Supersingular Galois representations and a generalization of a conjecture of Serre

Darrin Doud*
Brigham Young University
Department of Mathematics
292 TMCB
Provo, UT 84602

August 14, 2006

Abstract

Serre's conjecture relates two-dimensional odd irreducible Galois representations over $\bar{\mathbb{F}}_p$ to modular forms. We discuss a generalization of this conjecture to higher-dimensional Galois representations. In particular, for n-dimensional Galois representations which are irreducible when restricted to the decomposition group at p, we strengthen a conjecture of Ash, Doud, and Pollack. We then give computational evidence for this conjecture in the case of three-dimensional representations.

1 Introduction

In [ADP02], a conjecture connecting n-dimensional Galois representations over $\bar{\mathbb{F}}_p$ with arithmetic cohomology classes is described and computational evidence for the conjecture is given for three-dimensional Galois representations. This conjecture is a generalization of Serre's conjecture [Ser87] relating odd irreducible two-dimensional Galois representations and modular forms. An interesting case of the conjecture occurs when the restriction of the representation to a decomposition group at p remains irreducible. In this case we say that the representation is supersingular, and note that its restriction to inertia at p may be diagonalized in terms of *niveau* n fundamental characters. In [ADP02], several examples of such representations with $n = 3$ were given, and computational evidence for the conjecture was presented. Unfortunately, the levels of all of the examples were fairly high, and computational limitations did not allow exhaustive calculations to test whether the conjecture predicted all possible weights. We have now been able to complete these computations, and have discovered that the original conjecture failed to predict several weights which do in fact

*This work was partially supported by NSA Grant H98230-05-1-0244.

seem to work. In this paper, we modify the conjecture based on this computational evidence, and give additional computational evidence for the modified conjecture.

In addition to the computational evidence given here, we note that Florian Herzig [Her06] has come up with a description of the predicted weights for a supersingular three-dimensional Galois representation based on decomposition of characteristic p reductions of certain characteristic zero modules. The two predictions arrived at independently both yield the same set of weights, at least for what Herzig calls "regular" weights. Herzig's results will appear elsewhere—in this paper we concentrate on the computational evidence for the conjecture.

2 Statement of the conjecture

In this section we give brief definitions of the terms needed to state the conjecture, together with a statement of the conjecture, and a comparison of the current version of the conjecture with an older version.

For each prime q we fix a decomposition group D_q in $G_{\mathbb{Q}}$ together with the standard filtration of ramification subgroups $I_{q,i}$ for $0 \leq i$ inside this decomposition group. A Frobenius element Frob_q at q is then an element of D_q which generates $D_q/I_{q,0}$ and acts as the qth power map on residue fields.

2.1 Hecke operators and attached eigenvectors

Fix a prime p and positive integers n and N, with $(N,p)=1$, and let $\Gamma_0(N)$ be the subgroup of matrices in $\mathrm{SL}_n(\mathbb{Z})$ whose first row is congruent to $(*,0,\ldots,0)$ modulo N. Let S_N be the subsemigroup of matrices with integer entries in $\mathrm{GL}_n(\mathbb{Q})$, satisfying the same congruence condition. Then $(\Gamma_0(N), S_N)$ is a Hecke pair [AS86], and we define the Hecke algebra $\mathcal{H}(N)$ to be the commutative $\bar{\mathbb{F}}_p$-algebra of double cosets $\Gamma_0(N)\backslash S_N/\Gamma_0(N)$, as in [AS86]. For each prime $\ell \nmid N$ and each k between 0 and n, we denote by $T(\ell,k)$ the double coset with representative a diagonal matrix with k 1's followed by $n-k$ ℓ's.

We note that the Hecke algebra $\mathcal{H}(N)$ acts on homology and cohomology of $\Gamma_0(N)$ with coefficients in any $\bar{\mathbb{F}}_p[S_N]$-module. We then make the following definition:

Definition 2.1. Let V be an $\mathcal{H}(pN)$-module, and let $v \in V$ be a simultaneous eigenvector of all the $T(\ell,k)$ for which $\ell \nmid N$ and $0 \leq k \leq n$. Denote the eigenvalue of $T(\ell,k)$ acting on v by $a(\ell,k) \in \bar{\mathbb{F}}_p$. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{F}}_p)$ be a Galois representation unramified outside pN, and suppose that for all $\ell \nmid pN$,

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

Then we say that ρ is *attached* to v, or that v *corresponds* to ρ.

