Galois representations with specified Sato–Tate distributions

Daniel Miller

March 7, 2017

1 Introduction

(Summary of [3])

2 Notation and preliminary results

Now we loosely summarize the results of [1], adapting them as needed for our context. For a field F, write $G_F = \mathrm{Gal}(\overline{F}/F)$ for the absolute Galois group of F. If M is a G_F-module, write $\mathrm{H}^\bullet(F, M)$ in place of $\mathrm{H}^\bullet(G_F, M)$. All Galois representations will be to $\mathrm{GL}_2(\mathbf{Z}/l^n)$ or $\mathrm{GL}_2(\mathbf{Z}_l)$ for l a (fixed) rational prime, and all deformations will have fixed determinant, so we only consider the cohomology of $\mathrm{Ad}^0\,\bar{\rho}$, the induced representation on trace-zero matrices by conjugation.

If S is a set of rational primes, $\mathbf{Q}_S$ denotes the largest extension of $\mathbf{Q}$ unramified outside S. So $\mathrm{H}^i(\mathbf{Q}_S, -)$ is what is usually written as $\mathrm{H}^1(G_{\mathbf{Q},S}, -)$. If M is a $G_{\mathbf{Q}}$-module and S a finite set of primes, write

$$\text{Ш}^i_S(M) = \ker\left(\mathrm{H}^i(\mathbf{Q}_S, M) \to \prod_{p\in S} \mathrm{H}^i(\mathbf{Q}_p, M)\right).$$

If l is a rational prime and S a finite set of primes containing l, then for any $\mathbf{F}_l[G_{\mathbf{Q}_S}]$-module M, write $M^\vee = \hom_{\mathbf{F}_l}(M, \mathbf{F}_l)$ with the obvious $G_{\mathbf{Q}_S}$-action, and write $M^* = M^\vee(1)$ for the Cartier dual. By [2, Th. 8.6.7], there is an isomorphism $\text{Ш}^1_S(M^*) = \text{Ш}^2_S(M)^\vee$.

A *good (residual) representation* is an odd, absolutely irreducible, weight-2 representation $\bar{\rho}\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_l)$, where $l \geqslant 7$ is a rational prime. Roughly, good residual representations are well-behaved enough that we can prove a lot about them directly, without assume the modularity results of Khare–Wingenberger.

Theorem 1 ([4, Th. 1])**.** *Let $\bar{\rho}\colon G_{\mathbf{Q}_S} \to \mathrm{GL}_2(\mathbf{F}_l)$ be a good residual representation. Then there exists a weight-2 lift of $\bar{\rho}$ to $\mathbf{Z}_l$.*

Let $\bar\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_l)$ be a good representation. An unramified prime $p \not\equiv \pm 1 \pmod{l}$ is *nice* if $\mathrm{Ad}^0\,\bar\rho \simeq \mathbf{F}_l \oplus \mathbf{F}_l(1) \oplus \mathbf{F}_l(-1)$, i.e. if the eigenvalues of $\bar\rho(\mathrm{fr}_p)$ have ratio p. If p is nice, then all unramified torsion lifts of $\bar\rho|_{G_{\mathbf{Q}_p}}$ have lifts to characteristic zero.

Now we introduce some new terminology and notation to condense the lifting profess used in [1].

Fix a good residual representation $\bar\rho$. We will consider weight-2 deformations of $\bar\rho$ to $\mathbf{Z}/l^n$ and $\mathbf{Z}_l$. Call such a deformation a "lift of $\bar\rho$ to $\mathbf{Z}/l^n$ (resp. $\mathbf{Z}_l$)." We will often restrict the local behavior of such lifts, i.e. the restrictions of a lift to $G_{\mathbf{Q}_p}$ for p in some set of primes. The necessary constraints are captured in the following definition.

