MODULARITY LIFTING THEOREMS AND THE PROOF OF THE SATO-TATE CONJECTURE

MICHAEL SCHEIN

These are lecture notes for the first meetings of the seminar held at the Hebrew University in Fall 2006, offered without warranty. They aim to explain, following [CHT], [HSBT], and [Tay], how a certain powerful modularity lifting result implies the Sato-Tate conjecture.

1. Compatible systems

We consider an example to illustrate the ideas. Let $E/\mathbb{Q}$ be an elliptic curve and let l be a prime. For $n \geq 1$, denote by $E[n]$ the n-torsion points of E. Then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for all n. Thus we can consider the Tate module

$$T_l(E) = \varprojlim E[l^n] \simeq \mathbb{Z}_l \times \mathbb{Z}_l.$$

Clearly the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on E preserves n-torsion, as the "multiplication-by-n" maps on E are defined over $\mathbb{Q}$. Thus the groups acts on $T_l(E)$ and we get an l-adic Galois representation

$$\rho_{E.l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_l).$$

We can reduce modulo l to obtain a mod l Galois representation

$$\overline{\rho}_{E.l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_l).$$

We note that *any* continuous representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_l)$ has a well-defined (up to isomorphism) reduction modulo l. The following argument is attributed to N. Katz.

Theorem 1.1. *Let G be a compact Hausdorff group, and let $\rho : G \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ be a continuous representation. Then ρ is equivalent to a representation ρ' such that $\rho'(G) \subset \mathrm{GL}_n(\mathcal{O}_L)$, where $\mathcal{O}_L$ is the ring of integers of some finite extension $L/\mathbb{Q}_p$.*

Proof. Since G is compact and Hausdorff, it admits a Haar measure μ; without loss of generality, $\mu(G) = 1$. Now,

$$\mathrm{GL}_n(\overline{\mathbb{Q}}_p) = \bigcup_{[L:\mathbb{Q}_p]<\infty} \mathrm{GL}_n(L)$$

and hence

$$G = \bigcup_{[L:\mathbb{Q}_p]<\infty} \rho^{-1}(\mathrm{GL}_n(L)).$$

Date: October 21, 2006.

Since there are countably many finite extensions $L/\mathbb{Q}_p$, there must be some such finite extension L with $\mu(\rho^{-1}(\mathrm{GL}_n(L))) > 0$. Hence, $\rho^{-1}(\mathrm{GL}_n(L)) \subset G$ is a closed subgroup of finite index. Then $\rho^{-1}(\mathrm{GL}_n(\mathcal{O}_L))$ is an open subgroup of the compact group $\rho^{-1}(\mathrm{GL}_n(L))$, so it has finite index in it and thus in G. Let $g_1, \ldots, g_m$ be a collection of coset representatives for $\rho^{-1}(\mathrm{GL}_n(\mathcal{O}_L))$. Let $\Lambda \subset L^n$ be the lattice generated by $\rho(g_1)\mathcal{O}_L^n, \ldots, \rho(g_m)\mathcal{O}_L^n$. This is a lattice of maximal rank, so $\Lambda \simeq \mathcal{O}_L^n$. Furthermore, Λ is stable under the action of G. Let $T \in \mathrm{GL}_n(L)$ be a linear transformation that takes $\mathcal{O}_L^n$ to Λ, and set $\rho'(g) = T^{-1}\rho(g)T$. □

Returning to our elliptic curve example, recall that by Hasse's bound, for almost all primes p we have $\#E(\mathbb{F}_p) - 1 - p = a_p$ with $|a_p| \leq 2\sqrt{p}$. It is the case that for almost all p, the trace of $\rho_{E,l}(\mathrm{Frob}_p)$ is a_p; the point is that this is independent of l. The same holds for the determinant, so that the characteristic polynomial of $\rho_{E,l}(\mathrm{Frob}_p)$ does not depend on l. This makes the family of Galois representations $\rho_{E,l}$ an example of a *compatible system*:

Definition 1.2. Let F be a number field. A rank n compatible system of representations of $\mathrm{Gal}(\overline{F}/F)$ consists of the following data:

(1) A number field M.
(2) A finite set S of places of F.
(3) For all $v \notin S$ a monic degree n polynomial $Q_v(x) \in M[x]$.
(4) For all places w of M, a Galois representation

$$\rho_w : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(M_w)$$

such that if w has residual characteristic l, and v is a place of F such that $v \notin S$ and v does not divide l, then $\rho_w(\mathrm{Frob}_v)$ has characteristic polynomial $Q_v(x)$.

