EXPLICIT FROBENIUS CALCULATIONS SUPPORTING A GENERALIZATION OF A CONJECTURE OF SERRE

DARRIN DOUD AND BRIAN HANSEN

Abstract. In this paper we describe calculations which distinguish between two possibilities for Galois representations in examples given by Ash, Doud, and Pollack of a generalization of a conjecture of Serre. Our calculations allow us to strengthen the evidence for this conjecture.

1. Introduction

In [2, Sections 5.1.2 and 5.1.3], several examples of Galois representations are given, and conjectural connections between these Galois representations and Hecke eigenclasses are tested. The examples all consist of a twist of an even two-dimensional representation added to a character. In each example, there are two choices for the even two-dimensional representation, and the representation chosen is selected to give a convenient prediction for the weight associated to the resulting three-dimensional representation. However, the authors did not make explicit what the traces of Frobenius were for the chosen representation. This ambiguity means that for certain Frobenius elements, there are two possibilities for the trace under the three-dimensional representation. The aim of this paper is to describe how we resolve the ambiguity, computing the traces of Frobenius under the two-dimensional representation, and showing that these traces correspond to the computed Hecke eigenvalues in the three-dimensional case, as predicted by [2, Conjecture 3.1]. Thus, we strengthen the evidence given in [2] for the conjecture.

2. Statement of the conjecture

We begin by giving a statement of the conjecture that we wish to test. The statement given here will be simplified to the level 1 case and will be specific to three-dimensional Galois representations–for a complete statement see [2].

Fix a prime p. Let $M_3^+(\mathbb{Z})$ be the semigroup of matrices in $GL_3(\mathbb{Q})$ having integral coefficients and positive determinant. We define the Hecke algebra $\mathcal{H}$ to be the $\mathbb{F}_p$-algebra of double cosets $SL_3(\mathbb{Z})\backslash M_3^+(\mathbb{Z})/SL_3(\mathbb{Z})$. For a prime ℓ and an integer k with $0 \leq k \leq 3$, we define $T(\ell, k)$ to be the double coset corresponding to the diagonal matrix with $3-k$ 1's followed by k ℓ's on the diagonal.

Definition 1. Let $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_p)$ be a Galois representation (i.e. a continuous homomorphism), ramified only at p. Let V be an $\mathcal{H}$-module, and let $v \in V$ be a simultaneous eigenvector of all the $T(\ell, k)$ with $\ell \neq p$. Let $a(\ell, k)$ be the eigenvalue of $T(\ell, k)$ acting on v. We say that ρ is *attached* to v if for all $\ell \neq p$,

$$\sum_{k=0}^{3}(-1)^k a(\ell, k)\ell^{k(k-1)/2}X^k = \det(I - \rho(\mathrm{Frob}_\ell)X).$$

2000 *Mathematics Subject Classification.* 11F75,11F80.

To appear in JP Journal of Algebra, Number Theory, and Applications.

Note that the coefficient of X in the right-hand side is minus the trace of $\rho(\mathrm{Frob}_\ell)$, and the coefficient of X^2 will be called the cotrace of $\rho(\mathrm{Frob}_\ell)$, and denoted $T_2(\rho(\mathrm{Frob}_\ell))$.

The $\mathcal{H}$-module that we use in this paper will be a cohomology group $H^3(SL_3(\mathbb{Z}), V)$, where V is an irreducible $GL_3(\bar{\mathbb{F}}_p)$-module. We call the coefficient module V the weight.

The possible weights are described as follows:

Definition 2. An n-tuple of integers $(a_1, \ldots, a_n)$ is *p-restricted* if

$$0 \leq a_i - a_{i+1} \leq p-1$$

for $1 \leq i < n$, and $a_n \leq p-2$.

Proposition 3. [6] *Isomorphism classes of irreducible $GL_n(\mathbb{F}_p)$-modules are in one-to-one correspondence with p-restricted n-tuples.*

Definition 4. For a p-restricted triple (a, b, c), we denote the corresponding irreducible module by $F(a, b, c)$.

In [3, 2], the authors make predictions about which weights yield eigenclasses corresponding to given Galois representations. We will test these predictions by studying certain Galois representations, determining the eigenvalues that are required to correspond to them, and then computing the cohomology in the predicted weight in order to give evidence for the conjecture. The conjecture that we will test is a special case of the main conjecture of [2].

Conjecture 5. *Let p be an odd prime, and let $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_p)$ be an odd Galois representation (so that complex conjugation goes to a non-scalar matrix) ramified only at p. Then for certain weights V determined by ρ, ρ is attached to a cohomology eigenclass in $H^*(SL_3(\mathbb{Z}), V)$.*

Note that by [3, pg. 6], if ρ is either irreducible or the sum of an even two-dimensional representation plus a character, then we may take $*$ to be 3 in the conjecture. We do not give the complete formula for determining the weights V here, but refer the reader to [3] and [2] for more complete information.

