JEMS

Robert Guralnick · Michael Harris · Nicholas M. Katz

Automorphic realization of residual Galois representations

Abstract. We show that it is possible in rather general situations to obtain a finite-dimensional modular representation ρ of the Galois group of a number field F as a constituent of one of the modular Galois representations attached to automorphic representations of a general linear group over F, provided one works "potentially." The proof is based on a close study of the monodromy of the Dwork family of Calabi–Yau hypersurfaces; this in turn makes use of properties of rigid local systems and the classification of irreducible subgroups of finite classical groups with certain sorts of generators.

Keywords. Galois representations, automorphy, hypergeometric local systems

Introduction

The "Galois representations" of the title are modular representations ρ of the Galois groups of a number field F, and the "automorphic realization" refers to obtaining these representations as *constituents* of Galois representations attached to automorphic representations of general linear groups over F. The present article refines the moduli-theoretic arguments of [HST] to show that this is possible in rather general situations, provided one works "potentially," replacing ρ by its restriction to a certain infinite class of Galois extensions F'/F; this class is sufficiently large that the restriction to the Galois group of F' can be assumed injective.

In §1, we introduce the notion of potential stable automorphy of modular Galois representations, and state a general result on the ubiquity of such representations. In §2 we state some rather precise group-theoretic results on the monodromy of the Dwork family, strengthening the results of [HST], and use them to prove the general result of §1. In §3 we discuss variants and possible future applications of the general result. In §4 we prove the group-theoretic results stated in §2, as well as some supplements to those results. The

R. Guralnick: Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA; e-mail: guralnic@usc.edu

M. Harris: Centre de Mathématiques de Jussieu, Université Paris 7 Denis Diderot, Case Postale 7012, 2, place Jussieu, F-75251 Paris Cedex 05, France; e-mail: harris@math.jussieu.fr

N. M. Katz: Fine Hall, Department of Mathematics, Princeton University, Princeton, NJ 08544-1000, USA; e-mail: nmk@math.princeton.edu

techniques used in §4 are based on (1) relating the monodromy of the Dwork family to a rigid local system, then exploiting properties of rigid local systems, and (2) applying results on the classification of irreducible subgroups of finite classical groups with certain sorts of generators.

1. Stable automorphy of residual representations

Let F be a number field, $\Gamma_F = \mathrm{Gal}(\bar{\mathbb{Q}}/F)$, k a finite field of characteristic $\ell > 2$, $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Z}_\ell$ with residue field k, $\rho : \Gamma_F \to \mathrm{GL}(n, \mathcal{O})$ a continuous representation of Γ_F. We assume ρ is defined over a number field C in the sense that ρ is unramified at all primes of F outside a finite set S and, for $v \notin S$, the characteristic polynomial of (geometric) Frobenius Frob_v,

$$P_v(\rho, X) = \det(I - \rho(\mathrm{Frob}_v)X),$$

has coefficients in C. Fix an embedding $\iota : C \to \mathbb{C}$. One says that ρ is *automorphic* (relative to ι) if there is an automorphic representation Π of $\mathrm{GL}(n, F)$ such that, for almost all places v of F prime to ℓ, ρ is unramified at v and there is an equality of local Euler factors

$$L_v(s, \rho) = L(s, \Pi_v)$$

where $L_v(s, \rho) = P_v(\rho, Nv^{-s})$ and $L(s, \Pi_v)$ is the standard (Godement–Jacquet) local Euler factor of Π_v.

Let $\mathfrak{m}_\mathcal{O} \subset \mathcal{O}$ be the maximal ideal, and let $\sigma = \bar{\rho} : \Gamma_F \to \mathrm{GL}(n, k)$ be the reduction mod $m_\mathcal{O}$ of ρ. One says that ρ is *residually automorphic*, or that σ is automorphic, if there is an automorphic lift ρ' of σ to some finite extension $\mathcal{O}'$ of $\mathcal{O}$ with residue field k (one could also replace k by a finite extension, but with no added generality); by definition ρ' has to be defined over a number field with a chosen complex embedding. This is an intrinsic property of σ, so the definition remains valid without assuming a priori that σ lifts to characteristic zero.

One says that ρ is *potentially automorphic* if, for any finite extension L_0 of F, there is a finite Galois extension F'/F disjoint from L_0 such that $\rho|_{\Gamma_{F'}}$ is automorphic. One says that $\sigma : \Gamma_F \to \mathrm{GL}(n, k)$ is potentially automorphic if for any finite extension L_0 of F, there is a finite Galois extension F'/F disjoint from L_0 such that $\sigma_{F'} = \sigma|_{\Gamma_{F'}}$ is automorphic. This definition implies that $\sigma_{F'}$ admits a lift to characteristic zero for each such F', but this is not necessarily the case for the original σ.

The notion of residual automorphy is the starting point of the approach, initiated by Wiles and generalized in a variety of directions, to show that an ℓ-adic representation such as ρ is associated to automorphic forms. The notion of potential automorphy was introduced by Taylor and has proved a powerful tool for applications in which actual automorphy is either unnecessary or inaccessible; the proof of Serre's conjecture by Khare and Wintenberger suggests that it may eventually be possible to use a combination of automorphic and arithmetic techniques to deduce automorphy from potential automorphy.

In contrast to these two notions, whose fruitfulness has been amply demonstrated, the following notion may have no applications whatsoever:

Definition 1.1. Let ρ and σ be as above. Say ρ is *stably residually automorphic* (resp. σ is *stably automorphic*) if there exists a finite-dimensional representation $\sigma' : \Gamma_F \to \mathrm{GL}(n', k)$ such that $\bar{\rho} \oplus \sigma'$ (resp. $\sigma \oplus \sigma'$) is automorphic.

In the obvious way one combines this definition with the previous ones, and we can talk of *stably potentially automorphic representations*—that is, representations that are direct summands of potentially automorphic representations—or stably potentially residually automorphic representations. The main result of the present note is the following application of the method of potential automorphy as developed in the article [HST]:

Main Theorem 1.2. *Assume F is totally real and $k = \mathbb{F}_\ell$. Then any finite-dimensional representation $\sigma : \Gamma_F \to \mathrm{GL}(n, \mathbb{F}_\ell)$ is stably potentially automorphic. Moreover, the finite Galois extensions F' in the definition of potential automorphy can be assumed totally real.*

Remarks 1.3. (1) A representation σ as above is said to be *polarized of weight w* if it admits a nondegenerate pairing

$$\sigma \otimes \sigma \to k(-w)$$

where $k(-w)$ is the one-dimensional vector space over k on which Γ_F acts by the $-w$-power of the cyclotomic character. Likewise for ρ. It will be clear from the proof that if n is even and σ is symplectically polarized of weight $n-1$, or more generally of any weight w of parity opposite to n, one can take $\sigma' = (0)$—i.e. σ is itself potentially automorphic—unless $\ell \mid n + 1$, which is precisely where the argument breaks down. In general, one can take $\sigma' = \sigma^{\vee}(1 - 2n)$, unless $\ell \mid 2n + 1$. This smallest possible choice for σ' is not necessarily optimal, for reasons to be discussed in §3.

(2) Note that σ is not assumed odd when $F = \mathbb{Q}$ and $n = 2$. There is a sign obstruction to relating σ to a Galois representation arising in the cohomology of a Shimura variety, but this is compensated for by σ'.

(3) The assumption that F is totally real can be suppressed, as follows. Let $F^+ \subset F$ be the maximal totally real subfield. Let $\sigma^+ = \mathrm{Ind}_{\Gamma_F}^{\Gamma_{F^+}} \sigma$, and apply the theorem to σ^+. Then the restrictions of σ^+ to $\Gamma_{F \cdot F'}$, for F' as in the definition of potential automorphy, all contain $\sigma|_{\Gamma_{F \cdot F'}}$.

(4) One is entitled to expect stronger results when F is CM and σ is not polarized of weight $n - 1$ but rather that there is a nondegenerate pairing $\sigma \otimes \sigma \circ c \to \mathbb{F}_\ell(1 - n)$, where c is complex conjugation. The methods of [HST] do not apply to this situation. However, shortly after completing the first version of this article, the authors became aware of Barnet-Lamb's generalization in [BL] of the techniques of [HST], based on [Ka-AL]. This work may provide a more natural formulation for CM fields.

(5) The assumption that $k = \mathbb{F}_\ell$ is dispensable—just replace σ by the representation of dimension $[k : \mathbb{F}_\ell] \dim \sigma$—but since one cannot guarantee that the automorphic lifts of the indicated representations have coefficients in $W(k)$-algebras this is rather artificial. Again, the methods of [BL] should lead to a result over general finite residue field.

(6) The method breaks down completely when $\ell = 2$. Whether or not this is unfortunate is left to the reader's judgment.

2. A refined potential automorphy result

In view of the following result, the proof of the Main Theorem is an immediate application of the methods of [HST], whose notation we use freely. Let F be a number field, $d > 1$ a positive odd integer, N a positive integer. Define $T_0 = \mathbb{P}^1 \setminus \{\infty, \mu_d\}$ over $\mathbb{Z}[1/d]$ as in [HST], and let $V[N]$ be the natural representation of $\pi_1(T_0(\mathbb{C}), t)$ defined in [HST], with d replaced by $n + 1$. The following result is a substantial strengthening of Corollary 1.11 of [HST]. It is based on the rather miraculous rigidity properties of absolutely irreducible hypergeometric local systems, and on the explicit description by Levelt of such systems, which is perfectly adapted to "reduction mod ℓ" considerations.

Theorem 2.1. *Suppose N is relatively prime to $2d$. Then the natural map $\pi_1(T_0(\mathbb{C}), t) \to \mathrm{Sp}(V[N]) \simeq \mathrm{Sp}(d - 1, \mathbb{Z}/N\mathbb{Z})$ is surjective.*

Let W be a free $\mathbb{Z}/N\mathbb{Z}$-module of rank $d - 1$ with a continuous action of $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ and a perfect alternating pairing

$$\langle \, , \, \rangle_W : W \times W \to (\mathbb{Z}/N\mathbb{Z})(2 - d).$$

We may think of W as a lisse etale sheaf over $\mathrm{Spec}\, F$. Consider the functor from $T_0 \times \mathrm{Spec}\, F$-schemes to sets which sends X to the set of isomorphisms between the pull back of W and the pull back of $V[N]$ which sends $\langle \, , \, \rangle_W$ to the pairing we have defined on $V[N]$. As in the discussion following Corollary 1.11 of [HST], this functor is represented by a finite étale cover $T_W/T_0 \times \mathrm{Spec}\, F$. Theorem 2.1 implies the next corollary.