2. Automorphicity

Recall that if f is a cuspidal modular form which is an eigenform for the Hecke operators, then the classical construction of Deligne produces for almost all primes l a representation $\rho_{f,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_l)$ which is determined by the eigenvalues of f. In this section we describe an analogous notion in our setting.

Definition 2.1. Let F be a totally real field. A RAESDC (regular algebraic essentially self-dual cuspidal) automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_F)$ is a cuspidal automorphic representation such that:

(1) $\pi^\vee \simeq \chi\pi$ for some character $\chi : F^*\backslash\mathbb{A}_F^* \to \mathbb{C}^*$, with $\chi_v(-1)$ independent of v for all infinite places v of F.
(2) π_∞ has the same infinitesimal character as some irreducible algebraic representation of $\mathrm{Res}_{F/\mathbb{Q}}\mathrm{GL}_n$.

Definition 2.2. A weight is an element $a \in (\mathbb{Z}^n)^{\mathrm{Hom}(F,\mathbb{C})}$ such that for all $\tau \in \mathrm{Hom}(F,\mathbb{C})$ we have

$$a_{\tau,1} \geq \cdots \geq a_{\tau,n}.$$

If a is a weight, denote by Ξ_a the irreducible algebraic representation $\bigotimes_\tau F(a_{\tau,1},\ldots,a_{\tau,n})$ of $\prod_{\tau\in\mathrm{Hom}(F,\mathbb{C})} \mathrm{GL}_n$.

Definition 2.3. We say that a RAESDC π as above has weight a if π_∞ and Ξ_a have the same infinitesimal character.

Note that if π has weight a, then by the (essential) self-duality of π there exists an integer w_a such that $a_{\tau,i} + a_{\tau,n+1-i} = w_a$ for all $\tau \in \mathrm{Hom}(F,\mathbb{C})$ and all $1 \leq i \leq n$.

Let S be a finite set of finite places of F, and for $v \in S$ let ρ_v be an irreducible square-integrable representation of $\mathrm{GL}_n(F_v)$. We say that π has type $\{\rho_v\}_{v\in S}$ if π_v is an unramified twist of $\rho_v^\vee$ for all $v \in S$. If π is a RAESDC automorphic representation of $\mathrm{GL}_n(\mathbb{A}_F)$ of weight a and type $\{\rho_v\}_{v\in S}$, and ι is an isomorphism $\overline{\mathbb{Q}}_l \xrightarrow{\sim} \mathbb{C}$, then Clozel, Harris, and Taylor (essentially using a construction from [HT]) construct a continuous Galois representation

$$r_{l,\iota}(\pi) : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_l),$$

determined by a list of properties. The most important one is that for every place v of F not dividing l we have

$$r_{l,\iota}(\pi)|^{ss}_{\mathrm{Gal}(\overline{F_v}/F_v)} = r_l(\iota^{-1}\pi_v)^\vee(1-n)^{ss},$$

where $r_l(\pi)$ is the l-adic representation associated by Tate to the Weil-Deligne representation $\mathrm{rec}_l(\pi^\vee \otimes |\cdot|^{(1-n)/2})$.

As we saw earlier, $r_{l,\iota}(\pi)$ can be reduced modulo l. Let $\overline{r}_{l,\iota}(\pi) : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{F}}_l)$ be the semisimplification of the reduction.

Definition 2.4. A continuous semisimple representation $r : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_l)$ (resp. $\overline{r} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{F}_l)$) is called automorphic of weight a and level $\{\rho_v\}_{v\in S}$ if it is isomorphic to $r_{l,\iota}(\pi)$ (resp. $\overline{r}_{l,\iota}(\pi)$) for some choice of ι and some π of weight a and type $\{\rho_v\}_{v\in S}$ such that π_l is unramified.