Let $\bar\rho$ be a good representation, $h\colon \mathbf{R}^+ \to \mathbf{R}^+$. An *$h$-bounded lifting datum* is a tuple $(\rho_n, R, U, \{\rho_p\}_{p\in R\cup U})$, where

1. $\rho_n\colon G_{\mathbf{Q}_R} \to \mathrm{GL}_2(\mathbf{Z}/l^n)$ is a lift of $\bar\rho$.
2. R and U are finite sets of primes, R containing l and all primes at which ρ_n ramifies.
3. $\pi_R(x) \leqslant h(x)\pi(x)$ for all x.
4. $\text{Ш}^1_R(\mathrm{Ad}^0\,\bar\rho) = \text{Ш}^2_R(\mathrm{Ad}^0\,\bar\rho) = 0$.
5. For all $p \in R\cup U$, $\rho_p \equiv \rho_n|_{G_{\mathbf{Q}_p}} \pmod{l^n}$.
6. For all $p \in R$, ρ_p is ramified.
7. ρ_n admits a lift to $\mathbf{Z}/l^{n+1}$.

If $(\rho_n, R, U, \{\rho_p\})$ is an h-bounded lifting datum, we call another h-bounded lifting datum $(\rho_{n+1}, R', U', \{\rho_p\})$ a *lift of* $(\rho_n, R, U, \{\rho_p\})$ if $U \subset U'$, $R \subset R'$, and for all $p \in R\cup U$, the two possible "ρ_p" agree.

Theorem 2. *Let $\bar\rho$ be a good residual representation, $h\colon \mathbf{R}^+ \to \mathbf{R}^+$ decreasing to zero. If $(\rho_n, R, U, \{\rho_p\})$ is an h-bounded lifting datum, $U' \supset U$ is a finite set of primes disjoint from R, and $\{\rho_p\}_{p\in U'}$ extends $\{\rho_p\}_{p\in U}$, then there exists an h-bounded lift $(\rho_{n+1}, R', U', \{\rho_p\})$ of $(\rho_n, R, U, \{\rho_p\})$.*

Proof. By [1, Lem. 8], there exists a finite set N of nice primes, such that the map

$$\mathrm{H}^1(\mathbf{Q}_{R\cup N}, \mathrm{Ad}^0\,\bar\rho) \to \prod_{p\in R} \mathrm{H}^1(\mathbf{Q}_p, \mathrm{Ad}^0\,\bar\rho) \times \prod_{p\in U'} \mathrm{H}^1_{\mathrm{nr}}(\mathbf{Q}_p, \mathrm{Ad}^0\,\bar\rho) \tag{1}$$

is an isomorphism. In fact, $\#N = \dim \mathrm{H}^1(\mathbf{Q}_{R\cup N}, \mathrm{Ad}^0\,\bar\rho^*)$, and the primes in N are chosen, one at a time, from Chebotarev sets. This means we can force them to be large enough to ensure that the bound $\pi_{R\cup N}(x) \leqslant h(x)\pi(x)$ continues to hold.

By our hypothesis, ρ_n admits a lift to $\mathbf{Z}/l^{n+1}$; call one such lift ρ^*. For each $p \in R\cup U'$, $\mathrm{H}^1(\mathbf{Q}_p, \mathrm{Ad}^0\,\bar\rho)$ acts simply transitively on lifts of $\rho_n|_{G_{\mathbf{Q}_p}}$ to

$\mathbf{Z}/l^{n+1}$. In particular, there are cohomology classes $f_p \in \mathrm{H}^1(\mathbf{Q}_p, \mathrm{Ad}^0\,\bar\rho)$ such that $f_p \cdot \rho^* \equiv \rho_p \pmod{l^{n+1}}$ for all $p \in R \cup U'$. Moreover, for all $p \in U'$, the class f_p is unramified. Since the map (1) is an isomorphism, there exists $f \in \mathrm{H}^1(\mathbf{Q}_{R\cup N}, \mathrm{Ad}^0\,\bar\rho)$ such that $f \cdot \rho^*|_{G_{\mathbf{Q}_p}} \equiv \rho_p \pmod{l^{n+1}}$ for all $p \in R \cup U'$.