3. Defining the representations

We recall the construction of odd three-dimensional Galois representations from even two-dimensional Galois representations described in [3].

Proposition 6. *Let $\theta : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p)$ be an irreducible representation, such that θ is unramified outside p, the image of θ has order relatively prime to p, θ maps complex conjugation to a scalar matrix, and the image of the inertia group I_p at p has order dividing $p-1$. Then $\theta|_{I_p}$ is reducible as a sum of powers of cyclotomic characters,*

$$\theta|_{I_p} \sim \begin{pmatrix} \omega^a & 0 \\ 0 & \omega^b \end{pmatrix}.$$

Let j and k be integers, such that $j \not\equiv k \pmod 2$ if θ maps complex conjugation to the identity, and $j \equiv k \pmod 2$ otherwise. Then $\rho = \theta \otimes \omega^j \oplus \omega^k$ is an odd three-dimensional Galois representation, and if the triple $(a+j-2, k-1, b+j)$ is p-restricted, one of the weights predicted for ρ is $F(a+j-2, k-1, b+j)$.

We will use this proposition by finding even two-dimensional Galois representations θ, and constructing ρ as above. By choosing j and k carefully, we may find representations with relatively small predicted weight. We then compute the cohomology in this weight,

Class	1	2	3	4	5	6	7	8
Order	1	2	2	3	4	6	8	8
χ_1	2	2	0	-1	2	-1	0	0
χ_2	2	-2	0	-1	0	1	$\zeta_8+\zeta_8^3$	$\zeta_8^5+\zeta_8^7$
χ_3	2	-2	0	-1	0	1	$\zeta_8^5+\zeta_8^7$	$\zeta_8+\zeta_8^3$

TABLE 1. Irreducible degree two characters of $\widetilde{S}_4$

and find systems of Hecke eigenvalues. According to the conjecture, the eigenvalues that we find should be related to the images of Frobenius elements under ρ—we compare these values, and if they match for several primes, we claim to have evidence that the conjecture is true.

3.1. **Octahedral representations.**

Definition 7. A Galois representation $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ will be called octahedral if its composition with the canonical projection $GL_2(\mathbb{F}_p) \to PGL_2(\mathbb{F}_p)$ is isomorphic to S_4 (the group of symmetries of the octahedron).

Note that the polynomial

$$g(x) = x^8 - 3137(13204809x^6 - 17449903959258x^4 + 19634266857241x^2 - 2521744)$$

has Galois group $\widetilde{S}_4 \cong GL_2(\mathbb{F}_3)$. We will let $\widetilde{K}$ be its splitting field over $\mathbb{Q}$. Note that $\widetilde{K}$ contains an extension $K/\mathbb{Q}$ with Galois group isomorphic to S_4.

We note that $g(x)$ has all its roots real, so that $\widetilde{K}$ is contained in the reals. Hence complex conjugation acts trivially on $\widetilde{K}$. We also note that $p = 3137$ has ramification index 8 in $\widetilde{K}$, and that no other primes ramify.

Examining the irreducible degree two characters of $\widetilde{S}_4$ (Table 1), we see that there are two faithful representations defined over $\bar{\mathbb{F}}_p$. There are thus two possible representations $\theta : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p)$, both of which cut out $\widetilde{K}$. The two possibilities are contragredient to each other—in other words, one can be obtained from the other by composing with the transpose-inverse automorphism of $GL_2(\bar{\mathbb{F}}_p)$. Since inertia at p has image of order 8, we see that $\theta|_{I_p}$ must decompose into linear characters of order dividing 8. In fact, one sees easily that $\theta|_{I_p}$ must decompose as either

$$\begin{pmatrix} \omega^{3(p-1)/8} & 0 \\ 0 & \omega^{(p-1)/8} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \omega^{5(p-1)/8} & 0 \\ 0 & \omega^{7(p-1)/8} \end{pmatrix}.$$

We will choose θ so that its restriction to inertia is the first of these two possibilities.

Now, taking $j = -(p-1)/8 = -392$ and $k = 1$, we define $\rho = (\theta \otimes \omega^j) \oplus \omega^k$. Then Proposition 6 yields a predicted weight of $F(782, 0, 0)$.

Note from the character table of $\widetilde{S}_4$ that the order of an element determines the trace of its image under θ except when the order is 2 or 8. The two conjugacy classes of order 2 are easy to distinguish, since one is central and one is not. The classes of order 8 are significantly more difficult, however, and will require more work to determine.

3.2. **Icosahedral representations.**

Definition 8. A Galois representation $\rho : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p)$ will be called icosahedral if its composition with the canonical projection $GL_2(\bar{\mathbb{F}}_p) \to PGL_2(\bar{\mathbb{F}}_p)$ has image isomorphic to A_5 (the group of symmetries of the icosahedron).