Note that the negative of the coefficient of X in $\det(I-\rho(\mathrm{Frob}_\ell)X)$ is the trace of $\rho(\mathrm{Frob}_\ell)$, and the coefficient of X^n is $(-1)^n$ times the determinant of

$\rho(\mathrm{Frob}_\ell)$. For $n=3$, we will call the coefficient of X^2 in $\det(I-\rho(\mathrm{Frob}_\ell)X)$ the *cotrace* of $\rho(\mathrm{Frob}_\ell)$ and denote it by $T_2(\rho(\mathrm{Frob}_\ell))$.

In our conjecture, the $\mathcal{H}(pN)$-module used will be the cohomology group $H^3(\Gamma_0(N), W)$, with some coefficient module W. The values of N and W will be determined by the weight, level, and nebentype of the representation, defined below.

2.2 Level and Nebentype

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{F}}_p)$ be a Galois representation (i.e. a continuous homomorphism with respect to the profinite topology on $G_{\mathbb{Q}}$ and the discrete topology on $\mathrm{GL}_n(\bar{\mathbb{F}}_p)$). Let M be an n-dimensional $\bar{\mathbb{F}}_p$-vector space on which $G_{\mathbb{Q}}$ acts via ρ.

For each prime $q \neq p$, we set $g_i = |\rho(I_{q,i})|$ and

$$n_q = \sum_{i=0}^{\infty} g_i/g_0 \dim M/M^{I_{q,i}}$$

The n_q are nonnegative integers, and only finitely many of them are nonzero.

Definition 2.2. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{F}}_p)$ be a Galois representation. Then the *level* $N = N(\rho)$ of ρ is

$$N = \prod_{q \neq p} q^{n_q}.$$

Note that the level is a positive integer, relatively prime to p, and divisible by exactly those primes $q \neq p$ at which ρ is ramified.

Definition 2.3. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{F}}_p)$ be a Galois representation of level N. Then $\det \rho$ factors as $\omega^k \epsilon$, where ω is the mod p cyclotomic character, ϵ is unramified at p, and $0 \leq k \leq p-2$. By class field theory we may consider ϵ as a character $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \bar{\mathbb{F}}_p^\times$. We say that ϵ is the *nebentype* of ρ.

2.3 Weights

The generalization of the predicted weight of a Galois representation that we will use is an irreducible $\mathrm{GL}_n(\mathbb{F}_p)$-module. We begin by describing the set of such modules, together with certain relationships between irreducible modules. We then describe our prediction of which weights correspond to a given Galois representation.

2.3.1 Parametrization by p-restricted n-tuples

Definition 2.4. An n-tuple $(a_{n-1}, \ldots, a_0)$ is *p-restricted* if, for $1 \leq i \leq n-1$,

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

and

$$0 \leq a_0 \leq p-2.$$

Proposition 2.5. *[Gre80, DW92] The set of all irreducible $\bar{\mathbb{F}}_p[GL_n(\mathbb{F}_p)]$-modules is in one-to-one correspondence with the set of p-restricted n-tuples.*

The correspondence of Proposition 2.5 is made explicit by assigning a p-restricted n-tuple $(a_{n-1}, \ldots, a_0)$ to the unique simple submodule of the dual Weyl module with highest weights $(a_{n-1}, \ldots, a_0)$. We denote this module by $F(a_{n-1}, \ldots, a_0)$.

2.3.2 Prime and dagger notation

Definition 2.6. Given an n-tuple of integers $(a_{n-1}, \ldots, a_0)$, we define $(a_{n-1}, \ldots, a_0)'$ to be the set of all p-restricted n-tuples $(b_{n-1}, \ldots, b_0)$ such that each $b_i \equiv a_i \pmod{p-1}$.

Note that $(a_{n-1}, \ldots, a_0)'$ always contains at least one n-tuple, but it can contain more. For example, if $n = 3$ and $p = 11$, then $(1, 0, 0)' = \{(1, 0, 0), (11, 10, 0)\}$, and $(10, 0, 0)' = \{(0, 0, 0), (10, 0, 0), (10, 10, 0), (20, 10, 0)\}$.