Clearly $f \cdot \rho^*|_{G_{\mathbf{Q}_p}}$ admits a lift to $\mathbf{Z}_l$ for all $p \in R \cup U'$, but it does not necessarily admit such a lift for $p \in N$. By repeated applications of [3, Prop. 3.10], there exists a set $N' \supset N$, with $\#N' \leqslant 2\#N$, of nice primes and $g \in \mathrm{H}^1(\mathbf{Q}_{R\cup N'}, \mathrm{Ad}^0\,\bar\rho)$ such that $(g+f)\cdot\rho^*$ still agrees with ρ_p for $p \in R \cup U'$, and $(g+f)\cdot\rho^*$ is nice for all $p \in N'$. As above, the primes in N' are chosen one at a time from Chebotarev sets, so we can continue to ensure the bound $\pi_{R\cup N'}(x) \leqslant h(x)\pi(x)$. Let $\rho_{n+1} = (g+f)\cdot\rho^*$. Let $R' = R \cup N'$. For each $p \in R' \smallsetminus R$, choose a ramified lift ρ_p of $\rho_{n+1}|_{G_{\mathbf{Q}_p}}$ to $\mathbf{Z}_l$.

Since $\rho_{n+1}|_{G_{\mathbf{Q}_p}}$ admits a lift to $\mathbf{Z}/l^{n+2}$ (in fact, it admits a lift to $\mathbf{Z}_l$) for each p, and $Ш^2_{R'}(\mathrm{Ad}^0\,\bar\rho) = 0$, the deformation ρ_{n+1} admits a lift to $\mathbf{Z}/l^{n+2}$. Thus $(\rho_{n+1}, R', U', \{\rho_p\})$ is the desired lift of $(\rho_n, R, U, \{\rho_p\})$. □

3 Master theorem

Fix a good residual representation $\bar\rho$. We consider weight-2 deformations of $\bar\rho$. The final deformation, $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$, will be constructed as the inverse limit of a compatible collection of lifts $\rho_n\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/l^n)$. At any given stage, we will be concerned with making sure that there exists a lift to the next stage, that such a lift can be forced to have the necessary properties. Fix a sequence $(x_1, x_2, \dots)$ in $[-1,1]$. The set of unramified primes of ρ is not determined at the beginning, but at each stage there will be a large finite set U of primes which we know will remain unramified. Re-indexing (x_n) by these unramified primes, we will construct ρ so that for all unramified primes p, $\operatorname{tr}\rho(\mathrm{fr}_p) \in \mathbf{Z}$, satisfies the Hasse bound, and has $\operatorname{tr}\rho(\mathrm{fr}_p) \approx x_p$. Moreover, we can ensure that the set of ramified primes has density zero in a very strong sense (controlled by a parameter function h) and that our trace of Frobenii are very close to specified values, the "closeness" again controlled by a parameter function. Write $\pi_{\mathrm{ram}(\rho)}$ for the function which counts ρ_n-ramified primes.

Theorem 3. *Let l, $\bar\rho$, (x_n) be as above. Fix functions $h\colon \mathbf{R}^+ \to \mathbf{R}^+$ (resp. $b\colon \mathbf{R}^+ \to \mathbf{R}_{\geqslant 1}$) which decrease to zero (resp. increase to infinity). Then there exists a weight-2 deformation ρ of $\bar\rho$, such that*

1. *$\pi_{\mathrm{ram}(\rho)}(x) \ll h(x)\pi(x)$.*
2. *For each unramified prime p, $a_p = \operatorname{tr}\rho(\mathrm{fr}_p) \in \mathbf{Z}$ and satisfies the Hasse bound.*
3. *For each unramified prime p, $\left|\frac{a_p}{2\sqrt{p}} - x_p\right| \leqslant \frac{lb(p)}{2\sqrt{p}}$.*

Proof. Begin with $\rho_1 = \bar\rho$. By [1, Lem. 6], there exists a finite set R, containing the set of primes at which $\bar\rho$ ramifies, such that $Ш^1_R(\mathrm{Ad}^0\,\bar\rho) = Ш^2_R(\mathrm{Ad}^0\,\bar\rho) = 0$.