Corollary 2.2. *Suppose N is relatively prime to $2d$. Then the curve T_W is geometrically irreducible.*

The orthogonal analogue of Theorem 2.1 is not invoked in the proof of the Main Theorem but it is included for the sake of completeness. Suppose now $d > 0$ is *even*, ℓ an odd prime number, and define $V[\ell]$ as before.

Theorem 2.3. *Suppose ℓ is relatively prime to $2d$, $d \geq 10$. Moreover suppose neither $d - 1$ nor $d + 1$ is a power of ℓ. Then the image of the natural map $\pi_1(T_0(\mathbb{C}), t) \to O(V[\ell]) \simeq O(d - 1, \mathbb{Z}/\ell\mathbb{Z})$ is one of the following two subgroups of index 2 in $O(d - 1, \mathbb{Z}/\ell\mathbb{Z})$: either the subgroup*

$$\{g \in O(d - 1, \mathbb{Z}/\ell\mathbb{Z}) \mid \mathrm{ns}(g) = 1\}$$

or the subgroup

$$\{g \in O(d - 1, \mathbb{Z}/\ell\mathbb{Z}) \mid \mathrm{ns}(g) = \det(g)\},$$

where ns *is the spinor norm.*

Remark 2.4. A version of this theorem valid for $\mathbb{Z}/N\mathbb{Z}$-representations is proved in §4. The formulation is somewhat more complicated than the analogous statement for Theorem 2.1; see 4.10 for a precise statement.

Remark 2.5. The exceptional cases, when $d \pm 1$ is a power of ℓ, are analyzed in 4.11.

The proofs of Theorems 2.1 and 2.3 are given in §4.

Proof of the Main Theorem

As in [HST], the proof makes crucial use of the following variant of a theorem of Moret-Bailly [MB]:

Proposition 2.6. *Let F be a number field and let $S = S_1 \sqcup S_2 \sqcup S_3$ be a finite set of places of F such that S_2 contains no infinite place. Suppose that T/F is a smooth, geometrically connected variety. Suppose also that for $v \in S_1$, $\Omega_v \subset T(F_v)$ is a nonempty open (for the v-topology) subset; that for $v \in S_2$, $\Omega_v \subset T(F_v^{nr})$ is a nonempty open $\mathrm{Gal}(F_v^{nr}/F_v)$-invariant subset; and that for $v \in S_3$, $\Omega_v \subset T(\bar{F}_v)$ is a nonempty open $\mathrm{Gal}(\bar{F}_v/F_v)$-invariant subset. Suppose finally that L_0/F is a finite extension. Then there is a finite Galois extension F'/F and a point $P \in T(F')$ such that*

- *F'/F is linearly disjoint from L_0/F;*
- *every place v of S_1 splits completely in F' and if w is a prime of F' above v then $P \in \Omega_v \subset T(F_w')$;*
- *every place v of S_2 is unramified in F' and if w is a prime of F' above v then $P \in \Omega_v \cap T(F_w')$;*
- *if w is a prime of F' above $v \in S_3$ then $P \in \Omega_v \cap T(F_w')$.*

Corollary 2.2 is used to verify the irreducibility condition above for certain moduli spaces of Calabi–Yau hypersurfaces with level structure. In [HST], this was only known for level structures of modulus all of whose prime factors are sufficiently large.

One takes $N = \ell \cdot \ell'$ where ℓ is the characteristic of k, as before, and ℓ' is an absurdly large prime, as in [HST], to be specified presently. We take σ' any representation of dimension r such that

(a) $d = n + r + 1$ is odd and relatively prime to ℓ,
(b) $\sigma \oplus \sigma'$ is symplectically polarized of weight $d - 2$.

Remark 1.3(1) gives some suggestions for σ' provided $n + 1$ (or $2n + 1$) is prime to ℓ. If that is not the case, one can just add an innocuous additional factor of the appropriate dimension. We place ourselves in the setting of §3 of [HST], letting $t = 1$ in the statement of Theorem 3.1 there, with the dimension $n_1 = d - 1$. Let $\bar{\rho} = \sigma \oplus \sigma'$ and let E be an imaginary quadratic field. We let $\psi = \psi_1$ be (the finite part of) a Hecke character of the CM field M, cyclic of degree $d - 1$ over $\mathbb{Q}$, satisfying the properties listed at the beginning of the proof of Theorem 3.1 of [HST]. In particular, ψ is unramified at primes of M dividing ℓ and at any prime dividing a rational prime that does not split in $E/\mathbb{Q}$, its infinity type is as specified in the proof of Theorem 3.1 of [HST], and the automorphic induction of ψ to an automorphic representation of $\mathrm{GL}(d - 1, \mathbb{Q})$ is self-dual, cohomological (up to twist by a half-integral power of the norm character) and cuspidal.

Assume ℓ' is chosen as in the proof of Theorem 3.1 of [HST]. In particular, $\ell' \equiv 1$ (mod d) is a prime that is unramified in F and in the splitting field of $\sigma \oplus \sigma'$ and satisfies

$$\ell' > 8\left(\frac{d+1}{4}\right)^{(d-1)/2+1}.$$

Moreover, ℓ' is split in the extension of $E \cdot M$ generated by the values (at finite idèles) of the Hecke character ψ. The character ψ gives us a residual representation

$$I(\bar{\theta}) : \Gamma_{\mathbb{Q}} \to \mathrm{GSp}(d-1, \mathbb{F}_{\ell'}).$$

as in the proof of Theorem 3.1 of [HST]; in particular, our choice of ψ and the very large lower bound on ℓ' guarantee that $I(\bar{\theta})$ is *irreducible*.

In [HST] there is a prime q at which a lift of the representation taking the place of $\bar{\rho}$ is of Steinberg type. In our situation there is no given lift of $\bar{\rho}$, so q has nothing to do with ℓ, but we choose a $q > d$ at which $I(\bar{\theta})$ is unramified and whose residue class in $\mathbb{F}_{\ell'}^{\times}$ is of order $\geq d-1$. The choice of q is irrelevant in what follows but it is important to note that such q (obviously) exist in order to apply the results as stated in [HST].[1]

Now let W be the Galois module $W_{\ell} \times W_{\ell'} = \bar{\rho} \times I(\bar{\theta})$ of rank $d-1$ over $\mathbb{F}_{\ell} \times \mathbb{F}_{\ell'}$. By hypothesis (b) above and the construction of [HST] we see that the representation of Γ_F on W lies in $\mathrm{GSp}(d-1, \mathbb{F}_{\ell} \times \mathbb{F}_{\ell'})$. It follows from Corollary 2.2 and our hypotheses on ℓ and ℓ' that the curve T_W is geometrically irreducible. Hence the proof of Theorem 3.1 of [HST] applies to yield a totally real Galois extension F' of F, unramified at ℓ' and q, and a point $t \in T_W(F)$ corresponding to a Calabi–Yau hypersurface in the Dwork family with good reduction at ℓ' and totally degenerate reduction at q. At the request of the referee, we sketch the argument, since both the hypotheses and the conclusions are weaker than in [HST]. In Proposition 2.6 we take S_1 to be the set of archimedean primes of F, S_2 to be the set of primes dividing ℓ', and S_3 to be the set of primes dividing q. To prove that F' can be taken totally real, it suffices, by Moret-Bailly's theorem, to show that $T_W(\mathbb{R})$ is nonempty. This follows as in [HST] from the existence of the symplectic polarization of weight $d-2$ on $\bar{\rho}$ and the construction of $\bar{\theta}$. To prove that F' can be taken unramified at ℓ', we note as in [HST] that, on the one hand, $\bar{\rho}$ was assumed unramified at ℓ'; on the other hand, the other hypotheses on ψ and ℓ' imply, as in [HST], that there is a point of $T_W(\mathbb{Q}_{\ell'}^{\mathrm{unr}})$ lying above the Fermat point $0 \in T_0$. The condition at q does not appear in the statement of the Main Theorem, so we refer the reader to [HST] for the details on this point.

Moreover, Proposition 2.6 asserts that F' can be taken linearly disjoint over F from any finite extension L_0/F. Note that, in contrast to [HST], we do not assume F' unramified at ℓ.

Recall that the point t has the property that there is a compatible family of $(d-1)$-dimensional ℓ^*-adic representations $V_{\ell^*,t}$ of $\Gamma_{F'}$ (letting ℓ^* denote a variable prime), with symplectic polarizations of weight $d-2$, and with residual representations $V[\ell^*]_t$, such that

$$V[\ell]_t \simeq \bar{\rho}|_{\Gamma_{F'}}, \qquad V[\ell']_t \simeq I(\bar{\theta})|_{\Gamma_{F'}}.$$

Moreover, $V_{\ell',t}$ is crystalline with Hodge–Tate weights $0, 1, \ldots, d-2$, each with multiplicity one. Now Theorem 4.61 of [CHT] and Theorem 4.6 of [T] apply to show that $V_{\ell',t}$ is automorphic as a representation of $\Gamma_{F'}$. Thus $V_{\ell,t}$ is also automorphic, hence $\bar{\rho}|_{\Gamma_{F'}}$ is automorphic. This completes the proof of the Main Theorem.

---

[1] Given the results of the Paris book project, the choice of an auxiliary prime q at this stage is no longer necessary, and the article [BGHT] dispenses with this choice.

Remark 2.7. Note that the cited theorems of [CHT] and [T] actually state that $V_{\ell',t}$ and $V_{\ell,t}$ are automorphic of the type considered in those papers, namely correspond to self-dual cohomological automorphic representations Π' of $\mathrm{GL}(n, F')$ (with a local condition at some finite prime now known to be irrelevant). Moreover, the archimedean component of Π' is the unique tempered representation of $\mathrm{GL}(n, F' \otimes_{\mathbb{Q}} \mathbb{R})$ with nontrivial cohomology with coefficients in the trivial representation.

Remark 2.8. It is clear that the proof works just as well if $k = \mathbb{F}_\ell$ is replaced by $\mathbb{Z}/\ell^m\mathbb{Z}$ for any m. In particular, we find that any representation of Γ_F on a free rank n $\mathbb{Z}/\ell^m\mathbb{Z}$-module can be completed to a rank d representation, for appropriate d, that admits potential liftings, for a collection of totally real Galois extensions F'/F, to d-dimensional ℓ-adic representations ρ of $\Gamma_{F'}$ that are not only geometric in the sense of Fontaine–Mazur (unramified outside a finite set of primes and de Rham at primes dividing ℓ) but are in fact automorphic and indeed are attached to automorphic representations of the kind considered in [CHT]. We leave the details to the reader. It is likely that by paying more attention to the choice of ℓ' one can even take ρ to be *crystalline* at primes dividing ℓ—then one can expect F'/F to be highly ramified at ℓ—but we have not looked into the question carefully.