Definition 2.7. Given a p-restricted n-tuple of integers $(a_{n-1}, \ldots, a_0)$, we define $(a_{n-1}, \ldots, a_0)^\dagger$ to be the set of n-tuples $(b_{n-1}, \ldots, b_0)$ in $(a_{n-1}, \ldots, a_0)'$ such that each $b_i - b_{i-1} \geq a_i - a_{i-1}$.

As an example, when $n = 3$ and $p = 11$, $(10, 0, 0)^\dagger = \{(10, 0, 0), (20, 10, 0)\}$.

Definition 2.8. We define

$$F(a_{n-1}, \ldots, a_0)' = \{F(b_{n-1}, \ldots, b_0) : (b_{n-1}, \ldots, b_0) \in (a_{n-1}, \ldots, a_0)'\}$$

and

$$F(a_{n-1}, \ldots, a_0)^\dagger = \{F(b_{n-1}, \ldots, b_0) : (b_{n-1}, \ldots, b_0) \in (a_{n-1}, \ldots, a_0)^\dagger\}.$$

2.3.3 Extra weights

In case $n = 3$, we make the following definition.

Definition 2.9. Let (a_2, a_1, a_0) be a p-restricted triple. Then if $a_2 - a_0 < p - 2$, we define the *extra weight* associated to $F(a_2, a_1, a_0)$ to be

$$F(b_2, b_1, b_0) = \begin{cases} F(p - 2 + a_0, a_1, a_2 - (p - 2)) & \text{if } a_2 \geq p - 2 \\ F(2(p - 2) + a_0 + 1, a_1 + (p - 1), a_2 + 1) & \text{if } a_2 < p - 2. \end{cases}$$

For a detailed discussion of extra weights, and a motivation for their definition, see [ADP02, Remark 3.4].

2.4 Predicted weights

In order to predict the weights corresponding to a supersingular Galois representation, we diagonalize its restriction to inertia. By [ADP02, Thm 2.16], this diagonalization takes the form

$$\rho|_{I_{p,0}} \sim \begin{pmatrix} \psi_{n,1}^m & & \\ & \ddots & \\ & & \psi_{n,n}^m \end{pmatrix},$$

for some m, where $\psi_{n,1}, \ldots, \psi_{n,n}$ are the fundamental characters of *niveau* n [Ser72, p. 267]. Our prediction for the weight will depend on the exponent m in this decomposition. Note that by permuting the fundamental characters, we may multiply m by p^k for $0 \leq k \leq n-1$. In addition, since the fundamental characters have order $p^n - 1$, we see that m is only defined modulo $p^n - 1$. Our conjecture will be invariant under these choices.

We let $a_0, \ldots, a_{n-1}$ be any integers such that

$$m \equiv a_0 + a_1 p + \ldots + a_{n-1} p^{n-1} \pmod{p^n - 1}$$

Note that multiplying m by p permutes the set of a_i cyclically, and that the a_i depend only on the congruence class of m modulo $p^n - 1$. Note also that we may add a multiple of $p-1$ to each of the a_i to get another n-tuple satisfying the same relation.

Define integers $\{b_{n-1}, \ldots, b_0\}$ by relabeling the a_i so that each $b_i \geq b_{i-1}$. We will then define $c_i = b_i - i$. If the n-tuple $(c_{n-1}, \ldots, c_0)$ is p-restricted, then we predict all of the weights in $F(c_{n-1}, \ldots, c_0)^\dagger$, otherwise we do not predict any weights. If $n = 3$, we also predict any extra weights attached to these predicted weights. The difference between this prediction for the weights of ρ and the prediction of [ADP02] is the main point of the paper.

2.5 Statement and consequences of the conjecture

Conjecture 2.10. *Let $\rho : G_{\mathbb{Q}} \to GL_n(\bar{\mathbb{F}}_p)$ be a supersingular Galois representation such that the image of complex conjugation is similar to an upper triangular matrix with alternating 1's and -1's on the diagonal. Let N be the level of ρ and ϵ the nebentype. If V is any one of the weights predicted for ρ in Section 2.4, then ρ is attached to an eigenclass in*

$$H^*(\Gamma_0(N), V \otimes \epsilon).$$

Note that a supersingular representation is automatically irreducible. In addition, note that the condition on the image of complex conjugation is automatically satisfied if $p = 2$, or if $n = 2, 3$ and complex conjugation is a nonscalar matrix (in other words, if ρ is odd in the sense of [ADP02, pg. 522]). Finally, we note that for $n = 2$, if ρ is attached to any cohomology class in level N and coefficient module $V \otimes \epsilon$, then it is attached to one in $H^1(\Gamma_0(N), V \otimes \epsilon)$, and for $n = 3$, if ρ is attached to any cohomology class in level N and coefficient module $V \otimes \epsilon$, then it is attached to one in $H^3(\Gamma_0(N), V \otimes \epsilon)$ [AS00, pg. 6].