3. A modularity lifting theorem

We have now introduced the notions necessary to state Taylor's modularity lifting theorem, apart from a few technical conditions. In the following, c will always denote complex conjugation. Let the algebraic group $\mathcal{G}_n$ be the semidirect product of GL_n and GL_1 by $\mathbb{Z}/2\mathbb{Z} = \{1,\eta\}$, where η acts by ($g \in \mathrm{GL}_n$, $\mu \in \mathrm{GL}_1$)

$$\eta(g,\mu)\eta^{-1} = (\mu(g^{-1})^t, \mu).$$

Theorem 3.1 (Taylor)**.** *Let F be a CM field. In other words, F is a totally imaginary number field that contains a totally real subfield F^+ with $[F : F^+] = 2$. Let $n \geq 1$ and let $l > n$ be a prime unramified in F. Let*

$$r : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_l)$$

be a continuous irreducible Galois representation. Let

$$\overline{r} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{F}}_l)$$

be the semisimplification of its reduction, and let r' be the natural extension

$$r' : \mathrm{Gal}(\overline{F}/F^+) \to \mathcal{G}_n(\overline{Q}_l).$$

Assume the following:

1. *$r^c \simeq r^\vee \varepsilon^{1-n}$. Here ε is the l-adic cyclotomic character.*
2. *At almost all places of F, r is unramified.*
3. *For all places $v|l$ of F, the restriction $r|_{\mathrm{Gal}(\overline{F_v}/F_v)}$ is crystalline. (Here of course $r|_{\mathrm{Gal}(\overline{F_v}/F_v)}$ is defined up to equivalence by identifying $\mathrm{Gal}(\overline{F_v}/F_v)$ with a decomposition subgroup at v.)*
4. *There is an element $a \in (\mathbb{Z}^n)^{\mathrm{Hom}(F,\overline{\mathbb{Q}}_l)}$ such that*
   (a) *For all $\tau \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_l)$ we have either*
   $$l - 1 - n \geq a_{\tau,1} \geq \cdots \geq a_{\tau,n} \geq 0$$
   or
   $$l - 1 - n \geq a_{\tau c,1} \geq \cdots \geq a_{\tau,n} \geq 0.$$
   (b) *For all $\tau \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_l)$ and all $1 \leq i \leq n$ we have $a_{\tau c,i} = -a_{\tau,n+1-i}$.*
   (c) *For all $\tau \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_l)$ above a prime $v|l$ of F, we have*
   $$\dim_{\overline{\mathbb{Q}}_l} \mathrm{gr}^i(r \otimes_{\tau,F_v} B_{dR})^{\mathrm{Gal}(\overline{F_v}/F_v)} = \begin{cases} 1 & : i = a_{\tau,j} + n - j \mathrm{forsome} 1 \leq j \leq n \\ 0 & : \mathrm{otherwise} \end{cases}$$
5. *There exists a non-empty finite let S of places of F not dividing l, and for each $v \in S$ a square-integrable $\overline{\mathbb{Q}}_l$-representation ρ_v of $\mathrm{GL}_n(F_v)$ such that $r|^{ss}_{\mathrm{Gal}(\overline{F_v}/F_v)} = r_l(\rho_v)^\vee(1-n)^{ss}$.*
6. *FINISH THIS*
7. *$\overline{r}$ is irreducible and automorphic of weight a and type $\{\rho_v\}_{v\in S}$.*

Then r is automorphic of weight a and type $\{\rho_v\}_{v\in S}$.

Observe that if one member of a compatible system is automorphic of a certain weight and type, then so are all the other members. For instance, if we wish to prove that a certain Galois representation ρ is automorphic (we will see below that the Sato-Tate conjecture follows from the automorphicity of a family of ρ's), and we know that another representation ρ' is automorphic and can find a compatible system that contains both ρ and ρ', then we are done. Usually one is not so lucky. But suppose that there are representations ρ'' and ρ''' such that:

- ρ and ρ'' are contained in a compatible system.
- ρ' and ρ''' are contained in a compatible system.
- $\overline{\rho''} \simeq \overline{\rho'''}$.