Class	1	2	3	4	5	6	7	8	9
Order	1	2	3	4	5	5	6	10	10
χ_1	2	-2	-1	0	$\zeta_5+\zeta_5^4$	$\zeta_5^2+\zeta_5^3$	1	$-\zeta_5^2-\zeta_5^3$	$-\zeta_5-\zeta_5^4$
χ_2	2	-2	-1	0	$\zeta_5^2+\zeta_5^3$	$\zeta_5+\zeta_5^4$	1	$-\zeta_5-\zeta_5^4$	$-\zeta_5^2-\zeta_5^3$

TABLE 2. Irreducible degree two characters of $\widehat{A}_5$

In order to work with icosahedral representations, we begin with A_5-extensions of $\mathbb{Q}$. Let L_1 and L_2 be the splitting fields of the polynomials

$$h_1(x) = x^5 - 7402x^3 - 3701x^2 + 14804x + 11103$$

and

$$h_2(x) = x^5 - 3821x^3 - 3821x^2 + 3821x + 3821,$$

respectively. Then each L_i is a totally real A_5-extension of $\mathbb{Q}$, and is ramified at only one prime with ramification index $e = 5$ (L_1 is ramified at $p_1 = 3701$, and L_2 is ramified at $p_2 = 3821$).

The existence of L_i yields a representation $\bar{\theta}_i : G_{\mathbb{Q}} \to PGL_2(\bar{\mathbb{F}}_{p_i})$ with image isomorphic to A_5. By [3, Theorem 4.1], we see that each of these projective representations has a lift to a representation $\theta_i : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p)$ with image isomorphic to $\widehat{A}_5$ (the unique nonsplit central extension of A_5 by $\mathbb{Z}/2\mathbb{Z}$), and with θ_i ramified only at p_i. We will let $\widehat{L}_i$ be the fixed field of the kernel of θ_i, so that $\widehat{L}_i/\mathbb{Q}$ is an $\widehat{A}_5$-extension of $\mathbb{Q}$ ramified only at p_i. Note that we may choose θ_i so that $\widehat{L}_i/L_i$ is unramified [10, Cor. 2.1.7]. Examining the irreducible degree two characters of $\widehat{A}_5$ (Table 2), we see that $\widehat{A}_5$ has two two-dimensional faithful irreducible representations, so that there are two possible choices for θ_i having fixed field $\widehat{L}_i$. We see easily that the restrictions to inertia of the two possibilities have the forms

$$\begin{pmatrix} \omega^{3(p_i-1)/5} & 0 \\ 0 & \omega^{2(p_i-1)/5} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \omega^{(p_i-1)/5} & 0 \\ 0 & \omega^{4(p_i-1)/5} \end{pmatrix}.$$

We will choose θ_i so that its restriction to inertia is the first of these two possibilities.

As mentioned in [2, Section 5.1.3], both $\widehat{L}_1$ and $\widehat{L}_2$ are totally real, so that θ_i takes complex conjugation to the identity. We then set $j_i = -2(p_i - 1)/5$ and $k = 1$, and find that by Proposition 6, the representation

$$\rho_i = \theta_i \otimes \omega^{j_i} \oplus \omega^k$$

has predicted weight $F((p_i - 1)/5 - 2, 0, 0)$.

Table 2 shows that the order of an element determines the trace of its image under θ_i, except when that order is 5 or 10. We will describe techniques to distinguish these cases in the next section.

4. Determining Frobenius elements

Computing the order of a Frobenius element at a rational prime is a simple task, given a defining polynomial for an extension. When a Galois group has more than one conjugacy class of a given order, however, it can be difficult to determine which conjugacy class contains the Frobenius for a given prime. This problem was addressed in [7], but the techniques there work only for certain groups, and do not apply to the extensions that we study here. Instead we use more direct, but more computationally intensive, techniques. We begin with the following theorem, which is easily derived from the definition of a Frobenius element.

Theorem 9. *Let F be a Galois extension of $\mathbb{Q}$, and let $\mathfrak{p}$ be a prime of F lying over the prime p in $\mathbb{Q}$. Suppose that $\mathfrak{p}/p$ is unramified, and let $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ be a generator of the decomposition group of $\mathfrak{p}/p$. Let M be the fixed field of $\langle\sigma\rangle$ in F, and let $\mathfrak{q} = \mathfrak{p} \cap M$. If, for some $\alpha \in F$, $N_M^F(\sigma(\alpha) - \alpha^p) \notin \mathfrak{q}$, then σ is not a Frobenius for $\mathfrak{p}/p$.*

Proof. By the definition of the Frobenius element, if σ is the Frobenius of $\mathfrak{p}/p$, then $\sigma(\alpha) - \alpha^p \in \mathfrak{p}$. Hence, the norm of $\sigma(\alpha) - \alpha^p$, being a product of an element of $\mathfrak{p}$ with elements in $\mathfrak{O}_F$, is in $\mathfrak{q} = \mathfrak{p} \cap M$. We can then conclude that if this norm is not in $\mathfrak{q}$, then σ is not a Frobenius. □

Note that this theorem cannot be used to prove directly that a certain element of the Galois group is in fact a Frobenius element. Instead, it can be used to exclude all other possibilities until the only remaining possibility is that σ is a Frobenius.