If $n = 3$, the computational evidence would support extending the conjecture to claim that only the predicted weights yield eigenclasses corresponding to ρ. In higher dimensions, however, it is not clear exactly what the analogue of the extra weights should be.

The following theorems follow from the conjecture, with proofs similar to Theorems 3.6 and 3.10 in [ADP02].

Theorem 2.11. *If Conjecture 2.10 is true for a representation $\rho : G_{\mathbb{Q}} \to GL_n(\bar{\mathbb{F}}_p)$, then it is true for $\rho \otimes \omega^s$, where ω is the cyclotomic character modulo p, and $s \in \mathbb{Z}$.*

Theorem 2.12. *If Conjecture 2.10 is true for a representation $\rho : G_{\mathbb{Q}} \to GL_n(\bar{\mathbb{F}}_p)$, then it is true for the contragredient representation ρ^* given by composing ρ with the transpose-inverse automorphism of $GL_n(\bar{\mathbb{F}}_p)$.*

2.6 Comparison with original conjecture

The original conjecture (see [ADP02]) for supersingular representations predicted exactly the same level and nebentype for a given ρ, but had a different formula for the predicted weights. The original prediction involved writing m as

$$m = a_{n-1} + a_{n-2}p + \ldots + a_0 p^{n-1}$$

with $0 \leq a_i - a_0 \leq p-1$ for all i. We then sort and rename the a_i as $b_{n-1}, \ldots, b_0$, with $b_i \geq b_{i-1}$. The conjecture then predicts that some nonempty subset of $F(b_{n-1} - (n-1), \ldots, b_0 - 0)'$ will yield a cohomology class corresponding to ρ.

Note first that the conditions on the a_i in the original conjecture are much more restrictive than those in the new conjecture. Hence, the new conjecture tends to predict more weights. For most three dimensional representations (in particular, when $m = a + bp + cp^2$, with $0 \leq a, b, c \leq p-1$, and no two of a, b, c equal or consecutive) it is easy to see that the original conjecture predicted three weights (plus possible extra weights), while the modified conjecture predicts nine weights (six directly, plus three extra weights). In addition, however, the original conjecture makes no restriction that $(b_{n-1} - (n-1), \ldots, b_0)$ be p-restricted, so occasionally, the original conjecture can predict a weight not predicted by the new conjecture. Nevertheless, in all the examples of three-dimensional Galois representations investigated so far, the weights predicted by the original conjecture are a proper subset of those predicted by the new conjecture. In particular, all the computational evidence available for the original conjecture also supports the strengthened conjecture.

2.7 Computational evidence for the conjecture

In order to provide computational evidence for the conjecture, we begin by finding three-dimensional supersingular Galois representations, and determining their level, nebentype, and predicted weights. We then compute the appropriate cohomology, and determine the action of the Hecke operators $T(\ell, k)$ for all $\ell < 50$. If we find a simultaneous eigenvector with the correct eigenvalues (for all $\ell < 50$) to correspond to ρ, then we claim to have evidence for the conjecture. We remark that for computations in characteristics two and three, we do not actually compute $H^3(\Gamma_0(N), V \otimes \epsilon)$, but rather a group which is closely related. We note that by Shapiro's Lemma, $H^3(\Gamma_0(N), V \otimes \epsilon) \cong H^3(\Gamma, W)$, where $\Gamma = \mathrm{SL}_3(\mathbb{Z})$, and $W = \mathrm{Ind}_{\Gamma_0(N)}^{\Gamma}(V \otimes \epsilon)$. Using the natural duality between homology and cohomology, this is then isomorphic to $H_3(\Gamma, W)$. We actually compute

$$H_3^{\dagger}(\Gamma, W) = H_3(\Delta, W)^{\Gamma}$$

for Δ a torsion free subgroup of finite index in Γ (note that the homology is independent of the choice of Δ). The group $H_3^{\dagger}(\Gamma, W)$ is isomorphic to $H_3(\Gamma, W)$ in characteristics not equal to 2 and 3. For further details of the techniques used for our cohomology computations, see [ADP02] and [AAC98].