3. Variants

One interest of the Main Theorem is that it hints at the pathologies that may lurk in the unexplored regions of the *eigenvarieties* constructed by Chenevier [C1, C2] and studied in his book with Bellaïche [Be-Ch]. Let Π be an automorphic representation of $\mathrm{GL}(n, F)$. For almost all[2] ℓ, the (semisimplified) automorphic ℓ-adic Galois representations define points on these eigenvarieties, whereas the automorphic residual representations define discrete invariants. If the residual representation is reducible then one can ask about the reducibility locus on the corresponding component of the eigenvariety, which is expected to encode a wealth of arithmetic information.

One naturally wonders whether any (semi-stable) lifting of the residual representation occurs as a point of the eigenvariety, which is obviously an especially intriguing question when the residual representation is completely arbitrary (for example a sum of the reductions modulo ℓ of the two-dimensional representations one hopes to attach to Maass forms, cf. Remark 1.3(2)). One might someday hope to be able to prove automorphic lifting theorems for certain representations like the $\bar{\rho} = \sigma \oplus \sigma'$ introduced in the proof of the main theorem. Assuming this to be the case (a very optimistic assumption), this gives a (potentially) positive answer to the question raised by Langlands, whether all Galois representations are in some sense accessible by a combination of automorphic and congruence methods. This answer may not be very satisfying, even ignoring the difference between automorphy and potential automorphy, but in this generality it is hard to imagine a simpler answer.

---

[2] The exceptions are a subset of the ℓ such that, for some prime v of F dividing ℓ, the local component Π_v has no vector fixed by the maximal pro-ℓ subgroup of the Iwahori subgroup at v.

The "very optimistic" assumption above is a sort of overconvergent modularity lifting hypothesis—the point on the eigenvariety associated to the lifting of $(\sigma \oplus \sigma')|_{\Gamma_{F'}}$ corresponds to an overconvergent ℓ-adic automorphic form of finite slope. It is very optimistic even if σ is irreducible and polarized of weight $n - 1$ and σ' is taken trivial, mainly because current methods assume (a) $\ell > n$ (which we do not assume); (b) ℓ is unramified in each F' (which we cannot guarantee), and (c) σ admits a de Rham lifting with distinct Hodge–Tate weights, which is a restrictive condition even on residual representations. It is much more optimistic if σ' is not trivial—this includes every case when σ is a two-dimensional even representation—because modularity lifting theorems appear to be completely out of reach for reducible representations of dimension > 2. When $n = 2$ and $F = \mathbb{Q}$ one has the notoriously difficult Skinner–Wiles theorem.

Note that in §2 we constructed automorphic lifts of representations of the form $\sigma \oplus \sigma'$, but there is no reason not to take nontrivial extensions of σ by σ', provided the extensions admit symplectic polarizations of the right weight. If we take an extension such that $\mathrm{End}_{\Gamma_F}(\bar{\rho})$ is limited to scalars—it seems this can always be arranged—then the deformation functor of $\bar{\rho}$ is representable. Generalizing the Skinner–Wiles theorem to higher dimensions, as would be necessary to treat reducible $\bar{\rho}$, appears at present an insurmountable obstacle, but if that were not the case we would want to make judicious choices of σ' when possible. This suggests the following strengthening of the hypotheses (a) and (b) of "Proof of the Main Theorem" in §2:

(c) For every prime v of F dividing ℓ, σ is of Fontaine–Laffaille type at v with n distinct weights.

(d) If σ is not symplectically polarized of weight $d - 2$ (with d to be determined below), then the sets of Fontaine–Laffaille weights of σ and of $\sigma^\vee(2 - d)$ have empty intersection.

This already implies at least $\ell > 2n$, otherwise there is no room for $2n$ distinct Fontaine–Laffaille weights. In fact, we want $\ell > m_+ - m_-$, where m_+ (resp. m_-) is the largest (resp. smallest) Fontaine–Laffaille weight of $\sigma \oplus \sigma^\vee(2 - d)$, and we define $\sigma' = \sigma^\vee(2 - d) \oplus \tau$ where τ is an innocuous symplectically polarized representation of dimension $d - 1 - 2n$ such that (a) and (b) are satisfied and such that $\sigma \oplus \sigma'$ is of Fontaine–Laffaille type at each v dividing ℓ with weights $0, \ldots, d - 2$, each with multiplicity one. One can take τ to be induced from a CM Hecke character with the missing weights.

The Main Theorem shows that such $\sigma \oplus \sigma'$, after restriction to $\Gamma_{F'}$ for a large class of totally real F', admit automorphic lifts of the type indicated in Remark 2.8. One expects that one can replace F' by F, and it is plausible that every lift of $\sigma \oplus \sigma'$ to characteristic zero that is unramified at all but finitely many places and de Rham at primes dividing ℓ is automorphic of this type. This should have implications for lifts of the original σ that are not assumed symplectically polarized.

In the applications in [HST] it was always necessary to prove that F' can be chosen unramified at ℓ, in order to apply the modularity lifting theorems of [CHT] and [T]. This required in practice assuming that the residual representation $\bar{\rho}$ is a sum of (necessarily distinct) characters when restricted to the inertia group at any prime dividing ℓ. Without this assumption there is no way to guarantee that the moduli space T_W has rational points

over an unramified extension of $\mathbb{Q}_\ell$. Since T_W is a curve, its local ℓ-adic points have little room for variation. Lifting theorems for the $\bar{\rho}$ considered above will have to be valid for number fields in which ℓ is allowed to ramify. For ordinary liftings this has now been proved in D. Geraghty's Harvard thesis, and there are interesting partial results in other cases in a forthcoming preprint of Barnet-Lamb, Gee, and Geraghty.

4. Proofs of Theorems 2.1 and 2.3

4.1. The general setting

Recall the general setting. We work over $\mathbb{C}$. We are given an integer $d \geq 3$, and we consider the Dwork family of degree d hypersurfaces X_λ in $\mathbb{P}^{d-1}$, with homogeneous coordinates $X_1, \ldots, X_d$, defined by the equation

$$X_\lambda : \sum_{i=1}^{d} X_i^d - d\lambda \prod_{i=1}^{d} X_i = 0,$$

with parameter $\lambda \in T_0(\mathbb{C}) := \mathbb{P}^1 \setminus \{\infty, \mu_d\}$. For any chosen $t \in T_0(\mathbb{C})$, we have a representation of the (topological) fundamental group $\pi_1(T_0(\mathbb{C}), t)$ on the Betti cohomology group $H^{d-2}(X_t, \mathbb{Z})$, which is a free $\mathbb{Z}$-module of known rank. The cup product pairing

$$\langle\,,\rangle : H^{d-2}(X_t, \mathbb{Z}) \times H^{d-2}(X_t, \mathbb{Z}) \to H^{2d-4}(X_t, \mathbb{Z}) = \mathbb{Z}$$

is a perfect duality of free $\mathbb{Z}$-modules; it is alternating if d is odd, and symmetric if d is even. The action of $\pi_1(T_0(\mathbb{C}), t)$ respects this pairing.

When d is even, the $(d-2)/2$th power of the cohomology class of a hyperplane section is a $\pi_1(T_0(\mathbb{C}), t)$-invariant element $L \in H^{d-2}(X_t, \mathbb{Z})$ with $\langle L, L \rangle = d$. We define $\mathrm{Prim}^{d-2}(X_t, \mathbb{Z}[1/d])) \subset H^{d-2}(X_t, \mathbb{Z}[1/d])$ to be the orthogonal complement of L under the cup product pairing. Because we have now inverted d, the cup product induces an autoduality on $\mathrm{Prim}^{d-2}(X_t, \mathbb{Z}[1/d])$. If d is odd, we define $\mathrm{Prim}^{d-2}(X_t, \mathbb{Z}[1/d])) := H^{d-2}(X_t, \mathbb{Z}[1/d])$.

The finite group $H_0 := \{(\zeta_1, \ldots, \zeta_d) \in \mu_d^d \mid \prod_i \zeta_i = 1\}$ acts on our family, so induces a $\pi_1(T_0(\mathbb{C}), t)$-equivariant action on $\mathrm{Prim}^{d-2}(X_t, \mathbb{Z}[1/d]))$. The space of invariants

$$V := \mathrm{Prim}^{d-2}(X_t, \mathbb{Z}[1/d])^{H_0}$$

is a free $\mathbb{Z}[1/d]$-module of rank $d-1$, on which the cup product induces an autoduality. So we have a representation

$$\rho : \pi_1(T_0(\mathbb{C}), t) \to \mathrm{Aut}(V, \langle\,,\rangle),$$

with $\mathrm{Aut}(V, \langle\,,\rangle)$ either $\mathrm{Sp}(d-1, \mathbb{Z}[1/d])$ if d is odd, or $O(d-1, \mathbb{Z}[1/d])$ if d is even. For any integer N prime to d, we have the reduction mod N of this representation

$$\rho_N : \pi_1(T_0(\mathbb{C}), t) \to \mathrm{Aut}(V[N], \langle\,,\rangle),$$

where we write

$$V[N] := V/NV.$$

4.2. A descent

There is a slightly finer structure we will take advantage of. Consider the family over $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ given by

$$Y_\lambda : \lambda^{-1} X_1^d + \sum_{i=2}^d X_i^d = d \prod_{i=1}^d X_i.$$

This is a descent of the Dwork family through the dth power map (cf. [Ka-AL, Section 6]). [Indeed, its pullback Y_{λ^d} is

$$Y_{\lambda^d} : \lambda^{-d} X_1^d + \sum_{i=2}^d X_i^d = d \prod_{i=1}^d X_i,$$

which, by the change of variable $X_1 \mapsto \lambda X_1$, $X_i \mapsto X_i$ for $i \geq 2$, becomes X_λ.] Repeating everything for this descended family, we now get, for any $t \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$, the subspace

$$\tilde{V} := \mathrm{Prim}^{d-2}(Y_t, \mathbb{Z}[1/d])^{H_0},$$

the representation

$$\tilde{\rho} : \pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, t) \to \mathrm{Aut}(\tilde{V}, \langle\,,\,\rangle),$$

and, for each integer N prime to d, its reduction mod N,

$$\tilde{\rho}_N : \pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, t) \to \mathrm{Aut}(\tilde{V}[N], \langle\,,\,\rangle),$$

where we write $\tilde{V}[N] := \tilde{V}/N\tilde{V}$.

