Frobenius distributions

- Input, Computation, and Output
- Heuristic behavior in genus, degree, and sample size
- Moment sequences vs. orthogonality relations
- Strategy for non-generic curves
- One more example
- Expected orthogonality relations
- Conclusion
General setting

- The input:
  - A curve $C$ over $\mathbb{Q}$ of genus $g$.
  - The set $S = \{p_k\}_{k=1}^n$ of the first $n$ primes of good reduction of $C$.
  - A candidate subgroup $H$ of $G = \text{USp}(2g)$.
  - An unweighted degree $d$, for which we consider the set $I = I_d$ of dominant weights $\lambda$ of $G$ with $\sigma([\lambda]_\omega) \leq d$, and their corresponding irreducible characters $\chi_\lambda$ (which are pre-computed once and for all using Algorithm 1).
General setting

- **The input:**
  - A curve $C$ over $\mathbb{Q}$ of genus $g$.
  - The set $S = \{p_k\}_{k=1}^n$ of the first $n$ primes of good reduction of $C$.
  - A candidate subgroup $H$ of $G = \text{USp}(2g)$.
  - An upper bound $d$ for the unweighted degree which determines a set $I$ of dominant weights.

- **We compute:**
  - The (real) Weil polynomials $F_p$ of the Frobenius action, as a collection of values $\{(s_1, s_2, \ldots, s_g)_p\}_{p \in S}$.
  - For $\lambda, \mu \in I$, the error
    \[
    \text{err}_H(\lambda, \mu, n) = \frac{1}{n} \sum_{p \in S} \chi_\lambda(F_p) \chi_\mu(F_p) - \langle \chi_\lambda, \chi_\mu \rangle_H.
    \]
General setting

- **The input:**
  - A curve $C$ over $\mathbb{Q}$ of genus $g$.
  - The set $S = \{p_k\}_{k=1}^n$ of the first $n$ primes of good reduction of $C$.
  - A candidate subgroup $H$ of $G = \text{USp}(2g)$.
  - An upper bound $d$ for the unweighted degree which determines a set $I$ of dominant weights.

- **We compute:**
  - The set of Frobenius $\{F_p = (s_1, s_2, \ldots, s_g)_p\}_{p \in S}$
  - For $\lambda, \mu \in I$, the error
    $$\text{err}_H(\lambda, \mu, n) = \frac{1}{n} \sum_{p \in S} \chi_\lambda(F_p) \chi_\mu(F_p) - \langle \chi_\lambda, \chi_\mu \rangle_H.$$ 

- **Outputs:**
  - The maximal error $\text{Err}_H(n) := \max_{\lambda, \mu \in I} \text{err}_H(\lambda, \mu, n)$.
  - The standard deviation of errors $\text{SErr}_H(n) := \sqrt{\frac{\sum_{k=1}^n \text{Err}_H(k)^2}{n}}$. 

Yih-Dar Shieh (I2M)
Based on an analysis of experimental data for varying genus \( g \), degree \( d \), and sample size \( n \), we find:

- For fixed \( d \) and \( n \), \( \text{Err}(n) \) does not increase significantly when \( g \) increases.

- For a fixed curve \( C \) (so is \( g \)) and fixed \( n \), \( \text{Err}(n) \) increases very slowly when \( d \) increases (so the number of irreducible characters used increases).

- For a fixed \( C \) and fixed \( d \), \( \text{Err}(n) \approx O\left(\frac{1}{\sqrt{n}}\right)\).
We investigate the behavior of $\text{Err}(n)$ in $g$. We choose a generic hyperelliptic curve $y^2 = x^{2g+1} + x + 1$ of genus $g$ for $g = 2, 3, 4, 5, 6$, $H = \text{USp}(2g)$, $d = 1$ and $n \leq 2^{12}$. 