In order to reduce the number of computations that are needed to obtain evidence for the conjecture, we also make use of the fact that if a system of eigenvalues corresponding to a representation ρ shows up in cohomology in weight V, then the eigenvalues corresponding to the contragredient ρ^* will show up in the dual weight $V^* \otimes \det^{-(n-1)}$ [AS00, Prop. 2.8]. Hence, we only need to compute the cohomology in one of V and V^* to determine the eigenvalues appearing in both of them. This reduces the computations needed by a factor of about two.

In the computational examples which follow, all group theoretical and number field calculations were performed using either Magma [BCP97] or GP/PARI [The00].

3 Computational examples in characteristic two

In [APS04], surjective Galois representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_3(\mathbb{F}_2)$ are described, and computations are performed indicating that these representations are attached to Hecke eigenclasses. Three of these examples are supersingular. For each example, we obtain two contragredient representations, ρ and ρ^*. We see easily that one of ρ and ρ^* has $m = 1 \equiv 0 + 2p + p^2 \pmod 7$ with $p = 2$. This yields a prediction of $F(0,0,0)^{\dagger}$, so that the predicted weights include all the possible weights. The other representation has $m = 6 = 2 + 0p + p^2$, again yielding a predicted weight of $F(0,0,0)^{\dagger}$. Computations done in [APS04] showed that in each of the four possible weights, the correct eigenvalues appeared (for $\ell < 50$) to have both ρ and ρ^* attached to an eigenclass. These examples are entirely consistent with the extended conjecture.

Class	1	2	3	4	5	6
Order	1	2	3	4	7	7
χ_0	1	1	1	1	1	1
χ_1	3	-1	0	1	α	$\bar{\alpha}$
χ_2	3	-1	0	1	$\bar{\alpha}$	α
χ_3	6	2	0	0	-1	-1
χ_4	7	-1	1	-1	0	0
χ_5	8	0	-1	0	1	1

Table 1: Character Table of $\mathrm{PSL}_2(\mathbb{F}_7)$

4 Computational examples with small image

We now study three-dimensional Galois representations in characteristic 11 with image isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$. This group (the unique simple group of order 168) has two nonconjugate embeddings in $\mathrm{GL}_3(\bar{\mathbb{F}}_{11})$, as indicated by Table 1, where $\alpha, \bar{\alpha} = \frac{1\pm\sqrt{-7}}{2}$. Note that 11 is relatively prime to the order of $\mathrm{PSL}_2(\mathbb{F}_7)$, so that the standard complex character table corresponds to the modular character table.

Given a polynomial $f(x) \in \mathbb{Z}[x]$ with Galois group isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$, set $K/\mathbb{Q}$ to be a splitting field of $f(x)$, and define ρ by the composition

$$G_{\mathbb{Q}} \xrightarrow{\pi} \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\theta} \mathrm{GL}_3(\bar{\mathbb{F}}_{11})$$

where π is the canonical projection, and θ is one of the two inequivalent embeddings of $\mathrm{PSL}_2(\mathbb{F}_7)$ into $\mathrm{GL}_3(\bar{\mathbb{F}}_{11})$. We will choose θ from the two possibilities in order to give ρ certain desirable properties.

Suppose that in $K/\mathbb{Q}$, the primes lying over 11 in K have ramification index 7. Then, regardless of the choice of θ, the image under ρ of the inertia group at 11 has order 7. The restriction of ρ to inertia at 11 is then diagonalizable, with diagonal characters $\psi_{3,1}^{190}$, $\psi_{3,2}^{190}$, $\psi_{3,3}^{190}$, or with diagonal characters $\psi_{3,1}^{570}$, $\psi_{3,2}^{570}$, $\psi_{3,3}^{570}$. We will choose θ so that the first of these cases holds. Using the description of the predicted weights in Conjecture 2.10, we see that since (modulo $11^3 - 1$)