The point of considering this descent is this. The dth power map is a finite etale covering of $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ by $\mathbb{P}^1(\mathbb{C}) \setminus \{0, \mu_d, \infty\}$, so for a base point $t \in \mathbb{P}^1(\mathbb{C}) \setminus \{0, \mu_d, \infty\}$ and its image $t^d \in \mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$, $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{0, \mu_d, \infty\}, t)$ is a normal subgroup of $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, t^d)$ of index d, with cyclic quotient. So for any homomorphism

$$\Lambda : \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, t^d) \to G$$

toward any group G, its image and the image of its restriction $[d]^\star \Lambda$ to $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{0, \mu_d, \infty\}, t)$ are related as follows: Image($[d]^\star \Lambda$) is a normal subgroup of Image(Λ) of index dividing d, with cyclic quotient. We will apply this with Λ taken to be $\tilde{\rho}$, so that $[d]^\star \Lambda$ is our ρ.

We know that

(odd case) If $d \geq 3$ is odd, then Image($\tilde{\rho}$) $\subset \mathrm{Sp}(d-1, \mathbb{Z}[1/d])$ is Zariski dense in $\mathrm{Sp}(d-1, \mathbb{C})$.

(even case) If $d \geq 3$ is even, then Image($\tilde{\rho}$) $\subset O(d-1, \mathbb{Z}[1/d])$ is Zariski dense in $O(d-1, \mathbb{C})$

(cf. [HST, 1.9] or [Ka-AL, 8.7]). Moreover, we know [Ka-AL, 5.3 or 8.5] that the $\mathbb{C}$-local system $\tilde{V}_{\mathbb{C}}$ is a specific hypergeometric local system, $\mathbb{H}_{\mathbb{C}}$, whose local monodromies are

(at 0) an automorphism whose characteristic polynomial is $(T^d - 1)/(T - 1)$,

(at 1) a pseudoreflection of determinant $(-1)^{d-1}$, i.e., a transvection if d is odd, and a reflection if d is even,

(at ∞) a single unipotent Jordan block.

We will now exploit the rigidity of this local system.

4.3. Rigid local systems

Let us first recall the basic facts about local systems on $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ and their rigidity. For any ring R, an *R-local system* $\mathcal{F}$ of rank $n \geq 1$ on $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ is a locally constant sheaf of free R-modules of rank n. Picking bases, this is a homomorphism

$$\rho_{\mathcal{F}} : \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, t) \to \mathrm{GL}(n, R).$$

Concretely, this means a triple (M_0, M_1, M_∞) of elements in $\mathrm{GL}(n, R)$ satisfying $M_0 M_1 M_\infty = 1$; the M's are the local monodromies around the three missing points. An isomorphism between R-local systems (M_0, M_1, M_∞) and (N_0, N_1, N_∞) is an element $A \in \mathrm{GL}(n, R)$ which conjugates each M into the corresponding N, i.e., $A(M_0, M_1, M_\infty)A^{-1} = (N_0, N_1, N_\infty)$. Two R-local system are said to be *locally isomorphic* if there exist three elements $A_0, A_1, A_\infty \in \mathrm{GL}(n, R)$ such that

$$A_0 M_0 A_0^{-1} = N_0, \quad A_1 M_1 A_1^{-1} = N_1, \quad A_\infty M_\infty A_\infty^{-1} = N_\infty.$$

An R-local system $\mathcal{F}$ is said to be *rigid* if, whenever $\mathcal{G}$ is a second R-local system which is locally isomorphic to ρ, there exists an isomorphism of $\mathcal{F}$ with $\mathcal{G}$.

When R is a field k, and $\mathcal{F}$ is an **absolutely irreducible** k-local system, there is a numerical criterion that implies its rigidity. Cohomologically, it can be stated as follows. Denote by $j : \mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\} \subset \mathbb{P}^1(\mathbb{C})$ the inclusion. If the Euler characteristic $\chi(\mathbb{P}^1(\mathbb{C}), j_\star(\mathrm{End}(\mathcal{F})))$ is 2, then $\mathcal{F}$ is rigid (cf. [Ka-RLS, first half of the proof of 1.1.2, which works with coefficients k any field]). In terms of the local monodromy matrices (M_0, M_1, M_∞) in $\mathrm{GL}(n, k)$ giving $\mathcal{F}$, absolute irreducibility means that no proper nonzero subspace of $(k^{\mathrm{alg.cl}})^n$ is stable under each of M_0, M_1, M_∞. To make explicit the numerical criterion, we need a notation. Given an element $A \in \mathrm{GL}(n, k)$, denote by $Z(A) \in M_n(k)$ its centralizer, i.e., the set of matrices which commute with A. For any k-local system $\mathcal{F}$ of rank n, we have the Euler–Poincaré formula

$$\chi(\mathbb{P}^1(\mathbb{C}), j_\star(\mathrm{End}(\mathcal{F}))) = -n^2 + \sum_{s \in \{0, 1, \infty\}} \dim_k(Z(M_s)).$$

The numerical criterion for rigidity of an absolutely irreducible k-local system $\mathcal{F}$ of rank n on $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ is thus

$$\sum_{s \in \{0, 1, \infty\}} \dim(Z(M_s)) = n^2 + 2.$$

4.4. Hypergeometric local systems

We next define hypergeometric local systems. An endomorphism $A \in M_n(k)$ with characteristic polynomial $P_A(T) := \det(T\,\mathbb{I}_n - A)$ is said to be *cyclic*, or *of companion type*, if the pair (k^n, A) is k-isomorphic to the pair $(k[T]/P_A(T)k[T], T)$. A k-local system $\mathcal{F}$ on $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ is called *hypergeometric* if it satisfies the following conditions on its local monodromies:

(1) M_1 is a pseudoreflection, i.e., $\dim_k(\mathrm{Ker}(M_1 - 1)) = n - 1$, i.e., the fixed space of M_1 has codimension one.
(2) Both M_0 and M_∞ are of companion type.

A hypergeometric k-local system is absolutely irreducible if M_0^{-1} and M_∞ have relatively prime characteristic polynomials (i.e., have no common eigenvalue in any overfield of k), simply because if $\mathcal{G} \subset \mathcal{F}$ is a nonzero proper sub-local system, then on either $\mathcal{G}$ or on the quotient $\mathcal{F}/\mathcal{G}$, M_1 will be trivial, and on that piece we will have $M_0 M_\infty = 1$.

Lemma 4.4.1. *Let k be a field, and $\mathcal{F} \sim (M_0, M_1, M_\infty)$ a hypergeometric k-local system on $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ of rank $n \geq 1$. Suppose that M_0 and M_∞^{-1} have relatively prime characteristic polynomials. Then $\mathcal{F}$ is (absolutely irreducible and) rigid.*

Proof. We check the numerical criterion. As M_0 and M_∞ are of companion type, their commuting algebras each have dimension n. Because M_1 is a pseudoreflection, its commuting algebra has dimension $(n-1)^2 + 1$. And indeed $n + n + ((n-1)^2 + 1) = n^2 + 2$. □

4.5. Spreading out and reducing mod ℓ, via Levelt

Now let us return to our $\mathbb{C}$-local system $\tilde{V}_\mathbb{C}$, which we know [Ka-AL, 5.3 or 8.5] is a specific hypergeometric local system, $\mathbb{H}_\mathbb{C}$, whose local monodromies are

(at 0) an automorphism whose characteristic polynomial is $(T^d - 1)/(T - 1)$,
(at 1) a pseudoreflection of determinant $(-1)^{d-1}$, i.e., a transvection if d is odd, and a reflection if d is even,
(at ∞) a single unipotent Jordan block.

Next we recall Levelt's explicit description [BH, Thm. 3.5] of the unique $\mathbb{C}$-local system with such local monodromies. Denote by A the companion matrix of local monodromy at ∞, and by B the companion matrix of the inverse of local monodromy at 0. These matrices lie in $\mathrm{GL}(d - 1, \mathbb{Z})$. Taking BA^{-1} as local monodromy around 1, we get the matrix relation $B^{-1}(BA^{-1})A = 1$, so a $\mathbb{Z}$-local system $\mathbb{H}_\mathbb{Z}$ on $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$. For any field k in which d is invertible, the images of A and B in $\mathrm{GL}(d - 1, k)$ have no common eigenvalue, and the image of BA^{-1} is a pseudoreflection. For such a field k, the k-local system $\mathbb{H}_k$ on $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ is therefore absolutely irreducible, and any k-local system on $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ whose local monodromies in $\mathrm{GL}(d - 1, k)$ have these prescribed Jordan normal forms is k-isomorphic to $\mathbb{H}_k$.

We first apply this with $k = \mathbb{Q}$. Consider the $\mathbb{Q}$-local system $\tilde{V}_\mathbb{Q}$. Its local monodromies are $\mathbb{Q}$-forms of the complex local monodromies, and hence its local monodromies are

(at 0) an automorphism whose characteristic polynomial is $(T^d - 1)/(T - 1)$,
(at 1) a pseudoreflection of determinant $(-1)^{d-1}$, i.e., a transvection if d is odd, and a reflection if d is even,
(at ∞) a single unipotent Jordan block.

Therefore $\tilde{V}_{\mathbb{Q}}$ is $\mathbb{Q}$-isomorphic to $\mathbb{H}_{\mathbb{Q}}$. With this identification, $\tilde{V}$ and $\mathbb{H}_{\mathbb{Z}[1/d]}$ are two $\mathbb{Z}[1/d]$-forms of $\tilde{V}_{\mathbb{Q}}$. So for any prime ℓ prime to d, Brauer–Nesbitt tells us that the reductions mod ℓ of these two $\mathbb{Z}[1/d]$-forms, namely $\tilde{V}[\ell]$ and $\mathbb{H}_{\mathbb{F}_\ell}$, have isomorphic semisimplifications. As $\mathbb{H}_{\mathbb{F}_\ell}$ is irreducible, we infer that in fact $\tilde{V}[\ell]$ and $\mathbb{H}_{\mathbb{F}_\ell}$ are $\mathbb{F}_\ell$-isomorphic.