$g = 2$, $\text{Err}(n)$  

$g = 2$, $\text{SErr}(n)$  

$g = 5$, $\text{Err}(n)$  

$g = 5$, $\text{SErr}(n)$  

$g = 3$, $\text{Err}(n)$  

$g = 3$, $\text{SErr}(n)$  

$g = 6$, $\text{Err}(n)$  

$g = 6$, $\text{SErr}(n)$  

$g = 4$, $\text{Err}(n)$  

$g = 4$, $\text{SErr}(n)$
We are interested in how $\text{Err}(n)$ behave in $d$. We fix the genus $g = 2$. The number $\#(d)$ of irreducible characters is the number of solutions $(m_1, m_2)$ of $m_1 + m_2 \leq d$, i.e. $\#(d) = (d + 2)(d + 1)/2$.

$$
\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
    d   & 1   & 2 & 3 & 4 & 5 & 6 \\
\hline
\#(d) & 3   & 6 & 10 & 15 & 21 & 28 \\
\hline
\text{Err}(2^{12}) & 0.0155 & 0.1010 & 0.1893 & 0.2105 & 0.2105 & 0.2105 \\
\text{Err}(2^{14}) & 0.0060 & 0.0256 & 0.0378 & 0.0711 & 0.0988 & 0.1425 \\
\hline
\end{array}
$$

Errors's behavior in $d$ for $g = 2$
We wonder how many samples will give a reasonable result to identify the Sato-Tate group of $C$, so we study $\text{Err}(n)$ when $n$ increases. We fix $g = 1$, $E : y^2 = x^3 + x + 1$ and $d = 8$. We compute $2^{26}$ samples and plot the function $\text{Err}(n)$ for $n = 2^{10}k$, $k = 1, 2, \ldots, 2^{16}$. The following table shows the pictures of $\text{Err}(2^{10}k)$ and $\text{SErr}(2^{10}k)$:
Goal: Compare moment sequences with orthogonality relations of irreducible characters.

We write a normalized Weil polynomial as

\[ P(x) = x^{2g} - a_1 x^{2g-1} + a_2 x^{2g-2} + \cdots + a_{2g-2} x^2 - a_{2g-1} x + 1, \quad a_i = a_{2g-i}. \]

For a Frobenius distribution, we can study the moment sequences of \( a_1, a_2, \ldots, a_g \) with respect to the Haar measure of a conjectural Sato-Tate group \( H \).

Example 1: \( H = \text{USp}(4) \). The expected values of moments are given in the columns with \( N = \infty \). For \( n \geq 5 \), even with \( 2^{16} \) sample points, we don’t obtain useful approximations of \( M_n[a_1] \) and \( M_n[a_2] \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( N = 2^{12} )</th>
<th>( N = 2^{16} )</th>
<th>( N = \infty )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.002</td>
<td>0.006</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0.984</td>
<td>0.996</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>0.046</td>
<td>-0.001</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>2.833</td>
<td>2.970</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>0.196</td>
<td>-0.128</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>12.306</td>
<td>13.743</td>
<td>14</td>
</tr>
<tr>
<td>7</td>
<td>0.397</td>
<td>-1.487</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>66.441</td>
<td>81.446</td>
<td>84</td>
</tr>
<tr>
<td>9</td>
<td>-3.853</td>
<td>-14.304</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>409.298</td>
<td>565.972</td>
<td>594</td>
</tr>
</tbody>
</table>

\[ M_n[a_1] \]

\[ M_n[a_2] \]

Table: Moments for \( g = 2, \ H = \text{USp}(4), \ C : y^2 = x^5 + x + 1 \)
Now we use orthogonality relations of irreducible characters for $\text{USp}(4)$. We take $d = 2$. There are 6 irreducible characters and we denote them by $\chi_i$ for $0 \leq i \leq 5$.

\[ N = 2^{10} \]

Even with $2^{10}$ sample points, the numerical inner products approximate very well to the expected values. This comparison shows that the orthogonality relations of irreducible characters is much more suitable for the study of Sato-Tate groups than using moment sequences.
Example 2: Now we consider the family of non-hyperelliptic genus 3 curves $C$ with an involution, which are given by $y^4 + g(x)y^2 + h(x) = 0$. Such curves admit a degree 2 cover to an elliptic curve $E$.