Let R_2 be the union of R and all primes p with $\frac{l}{2\sqrt{p}} > 2$. For all $p \notin R_2$ and any $a \in \mathbf{F}_l$, there exists $a_p \in \mathbf{Z}$ satisfying the Hasse bound with $a_p \equiv a \pmod{l}$. In fact, given any $x_p \in [-1,1]$, there exists $a_p \in \mathbf{Z}$ satisfying the Hasse bound such that $\left|\frac{a_p}{2\sqrt{p}} - x_p\right| \leqslant \frac{l}{2\sqrt{p}}$. Choose, for all primes $p \in R_2$, a ramified lift ρ_p of $\rho_1|_{G_{\mathbf{Q}_p}}$. Let U_2 be the set of primes not in R_2 such that $\frac{l^2}{2\sqrt{p}} > \min\left(2, \frac{lb(p)}{2\sqrt{p}}\right)$. For each $p \in U_2$, there exists $a_p \in \mathbf{Z}$, satisfying the Hasse bound, such that

$$\left|\frac{a_p}{2\sqrt{p}} - x_p\right| \leqslant \frac{l}{2\sqrt{p}} \leqslant \frac{lb(p)}{2\sqrt{p}},$$

and moreover $a_p \equiv \operatorname{tr}\bar{\rho}(\mathrm{fr}_p) \pmod{l}$. For each $p \in U_2$, let ρ_p be an unramified lift of $\bar{\rho}|_{G_{\mathbf{Q}_p}}$ with $a_p \equiv \operatorname{tr}\rho_p(\mathrm{fr}_p) \pmod{l}$. It may not be that $\pi_{R_2}(x) \leqslant h(x)\pi(x)$ for all x, but there is a scalar multiple h^* of h so that $\pi_{R_2}(x) \leqslant h^*(x)\pi(x)$ for all x.

We have constructed our first h^*-bounded lifting datum $(\rho_1, R_2, U_2, \{\rho_p\})$. We proceed to construct $\rho = \varprojlim \rho_n$ inductively, by constructing a new h^*-bounded lifting datum for each n. We ensure that U_n contains all primes for which $\frac{l^n}{2\sqrt{p}} > \min\left(2, \frac{lb(p)}{2\sqrt{p}}\right)$, so there are always integral a_p satisfying the Hasse bound which satisfy any mod-l^n constraint, and that can always choose these a_p so as to preserve statement 2 in the theorem.

The base case is already complete, so suppose we are given $(\rho_n, R_n, U_n, \{\rho_p\})$. We may assume that U_n contains all primes for which $\frac{l^n}{2\sqrt{p}} > \min\left(2, \frac{lb(p)}{2\sqrt{p}}\right)$. Let U_{n+1} be the set of all primes not in R_n such that $\frac{l^{n+1}}{2\sqrt{p}} > \min\left(2, \frac{lb(p)}{2\sqrt{p}}\right)$. For each $p \in U_{n+1} \setminus U_n$, there is an integer a_p, satisfying the Hasse bound, such that $a_p \equiv \rho_n(\mathrm{fr}_p) \pmod{l^n}$, and moreover $\left|\frac{a_p}{2\sqrt{p}} - x_p\right| \leqslant \frac{lb(p)}{2\sqrt{p}}$. For such p, let ρ_p be an unramified lift of $\rho_n|_{G_{\mathbf{Q}_p}}$ such that $a_p \equiv \operatorname{tr}\rho_n(\mathrm{fr}_p) \pmod{l^n}$. By Theorem 2, there exists an h^*-bounded lifting datum $(\rho_{n+1}, R_{n+1}, U_{n+1}, \{\rho_p\})$ extending and lifting $(\rho_n, R_n, U_n, \{\rho_p\})$. This completes the inductive step. $\square$

4 Main construction

For $k \geqslant 1$, let $U_k(\theta) = \frac{\sin((k+1)\theta)}{\sin\theta}$, the trace of the k-th symmetric power under the identification of $[0,\pi]$ with conjugacy classes in $\mathrm{SU}(2)$. Recall that $U_k(\cos^{-1} t)$ is a polynomial in t.

