On Sato-Tate groups $\mathrm{SO}(2n+1)$ and the exceptional group UG_2

David Kohel
Institut de Mathématiques de Marseille

Frobenius distributions III
5-7 October 2022

Abelian varieties and Galois representations

Let A/K be an abelian variety over a number field K, $\mathcal{O} = \mathcal{O}_K[1/N\ell]$ be an S-order over which A has good reduction. We associate a Frobenius $\pi_\mathfrak{p} \in \mathrm{Aut}(T_\ell(A))$ to any prime $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$, acting on the Tate module by means of its reduction

$$T_\ell(A) \simeq T_\ell(\overline{A}), \tag{1}$$

giving characteristic polynomial

$$P(T) = T^{2g} - a_1 T^{2g-1} + \cdots + p^g \tag{2}$$

The isomorphism (1) depends on a choice of place v over $\mathfrak{p}$ in $K_{A,\ell} = K[A[\ell^\infty]]$ in order to fix the compatible isomorphisms

$$\begin{tikzcd} A[\ell^n] \arrow[r] \arrow[d, hook] & \overline{A}[\ell^n] \arrow[d, hook] \\ A(K_{A,\ell}) \arrow[r] & A(k_v) \end{tikzcd}$$

from which (1) is induced. Any other choice induces a conjugate lifting of $\pi_\mathfrak{p}$ to $\mathrm{Aut}(T_\ell(A))$, and the characteristic polynomial (2) remains invariant of this choice.

Abelian varieties and Galois representations

Choosing a symplectic basis for $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}_\ell$ with respect to the Weil paring, we let

$$\begin{tikzcd} \rho_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \arrow[rr] \arrow[dr, two heads] & & \mathrm{GSp}(2g, \mathbb{Q}_\ell) \cong \mathrm{Aut}(V_\ell(A)). \\ & \mathrm{Gal}(K_{A,\ell}/K) \arrow[ur, hook] & \end{tikzcd}$$

Let G_ℓ be the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}(\overline{K}/K))$, and G_ℓ^1 be the unitary subgroup with respect to the symplectic structure.

Let $\iota : \mathbb{Q}_\ell \longrightarrow \mathbb{C}$ be a fixed embedding, from which we obtain

$$\mathrm{GSp}(2g, \mathbb{Q}_\ell) \to \mathrm{GSp}(2g, \mathbb{Q}_\ell) \otimes_\iota \mathbb{C} = \mathrm{GSp}(2g, \mathbb{C}),$$

the induced image in $\mathrm{GSp}(2g, \mathbb{C})$. Finally, we denote by $\mathrm{USp}(2g)$ the compact subgroup of unitary symplectic matrices.

Sato-Tate groups

Definition

The Sato-Tate group $\mathrm{ST}(A)$ *is a maximal compact Lie subgroup of* $G_\ell^1 \otimes_\iota \mathbb{C}$ *in* $\mathrm{USp}(2g)$.

As a consequence of the definition, while the lift of the Frobenius automorphism depends on a choice of place over $\mathfrak{p}$, its normalized conjugacy class

$$\left[\pi_{\mathfrak{p}} \otimes_\iota \frac{1}{\sqrt{N\mathfrak{p}}}\right] = \left[\rho_{A,\ell}(\mathrm{Frob}(\mathfrak{p})) \otimes_\iota \frac{1}{\sqrt{N\mathfrak{p}}}\right]$$

lies in $G_\ell^1 \otimes_\iota \mathbb{C}$ and is well-defined in the set $\mathrm{C}\ell(\mathrm{ST}(A))$ of conjugacy classes. Its characteristic polynomial is

$$P(T) = T^{2g} - \tilde{a}_1 T^{2g-1} + \cdots - \tilde{a}_1 T + 1,$$

where $\tilde{a}_i = \dfrac{a_i}{\sqrt{N\mathfrak{p}}^i} = \tilde{a}_{2g-i}$, interpretted as a character on $\mathrm{ST}(A)$.