- We have $0 \rightarrow A \rightarrow \text{Jac}(C) \xrightarrow{\pi_*} E \rightarrow 0$ of abelian varieties, where $A$ is the kernel of $\pi_*$.  
- For any Frobenius action $F_{p,C}$ on $C$, we obtain a pair $(F_{p,E}, F_{p,A})$ of Frobenius on $E$ and $A$ and their characteristic polynomials satisfy $P_{p,C} = P_{p,E}P_{p,A}$.

We can study the distributions of both $F_{p,E}$ and $F_{p,A}$ over the family. We use the groups $SU(2)$ and $USp(4)$, respectively. We computed the data for $p \leq 47$ and over a set of curves in this family. The results show that both distributions are the generic cases.

<table>
<thead>
<tr>
<th>Using SU(2)</th>
<th>Using USp(4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00 0.07 -0.01 0.00 0.00 0.00</td>
<td>1.00 0.00 -0.06 0.07 0.00 0.02</td>
</tr>
<tr>
<td>0.07 0.99 0.07 -0.01 0.00 0.00</td>
<td>0.00 1.01 0.00 0.00 0.01 0.00</td>
</tr>
<tr>
<td>-0.01 0.07 0.99 0.07 -0.01 0.00</td>
<td>-0.06 0.00 1.09 -0.01 0.00 -0.09</td>
</tr>
<tr>
<td>0.00 -0.01 0.07 0.99 0.07 -0.01</td>
<td>0.07 0.00 -0.01 1.02 0.00 0.07</td>
</tr>
<tr>
<td>0.00 0.00 -0.01 0.07 0.99 0.06</td>
<td>0.00 0.01 0.00 0.00 1.06 0.00</td>
</tr>
<tr>
<td>0.00 0.00 0.00 -0.01 0.06 0.92</td>
<td>0.02 0.00 -0.09 0.07 0.00 1.08</td>
</tr>
</tbody>
</table>
If we consider the distribution of $F_{p,C}$ and use the irreducible characters of $\text{USp}(6)$, we obtain

\[
\begin{array}{cccccc}
1.00 & 0.07 & 0.94 & -0.27 & 0.07 & -0.16 \\
0.07 & 2.01 & -0.35 & 0.95 & -0.06 & 2.04 \\
0.94 & -0.35 & 3.00 & -0.31 & 1.06 & -1.16 \\
-0.27 & 0.95 & -0.31 & 2.13 & -0.70 & 2.05 \\
0.07 & -0.06 & 1.06 & -0.70 & 3.07 & -1.16 \\
-0.16 & 2.04 & -1.16 & 2.05 & -1.16 & 6.24
\end{array}
\]

Using $\text{USp}(6)$

\[
\begin{array}{cccccc}
1 & 0 & 1 & 0 & 0 & 0 \\
0 & 2 & 0 & 1 & 0 & 2 \\
1 & 0 & 3 & 0 & 1 & -1 \\
0 & 1 & 0 & 2 & -1 & 2 \\
0 & 0 & 1 & -1 & 3 & -1 \\
0 & 2 & -1 & 2 & -1 & 6
\end{array}
\]

\[
\begin{array}{cccccc}
1 & 0 & 1 & 0 & 0 & 0 \\
0 & 2 & 0 & 1 & 0 & 2 \\
1 & 0 & 3 & 0 & 1 & 0 \\
0 & 1 & 0 & 2 & 0 & 2 \\
0 & 0 & 1 & 0 & 3 & 0 \\
0 & 2 & 0 & 2 & 0 & 6
\end{array}
\]