4.6. Proof of 2.1

With these preliminaries established, we now turn to the proofs of Theorems 2.1 and 2.3. We begin with 2.1. Thus $d \geq 3$ is odd. If ℓ is an odd prime not dividing d, the group $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$ has no proper nontrivial normal subgroup other than its center $\{\pm 1\}$, the group $\mathrm{PSp}(d-1, \mathbb{F}_\ell) := \mathrm{Sp}(d-1, \mathbb{F}_\ell)/\{\pm 1\}$ is simple, and for fixed d but variable ℓ these simple groups are pairwise nonisomorphic (cf. [Ar, 5.1, 5.2]). And for any power ℓ^n, $n \geq 2$, of ℓ, the group $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$ maps onto $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$ with kernel an ℓ-group. By Goursat's lemma, if $N = \prod_i \ell_i^{n_i}$ is prime to d, then any subgroup of $\mathrm{Sp}(d-1, \mathbb{Z}/N\mathbb{Z}) \cong \prod_i \mathrm{Sp}(d-1, \mathbb{Z}/\ell_i^{n_i}\mathbb{Z})$ which maps onto each factor must be the entire group $\mathrm{Sp}(d-1, \mathbb{Z}/N\mathbb{Z})$. [We apply Goursat's lemma by induction on the number of factors, separating out one prime ℓ_1 from the others. We must show that $\mathrm{Sp}(d-1, \mathbb{Z}/\ell_1^{n_1}\mathbb{Z})$ and $\prod_{i \geq 2} \mathrm{Sp}(d-1, \mathbb{Z}/\ell_i^{n_i}\mathbb{Z})$ have no common nontrivial quotient. For this, we argue as follows. The only composition factors $\mathrm{Sp}(d-1, \mathbb{Z}/\ell_1^{n_1}\mathbb{Z})$ and $\prod_{i \geq 2} \mathrm{Sp}(d-1, \mathbb{Z}/\ell_i^{n_i}\mathbb{Z})$ have in common are ± 1. So if $\mathrm{Sp}(d-1, \mathbb{Z}/\ell_1^{n_1}\mathbb{Z})$ and $\prod_{i \geq 2} \mathrm{Sp}(d-1, \mathbb{Z}/\ell_i^{n_i}\mathbb{Z})$ have a common nontrivial quotient, that nontrivial quotient is a 2-group, which itself has a $\mathbb{Z}/2\mathbb{Z}$ quotient. But $\mathrm{Sp}(d-1, \mathbb{Z}/\ell_1^{n_1}\mathbb{Z})$ does not have a $\mathbb{Z}/2\mathbb{Z}$ quotient. Indeed, as ℓ_1 is odd, any homomorphism from $\mathrm{Sp}(d-1, \mathbb{Z}/\ell_1^{n_1}\mathbb{Z})$ to $\mathbb{Z}/2\mathbb{Z}$ must factor through the $\mathrm{Sp}(d-1, \mathbb{F}_{\ell_1})$ quotient, and this last group has no such quotient.]

We apply this to the image of ρ_N. So to prove Theorem 2.1, it suffices to show that for each odd prime power ℓ^n prime to d, the image of ρ_{ℓ^n} is the full group $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$. For this, it suffices to show that the image of $\tilde{\rho}_{\ell^n}$ is the full group $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$. [Indeed, as explained above, $\mathrm{Image}(\rho_{\ell^n})$ is a normal subgroup of $\mathrm{Image}(\tilde{\rho}_{\ell^n})$ of index dividing d, with cyclic quotient. But the group $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$ has no such normal subgroup other than itself: any homomorphism from $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$ onto a nontrivial cyclic group of order prime to ℓ factors through its $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$ quotient, and this last group has no nontrivial cyclic quotient.]

We first show that $G := \mathrm{Image}(\tilde{\rho}_\ell)$ is the full group $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$. It is an irreducible subgroup of $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$, generated by three elements x, y, z with $xyz = 1$, x an element of order d, y a transvection, and z a unipotent element with a single Jordan block. One knows that any irreducible subgroup of $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$ generated by transvections is the full group (cf. [M], [ZS1]). Let $N \triangleleft G$ denote the normal subgroup generated by all the

G-conjugates of y. Then G/N is generated by the images $\bar{x}$ and $\bar{z}$ of x and z, and $\bar{x}\bar{z} = 1$. But $\bar{x}$ has order dividing d, while $\bar{z}$ has order a power of ℓ, which is prime to d. Hence $G = N$ is generated by all the G-conjugates of y, so is generated by transvections, and we are done.

Now consider the closed subgroup $\Gamma \subset \mathrm{Sp}(d-1, \mathbb{Z}_\ell)$ defined as the ℓ-adic closure of the image of $\tilde{\rho} : \pi_1 \to \mathrm{Sp}(d-1, \mathbb{Z}[1/d])$. Local monodromy around 1 gives us an element $\gamma \in \Gamma$ which is a transvection when viewed in $\mathrm{Sp}(d-1, \mathbb{Q}_\ell)$ and which remains a transvection when reduced mod ℓ in $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$. By the previous paragraph, we know that Γ maps onto $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$. The following lemma tells us that any such Γ maps onto every finite quotient $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$ (and hence is the entire group $\mathrm{Sp}(d-1, \mathbb{Z}_\ell)$). [See [Wei, Thm. B] and [Vas, 1.3] for other approaches to this question.] Thus the image of $\tilde{\rho}_{\ell^n}$ is the full group $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$ for every $n \geq 1$.

Lemma 4.6.1. *Let $d \geq 3$ be odd, and ℓ an odd prime. Let $\Gamma \subset \mathrm{Sp}(d-1, \mathbb{Z}_\ell)$ be a closed subgroup which maps onto $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$. Suppose that there is an element $\gamma \in \Gamma$ which is a transvection when viewed in $\mathrm{Sp}(d-1, \mathbb{Q}_\ell)$ and which remains a transvection when reduced mod ℓ in $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$. Then Γ maps onto every finite quotient $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$, and $\Gamma = \mathrm{Sp}(d-1, \mathbb{Z}_\ell)$.*

Proof. Let us denote by $\Gamma_i \subset \Gamma$ the intersection of Γ with $1 + \ell^i M_{d-1}(\mathbb{Z}_\ell)$. Thus Γ_i consists of the elements of Γ which die in $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^i\mathbb{Z})$. Then Γ/Γ_1 is $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$, and for every $i \geq 1$, the quotient Γ_i/Γ_{i+1} is an $\mathbb{F}_\ell$-subspace of the $\mathbb{F}_\ell$-Lie algebra $\mathrm{Lie}(\mathrm{Sp}(d-1))(\mathbb{F}_\ell)$. The group Γ acts by conjugation on itself, preserving each subgroup Γ_i, and so acting on each quotient Γ_i/Γ_{i+1}, $i \geq 1$. This last action factors through $\Gamma/\Gamma_1 = \mathrm{Sp}(d-1, \mathbb{F}_\ell)$, and makes Γ_i/Γ_{i+1} into an $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$-stable subspace of $\mathrm{Lie}(\mathrm{Sp}(d-1))(\mathbb{F}_\ell)$. But one knows that $\mathrm{Lie}(\mathrm{Sp}(d-1))(\mathbb{F}_\ell)$ is $\mathrm{Sp}(d-1, \mathbb{F}_\ell)$-irreducible (cf. [Bor, 6.3, 6.4, 7.3], [Cur]). So for each $i \geq 1$, Γ_i/Γ_{i+1} is either 0 or $\mathrm{Lie}(\mathrm{Sp}(d-1))(\mathbb{F}_\ell)$.

We now use the element γ to show that Γ_i/Γ_{i+1} is never 0. Indeed, the element $N := \gamma - 1 \in M_{d-1}(\mathbb{Z}_\ell)$ has $N^2 = 0$ (because γ is a transvection in $\mathrm{Sp}(d-1, \mathbb{Q}_\ell)$) and $N \neq 0$ in $M_{d-1}(\mathbb{F}_\ell)$ (because γ remains a transvection mod ℓ). So $\gamma = 1 + N$ has $\gamma^r = 1 + rN$ for any integer $r \geq 1$. Taking $r = \ell^i$, we get $\gamma^{\ell^i} = 1 + \ell^i N$, whose image in Γ_i/Γ_{i+1} is nonzero (because N is nonzero mod ℓ). Once we know that each Γ_i/Γ_{i+1} is the full $\mathrm{Lie}(\mathrm{Sp}(d-1))(\mathbb{F}_\ell)$, a counting argument shows that $\Gamma/\Gamma_n \subset \mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$ is, for each $n \geq 1$, the full group $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$. Hence $\Gamma \subset \mathrm{Sp}(d-1, \mathbb{Z}_\ell)$ is a closed subgroup which maps onto every $\mathrm{Sp}(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$, so is dense, so must be the entire group. $\square$

4.7. Proof of 2.3

We now turn to proving 2.3. Here also it suffices to show that $\tilde{\rho}_\ell$ has one of the two asserted images. Indeed, for both of these asserted images, the only possibly nontrivial proper normal subgroups are the center, which is either trivial or is ± 1, and the subgroup $\Omega(d-1, \mathbb{F}_\ell)$ of index two, defined by $\det = \mathrm{ns} = 1$, which is a simple group (remember

$d - 1 \geq 5$ is odd). On the other hand, the image of ρ_ℓ is a normal subgroup of the asserted image, of index dividing d, and with cyclic quotient. The cyclicity of the quotient disqualifies the center and the trivial group, leaving only $\Omega(d - 1, \mathbb{F}_\ell)$ or the full asserted image as possibilities. The group $\Omega(d-1, \mathbb{F}_\ell)$ is ruled out because it lies in $SO(d-1, \mathbb{F}_\ell)$, but the image of ρ_ℓ contains reflections: the dth power map is finite etale over 1, so the local monodromy of $V[\ell]$ around each dth root of unity is a reflection.

Thus $d \geq 10$ is even, ℓ is an odd prime which is prime to d, and neither $d - 1$ nor $d + 1$ is a power of ℓ. Now $G := \text{Image}(\tilde{\rho}_\ell)$ is an irreducible subgroup of $O(d - 1, \mathbb{F}_\ell)$, generated by three elements x, y, z with $xyz = 1$, x an element of order d, y a reflection, and z a unipotent element with a single Jordan block. The same G/N argument as above shows that $G := \text{Image}(\tilde{\rho}_\ell)$ is an irreducible subgroup of $O(d - 1, \mathbb{F}_\ell)$ generated by reflections, indeed by all the G-conjugates of y.