Then if ρ' is automorphic, then so is ρ''', and hence so is $\overline{\rho'''}$. If we have a sufficiently good modularity lifting theorem, we can prove that ρ'' is automorphic, and hence that ρ is automorphic.

In order to apply this strategy to prove automorphicity of Galois representations, one must be able to do two things sufficiently well: prove modularity lifting theorems and construct compatible systems. In our case, a sufficiently strong modularity lifting theorem was proved by Clozel, Harris, and Taylor [CHT], assuming that an analogue of Ihara's lemma was true. Taylor [Tay] then found a way, using Kisin's work, to modify the argument to remove the dependence on Ihara's lemma and make it unconditional.

Compatible systems are generally obtained from the cohomology of algebraic varieties, as in the elliptic curves example at the beginning of these notes. Harris, Shepherd-Barron, and Taylor [HSBT] consider a family of Calabi-Yau varieties, which were studied by Dwork in the 1960's and then more extensively by mirror symmetry people. These produce the compatible systems used in the proof of Sato-Tate.

4. The Sato-Tate conjecture

Let $E/\mathbb{Q}$ be an elliptic curve. We have already mentioned the Hasse bound

$$|\#E(\mathbb{F}_p) - 1 - p| \leq 2\sqrt{p}.$$

Equivalently,

$$\#E(\mathbb{F}_p) = 1 + p - \sqrt{p}(e^{i\theta_p} + e^{-i\theta_p})$$

for some angle $\theta_p \in [0, \pi]$. If we fix an elliptic curve E and vary p, then we may ask how θ_p is distributed.

Definition 4.1. Let μ be a measure on the interval $[0, \pi]$. A sequence x_n of points on this interval is said to be equidistributed with respect to μ if for all continuous functions f on $[0, \pi]$ we have

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(x_n) = \mu(f).$$

Conjecture 1 (Sato and Tate, 1960)**.** If E is an elliptic curve without complex multiplication (i.e. $\mathrm{End}(E) = \mathbb{Z}$), then the sequence θ_p is equidistributed with respect to the measure $\frac{2}{\pi}\sin^2\theta d\theta$.

Now let G be a compact group and X the space of its conjugacy classes. We will denote by μ both the Haar measure on G and the measure it induces on X. A sequence of elements x_n of X is μ-equidistributed if and only if for any irreducible character χ of G we have

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi(x_i) = \mu(\chi).$$

Indeed, by the Peter-Weyl theorem the irreducible characters generate a dense subspace of the space $C(X)$ of continuous functions on X, and we obtain the desired statement for all of $C(X)$ by a standard equicontinuity argument. Therefore, if $\mu(G) = 1$ then the sequence x_n is μ-equidistributed if and only if for every non-trivial irreducible character χ we have

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi(x_i) = 0.$$

Indeed, we also need the following condition for the trivial character $\chi = 1$, but it always holds trivially:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi(x_i) = 1.$$

Returning to our elliptic curve, if $\rho_{E,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_l)$ is unramified at p, then it is known that

$$\rho_{E,l}(\mathrm{Frob}_p) \sim \sqrt{p} \begin{pmatrix} e^{i\theta_p} & \\ & e^{-i\theta_p} \end{pmatrix}.$$

In particular, the trace of $\rho_{E,l}(\mathrm{Frob}_p)$ is a_p, as we mentioned earlier. Let $G = \mathrm{SU}(2)$. Then every element of G is conjugate to a unique matrix of the form $\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$ with $0 \le \theta \le \pi$, so the space X of conjugacy classes is homeomorphic to the interval $[0, \pi]$. Moreover, the Haar measure on G induces the measure $\frac{2}{\pi} \sin^2 \theta d\theta$ on X. Hence the Sato-Tate conjecture may be reformulated as follows:

The sequence $\frac{1}{\sqrt{p}} \rho_{E,l}(\mathrm{Frob}_p)$ *of points on* X *is equidistributed with respect to the Haar measure.*

If r is the natural 2-dimensional representation of $\mathrm{SU}(2)$, then the non-trivial irreducible representations of $\mathrm{SU}(2)$ are precisely the symmetric powers $\mathrm{Sym}^n r$ for $n \ge 1$. By the considerations above, to prove Sato-Tate we need to show that for all $n > 1$:

$$\lim_{x\to\infty} \frac{\sum_{p\le x} \frac{\mathrm{trSym}^{n-1} \rho_{E,l}(\mathrm{Frob}_p)}{p^{(n-1)/2)}}}{\sum_{p\le x} 1} = \lim_{x\to\infty} \frac{\log x}{x} \sum_{p\le x} \frac{\mathrm{trSym}^{n-1} \rho_{E,l}(\mathrm{Frob}_p)}{p^{(n-1)/2}} = 0. \tag{1}$$

5. L-functions

How are L-functions relevant to any of this? The standard construction of the L-function of a representation yields:

$$L(\mathrm{Sym}^{n-1} \rho_{E,l}, s) = \prod_p \left(\det \left(1 - \frac{\mathrm{Sym}^{n-1} \rho_{E,l}(\mathrm{Frob}_p)}{p^s} \right) \right)^{-1}.$$

This converges for $\mathrm{Re}s > \frac{n+1}{2}$. A fun exercise for the reader is to compute the logarithmic derivative of this:

$$(\log L)' = \frac{L'}{L} = -\sum_p \frac{(\log p)\mathrm{trSym}^{n-1}\rho(\mathrm{Frob}_p)}{p^s} + \Delta,$$

where Δ converges in $\mathrm{Re}s > \frac{n}{2}$. Comparing this with equation (1) above, we see that the following conjecture implies Sato-Tate:

Conjecture 2 (Tate)**.** If E does not have complex multiplication, then $L(\mathrm{Sym}^{n-1}\rho_{E,l}, s)$ has analytic continuation to $\mathrm{Re}s > \frac{n+1}{2}$ and does not vanish in this region.

By virtue of the good behavior of L-functions of cuspidal automorphic representations, it is easy to see that the following implies Conjecture 2:

Conjecture 3. For all $n > 1$ there is a cuspidal automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$ such that $L(\pi, s) = L(\mathrm{Sym}^{n-1}\rho, s)$ on $\mathrm{Re}s > \frac{n+1}{2}$.

This is known for $n = 2, 3$ by work of Gelbart and Jacquet, and for $n = 4, 5$ by Kim and Shahidi, but unfortunately it is not yet known in general. Instead, Taylor and collaborators proved the following potential version of the conjecture, which is sufficient to imply Conjecture 2.

Proposition 5.1. *For all $n > 1$ there is a totally real field F, which is a Galois extension of $\mathbb{Q}$, and a cuspidal automorphic representation π_F of $\mathrm{GL}_n(\mathbb{A}_F)$ such that $L(\pi_F, s) = L(\mathrm{Sym}^{n-1}\rho|_{\mathrm{Gal}(\overline{F}/F)}, s)$.*

To see why this implies Conjecture 2, observe that if $\mathbb{Q} \subset L \subset F$ is an intermediate extension with F/L solvable, then by Langlands base change there is a cuspidal automorphic representation π_L of $\mathrm{GL}_n(\mathbb{A}_L)$ with $L(\pi_L, s) = L(\mathrm{Sym}^{n-1}\rho|_{\mathrm{Gal}(\overline{L}/L)}, s)$. By Brauer's theorem, we can decompose the trivial representation $\mathbf{1}$ of $\mathrm{Gal}(F/\mathbb{Q})$ as follows:

$$\mathbf{1} = \sum_{i \in I} n_i Ind_{\mathrm{Gal}(F/F_i)}^{\mathrm{Gal}(F/\mathbb{Q})} \chi_i,$$

where I is a finite set and for each $i \in I$, $n_i \in \mathbb{Z}$, $\mathrm{Gal}(F/F_i)$ is solvable, and χ_i is a one-dimensional representation of $\mathrm{Gal}(F/F_i)$.