Let $\mu = f(t)\,\mathrm{d}t$ be a probability measure on $[0,\pi]$. We assume f is bounded, that $f(t) \ll \sin(t)$, and that moreover $f(\pi/2 - \theta) = f(\theta)$. Call such μ *nice*.

The key facts about Sato–Tate compatible measures are that $\cos_* \mu$ satisfies the hypotheses of Theorem **??**, so there are "$N^{-\alpha}$-decaying van der Corput sequences" for $\cos_* \mu$, and also that since $\cos\colon [0,\pi] \to [-1,1]$ is an order anti-isomorphism, we know that for any sequence (x_n) on $[-1,1]$, there is equality $\mathrm{D}(\{x_n\}^N, \cos_* \mu) = \mathrm{D}(\cos^{-1}(x_n)^N, \mu)$.

Theorem 4. *Let μ be a Sato–Tate compatible measure, and fix $\alpha \in (0, 1/2)$. Then there exists a sequence of integers a_p satisfying the Hasse bound, such that if we set $\theta_p = \cos^{-1}\left(\frac{a_p}{2\sqrt{p}}\right)$, then $\mathrm{D}^\star(\{\theta\}^N, \mu) = \Theta(\pi(N)^{-\alpha})$.*

Proof. Apply Theorem **??** to find a sequence (x_n) such that $\mathrm{D}(\{x_n\}^N, \cos_* \mu) = \Theta(\pi(N)^{-\alpha})$. For each prime p, there exists an integer a_p such that $|a_p| \leqslant 2\sqrt{p}$ and $\left|\frac{a_p}{2\sqrt{p}} - x_p\right| \leqslant p^{-1/2}$. Let $y_p = \frac{a_p}{2\sqrt{p}}$. Now apply Lemma **??** with $\epsilon = N^{-1/2}$. We obtain

$$\left|\mathrm{D}(\{x\}^N, \cos_* \mu) - \mathrm{D}(\{y\}^N, \cos_* \mu)\right| \ll N^{-1/2} + \frac{\pi(N^{1/2})}{\pi(N)},$$

which tells us that $\mathrm{D}(\{y\}^N, \cos_* \mu) = \Theta(\pi(N)^{-\alpha})$. Now let $\{\theta\} = \cos^{-1}(\{y\})$. Apply Lemma **??** to $\{\theta\} = \cos^{-1}(\{y\})$, and we see that $\mathrm{D}(\{\theta\}^N, \mu) = \Theta(\pi(N)^{-\alpha})$. □

We can improve this example by controlling the behavior of sums of the form $\sum_{p \leqslant N} U_k(\theta_p)$ for odd k. Let σ be the involution of $[0, \pi]$ given by $\sigma(\theta) = \pi - \theta$. Note that $\sigma_* \mathrm{ST} = \mathrm{ST}$. Moreover, note that for any odd k, $U_k \circ \sigma = -U_k$, so $\int U_k \, \mathrm{dST} = 0$. (Of course, $\int U_k = 0$ for the reason that U_k is the trace of a non-trivial unitary representation, but we will directly exploit the "oddness" of U_k in what follows.)

Theorem 5. *Let μ be a σ-invariant Sato–Tate compatible measure. Fix $\alpha \in (0, 1/2)$. Then there is a sequence of integers a_p, satisfying the Hasse bound, such that for $\theta_p = \cos^{-1}\left(\frac{a_p}{2\sqrt{p}}\right)$, we have*

1. *$\mathrm{D}(\{\theta\}^N, \mu) = \Theta(\pi(N)^{-\alpha})$.*
2. *For all odd k, $\left|\sum_{k \leqslant N} U_k(\theta_p)\right| \ll \pi(N)^{1/2}$.*