Characters on compact Lie groups

The interpretation of $\tilde{a}_i$ as a character on $\mathrm{ST}(A)$ implies that its expectation

$$\mathbb{E}[\tilde{a}_i] = \int_G \tilde{a}_i d\mu_G$$

is an integer. In fact

$$\langle \tilde{a}_i, \tilde{a}_j \rangle = \mathbb{E}[\tilde{a}_i \overline{\tilde{a}_j}]$$

is the inner product of characters : if

$$\tilde{a}_i = \sum_k m_k \chi_{\varepsilon_k}, \quad \tilde{a}_j = \sum_k n_k \chi_{\varepsilon_k},$$

then

$$\langle \tilde{a}_i, \tilde{a}_j \rangle = \sum_k m_k n_k \in \mathbb{N},$$

by the orthogonality relations on characters.

Effective characters

$\mathbb{E}[\chi]$ can be effectively computed: if S is a finite initial set of primes (ordered by norm), set

$$\mathbb{E}_S[\chi] = \frac{1}{|S|}\sum_{\mathfrak{p}\in S}\chi(\pi_{\mathfrak{p}}), \text{ and so } \mathbb{E}[\chi] = \lim_{|S|\to\infty}\mathbb{E}_S[\chi].$$

We represent χ as a polynomial in $\mathbb{Q}[\tilde{a}_1, \ldots, \tilde{a}_g]$.

N.B. While the characters $\{\tilde{a}_1, \ldots, \tilde{a}_g\}$ form a set of fundamental characters (generating the virtual character ring) for $\mathrm{USp}(2g)$, the restriction to a subgroup G may require rational coefficients to express the irreducible characters.

Since $\{\tilde{a}_1, \ldots, \tilde{a}_g\}$ for $\mathrm{USp}(2g)$ are real, $\langle \tilde{a}_i, \tilde{a}_j\rangle = \mathbb{E}[\tilde{a}_i\tilde{a}_j]$.

We may adjoin characters of the finite group G/G_0, where G_0 is the connected component to extend the known characters for G.

Moment sequences

Previous approaches considered the fixed characters $\tilde{a}_1, \ldots, \tilde{a}_g$ and sought to "recognize" $\mathrm{ST}(A)$ by the moment sequences

$$\begin{aligned} M_n(\tilde{a}_1) &= \mathbb{E}[\tilde{a}_1^n], \\ &\vdots \\ M_n(\tilde{a}_g) &= \mathbb{E}[\tilde{a}_g^n], \quad \text{for} \quad 1 \leq n \leq B. \end{aligned}$$

The problem with moment sequences is the growth: $\tilde{a}_i^n$ represents the n-th tensor product character, which decomposes into many smaller characters of high multiplicities. Thus for $\tilde{a}_i = \overline{\tilde{a}}_i$ real:

$$\langle \tilde{a}_i^n, \tilde{a}_i^n \rangle = M_{2n}(\tilde{a}_i) = \sum_k n_k^2 \text{ where } \tilde{a}_i^n = \sum_k n_k \chi_{\varepsilon_k},$$

giving a large integer $M_{2n}(\tilde{a}_i)$, whose convergence requires a large sample size, made worse by the large *variance* of $\tilde{a}_i^n$.

Variance

The moment $M_{2n}(\chi)$ is the self inner product of the character χ^n:

$$M_{2n}(\chi) = \mathbb{E}[\chi^{2n}] = \langle \chi^n, \chi^n \rangle.$$

Its variance is a a measure of the spread or dispersion of the distribution; by definition

$$\begin{aligned} \mathrm{var}(\chi^n) &= \mathbb{E}\left[\left(\chi^n - \mathbb{E}[\chi^n]\right)^2\right] \\ &= \mathbb{E}[\chi^{2n}] - \mathbb{E}[\chi^n]^2 = M_{2n}(\chi) - M_n(\chi)^2. \end{aligned}$$

When $M_n(\chi) = 0$, the variance equals $M_{2n}(\chi)$, and in general the growth of the moment sequence is exponential in n so that $M_{2n}(\chi)$ gives the dominate term in $\mathrm{var}(\chi^n)$.

Conclusion. The moment sequence is an interesting mathematical invariant, but computationally inefficient and impractical.

Character theory method

In his thesis Yih-Dar Shieh proposed instead to (pre)-compute some irreducible characters of a target $G \subset \mathrm{USp}(2g)$, in order to answer the question "Is $\mathrm{ST}(A) \subseteq G$?" to address "Is $G = \mathrm{ST}(A)$?".