4.8. The spinor norm

Let us denote by

$$\text{ns} : O(d - 1, \mathbb{F}_\ell) \to \pm 1$$

the spinor norm with respect to the quadratic form on $\tilde{V}[\ell]$ given by cup product. Recall [Ka-Irr, §6] that when $d - 1$ is odd, as it is here, there is only one orthogonal group $O(d - 1, \mathbb{F}_\ell)$, because the two isomorphism classes of nondegenerate quadratic forms in $d - 1$ variables over $\mathbb{F}_\ell$ are proportional: if Ψ is one of them, then the other is $\alpha\Psi$, for any nonsquare $\alpha \in \mathbb{F}_\ell^\times$. The spinor norm **depends** on the choice of the quadratic form Ψ, so should be denoted ns_Ψ. For a nonisotropic vector v, we have the reflection $R_v \in O(d - 1, \mathbb{F}_\ell)$, given by

$$R_v : w \mapsto w - 2\frac{\Psi(w, v)}{\Psi(v, v)}v.$$

Its spinor norm is given by

$$\text{ns}_\Psi(R_v) = \text{the class mod squares of } \Psi(v, v).$$

Since $O(d - 1, \mathbb{F}_\ell)$ is generated by reflections, this determines the spinor norm. If we pass from Ψ to $\alpha\Psi$, $\alpha \in \mathbb{F}_\ell^\times$ a nonsquare, then for any $g \in O(d - 1, \mathbb{F}_\ell)$, we have

$$\text{ns}_{\alpha\Psi}(g) = \det(g)\,\text{ns}_\Psi(g).$$

So the effect of passing from Ψ to $\alpha\Psi$, $\alpha \in \mathbb{F}_\ell^\times$ a nonsquare, is to interchange the two characters ns and det $\times$ ns, and so to interchange cases (3) and (4) in the classification just below.

4.9. Classification, and its use

One knows [W2], [ZS2] that if $d \geq 10$ and ℓ is odd, an irreducible subgroup of $O(d - 1, \mathbb{F}_\ell)$ which is generated by reflections **and** which is **primitive** is one of the following five groups.

(1a) the symmetric group S_d in its deleted permutation representation, if ℓ is prime to d,
(1b) the symmetric group S_{d+1} in its doubly deleted permutation representation, if ℓ divides $d + 1$,
 (2) the full group $O(d - 1, \mathbb{F}_\ell)$,
 (3) the index two subgroup of $O(d - 1, \mathbb{F}_\ell)$ where ns = 1,
 (4) the index two subgroup of $O(d - 1, \mathbb{F}_\ell)$ where ns = det.

[Recall that the *deleted permutation representation* of S_d is the $d - 1$-dimensional $\mathbb{F}_\ell$-representation given by its action on the space of those linear forms $\sum_{i=1}^{d} a_i X_i$ satisfying $\sum_i a_i = 0$. When ℓ divides $d + 1$, the *doubly deleted permutation representation* of S_{d+1} is the $d - 1$-dimensional $\mathbb{F}_\ell$-representation which is the quotient of its deleted permutation representation by the line spanned by $\sum_{i=1}^{d+1} X_i$.]

In our case, G cannot be the entire group $O(d - 1, \mathbb{F}_\ell)$, for the following reason. The element z has order a power of ℓ, so ns$(z) = \det(z) = 1$. Therefore we have ns$(x) =$ ns(y) and $\det(x) = \det(y) = -1$, so whichever of ns or det $\times$ ns is trivial on y is trivial on x as well (and is also trivial on z). So G certainly lies inside one of the groups (3) or (4).

Furthermore, because d is prime to ℓ, and neither $d - 1$ nor $d + 1$ is a power of ℓ, we cannot be in case (1a) or in case (1b). Consider first case (1a). Here G cannot be S_d, simply because the element z cannot lie in S_d. Indeed, under the action of the cyclic group generated by z, $\mathbb{H}_{\mathbb{F}_\ell}$ is indecomposable. The only elements $\gamma \in S_d$ which can possibly act indecomposably in the deleted permutation representation are either a single d-cycle, or a single $(d - 1)$-cycle. The first has order d, and the second has order $d - 1$, while z has order a power of ℓ.

When ℓ divides $d + 1$, but $d + 1$ is not a power of ℓ, we cannot be in case (1b): the element z cannot lie in S_{d+1}. As before, $\mathbb{H}_{\mathbb{F}_\ell}$ is indecomposable under the cyclic group generated by z. But the only elements $\gamma \in S_{d+1}$ which can possibly act indecomposably in the doubly deleted permutation representation are either a single $d+1$-cycle, or a single d-cycle, or a single $(d - 1)$-cycle. The first has order $d + 1$, the second has order d, the third has order $d - 1$, while z has order a power of ℓ.

So we are reduced to proving that G is primitive whenever $d \geq 10$, ℓ is an odd prime which is prime to d, and neither $d - 1$ nor $d + 1$ is a power of ℓ. We argue by contradiction. Again by classification [ZS2], if G is not primitive, then in a suitable basis of $\mathbb{H}_{\mathbb{F}_\ell}$, G is permutation-shaped, i.e., it stabilizes the collection of $d - 1$ lines spanned by the basis vectors. So we have a homomorphism of G onto a transitive subgroup K of S_{d-1}, by looking at its action on these $d - 1$ lines. The image of y must be nontrivial, since G is generated by the conjugates of y. And y must map to a transposition, since it acts as a reflection on $\mathbb{H}_{\mathbb{F}_\ell}$. Since G is generated by the conjugates of y, the image group K is a transitive subgroup of S_{d-1} generated by transpositions, so $K = S_{d-1}$. In this image group S_{d-1}, we have $\bar{x}\bar{y}\bar{z} = 1$, so $\bar{z}\bar{x} = \bar{y}^{-1}$ is a reflection, and S_{d-1} is generated by $\bar{x}$, $\bar{y}$, and $\bar{z}$.

We claim that either $\bar{x}$ or $\bar{z}$ is a $(d - 1)$-cycle, and that the other is the product of two disjoint cycles. Granting this, we reach a contradiction as follows. If $\bar{x}$ is a $(d - 1)$-cycle, then it has order $d - 1$. But x had order d, so $\bar{x}$ has order dividing d, hence $\bar{x} = 1$. But

this is impossible, for then S_{d-1} would be generated by $\bar{y}$ and $\bar{z}$, with $\bar{y}\bar{z} = 1$, so S_{d-1} would be generated by $\bar{y}$, so would be cyclic of order 2. If $\bar{z}$ is a $(d-1)$-cycle, then it has order $d-1$, but z had order a power of ℓ, so $\bar{z}$ has order either 1 or a power of ℓ. Since $d-1$ is not a power of ℓ, $\bar{z}$ must be trivial, and we reach the same contradiction.

Here is a monodromy-theoretic proof of the claim.

Lemma 4.9.1. *Let $d \geq 4$, and $a, b, c \in S_{d-1}$ elements with $abc = 1$ which generate S_{d-1}. Suppose that b is a transposition. Then one of a or c is a $(d-1)$-cycle, and the other is the product of two disjoint cycles.*

Proof. View S_{d-1} inside $O(d-1, \mathbb{C})$ by the permutation representation, and denote by $A, B, C \in O(d-1, \mathbb{C})$ the images of a, b, c respectively. Denote by $\mathcal{F}$ the $\mathbb{C}$-local system on $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ of rank $d-1$ whose local monodromies at $0, 1, \infty$ are A, B, C respectively. Consider the inclusion $j : \mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\} \to \mathbb{P}^1(\mathbb{C})$, and form the cohomology groups $H^i(\mathbb{P}^1(\mathbb{C}), j_\star \mathcal{F})$, whose dimensions we denote simply h^i. Thus $h^i = 0$ for i outside $\{0, 1, 2\}$. The permutation representation of S_{d-1} has one-dimensional spaces of invariants and of coinvariants, so $h^0 = h^2 = 1$. Because $\mathcal{F}$ is orthogonally self-dual, $H^i(\mathbb{P}^1(\mathbb{C}), j_\star \mathcal{F})$ is symplectically self-dual, so h^1 is even. The Euler–Poincaré formula gives

$$\chi(\mathbb{P}^1(\mathbb{C}), j_\star \mathcal{F}) := h^0 - h^1 + h^2 = 2 - h^1$$
$$= \chi(\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}, \mathcal{F}) + \sum_{s \in \{0,1,\infty\}} \text{(dim of invar.'s of local mono. at } s)$$
$$= -(d-1) + \dim(\mathrm{Ker}(A-1)) + \dim(\mathrm{Ker}(B-1)) + \dim(\mathrm{Ker}(C-1)).$$

As B is a reflection, $\dim(\mathrm{Ker}(B-1)) = d-2$, so we get

$$2 - h^1 = -1 + \dim(\mathrm{Ker}(A-1)) + \dim(\mathrm{Ker}(C-1)),$$

i.e.,

$$-h^1 = \dim(\mathrm{Ker}(A-1)) + \dim(\mathrm{Ker}(C-1)) - 3.$$

Since h^1 is ≥ 0 and even, we get the inequality

$$\dim(\mathrm{Ker}(A-1)) + \dim(\mathrm{Ker}(C-1)) \leq 3,$$

and the information that $\dim(\mathrm{Ker}(A-1)) + \dim(\mathrm{Ker}(C-1))$ is odd. But $\dim(\mathrm{Ker}(A-1))$, respectively $\dim(\mathrm{Ker}(C-1))$, is just the number of cycles in a, resp. in c, when that element of S_{d-1} is written as a product of disjoint cycles, including cycles of length one. So either a or c is a single cycle, and the other is the product of two disjoint cycles.   □

Although we do not need it, here for the sake of completeness is a more elementary (but perhaps less satisfying conceptually) proof of a slightly stronger statement.

Lemma 4.9.2. *Let $d \geq 4$, and $a, b, c \in S_{d-1}$ elements with $abc = 1$ which generate a transitive subgroup of S_{d-1}. Suppose that b is a transposition. Then one of a or c is a $(d-1)$-cycle, and the other is the product of two disjoint cycles.*

Proof. To fix ideas, renumber so that the transposition b is $(1, 2)$, and remember that $a^{-1} = bc$, so that b and c generate a transitive subgroup. If c is a $(d-1)$-cycle write c as $(1, \ldots, x, 2, \ldots, y)$. Then $a^{-1} = bc = (1, \ldots, x)(2, \ldots, y)$ is the product of two disjoint cycles. If c is the product of two disjoint cycles, then the symbols 1 and 2 cannot be in the same cycle, otherwise b fixes every element of the other cycle, contradicting the fact that b and c generate a transitive subgroup. So we can write $c = (1, \ldots, x)(2, \ldots, y)$. But then $a^{-1} = bc = (1, \ldots, x, 2, \ldots, y)$ is a $(d-1)$-cycle. Finally, c cannot be the product of three or more disjoint cycles, for then at least one of them contains neither 1 nor 2, and then b fixes every element of such a cycle, again contradicting the transitivity. $\square$

4.10. Analysis of the mod N representation

We begin with the orthogonal analogue of Lemma 4.6.1.