Now we see that

$$\begin{aligned} L(\mathrm{Sym}^{n-1}\rho, s) &= \prod_i L(\mathrm{Sym}^{n-1}\rho \otimes Ind\chi_i, s)^{n_i} = & (2)\\ &\prod_i L(\mathrm{Sym}^{n-1}\rho|_{\mathrm{Gal}(\overline{F_i}/F_i)} \otimes \chi_i, s)^{n_i} = & (3)\\ &\prod_i L(\pi_{F_i} \otimes \chi_i, s)^{n_i}, & (4)\end{aligned}$$

and since the L-functions in the bottom line have the desired properties, so does their product.

6. Strategy to prove Proposition 5.1

Recall that E has multiplicative reduction at a prime q, and we need to show for every $n > 1$ that $\mathrm{Sym}^{n-1}\rho_{E,l}$ is automorphic for some prime l. Suppose n fixed, and choose $l > n$ such that E has good reduction at l and l does not divide $q^i - 1$ for $1 \leq i \leq n$.

Now choose a prime l' and a totally real field F' which is Galois over $\mathbb{Q}$ and in which l and l' are unramified and q splits completely. Choose an elliptic curve E'/F' with good reduction at l and l', multiplicative reduction at q, and such that $\overline{\rho}_{E',l} \simeq \overline{\rho}_{E,l}$ and $\overline{\rho}_{E',l'}|_{I_{l'}} \simeq 1 \oplus \varepsilon_{l'}^{-1}$. Here of course $\varepsilon_{l'}$ is the mod l' cyclotomic character, and the statement that such an E' exists (as well as other choices that will be made below) is not entirely trivial (see [HSBT], Theorem 3.3).

We will find a prime l'' and a totally real extension F''/F' such that l, l', and l'' are unramified in F'', such that q splits completely there, and such that F'' is Galois over $\mathbb{Q}$. We will then construct a compatible system of representations $r_p : \mathrm{Gal}(\overline{F''}/F'') \to \mathrm{GSp}_n(\mathbb{Z}_p)$ (we only defined compatible systems above for representations into GL_n, but it should be clear what is meant here) for which:

(1) There is a finite set S of primes such that $l, l', l'' \notin S$ and for all $p \notin S$, r_p is crystalline with Hodge-Tate weights $0, 1, \ldots, n-1$. (Note that finite flat group schemes have Hodge-Tate numbers 0 and 1. This is why we cannot use torsion of abelian varieties to produce our compatible system in dimension $n > 2$.)
(2) $\overline{r}_{l'} \simeq \mathrm{Sym}^{n-1}\overline{\rho}_{E',l'}$.
(3) $\overline{r}_{l''} \simeq \overline{Ind\theta}$, where $\theta : \mathrm{Gal}(\overline{M}/M)$ arises from a suitable CM extension M/F''.
(4) For all primes $p \neq q$, we have $r_p|^{ss}_{\mathrm{Gal}(\overline{F''_q}/F''_q)} = 1 \oplus \varepsilon_q^{-1} \oplus \cdots \oplus \varepsilon_q^{-(n-1)}$.

If we can do this, we will be finished, since $Ind\theta$ is automorphic by automorphic induction, and hence (given the modularity lifting theorem), so is $r_{l''}$. Hence $r_{l'}$ is automorphic, whence $\overline{r}_{l'} = \mathrm{Sym}^{n-1}\overline{r}_{E',l'}$ is, whence (using modularity lifting and another compatible system) $\mathrm{Sym}^{n-1}\rho_{E,l}$ is automorphic as desired. It is necessary to introduce the auxiliary elliptic curve E', and generally to carry around a large number of technical conditions, in order to make sure that the hypotheses of the modularity lifting theorems are satisfied. We will now sketch how to construct the compatible system of r_p's.