We will use this theorem for our representations by explicitly computing the action of elements of the Galois group on complex approximations of elements in the fields in which we are interested. We will compute minimal polynomials of these elements and, since the elements are algebraic integers, we will know that the minimal polynomials have integer coefficients. After computing them to high precision, we may thus round off the coefficients to the nearest integer. We will then use GP/PARI [11] to study the elements defined by the polynomials thus obtained.

4.1. **Octahedral example.** We begin by determining the Galois group of $g(x)$ as a permutation group on the eight roots of $g(x)$ using Magma [4]. Magma shows that for the ordering

$$\alpha_1 = 1.0607\ldots, \quad \alpha_2 = .0003584\ldots, \quad \alpha_3 = -203524.358\ldots, \quad \alpha_4 = -1149.5747\ldots,$$

$$\alpha_5 = -1.0607\ldots, \quad \alpha_6 = -.0003584\ldots, \quad \alpha_7 = 203524.358\ldots, \quad \alpha_8 = 1149.5747\ldots$$

of the roots, the Galois group is generated by the two elements $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$ and $\tau = (1\ 3\ 8)(4\ 5\ 7)$. We choose a prime $q \in \mathbb{Q}$ unramified in $\widetilde{K}$ and having inertial degree 8 in $\widetilde{K}/\mathbb{Q}$. The decomposition group D of any prime $\mathfrak{q}$ of $\widetilde{K}$ lying over q is then cyclic of order 8. Since all cyclic subgroups of order 8 in $\widetilde{S}_4$ are conjugate, we may choose a specific prime $\mathfrak{q}$ lying over q and having decomposition group generated by σ. In fact, we may even go further, and use the fact that σ is conjugate to σ^3 and σ^5 is conjugate to σ^7 to choose $\mathfrak{q}$ so that its Frobenius is either σ or σ^7. We now need to determine exactly which of σ and σ^7 is the Frobenius of $\mathfrak{q}/q$. To do this we will use Theorem 9.

We set α to be the root α_1 of $g(x)$, and consider $\beta_1 = \sigma(\alpha) - \alpha^q = \alpha_2 - \alpha_1^q$ and $\beta_7 = \sigma^7(\alpha) - \alpha^q = \alpha_8 - \alpha_1^q$. If $\beta_1 \notin \mathfrak{q}$, then σ^7 must be the Frobenius of $\mathfrak{q}/q$, and if $\beta_7 \notin \mathfrak{q}$, then σ must be the Frobenius of $\mathfrak{q}/q$. If it happens that both β_1 and β_7 are in $\mathfrak{q}$, then we obtain no information (this never happened in our computations).

Let $D = \langle\sigma\rangle$, let $\psi_1, \ldots, \psi_6$ be coset representatives of D in $\widetilde{S}_4$, and let K_6 be the fixed field of D in $\widetilde{K}$. Then $\gamma_1 = N_{K_6}^{\widetilde{K}}(\beta_1)$ is a root of

$$h_1(x) = \prod_{i=1}^{6}(x - \psi_i(\gamma_1)).$$

Since β_1 (and hence γ_1) are written in terms of the roots of $g(x)$, and we know how elements of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ act on roots of $g(x)$, we can easily compute a complex approximation to $h_1(x)$ to any desired precision. As mentioned above, we compute $h_1(x)$ to high precision, note that $h_1(x)$ has integer coefficients, and round off to compute $h_1(x)$ exactly. Similarly, we may compute a polynomial $h_7(x)$ having $\gamma_7 = N^{\widetilde{K}}_{K_6}(\beta_7)$ as a root. Using GP/PARI, we can easily determine whether a root of $h_i(x)$ lies inside a degree 1 prime of $Q(\gamma_i)$, and hence determine which of σ and σ^7 is the Frobenius of $\mathfrak{q}/q$.

For our purposes, we note that 3 has inertial degree 8 in $\widetilde{K}$, and that, using the ordering of the roots listed above, $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$ is a Frobenius above 3.

4.2. **Icosahedral examples.** Computing the conjugacy class of $\widehat{A}_5$ containing the Frobenius element at a prime is slightly more difficult. To begin, we only have a defining polynomial for L_i, not $\widehat{L}_i$. We overcome this problem using class field theory.