Rounded values \quad Expected values

We obtain negative numbers on the left side of the above table, which should not appear, and they are caused by the small number of primes used to produce the sample.
We guess that the distribution of $F_{p,C}$ is determined by $\text{SU}(2) \times \text{USp}(4)$. However, we need to verify that the distributions on $E$ and on $A$ are independent. We use the products of the first 4 irreducible characters of $\text{SU}(2)$ and $\text{USp}(4)$, which are irreducible characters of $\text{SU}(2) \times \text{USp}(4)$, and the data supports our conjecture.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>0.1</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>-0.1</th>
<th>-0.3</th>
<th>0</th>
<th>0</th>
<th>0.1</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.3</td>
<td>-0.1</td>
<td>-0.3</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.3</td>
<td>-0.1</td>
<td>-0.3</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.3</td>
<td>-0.1</td>
<td>-0.3</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>-0.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.2</td>
<td>1</td>
<td>-0.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.2</td>
<td>1</td>
<td>-0.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>-0.1</td>
<td>-0.3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>-0.3</td>
<td>-0.1</td>
<td>-0.3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>0</td>
<td>-0.3</td>
<td>0</td>
<td>-0.2</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>-0.3</td>
<td>-0.1</td>
<td>-0.3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>1</td>
<td>0.1</td>
<td>0</td>
<td>-0.2</td>
<td>0</td>
<td>-0.2</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>-0.3</td>
<td>-0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-0.2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.3</td>
<td>0</td>
<td>1</td>
<td>-0.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.3</td>
<td>0</td>
<td>-0.2</td>
<td>0</td>
<td>-0.2</td>
<td>0</td>
<td>-0.1</td>
<td>0</td>
<td>-0.1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.2</td>
<td>0</td>
<td>-0.2</td>
<td>0</td>
<td>-0.2</td>
<td>0</td>
<td>-0.1</td>
<td>1</td>
<td>-0.1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-0.1</td>
<td>0</td>
<td>0</td>
<td>-0.1</td>
</tr>
</tbody>
</table>

Using $\text{SU}(2) \times \text{USp}(4)$
Example 3: We study the curve $C : y^2 = x^8 + 1$, studied in [Fité-Sut.].

- We have the quotient maps:

- We focus on the identity component, and thus restrict to $p \equiv 1 \pmod{8}$. In this case, $E_2 \cong \tilde{E}_2$ over $\mathbb{F}_p$.

- The identity component of the Sato-Tate group of $C$ is determined by $E_1$ and $E_2$, which both have CM, hence it should be $SO(2)^2$. We verify this using $2^{12}$ points on each curve, rather than $2^{40}$ in [Fité-Sut.].
Here is a list of the expected values of the orthogonality relations, for the irreducible characters $\chi_0, \chi_1, \chi_2$ and $\chi_{(2,0)}$ of $\text{USp}(4)$ restricting to some subgroups.

The groups $F_\ast$ are those Sato-Tate groups whose identity component is $F = \text{SO}(2) \times \text{SO}(2)$.

\[
\begin{array}{cccc}
1 & 0 & 1 & 2 \\
0 & 4 & 0 & 0 \\
1 & 0 & 5 & 6 \\
2 & 0 & 6 & 12 \\
\end{array} & \begin{array}{cccc}
1 & 0 & 1 & 1 \\
0 & 3 & 0 & 0 \\
1 & 0 & 3 & 3 \\
1 & 0 & 3 & 7 \\
\end{array} & \begin{array}{cccc}
1 & 0 & 1 & 0 \\
0 & 2 & 0 & 0 \\
1 & 0 & 3 & 2 \\
0 & 0 & 2 & 8 \\
\end{array} & \begin{array}{cccc}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 2 & 1 \\
0 & 0 & 1 & 4 \\
\end{array} & \begin{array}{cccc}
1 & 0 & 1 & 0 \\
0 & 2 & 0 & 0 \\
1 & 0 & 2 & 1 \\
0 & 0 & 1 & 5 \\
\end{array}
\]

\[
\begin{array}{cccc}
1 & 0 & 1 & 1 \\
0 & 3 & 0 & 0 \\
1 & 0 & 3 & 3 \\
1 & 0 & 3 & 6 \\
\end{array} & \begin{array}{cccc}
1 & 0 & 1 & 0 \\
0 & 2 & 0 & 0 \\
1 & 0 & 2 & 1 \\
0 & 0 & 1 & 4 \\
\end{array} & \begin{array}{cccc}
1 & 0 & 1 & 0 \\
0 & 2 & 0 & 0 \\
1 & 0 & 2 & 1 \\
0 & 0 & 1 & 3 \\
\end{array} & \begin{array}{cccc}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 2 & 0 \\
0 & 0 & 0 & 2 \\
\end{array} & \begin{array}{cccc}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
\end{array}
\]