Lemma 4.10.1. *Let $d \geq 4$ be even, and ℓ an odd prime. Denote by*

$$O_1(d-1, \mathbb{F}_\ell) \subset O(d-1, \mathbb{F}_\ell)$$

any chosen one of the five subgroups containing $\Omega(d-1, \mathbb{F}_\ell)$. Denote by $O_1(d-1, \mathbb{Z}_\ell) \subset O(d-1, \mathbb{Z}_\ell)$, resp. by $O_1(d-1, \mathbb{Z}/\ell^n\mathbb{Z}) \subset O(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$, the complete inverse image of $O_1(d-1, \mathbb{F}_\ell)$ under the "reduction mod ℓ" map. Let $\Gamma \subset O_1(d-1, \mathbb{Z}_\ell)$ be a closed subgroup which maps onto $O_1(d-1, \mathbb{F}_\ell)$. Suppose that there is an element $\gamma \in \Gamma$ which is a regular unipotent element (i.e., unipotent with a single Jordan block) when viewed in $O(d-1, \mathbb{Q}_\ell)$ and which remains a regular unipotent element when reduced mod ℓ in $O(d-1, \mathbb{F}_\ell)$. Then Γ maps onto $O_1(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$ for every $n \geq 1$, and $\Gamma = O_1(d-1, \mathbb{Z}_\ell)$.

Proof. Let us denote by $\Gamma_i \subset \Gamma$ the intersection of Γ with $1 + \ell^i M_{d-1}(\mathbb{Z}_\ell)$. Thus Γ_i consists of the elements of Γ which die in $O(d-1, \mathbb{Z}/\ell^i\mathbb{Z})$. Then Γ/Γ_1 is $O_1(d-1, \mathbb{F}_\ell)$, and for every $i \geq 1$, the quotient Γ_i/Γ_{i+1} is an $\mathbb{F}_\ell$-subspace of the $\mathbb{F}_\ell$-Lie algebra $\text{Lie}(SO(d-1))(\mathbb{F}_\ell)$. The group Γ acts by conjugation on itself, preserving each subgroup Γ_i, and so acting on each quotient Γ_i/Γ_{i+1}, $i \geq 1$. This last action factors through $\Gamma/\Gamma_1 = O_1(d-1, \mathbb{F}_\ell)$, and makes Γ_i/Γ_{i+1} into an $O_1(d-1, \mathbb{F}_\ell)$-stable subspace of $\text{Lie}(SO(d-1))(\mathbb{F}_\ell)$. One knows that $\text{Lie}(SO(d-1))(\mathbb{F}_\ell)$ is $\text{Spin}(d-1, \mathbb{F}_\ell)$-irreducible (cf. [Bor, 6.3, 6.4, 7.3], [Cur]). The adjoint action of $\text{Spin}(d-1, \mathbb{F}_\ell)$ on its Lie algebra factors through its $\Omega(d-1, \mathbb{F}_\ell)$ quotient. Since $O_1(d-1, \mathbb{F}_\ell)$ contains $\Omega(d-1, \mathbb{F}_\ell)$, we see that $\text{Lie}(SO(d-1))(\mathbb{F}_\ell)$ is $O_1(d-1, \mathbb{F}_\ell)$- irreducible. So for each $i \geq 1$, Γ_i/Γ_{i+1} is either 0 or $\text{Lie}(SO(d-1))(\mathbb{F}_\ell)$. We now use the element γ to show that Γ_i/Γ_{i+1} is never 0.

If ℓ is large, i.e. if $\ell \geq d-1$, then $N^\ell = 0$, and we can use the powers $\gamma^{\ell^i} = 1 + \ell^i(N + \text{higher terms in } N)$ exactly as in the proof of Lemma 4.6.1 to get the asserted result.

In the general case, let us denote by ℓ^v the least power of ℓ with $\ell^v \geq d-1$. Then $N^{\ell^v} = 0$, but $N^{\ell^{v-1}} \neq 0$ in $M_{d-1}(\mathbb{F}_\ell)$ (because γ remains a regular unipotent element mod ℓ). Then we claim that $\gamma^{\ell^v} = 1 + \ell N_0$ for some nilpotent N_0 with $N_0 \neq 0$ in

$M_{d-1}(\mathbb{F}_\ell)$. Indeed, when we expand $\gamma^{\ell^v} = (1 + N)^{\ell^v}$ by the binomial theorem, the last term N^{ℓ^v} vanishes, and the intermediate terms all have coefficients divisible by ℓ, so our N_0 is given by

$$N_0 = (1/\ell) \sum_{a=1}^{\ell^v - 1} \text{Binom}(\ell^v, a) N^a.$$

Since $N^{\ell^{v-1}} \neq 0$ in $M_{d-1}(\mathbb{F}_\ell)$, it suffices to show that for some integer $1 \leq a \leq \ell^{v-1}$, we have $\text{ord}_\ell(\text{Binom}(\ell^v, a)) = 1$. For the least such a, we have $N_0 = (\ell\text{-adic unit})N^a + \cdots$. But $a = \ell^{v-1}$ is such an a. Once we know that $\gamma^{\ell^v} = 1 + \ell N_0$ with N_0 nilpotent and $N_0 \neq 0$ in $M_{d-1}(\mathbb{F}_\ell)$, we proceed inductively, examining the ℓ^i powers of γ^{ℓ^v}. For each $i \geq 0$, we have $\gamma^{\ell^{v+i}} = 1 + \ell^{i+1} N_i$ for some nilpotent N_i with $N_i \neq 0$ in $M_{d-1}(\mathbb{F}_\ell)$, indeed $N_{i+1} = N_i + \text{higher terms in } N_i$. We then use these powers $\gamma^{\ell^{v+i}}$ exactly as in the proof of Lemma 4.6.1 to get the asserted result. □

Corollary 4.10.2. *Suppose ℓ is an odd prime, $d \geq 10$ is even and prime to ℓ, and neither $d - 1$ nor $d + 1$ is a power of ℓ. Denote by $O_1(d - 1, \mathbb{F}_\ell) \subset O(d - 1, \mathbb{F}_\ell)$ the common image of ρ_ℓ and of $\tilde{\rho}_\ell$. Then for every $n \geq 1$, the images of ρ_{ℓ^n} and $\tilde{\rho}_{\ell^n}$ are both the group $O_1(d - 1, \mathbb{Z}/\ell^n\mathbb{Z})$.*

Proof. For both ρ and $\tilde{\rho}$, apply the previous result with Γ the ℓ-adic image, using local monodromy around ∞ as γ. □

Suppose $d \geq 10$ is even, and $N = \prod_i \ell_i^{n_i} \geq 3$ is an odd integer which is relatively prime to d. Suppose also that neither $d - 1$ nor $d + 1$ is a power of any ℓ_i dividing N. We have the product group $\prod_i O_1(d - 1, \mathbb{Z}/\ell_i^{n_i}\mathbb{Z})$. Each of its factors $O_1(d - 1, \mathbb{Z}/\ell_i^{n_i}\mathbb{Z})$ has a determinant homomorphism toward the same "abstract" group ± 1. We denote by

$$O_{1,=\det}(d - 1, \mathbb{Z}/N\mathbb{Z}) \subset \prod_i O_1(d - 1, \mathbb{Z}/\ell_i^{n_i}\mathbb{Z})$$

the subgroup of elements $(\gamma_i)_i$ all of whose components $f\gamma_i$ have the same determinant in ± 1 as each other. We have obvious inclusions

$$\text{Image}(\rho_N) \subset \text{Image}(\tilde{\rho}_N) \subset O_{1,=\det}(d - 1, \mathbb{Z}/N\mathbb{Z}),$$

the second inclusion simply because $\tilde{\rho}_N$ is the reduction mod N of an orthogonal representation in characteristic zero.

Lemma 4.10.3. *In the situation of the paragraph above, we have*

$$\text{Image}(\rho_N) = \text{Image}(\tilde{\rho}_N) = O_{1,=\det}(d - 1, \mathbb{Z}/N\mathbb{Z}).$$

Proof. We show this by induction on the number of distinct ℓ_i. If there is only one, this is the previous result. Separate ℓ_1 from the others, and define $N_0 := N/\ell_1^{n_1}$. Then we have

$$\text{Image}(\rho_N) \subset O_1(d - 1, \mathbb{Z}/\ell_1^{n_1}\mathbb{Z}) \times O_{1,=\det}(d - 1, \mathbb{Z}/N_0\mathbb{Z}),$$

and the subgroup $\mathrm{Image}(\rho_N)$ maps onto each factor, by induction. So by Goursat's lemma, this subgroup is the complete inverse image of an isomorphism between isomorphic quotients of the two factors. The only composition factors in the first factor are the simple group $\Omega(d-1, \mathbb{F}_{\ell_1})$, a single ± 1, and possibly some copies of $\mathbb{F}_{\ell_1}$. The only composition factors in the second factor are the simple groups $\Omega(d-1, \mathbb{F}_{\ell_i})$ with $i \geq 2$, possibly various copies of $\mathbb{F}_{\ell_i}$ with $i \geq 2$, and some copies of ± 1. So the only possible common nontrivial quotient of the two factors is the single group ± 1. Now on the first factor such a quotient must be a quotient of $O_1(d-1, \mathbb{F}_{\ell_1})$, since the kernel of reduction mod ℓ_1 is an ℓ_1-group. Similarly, on the second factor, such a quotient must be a quotient of $O_{1,=\det}(d-1, \mathbb{Z}/N_0^{\mathrm{red}}\mathbb{Z})$, where we write $N_0^{\mathrm{red}} := \prod_{i \geq 2} \ell_i$. But in each group $O_1(d-1, \mathbb{F}_{\ell_i})$, the elements of determinant one are precisely the simple group $\Omega(d-1, \mathbb{F}_{\ell_i})$. So we have a short exact sequence

$$\{1\} \to \prod_{i \geq 2} \Omega(d-1, \mathbb{F}_{\ell_i}) \to O_{1,=\det}(d-1, \mathbb{Z}/N_0^{\mathrm{red}}\mathbb{Z}) \xrightarrow{\det} \pm 1 \to \{1\}.$$

Thus the only ± 1 quotient of $O_{1,=\det}(d-1, \mathbb{Z}/N_0^{\mathrm{red}}\mathbb{Z})$ is by the determinant. So by Goursat, $\mathrm{Image}(\rho_N)$ is either the full product $O_1(d-1, \mathbb{Z}/\ell_1^{n_1}\mathbb{Z}) \times O_{1,=\det}(d-1, \mathbb{Z}/N_0\mathbb{Z})$ or the subgroup of this product consisting of pairs with equal determinants, i.e., the group $O_{1,=\det}(d-1, \mathbb{Z}/N\mathbb{Z})$. But as already noted, we have the a priori inclusion of the image in $O_{1,=\det}(d-1, \mathbb{Z}/N\mathbb{Z})$. □

4.11. Analysis of the exceptional cases

What becomes of Theorem 2.3 in the two excluded cases, when $d \pm 1$ is a power of ℓ?