Let M_i be a degree six subextension of L_i. We may find a defining polynomial for M_i by using a resolvent calculation on the polynomial h_i, as described in [5, Algorithm 6.3.9]. Using Magma, we find that the subgroup of $\widehat{A}_5$ fixing this field has a unique normal subgroup of index 4 with cyclic quotient. Hence, the Galois correspondence tells us that M_i has a unique cyclic extension N_i of degree 4 contained in $\widehat{L}_i$. Since the only ramified prime in $\widehat{L}_i/\mathbb{Q}$ is p, which has ramification index 5, we see that N_i/M_i must be unramified and abelian. As such, it is contained in the Hilbert class field of M_i, its Galois group is a quotient of the ideal class group of M_i, and we may use Artin reciprocity to determine the inertial degrees of primes in N_i/M_i. Since the Galois closure of N_i is $\widehat{L}_i$, we may thus determine the inertial degrees of primes in $\widehat{L}_i/\mathbb{Q}$.

As an example, we note that in $L_1/\mathbb{Q}$ the prime 2 has inertial degree 5. We easily determine that in $M_1/\mathbb{Q}$ 2 splits into two primes, $\mathfrak{q}_1$ of inertial degree 1 and $\mathfrak{q}_2$ of inertial degree 5. Using GP/PARI to compute their images in the class group, we find that both are principal, so that they split completely in N_1. Hence, the primes lying over 2 in N_1 all have inertial degree 1 or 5. We then see that in $\widehat{L}_1$, 2 must have inertial degree 5. Similarly, we see that in $\widehat{L}_1$, the prime 3 has inertial degree 4.

Working with $L_2/\mathbb{Q}$, we find by similar techniques that 2 has inertial degree 10 and 3 has inertial degree 5 in $\widehat{L}_2$.

In order to distinguish the conjugacy classes of orders 5 and 10, we note that it suffices to distinguish the conjugacy classes of order 5 in A_5. This is clear, since the two conjugacy classes of order 5 in $\widehat{A}_5$ each lie over distinct conjugacy classes of order 5 in A_5. Similarly, the classes of order 10 in $\widehat{A}_5$ lie over distinct classes of order 5 in A_5. Hence, knowing the order of the Frobenius in $\widehat{L}_i/\mathbb{Q}$ and the conjugacy class of the Frobenius in $L_i/\mathbb{Q}$ determines the conjugacy class of the Frobenius in $\widehat{L}_i/\mathbb{Q}$.

In order to determine the conjugacy class of the Frobenius at p in L_i for a prime p of inertial degree 5, we may proceed as in the octahedral case, using Theorem 9 and complex approximations, or we may use the methods of [7] (since we are working in an A_5-extension, rather than an $\widehat{A}_5$-extension, the techniques in [7] are applicable).

In our examples, we ordered the roots of h_1 and h_2 in increasing order. In $\widehat{L}_1$, the prime 2 has inertial degree 5, and we find that its Frobenius in $\mathrm{Gal}(L_1/\mathbb{Q})$ is the five-cycle $(1\ 2\ 3\ 4\ 5)$. In $\widehat{L}_2$, 2 has inertial degree 10 and 3 has inertial degree 5. The Frobenius elements for 2 and 3 in $\mathrm{Gal}(L_2/\mathbb{Q})$ are $\mathrm{Frob}_2 = \mathrm{Frob}_3 = (1\ 2\ 3\ 4\ 5)$. Note that they both have order five, as there are no elements of order 10 in $\mathrm{Gal}(L_2/\mathbb{Q})$.

5. Cyclotomic characters

5.1. **Octahedral example.** We have chosen the Galois representation θ so that its restriction to inertia at I_p (where $p = 2713$) is diagonal, with diagonal characters $\omega^{(p-1)/8}$

and $\omega^{3(p-1)/8}$. We have also described how to determine whether a given element σ of order 8 is a Frobenius at a prime having inertial degree 8 in $\widetilde{K}/\mathbb{Q}$. We will now consider σ as a generator of an inertia group at p, and compute its trace under θ.