7. A family of Calabi-Yau varieties

Let n be even (we will explain at the very end how to get Proposition 5.1 for odd n) and consider the scheme $Y \subset \mathbb{P}^n \times \mathbb{P}^1$ defined over $\mathbb{Z}[\frac{1}{n+1}]$ by the equation

$$s(X_0^{n+1} + \cdots + X_n^{n+1}) = (n+1)tX_0 \cdots X_n.$$

Here $[X_0 : \cdots : X_n]$ and $[s : t]$ are the homogenous coordinates on $\mathbb{P}^n$ and $\mathbb{P}^1$, respectively.

Let $\pi : Y \to \mathbb{P}^1$ be the projection to the second factor, and let Y_t be the fiber above the point $[1 : t]$ ($t = \infty$ is allowed). Consider the scheme $T_0/\mathbb{Z}[\frac{1}{n+1}]$ given by $T_0 = \mathbb{P}^1 \backslash \{\infty \cup \mu_{n+1}\}$, where μ_{n+1} is the scheme of $(n+1)$-st roots of unity. Then the map $Y|_{T_0} \to T_0$ is smooth; if $t \in \mu_{n+1}$,

then Y_t has isolated ordinary quadratic singularities at points where the X_i are all in μ_{n+1} and $X_0 \cdots X_n = t^{-1}$.

Let $H = (\mu_{n+1})^{n+1}/\mu_{n+1}$, where the subgroup μ_{n+1} in question is embedded diagonally. Over $\mathbb{Z}[\frac{1}{n+1}, \mu_{n+1}]$, H acts on Y by

$$(\zeta_0, \ldots, \zeta_n)[X_0 : \cdots : X_n] = [\zeta_0 X_0 : \cdots : \zeta_n X_n].$$

Let $H_0 = \{(\zeta_0, \ldots, \zeta_n) \in H : \zeta_0 \cdots \zeta_n = 1\}$. Then it is easy to see that H_0 preserves each fiber Y_t. If $t \in \mu_{n+1}$, then H_0 permutes the singularities transitively. If $(N, n+1) = 1$, define a lisse sheaf on $T_0 \times \mathbb{Z}[\frac{1}{N(n+1)}]$ by

$$V_n[N] = V[N] = (R^{n-1}\pi_* \mathbb{Z}/N\mathbb{Z})^{H_0}.$$

If l is a prime that does not divide $n+1$, then let $V_{n,l} = V_l = \varprojlim V[l^m] \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$.

Similarly, define $V = (R^{n-1}\pi_* \mathbb{Z})^{H_0}$. Note that since Y is an $(n-1)$-dimensional variety, Poincaré duality gives us alternating perfect pairings:

$$\begin{aligned} V[N] \times V[N] &\to (\mathbb{Z}/N\mathbb{Z})(1-n) \\ V_l \times V_l &\to \mathbb{Q}_l(1-n) \\ V \times V &\to \mathbb{Z}. \end{aligned}$$

Note that $V[N]$, V_l, and $V \otimes \mathbb{Q}$ are locally free of rank n. This and other basic facts about our family were known to Dwork in the 1960's. Observe that the map

$$\begin{aligned} (\mathbb{P}^1 \backslash \{0, \infty\}) \times \mathbb{C} &\to (\mathbb{P}^1 \backslash \{0, \infty\}) \\ t &\mapsto t^{n+1} \end{aligned}$$

is a finite étale Galois cover with Galois group H/H_0. Thus V descends to a locally constant sheaf $\tilde{V}$ on $\mathbb{P}^1(\mathbb{C}) \backslash \{0, 1, \infty\}$. We still have an alternating pairing $\tilde{V} \times \tilde{V} \to \mathbb{Z}$. As usual, let $\mathrm{Sp}(\tilde{V}_z \otimes \mathbb{C})$ be the group of automorphisms that respect the pairing. By studying monodromy, one can prove:

Lemma 7.1. *If $z \in \mathbb{P}^1(\mathbb{C}) \backslash \{0, 1, \infty\}$, then the map $\pi_1(\mathbb{P}^1(\mathbb{C}) \backslash \{0, 1, \infty\}, z) \to \mathrm{Sp}(\tilde{V}_z \otimes \mathbb{C})$ has Zariski dense image.*