Lemma 4.11.1. *Suppose ℓ is an odd prime, and $d - 1 \geq 5$ is a power of ℓ. Then the images of ρ_ℓ and of $\tilde{\rho}_\ell$ are both the symmetric group $S_d \subset O(d-1, \mathbb{F}_\ell)$, S_d in its deleted permutation representation.*

Proof. It suffices to prove that the image of $\tilde{\rho}_\ell$ is S_d, since the image of ρ_ℓ is then a normal subgroup of S_d of index dividing d, with cyclic quotient. The only such proper subgroup is the alternating group A_d, but this lies inside $SO(d-1, \mathbb{F}_\ell)$, whereas the image of ρ_ℓ contains reflections. To show that $\tilde{\rho}_\ell$ has the asserted image, we use the absolute irreducibility and the rigidity of our mod ℓ local system. Inside the subgroup $S_d \subset O(d-1, \mathbb{F}_\ell)$ we indeed have three elements x, y, z with $xyz = 1$ and which generate S_d, such that x has eigenvalues all the nontrivial dth roots of unity, y is a reflection, and z is a regular unipotent element. Namely, we take $x^{-1} := (1, 2, \ldots, d)$, $y := (1, 2)$, and $z := (2, 3, \ldots, d)$. [To see that z is a regular unipotent element, notice first that it is unipotent because it has ℓ power order. Now view z as lying in S_{d-1}. Then the given mod ℓ representation of $\langle z \rangle$ is the restriction of the permutation representation of S_{d-1}; in this representation, z has a one-dimensional space of invariants. Thus z is a unipotent element with a one-dimensional space of invariants, which is precisely a regular unipotent element.] □

Lemma 4.11.2. *Suppose ℓ is an odd prime, and $d + 1 \geq 5$ is a power of ℓ. Then the images of ρ_ℓ and of $\tilde{\rho}_\ell$ are both the symmetric group $S_{d+1} \subset O(d-1, \mathbb{F}_\ell)$, S_{d+1} in its doubly deleted permutation representation.*

Proof. Exactly as in the lemma above, it suffices to show that the image of $\tilde{\rho}_\ell$ is S_{d+1}. We again use the absolute irreducibility and the rigidity of our mod ℓ local system. Inside the subgroup $S_{d+1} \subset O(d-1, \mathbb{F}_\ell)$ we indeed have three elements x, y, z with $xyz = 1$ and which generate S_{d+1}, such that x has eigenvalues all the nontrivial dth roots of unity, y is a reflection, and z is a regular unipotent element. Namely, we take $x^{-1} := (2, 3, \ldots, d+1)$, $y := (1, 2)$, and $z := (1, 2, \ldots, d+1)$. [To see that z is a regular unipotent element, notice again that it is unipotent because it has ℓ power order. When we view z as lying in S_{d+1}, it gives a regular unipotent element in $O(d+1, \mathbb{F}_\ell)$ in the full permutation representation of S_{d+1}, i.e., it gives a unipotent element of companion type. Our $d-1$-dimensional representation is a subquotient of this one, and the property of being of companion type passes to subquotients.] □

We can also be more precise about the entire ℓ-adic image in these two excluded cases.

Lemma 4.11.3. *Suppose $d-1 \geq 7$, respectively $d+1 \geq 7$, is a power of the odd prime ℓ. Denote by*

$$O_S(d-1, \mathbb{F}_\ell) \subset O(d-1, \mathbb{F}_\ell)$$

the symmetric group $S_d \subset O(d-1, \mathbb{F}_\ell)$, respectively $S_{d+1} \subset O(d-1, \mathbb{F}_\ell)$. Denote by $O_S(d-1, \mathbb{Z}_\ell) \subset O(d-1, \mathbb{Z}_\ell)$, resp. by $O_S(d-1, \mathbb{Z}/\ell^n\mathbb{Z}) \subset O(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$, the complete inverse image of $O_S(d-1, \mathbb{F}_\ell)$ under the "reduction mod ℓ" map. Let $\Gamma \subset O_S(d-1, \mathbb{Z}_\ell)$ be a closed subgroup which maps onto $O_S(d-1, \mathbb{F}_\ell)$. Suppose that there is an element $\gamma \in \Gamma$ which is a regular unipotent element (i.e., unipotent with a single Jordan block) when viewed in $O(d-1, \mathbb{Q}_\ell)$ and which remains a regular unipotent element when reduced mod ℓ in $O(d-1, \mathbb{F}_\ell)$. Then Γ maps onto $O_S(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$ for every $n \geq 1$, and $\Gamma = O_S(d-1, \mathbb{Z}_\ell)$.

Proof. The key point is that the subgroup $O_S(d-1, \mathbb{F}_\ell) \subset O(d-1, \mathbb{F}_\ell)$ acts irreducibly on $\mathrm{Lie}(SO(d-1))$. In fact already the alternating group, A_d or A_{d+1} in the two cases, acts irreducibly (cf. [MagMal, Prop. 2.5, Table 2.1]). Using this fact, the proof is then identical to the proof of Lemma 4.10.1. □

Corollary 4.11.4. *Suppose $d - 1 \geq 7$, respectively $d + 1 \geq 7$, is a power of the odd prime ℓ. Then for every $n \geq 1$, the images of ρ_{ℓ^n} and $\tilde{\rho}_{\ell^n}$ are both the group $O_S(d-1, \mathbb{Z}/\ell^n\mathbb{Z})$.*

References

[Ar]   Artin, E.: Geometric Algebra. Interscience (1957); reprinted in Wiley Classics Library, Wiley (1988)   Zbl 0642.51001   MR 1009557

[BL]   Barnet-Lamb, T.: Potential automorphy for certain Galois representations to GL_{2n}. arXiv:0811.158

[BGHT]   Barnet-Lamb, T., Geraghty, D., Harris, M., Taylor, R.: A family of Calabi–Yau varieties and potential automorphy, II. http://people.math.jussieu.fr/~harris/resarticles.html

[Be-Ch]   Bellaïche, J., Chenevier, G.: p-adic families of Galois representations and higher rank Selmer groups. http://arxiv.org/abs/math/0602340

[BH]   Beukers, F., Heckman, G.: Monodromy for the hypergeometric function $_nF_{n-1}$. Invent. Math. **95**, 325–354 (1989)   Zbl 0663.30044   MR 0974906

[Bor]   Borel, A.: Properties and linear representations of Chevalley groups. In: Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Math. 131, Springer, Berlin, 1–55 (1970)   Zbl 0197.30501   MR 0258838

[C1]   Chenevier, G.: Familles p-adiques de formes automorphes pour $\mathrm{GL}(n)$. J. Reine Angew. Math. **570**, 143–217 (2004)   Zbl 1093.11036   MR 2075765

[C2]   Chenevier, G.: Une application des variétés de Hecke des groupes unitaires. http://www.math.polytechnique.fr/~chenevier/pub.html

[CHT]   Clozel, L., Harris, M., Taylor, R.: Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations. Publ. Math. IHES **108**, 1–181 (2008)   Zbl 1169.11020   MR 2470687

[Cur]   Curtis, C. W.: On projective representations of certain finite groups. Proc. Amer. Math. Soc. **11**, 852–860 (1960)   Zbl 0098.25303   MR 0118776

[HST]   Harris, M., Shepherd-Barron, N., Taylor, R.: A family of Calabi–Yau varieties and potential automorphy. Ann. of Math. **171**, 779–813 (2010)   Zbl pre05712744

[Ka-AL]   Katz, N. M.: Another look at the Dwork famlly. In: Manin Festschrift, to appear; www.math.princeton.edu/~nmk

[Ka-Irr]   Katz, N. M.: Report on the irreducibility of L-functions. In: Lang Memorial Volume, to appear; www.math.princeton.edu/~nmk/irredLfct49.pdf

[Ka-RLS]   Katz, N. M.: Rigid Local Systems. Ann. of Math Stud. 139, Princeton Univ. Press (1996)   Zbl 0864.14013   MR 1366651

[MagMal]   Magaard, K., Malle, G.: Irreducibility of alternating and symmetric squares. Manuscripta Math. **95**, 169–180 (1998)   Zbl 0919.20009   MR 1603309

[M]   McLaughlin, J.: Some groups generated by transvections. Arch. Math. (Basel) **18**, 364–368 (1967)   Zbl 0232.20084   MR 0222184

[MB]   Moret-Bailly, L.: Groupes de Picard et problèmes de Skolem II. Ann. Sci. École Norm. Sup. **22**, 181–194 (1989)   Zbl 0704.14015   MR 1005158

[T]   Taylor, R.: Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations, II. Publ. Math. IHES **108**, 183–239 (2008)   Zbl 1169.11021

[Vas]   Vasiu, A.: Surjectivity criteria for p-adic representations. I. Manuscripta Math. **112**, 325–355 (2003)   Zbl 1117.11064   MR 2067042

[W1]   Wagner, A.: Determination of the finite primitive reflection groups over an arbitrary field of characteristic not 2. I. Geom. Dedicata **9**, 239–253 (1980)   Zbl 0443.51009   MR 0578199

[W2]   Wagner, A.: Determination of the finite primitive reflection groups over an arbitrary field of characteristic not two. II, III. Geom. Dedicata **10**, 191–203, 475–523 (1981)   Zbl 0471.51015   MR 0608141

[Wei]   Weigel, T.: On the profinite completion of arithmetic groups of split type. In: Lois d'algèbres et variétés algébriques (Colmar, 1991), Travaux en Cours 50, Hermann, Paris, 79–101 (1996)   Zbl 0948.20024 MR 1600994

[ZS1]   Zalesskiĭ, A. E., Serežkin, V. N.: Linear groups generated by transvections. Izv. Akad. Nauk SSSR Ser. Mat. **40**, 26–49, 221 (1976) (in Russian); English transl.: Math. USSR-Izv. **10**, 25–46 (1976)   Zbl 0333.20038 and   Zbl 0355.20044 MR 0412295

[ZS2]   Zalesskiĭ, A. E., Serežkin, V. N.: Finite linear groups generated by reflections. Izv. Akad. Nauk SSSR Ser. Mat. **44**, 1279–1307, 1438 (1980) (in Russian); English transl.: Math. USSR-Izv. **17**, 477–503 (1981)   MR 0603578