We begin by choosing a prime $\mathfrak{p}$ of $\widetilde{K}$ lying over p, such that the inertia group of $\mathfrak{p}/p$ is $\langle\sigma\rangle$. We note that $\mathfrak{p}/p$ has inertial degree 1. Hence the localization $\widetilde{K}_\mathfrak{p}/\mathbb{Q}_p$ is totally ramified of degree 8, with Galois group generated by σ. Note that since $p \equiv 1 \pmod 8$, $\mathbb{Q}_p$ contains the eighth roots of unity. We note that $g(x)$ remains irreducible over $\mathbb{Q}_p$, and that clearly $\alpha \in \widetilde{K} \subset \widetilde{K}_\mathfrak{p}$ is a uniformizer at $\mathfrak{p}$. If we let τ be an element of the inertia group in $\bar{\mathbb{Q}}_p/\mathbb{Q}_p$ whose restriction to $K_\mathfrak{p}$ is σ, then by [8] and [9, pg. 67, Proposition 7] we see that

$$\omega^{(p-1)/8}(\tau) \equiv \frac{\tau(p^{1/8})}{p^{1/8}} \equiv \frac{\tau(\alpha)}{\alpha} \equiv \frac{\sigma(\alpha)}{\alpha} \pmod{\mathfrak{p}}.$$

Note that this value is a well-defined eighth root of unity in $\mathbb{F}_p$. We use the fact that this root of unity is the image modulo $\mathfrak{p}$ of some rational integer in $\widetilde{K}$. Our strategy is to work in the global field $\widetilde{K}/\mathbb{Q}$, compute $\sigma(\alpha)/\alpha \in \widetilde{K}$, and then for integers n, determine the valuation of $\sigma(\alpha)/\alpha - n$ at $\mathfrak{p}$. If this valuation is positive, then the images of $\sigma(\alpha)/\alpha$ and n are equal in $\mathbb{F}_p$, otherwise they are unequal. Note that although $\sigma(\alpha)/\alpha$ may not be an algebraic integer, we know that it is a $\mathfrak{p}$-adic integer (in fact a $\mathfrak{p}$-adic unit).

We compensate for the fact that $\sigma(\alpha)/\alpha$ is not necessarily an algebraic integer by finding the primes in $\mathbb{Q}$ divisible by primes in $\widetilde{K}$ not equal to $\mathfrak{p}$, but dividing the principal ideal (α) in $\mathfrak{O}_{\widetilde{K}}$. It is clear that these primes are just the primes dividing the norm of α. Then, although $\sigma(\alpha)/\alpha - n$ may not be an algebraic integer, $\beta = k(\sigma(\alpha)/\alpha - n)$ will be an algebraic integer for some integer k divisible only by primes dividing the norm of α. We compute the norm from $\widetilde{K}$ to K_6 of β just as above, and determine the valuation of the norm at $\mathfrak{p} \cap K_6$. If this valuation is positive, it is possible (but not proven) that $\sigma(\alpha)/\alpha \equiv n \pmod{\mathfrak{p}}$ (since the norm contains several other factors that could be divisible by $\mathfrak{p}$). If the valuation is zero, it proves conclusively that $\sigma(\alpha)/\alpha \not\equiv n \pmod{\mathfrak{p}}$. Since there are only eight values of n that are eighth roots of unity modulo p, we can easily determine the reduction modulo $\mathfrak{p}$ of $\sigma(\alpha)/\alpha$. In fact, the calculation that we perform is somewhat simpler: we note that if ξ is an eighth root of unity, then $\xi + \xi^3$ is a square root of -2. Hence, we set η to be an integer whose square is congruent to -2 modulo p, and determine (using the above methods) which of $\pm\eta$ is congruent to $\sigma(\alpha)/\alpha + \sigma(\alpha)^3/\alpha^3$ modulo $\mathfrak{p}$.

In our example, taking $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$ with the ordering of the roots given in Section 4.1, and taking $k = 2^{12}397^8$, we find that $\omega^{(p-1)/8}(\tau) = \xi$ with $\xi + \xi^3 = 3040$ in $\mathbb{F}_{3137}$. Note that this value of k is the smallest that works: using a smaller value of k yields a β which is not an algebraic integer, so that its minimal polynomial does not have integral coefficients. Note also that σ is the image in $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ of both Frob_3 and the element τ of the inertia group at p. Since θ factors through this Galois group, we see that

$$\mathrm{Tr}(\theta(\mathrm{Frob}_3)) = \mathrm{Tr}(\theta(\tau)) = \omega^{(p-1)/8}(\tau) + \omega^{3(p-1)/8}(\tau) = 3040.$$

5.2. **Icosahedral examples.** Let σ be an element of order five in $\mathrm{Gal}(L_i/\mathbb{Q})$, and consider σ as a generator of inertia for a prime $\mathfrak{P}$ lying over p_i. Let τ be a lift of σ to the absolute inertia group above p. Then we wish to determine $\omega^{3(p_i-1)/5}(\tau) + \omega^{2(p_i-1)/5}(\tau) = \mathrm{Tr}(\theta_i(\tau))$. We proceed as above, letting F_i be a root field of h_i, and letting $\mathfrak{p}$ be the unique prime of F_i lying over p_i. We choose a uniformizer α of $\mathfrak{p}$ (in both of our examples, the uniformizer that we used was a root of h_i), and compute a complex approximation to

$(\sigma(\alpha)/\alpha)^2+(\sigma(\alpha)/\alpha)^3$. We proceed as in the octahedral case to determine the reduction of this element modulo $\mathfrak{P}$.