By expressing $\chi_\varepsilon \in \mathbb{Q}[\tilde{a}_1, \ldots, \tilde{a}_g]$ as a polynomial, we have

$$\langle \chi_\varepsilon, \chi_{\varepsilon'} \rangle = \begin{cases} 1 & \text{if} \quad \varepsilon = \varepsilon', \\ 0 & \text{if} \quad \varepsilon \neq \varepsilon'. \end{cases}$$

The symplectic characters $\tilde{a}_1, \ldots, \tilde{a}_g$ are real, but a subgroup may have complex characters, for which we cannnot decompose further than $\chi = \chi_\varepsilon + \overline{\chi}_\varepsilon$. For such a character,

$$\langle \chi, \chi \rangle = \langle \chi_\varepsilon + \overline{\chi}_\varepsilon, \chi_\varepsilon + \overline{\chi}_\varepsilon \rangle = 2.$$

Weyl character ring

The *Weyl virtual character ring* $\mathcal{R}(G)$ is the formal direct sum module on irreducible characters. The irreducible characters can be indexed by a fundamental cone $\Lambda^+ \subset \mathbb{Z}^h$, where $h = \mathrm{rank}(G)$ and $\mathbb{Z}^h = \mathrm{Hom}(T, \mathrm{U}(1))$, for a maximal torus $T \subset G$.

The $\mathbb{Z}$-module $\mathcal{R}(G)$ forms a ring, equipped with tensor product as multiplication; addition is identified with direct sum.

Restriction of characters determines a homomorphism:

$$\mathrm{Res} : \mathcal{R}(\mathrm{USp}(2g)) = \mathbb{Z}[\tilde{a}_1, \ldots, \tilde{a}_g] \longrightarrow \mathcal{R}(\mathrm{ST}(A)) = \bigoplus_{\varepsilon \in \Lambda^+} \mathbb{Z}\chi_\varepsilon.$$

In what follows we will generalize this construction to families of abelian varieties with $\mathrm{ST}(A) \subseteq \mathrm{SO}(2n+1)$.

Orthogonal representations

Let $\mathrm{SO}(2n+1)$ be an orthogonal group, of rank n. The characteristic polynomial of an element A is:

$$P(T) = T^N - \tilde{a}_1 T^{N-1} + \tilde{a}_2 T^{N-2} - \cdots + \tilde{a}_{2n} T - 1.$$

and since $A^{-1} = A^t$, the eigenvalues are closed under the involution $\alpha \longmapsto \overline{\alpha} = \alpha^{-1}$ and hence

$$\begin{aligned} P(T) &= (T-1)\prod_{i=1}^{n}(T-\alpha_i)(T-\overline{\alpha}_i) \\ &= (T-1)\prod_{i=1}^{n}(T^2 - \tau_i T + 1). \end{aligned}$$

N.B. In particular there are n degrees of freedom in $P(T)$; here τ_i denotes $2\cos(\theta_i)$ in terms of the Frobenius angles.

Some combinatorics

This motivates the definition of the polynomial

$$Q(T) = \prod_{i=1}^{n}(T - \tau_i) = \sum_{i=0}^{n}(-1)^{(n-i)} s_i T^{n-i},$$

such that $P(T) = (T-1)T^n Q\left(\frac{T^2+1}{T}\right)$.

Suppose we are given, for $0 \le r \le n$, the data of Frobenius traces:

$$\mathrm{Tr}(\pi^r) = 1 + p_r = 1 + \sum_{i=1}^{n}(\alpha_i^r + \overline{\alpha}_i^r).$$

Then by the Girard-Newton formulae, we have

$$s_k = \frac{1}{k}\sum_{i=1}^{k}(-1)^{k-1} s_{k-i} p_i$$

from which we can construct s_k, hence $Q(T)$ and $P(T)$.