Combining this with a theorem of Matthews, Vaserstein, and Weisfeiler (Hy"d) whose proof relies upon the classification of finite simple groups, we obtain

Lemma 7.2. *There exists a constant $C(n)$ such that if $t \in T_0(\mathbb{C})$ and all the prime factors of N are greater than $C(n)$, then the map $\pi_1(T_0(\mathbb{C}), t) \to \mathrm{Sp}(V[N]_t)$ is surjective.*

If F is a number field, let W be a free rank n $\mathbb{Z}/N\mathbb{Z}$-module with a continuous action of $\mathrm{Gal}(\overline{F}/F)$ and a perfect alternating pairing $\langle , \rangle_W : W \times W \to \mathbb{Z}/N\mathbb{Z}(1-n)$. View W as a sheaf over Spec F, and consider the functor $\{T_0 \times F-\text{schemes}\} \to \{\text{Sets}\}$ that sends a $T_0 \times F$-scheme X to the set of isomorphisms between (the pullbacks to X of) W and $V[N]$ that are compatible with the pairings.

This functor is represented by a finite étale scheme $T_W/(T_0 \times F)$. Then a corollary of the previous lemma is that

Corollary 7.3. *If the prime factors of N are all greater than $C(n)$, then $T_W(\mathbb{C})$ is connected for any $F \hookrightarrow \mathbb{C}$, i.e. T_W is geometrically irreducible.*

Observe that if F is a number field and $t \in T_0(F)$, then the $V_{l,t}$ are a compatible system of l-adic representations of $\mathrm{Gal}(\overline{F}/F)$. Let $N = l'l''$, and, choosing W appropriately, consider the scheme T_W that parametrizes $t \in T_0$ with $V_t[l'] \simeq \mathrm{Sym}^{n-1}\overline{\rho}_{E',l'}$ and $V_t[l''] \simeq Ind\overline{\theta}_{l''}$.

It is now clear that to obtain our compatible system we just need to show that there exists a totally real field K such that $T_W(K) \neq \varnothing$. To do this, we use the following "local-to-global principle" of Moret-Bailly.

Theorem 7.4. *Let F be a number field and let T/F be a smooth geometrically irreducible variety. Let $S = S_1 \coprod S_2$ be a finite set of places of F such that S_2 contains no infinite places. If $v \in S_1$ (resp. $w \in S_2$) assume that there is a non-empty (v-adically) open set $\Omega_v \subset T(F_v)$ (resp. a non-empty open $\mathrm{Gal}(F_w^{nr}/F_w)$-invariant subset $\Omega_w \subset T(F_w^{nr})$). Here F_w^{nr} is the maximal unramified extension of F_w. Fix a finite extension L/F.*

Then there exists a finite Galois extension $K/\mathbb{Q}$ and a point $P \in T(K)$ such that

1. *L and K are linearly disjoint over $\mathbb{Q}$.*
2. *For all $v \in S_1$, v splits completely in K and $P \in \Omega_v$. For all $w \in S_2$, w is unramified in S_2 and also $P \in \Omega_w$.*

We wish to apply this theorem with $T = T_W$ and $S_1 = \{\infty, q, \dots\}$ and $S_2 = \{l, l', l'', \dots\}$. Note that $\infty \in S_1$ forces the field K given by the theorem to be totally real. As we already know the geometric irreducibility of T_W, it remains to show the existence of the open sets Ω_v, Ω, w.

References

[CHT] Laurent Clozel, Michael Harris, and Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l representations. *Preprint* (2006).

[HSBT] Michael Harris, Nicholas Shepherd-Barron, and Richard Taylor. Ihara's lemma and potential automorphy. *Preprint* (2006).

[HT] Michael Harris and Richard Taylor. *The geometry and cohomology of some simple Shimura varieties*, volume 151 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2001. With an appendix by Vladimir G. Berkovich.

[Tay] Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l representations II. *Preprint* (2006).

Institute of Mathematics, Hebrew University of Jerusalem, Givat Ram, Jerusalem 91904, ISRAEL

E-mail address: mschein@math.huji.ac.il