We simplified our calculations slightly, using the fact that we are interested in computing $\omega^{2(p-1)/5}(\tau)+\omega^{3(p-1)/5}(\tau)$. This value will be a sum $\xi^2+\xi^3$ where $\xi \in \mathbb{F}_{p_i}$ is a primitive fifth root of unity. For $p_1 = 3701$, there are two possible values for this sum: 940 and 2760. Our computations show that for $\sigma = (1\ 2\ 3\ 4\ 5)$, the value of $\omega^{2(p-1)/5}(\tau)+\omega^{3(p-1)/5}(\tau)$ is 940.

Similarly, for $p_2 = 3821$ there are two possibilities for $\xi^2+\xi^3$, namely 1474 and 2346. We found that for $\sigma = (1\ 2\ 3\ 4\ 5)$, the value of $\omega^{2(p-1)/5}(\tau)+\omega^{3(p-1)/5}(\tau)$ is 1474.

Finally, we note that there are two elements of $\mathrm{Gal}(\widehat{K}_i/\mathbb{Q})$ lying over $(1\ 2\ 3\ 4\ 5)$ in $\mathrm{Gal}(K/\mathbb{Q})$: η of order five and η' of order ten. One sees easily that $\theta_i(\eta') = -\theta_i(\eta)$, and that

$$\mathrm{Tr}(\theta_i(\eta)) = \omega^{2(p-1)/5}(\tau)+\omega^{3(p-1)/5}(\tau).$$

Hence, we find that $\mathrm{Tr}(\theta_1(\mathrm{Frob}_2)) = 940 \in \mathbb{F}_{3701}$, that $\mathrm{Tr}(\theta_2(\mathrm{Frob}_3)) = 1474 \in \mathbb{F}_{3821}$ and that $\mathrm{Tr}(\theta_2(\mathrm{Frob}_2)) = -1474 = 2347 \in \mathbb{F}_{3821}$.

6. Comparison with cohomology calculations

6.1. **Octahedral example.** For the octahedral example given here, we have that $p = 3137$. Hence, we see that

$$\theta|_{I_p} \sim \begin{pmatrix} \omega^{3(392)} & 0 \\ 0 & \omega^{392} \end{pmatrix}.$$

Taking $j = -392$ and $k = 1$ in Proposition 6, we have that $\rho = \theta\otimes\omega^j\oplus\omega^k$ has a predicted weight of $F(2(392)-2,0,0) = F(782,0,0)$. Computing the "excess" cohomology (see [1] for the definition of excess cohomology, and the techniques for computing it) in $H^3(SL_3(\mathbb{Z}), F(782,0,0))$ yields a one-dimensional space, on which the Hecke eigenvalues $T(2,k)$ and $T(3,k)$ act as scalars. We have the eigenvalues given below.

k	1	2
$a(2,k)$	3	1570
$a(3,k)$	60	2167

Note that 2 has a Frobenius of order 3, and 3 has a Frobenius of order 8. Hence, $\mathrm{Tr}(\theta(\mathrm{Frob}_2)) = -1$, and Section 5.1 shows that $\mathrm{Tr}(\theta(\mathrm{Frob}_3)) = 3040$. Using the definition of ρ in terms of θ, we see that $\mathrm{Tr}(\rho(\mathrm{Frob}_2)) = 2^{-392}\mathrm{Tr}(\theta(\mathrm{Frob}_2)) + 2^1 = 3 = a(2,1)$, and $T_2(\rho(\mathrm{Frob}_2)) = 3 = 2a(2,2)$. In addition, we see that $\mathrm{Tr}(\rho(\mathrm{Frob}_3)) = 3^{-392}\mathrm{Tr}(\theta(\mathrm{Frob}_3)) + 3 = 60 = a(3,1)$, and $T_2(\rho(\mathrm{Frob}_3)) = 227 = 3a(3,2)$. These are exactly the values predicted by the conjecture.

6.2. **Icosahedral examples.** We have two icosahedral examples, namely θ_1, with $p = 3701$, and θ_2, with $p = 3821$. Hence, for $i = 1,2$, we have that

$$\theta_i|I_p \sim \begin{pmatrix} \omega^{3(p-1)/5} & 0 \\ 0 & \omega^{2(p-1)/5} \end{pmatrix}.$$

Taking $j = -2(p-1)/5$ and $k = 1$ in Proposition 6, we have that $\rho_i = \theta_i \otimes \omega^j \oplus \omega^k$ has a predicted weight of $F((p-1)/5-2,0,0)$. This yields a predicted weight for ρ_1 of $F(738,0,0)$ and for ρ_2 of $F(762,0,0)$.