Katz character sums

In *Notes on* G_2, Katz introduced the exponential sums

$$S_r(\chi, \psi, x^N - tx) = \sum_{x \in \mathbb{F}_{p^r}} \chi_r(x)\psi_r(x^N - tx) \in \mathbb{Z}[\zeta_m, \zeta_p] \qquad (1)$$

where $\chi_r = \chi \circ \mathrm{N}_{\mathbb{F}_{p^r}/\mathbb{F}_p}$ and $\psi_r = \psi \circ \mathrm{Tr}_{\mathbb{F}_{p^r}/\mathbb{F}_p}$, with

- χ a multiplicative character of order m,
- ψ an additive character (of order p), and
- for any $p > 2N + 1$ and $N \geq 3$.

For $m = 2$, we define the normalized Katz sums:

$$\tilde{S}_r(\chi, \psi, x^N - tx) = \frac{S_r(\chi, \psi, x^N - tx)}{\eta(N)^r}.$$

where $\eta(N) = \chi(\varepsilon(N)N)G(\chi, \psi)$ is a Gauss sum.

Katz orthogonal sums

For $m = 2$ and odd N, Katz proves that his normalized sums

$$\tilde{S}_r(\chi, \psi, x^N - tx)$$

satisfy the trace distribution (as t varies) for a degree N representation of

$$\begin{array}{rll} & \mathrm{SO}(N) = \mathrm{SO}(2n+1) & \text{when } N \text{ is odd,} \\ \text{EXCEPT} & \mathrm{UG}_2 \subset \mathrm{SO}(7) & \text{when } N = 7. \end{array}$$

For even N, the sums to follow the trace distribution on $\mathrm{SU}(N)$.†

Here G_2 is the exceptional Lie group and we denote its compact subgroup in $\mathrm{SO}(7)$ by UG_2.

---

†This is a purely empirical observation, not treated by Katz in *Notes on G_2*.

Katz curves

Motivated by Katz sums, we define the Katz curve C_m for each m, equipped with a covering of C_1, as follows:

$$\begin{array}{l} C_m : y^p - y = x^N - tx \text{ where } x = z^m \\ \Big\downarrow \\ C_1 : y^p - y = x^N - tx \end{array}$$

It follows from the definition that

$$-\sum\sum S_r(\chi, \psi, x^N - tx) = |C_m(\mathbb{F}_{p^r})| - |C_1(\mathbb{F}_{p^r})|,$$

from which we see that the Katz sums determine the zeta function of the Prym variety B_m in the exact sequence

$$0 \longrightarrow B_m \longrightarrow \mathrm{Jac}(C_m) \longrightarrow \mathrm{Jac}(C_1) \longrightarrow 0.$$

Katz representations

This is rather remarkable: a family of abelian varieties whose Sato-Tate groups[‡] are naturally embedded in $\mathrm{SO}(2n+1)$, but, as the following lemma indicates, the genera are huge.

Lemma

$$g(C_m) - g(C_1) = \frac{(p-1)}{2}(m-1)N \text{ and } g(C_1) = \frac{(p-1)}{2}(N-1).$$

Remark. The cohomology modules $H^1(B_m)$ and $H^1(\mathrm{Jac}(C_1))$ are modules over $\mathbb{Z}[\zeta_m, \zeta_p]$ and $\mathbb{Z}[\zeta_p] \subset \mathbb{C}$, respectively, which, for m prime, should be considered as complex modules of dimension N and $N-1$. For computing their zeta functions, they behave like abelian varieties of dimension $n = \lfloor N/2 \rfloor = \mathrm{rank}(\mathrm{SO}(N))$.

[‡]The distribution is over t, which we refer to as a vertical Sato-Tate group.

Katz curves

Remark. The parameter t of C_m gives an absolute geometric invariant. As such, the curves C_m (or the Prym varieties B_m) have a one-dimensional moduli space, analogous to elliptic curves, to fake elliptic curves (QM abelian surfaces parametrized by Shimura curves), or certain genus 3 curves with prescribed automorphisms or configurations of Weierstrass points.

Despite the lower complexity of these objects, they exhibit behavior not observed in lower dimension. In particular $N = 7$ (and $m = 2$), this gives a representation of G_2.