Proof. The basic ideas is as follows. Enumerate the primes

$$p_1 = 2, q_1 = 3, p_2 = 5, q_2 = 7, p_3 = 11, q_3 = 13, \ldots.$$

Consider the measure $\mu|_{[0,\pi/2)}$. An argument nearly identical to the proof of Theorem 4 shows that we can choose a_{p_i} satisfying the Hasse bound so that

$$\mathrm{D}\left(\{\theta_{p_i}\}_{i \leqslant N}, \mu|_{[0,\pi/2)}\right) = \Theta(N^{-\alpha}).$$

We can also choose the $a_{q_i} \in [\pi/2, \pi]$ so that

$$\left|\frac{a_{p_i}}{2\sqrt{p_i}} + \frac{a_{q_i}}{2\sqrt{q_i}}\right| \ll \frac{1}{\sqrt{p_i}}.$$

If $\{x\}$ is the sequence of the $\frac{a_{p_i}}{2\sqrt{p_i}}$ and $\{y\}$ is the similar sequence with the q_i-s, then Lemma **??**, Lemma **??**, and Theorem **??** tell us that $\mathrm{D}((\{x\} \wr \{y\})^N, \mu) = \Theta(N^{-\alpha})$.

Moreover, $U_k(\cos^{-1} t)$ is an odd polynomial in t, so if $|x_i - (-y_i)| \ll p_i^{-1/2}$, then $|U_k(\theta_{p_i}) + U_k(\theta_{q_i})| \ll p_i^{-1/2}$. We can then bound

$$\left|\sum_{i \leqslant N} U_k(\theta_{p_i}) + U_k(\theta_{q_i})\right| \ll \sum_{p \leqslant N} p^{-1/2} \ll \pi(N)^{1/2}.$$

□

Now we combine the results of the last section and Chapter **??** to obtain a "beefed-up" version of Theorem 5.

Theorem 6. *Let μ be a Sato–Tate compatible σ-invariant measure on $[0, \pi]$. Fix $\alpha \in (0, 1/2)$ and a good residual representation $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_l)$. Then there exists a weight-2 lift $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$ of $\bar\rho$ such that*

1. *$\pi_{\mathrm{ram}(\rho)}(x) \ll e^{-x}\pi(x)$.*
2. *For each unramified prime p, $a_p = \mathrm{tr}\,\rho(\mathrm{fr}_p) \in \mathbf{Z}$ and satisfies the Hasse bound.*
3. *If, for unramified p we set $\theta_p = \cos^{-1}\left(\frac{a_p}{2\sqrt{p}}\right)$, then $\mathrm{D}(\{\theta\}^N, \mu) = \Theta(\pi(N)^{-\alpha})$.*
4. *For each odd k, the function $L(\mathrm{sym}^k \rho, s)$ satisfies the Riemann Hypothesis.*

Proof. Let $\{x\}$ be an $N^{-\alpha}$-decay van der Corput sequence for $\cos_* \mu|_{[0,\pi/2)}$. Let $\boldsymbol{y} = -\boldsymbol{x}$. Then $\mathrm{D}((\{x\} \wr \{y\})^N, \cos_* \mu) = \Theta(N^{-\alpha})$. Set $h(x) = e^{-x}$ and $b(x) = \log(x)$. By Theorem 3, there is a $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$ lifting $\bar\rho$ such that parts 1 and 2 of the theorem hold. The discrepancy estimate comes from Lemma **??**, Lemma **??**, and Theorem **??** as above, while the Riemann Hypothesis for odd symmetric powers follows from the proof of Theorem 5. □

References

[1] C. Khare, M. Larsen and R. Ramakrishna. Constructing semisimple p-adic Galois representations with prescribed properties, in *Amer. J. Math.* **127**(4) (2005), 709–734.

[2] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields (2nd edition)*, (Springer–Verlag, 2008).

[3] A. Pande. Deformations of Galois representations and the theorems of Sato–Tate and Lang–Trotter, in *Int. J. Number Theory* **7**(8) (2011), 2065–2079.

[4] R. Ramakrishna. Deforming Galois representations and the conjectures of Serre and Fontaine–Mazur, in *Ann. of Math (2)* **156**(1) (2002), 115–154.