We now deal with ρ_1. Computing the excess cohomology $H^3(SL_3(\mathbb{Z}), F(738,0,0))$ yields a one-dimensional space with the eigenvalues given by the table below.

k	1	2
$a(2,k)$	1691	34
$a(3,k)$	3	380

In the field $\widehat{K}_1$, we see easily that 2 has Frobenius of order 5 and 3 has Frobenius of order 4. For a prime ℓ with Frobenius of order 4 in $\mathrm{Gal}(\widehat{K}_1/\mathbb{Q})$, we see that $\mathrm{Tr}(\theta_1(\mathrm{Frob}_\ell)) = 0$, and $T_2(\theta_1(\mathrm{Frob}_\ell)) = 0$. Hence, $\mathrm{Tr}(\rho_1(\mathrm{Frob}_3)) = 3 = a(3,1)$ and $T_2(\rho_1(\mathrm{Frob}_3)) = 1140 = 3a(3,2)$. In addition, Section 5.2 shows that $\mathrm{Tr}(\theta_1(\mathrm{Frob}_2)) = 940$. This yields values of $\mathrm{Tr}(\rho_1(\mathrm{Frob}_2)) = 1691 = a(2,1)$ and $T_2(\rho_1(\mathrm{Frob}_2)) = 68 = 2a(2,2)$. All of these traces and cotraces exactly match the computed Hecke eigenvalues.

Finally, we deal with ρ_2. The excess cohomology $H^3(SL_3(\mathbb{Z}), F(782,0,0))$ is once again one-dimensional, with Hecke eigenvalues defined below.

k	1	2
$a(2,k)$	2349	437
$a(3,k)$	649	2504

The images of Frob_2 and Frob_3 under θ_2 have orders 10 and 5, respectively. In Section 5.2 we determined that $\mathrm{Tr}(\theta_2(\mathrm{Frob}_2)) = 2347$ and $\mathrm{Tr}(\theta_2(\mathrm{Frob}_3)) = 1474$. We then find that $\mathrm{Tr}(\rho_2(\mathrm{Frob}_2)) = 2349 = a(2,1)$ and $T_2(\rho_2(\mathrm{Frob}_2)) = 874 = 2a(2,2)$, and that $\mathrm{Tr}(\rho_2(\mathrm{Frob}_3)) = 649 = a(3,1)$ and $T_2(\rho_2(\mathrm{Frob}_3)) = 3691 = 3a(3,2)$. Hence the computed traces and cotraces exactly match the computed Hecke eigenvalues, as predicted by the conjecture.

7. Conclusion

In summary, for three examples of Galois representations from [2] for which the authors of [2] were unable to distinguish between certain conjugacy classes of Frobenius elements, we have distinguished between these classes. Our calculations allow us to determine the traces and cotraces of Frobenius elements, and these computed traces and cotraces precisely match the Hecke eigenvalues of certain cohomology classes, exactly as predicted by [2, Conjecture 3.1]. Hence, we have strengthened the evidence for the conjecture.

8. Acknowledgments

Computations in this paper were performed using the Magma [4] and GP/PARI [11] computer algebra systems. The authors thank the Brigham Young University College of Physical and Mathematical Sciences for funding to complete this research. Doud's work was supported by NSA Grant H98230-05-1-0244.

References

1. Gerald Allison, Avner Ash, and Eric Conrad, *Galois representations, Hecke operators, and the mod-p cohomology of* $\mathrm{GL}(3,\mathbb{Z})$ *with twisted coefficients*, Experiment. Math. **7** (1998), no. 4, 361–390.
2. Avner Ash, Darrin Doud, and David Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. **112** (2002), no. 3, 521–579.
3. Avner Ash and Warren Sinnott, *An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod p cohomology of* $GL(n,\mathbb{Z})$, Duke Math. J. **105** (2000), no. 1, 1–24.
4. Wieb Bosma, John Cannon, and Catherine Playoust, *The MAGMA algebra system, I: The user language*, J. Symb. Comp. **24** (1997), 235–265.
5. Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.
6. Stephen R. Doty and Grant Walker, *The composition factors of* $F_p[x_1,x_2,x_3]$ *as a* $GL(3,p)$*-module*, Journal of Algebra **147** (1992), 411–441.
7. David P. Roberts, *Frobenius classes in alternating groups*, Rocky Mountain J. Math. **34** (2004), no. 4, 1483–1496.

8. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
9. ______, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979.
10. Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992, Lecture notes prepared by Henri Darmon, with a foreword by Darmon and the author.
11. The PARI-Group, Bordeaux, *PARI/GP, Version 2.1.5*, 2000, available from `http://www.parigp-home.de`.

Brigham Young University, Department of Mathematics, 292 TMCB, Provo, UT 84602
E-mail address: `doud@math.byu.edu`

E-mail address: `bfh@math.byu.edu`