On SO(7) and UG$_2$

We specialize to the parameters of $N = 7$ and $m = 2$, for which Katz normalized sums for $\mathrm{UG}_2 \subset \mathrm{SO}(7)$ decompose as:

$$\tilde{S}_r(\chi, \psi, t) = 1 + \alpha_1^r + \overline{\alpha}_1^r + \alpha_2^r + \overline{\alpha}_2^r + \alpha_3^r + \overline{\alpha}_3^r,$$

satisfying the defining relation $\alpha_1\alpha_2\alpha_3 = 1$ for UG$_2$. We write

$$P(T) = (T-1)\prod_{i=1}^{3}(T-\alpha_i)(T-\overline{\alpha}_i) = (T-1)\prod_{i=1}^{3}(T^2 - \tau_i T + 1).$$

and set

$$(s_1, s_2, s_3) = (\tau_1 + \tau_2 + \tau_3,\ \tau_1\tau_2 + \tau_1\tau_3 + \tau_2\tau_3,\ \tau_1\tau_2\tau_3).$$

The condition $\alpha_1\alpha_2\alpha_3 = 1$ for UG$_2$ translates as

$$\tau_1^2 + \tau_2^2 + \tau_3^2 = \tau_1\tau_2\tau_3 + 4,$$

or $s_1^2 = 2s_2 + s_3 + 4$ in terms of the symmetric sums.

Branching rules: from SO(7) to UG$_2$

Branching rules associated to an inclusion $H \subset G$ of Lie groups are decomposition formulas for irreducible characters under restriction:

$$\mathrm{Res} : \mathcal{R}(G) \longrightarrow \mathcal{R}(H).$$

For $G = \mathrm{SO}(7)$ and $H = \mathrm{UG}_2$ we have restriction map,

$$\mathrm{Res} : \mathcal{R}(\mathrm{SO}(7)) = \mathbb{Z}[s_1, s_2, s_3] \longrightarrow \mathcal{R}(\mathrm{UG}_2) = \mathbb{Z}[s_1, s_2]$$

taking s_3 to $s_1^2 - 2s_2 - 4$. The branching rules on the first irreducible characters are:

ε_i	χ_i	deg	$\mathrm{Res}(\chi_i)$	deg
$(1,0,0)$	$\chi_1 = s_1 + 1$	7	$\psi_1 = s_1 + 1$	7
$(0,1,0)$	$\chi_2 = s_1 + s_2 + 3$	21	$\psi_1 + \psi_2$	$7 + 14$
$(0,0,1)$	$\chi_3 = 2s_1 + s_2 + s_3 + 3$	35	$1 + \psi_1 + \psi_{(2,0)}$	$1 + 7 + 27$

Here χ_1, χ_2, χ_3 are the fundamental characters for $\mathrm{SO}(7)$, and ψ_1, ψ_2 are the fundamental characters for UG_2.

Recognizing UG_2

For identifying or *recognizing* a UG_2 representation inside of $\mathrm{SO}(7)$, it suffices to know data for only two symmetric sums (s_1, s_2).

The relation $s_1^2 = 2s_2 + s_3 + 4$ can be verified if we know s_3, which might be (computationally) expensive; otherwise we test whether

$$(\chi_1, \chi_2) = (s + 1,\ s_1 + s_2 + 3),$$

are irreducible, as on $\mathrm{SO}(7)$, or decompose as

$$(\chi_1, \chi_2) = (\psi_1, \psi_1 + \psi_2),$$

as on UG_2. This reduces to a simple test of the inner product matrix:

$$(\langle \chi_i, \chi_j \rangle) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Thanks for your attention!

RECOGNIZING UG_2

For identifying or *recognizing* a UG_2 representation inside of $\mathrm{SO}(7)$, it suffices to know data for only two symmetric sums (s_1, s_2).

The relation $s_1^2 = 2s_2 + s_3 + 4$ can be verified if we know s_3, which might be (computationally) expensive; otherwise we test whether

$$(\chi_1, \chi_2) = (s + 1,\ s_1 + s_2 + 3),$$

are irreducible, as on $\mathrm{SO}(7)$, or decompose as

$$(\chi_1, \chi_2) = (\psi_1, \psi_1 + \psi_2),$$

as on UG_2. This reduces to a simple test of the inner product matrix:

$$(\langle \chi_i, \chi_j \rangle) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Thanks for your attention!