$G_{1,3} = \text{SO}(2) \times \text{SU}(2)$ and $G_{3,3} = \text{SU}(2) \times \text{SU}(2)$. 
The moment sequences of $a_1^2$ and $a_2$ for the groups $D_{6,2}$ and $F_{ab}$ are given by

$$
\begin{array}{cccccc}
 n & 1 & 2 & 3 & 4 & 5 & 6 \\
 D_{6,2} & 2 & 18 & 200 & 2450 & 31752 & 427812 \\
 F_{ab} & 2 & 18 & 200 & 2450 & 31752 & 426888 \\
\end{array}
$$

Using orthogonality relations, we also need to consider more irreducible characters to distinguish them.

Expected values for $F_{ab}$

$$
\begin{array}{cccccccc}
1 & 0 & 1 & 0 & 0 & 2 & 0 & 1 & 0 & 1 \\
0 & 2 & 0 & 0 & 4 & 0 & 4 & 0 & 6 & 0 \\
1 & 0 & 3 & 2 & 0 & 4 & 0 & 7 & 0 & 5 \\
0 & 0 & 2 & 8 & 0 & 4 & 0 & 14 & 0 & 8 \\
0 & 4 & 0 & 0 & 12 & 0 & 12 & 0 & 20 & 0 \\
2 & 0 & 4 & 4 & 0 & 10 & 0 & 14 & 0 & 10 \\
0 & 4 & 0 & 0 & 12 & 0 & 14 & 0 & 22 & 0 \\
1 & 0 & 7 & 14 & 0 & 14 & 0 & 37 & 0 & 25 \\
0 & 6 & 0 & 0 & 20 & 0 & 22 & 0 & 40 & 0 \\
1 & 0 & 5 & 8 & 0 & 10 & 0 & 25 & 0 & 20 \\
\end{array}
$$

Sample means for $D_{6,2}$ from $y^2 = x^6 + 2$ over $\mathbb{Q}$, using $2^{16}$ sample points
To distinguish the case of $D_{6,2}$ from $F_{ab}$, one can consider the primes $p$ for which we have $\tilde{a}_1^2 - 4(\tilde{a}_2 - 2p) = 0$ and $\tilde{a}_1 \neq 0$. If the Sato-Tate group is $D_{6,2}$, restricting to such primes gives the identity component $SO(2)$ of $D_{6,2}$.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>0</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>11</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>18</td>
<td>34</td>
<td></td>
</tr>
</tbody>
</table>

Expected values for $SO(2)$

<table>
<thead>
<tr>
<th></th>
<th>1.0</th>
<th>0.0</th>
<th>3.0</th>
<th>3.9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0</td>
<td>7.9</td>
<td>0.0</td>
<td>-0.1</td>
<td></td>
</tr>
<tr>
<td>3.0</td>
<td>0.0</td>
<td>10.8</td>
<td>17.4</td>
<td></td>
</tr>
<tr>
<td>3.9</td>
<td>-0.1</td>
<td>17.4</td>
<td>32.8</td>
<td></td>
</tr>
</tbody>
</table>

Sample means for $D_{6,2}$ from $y^2 = x^6 + 2$ over $\mathbb{Q}$, for a sample of size about 1350 that satisfy $\tilde{a}_1^2 - 4(\tilde{a}_2 - 2p) = 0$ and $\tilde{a}_1 \neq 0$. 
Conclusion

The analysis of empirical data shows that the errors of experimental values with respect to the expected values

- do not increase significantly when the genus $g$ increases,
- increase very slowly when the number of irreducible characters increases,
- is of order $O\left(\frac{1}{\sqrt{n}}\right)$ with respect to the sample size,
- are very small, especially compared to the approach of using moments,

when the expected values of the inner products are small (e.g. generic case). For non-generic cases, we have seen that it is better to use the character theory of the smallest group we know containing the Sato-Tate group. When we study families of curves with particular structure, like RM curves, this is very useful. This way, the orthogonality relations always have small integer entries.

Conclusion: Character theory with orthogonality relations is a good approach for the study of Sato-Tate groups!