$$\begin{aligned} 190 &= 3 + 6(11) + 1(11^2) \\ &= 14 + 5(11) + 1(11^2) \\ &\equiv 13 + 5(11) + 12(11^2) \\ &\equiv 12 + 5(11) + 23(11^2) \\ &\equiv 2 + 6(11) + 12(11^2) \\ &\equiv 2 + 17(11) + 11(11^2), \end{aligned}$$

we have predicted weights of

$$F(4,2,1), F(12,4,1), F(11,11,5), F(21,11,5), F(10,5,2), F(15,10,2).$$

In addition to these weights, we also obtain extra weights

$$F(11,5,1), F(14,11,2), F(20,12,5).$$

The conjecture predicts that each of these weights should yield eigenvalues corresponding to ρ. We now give two examples.

Example 4.1. [ADP02, Section 7.2] Let $f = x^7 - 11x^5 - 22x^4 + 33x^2 + 33x + 11$. This polynomial has Galois group $\mathrm{PSL}_2(\mathbb{F}_7)$, and in its splitting field, 11 has ramification index 7, as desired. Constructing ρ as above, we see [ADP02, Section 7.2], that ρ has level 31^2 and trivial nebentype. As in [ADP02], we set $\rho' = \rho \otimes \epsilon_{31}$, where ϵ_{31} is the quadratic character modulo 11 ramified only at 31. Then ρ' has level 31, nebentype ϵ_{31}, and the same restriction to inertia at 11 as ρ (since ϵ_{31} is not ramified at 11).

In [ADP02, Section 7.2], it was determined that eigenclasses with the correct eigenvalues (for $\ell < 50$) to correspond to ρ' existed in weights $F(4,2,1)$, $F(11,11,5)$, and $F(10,5,2)$ (which are the only weights predicted by the original conjecture of [ADP02]). Subsequent computations have shown that the same eigenvalues occur in each of the weights $F(12,4,1)$, $F(21,11,5)$, $F(15,10,2)$, $F(11,5,1)$, $F(14,11,2)$, and $F(20,12,5)$. Hence each of the weights predicted by the new conjecture works. In addition, computations in all other possible weights modulo 11 show that these are the only weights in which the correct eigenvalues appear. Hence, for this representation, the conjecture seems to be complete and correct.

Example 4.2. Let $f = x^7 - 11x^5 - 55x^3 - 264x^2 - 44x + 176$. The Galois group of f is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$. Let $K/\mathbb{Q}$ be a splitting field of f. Then in $K/\mathbb{Q}$, 11 has ramification index 7 and 103 has ramification index 2. Constructing ρ as above, we find that ρ has level 103^2 and trivial nebentype. Twisting by ϵ_{103}, the unique quadratic character modulo 11 ramified only at 103, we obtain $\rho' = \rho \otimes \epsilon_{103}$, which has level 103 and nebentype ϵ_{103}. As in example 4.1, ρ' has the same predicted weights as ρ. Because of the large level of this representation, we have been unable to do exhaustive computations in all weights; nevertheless, using the same techniques as in [ADP02, Section 7.2] we have been able to calculate the trace and cotrace of Frobenius elements under ρ', and confirm that the correct eigenvalues do occur (for $\ell < 50$) in weights $F(4,2,1)$, $F(12,4,1)$, $F(11,11,5)$, $F(10,5,2)$ and $F(11,5,1)$. In addition, we have computed the homology in all weights $F(a,b,c)$ with $a - c < 11$, and found that the correct eigenvalues to correspond to ρ' do not occur in any such weights except the predicted ones. In other words, in every predicted weight in which we are able to compute the cohomology, the correct eigenvalues occur, and in every other weight in which we can compute the cohomology, the correct eigenvalues do not occur.

We note that the two examples given here have very similar ramification structures. Glen Simpson [Sim04] has performed a series of targeted Hunter searches to find other examples of $\mathrm{PSL}_2(\mathbb{F}_7)$-extensions ramified at 11 with $e = 7$ and at one other prime q with $e = 2$. His search shows that there are no examples besides these two with $3 \leq q \leq 103$.

5 Computational examples coming from induced representations

We give several examples of three-dimensional representations induced from a ray class character of a non-Galois cubic field. The first of these examples was already described in detail in [ADP02], but we give more computational evidence for it. The other example is new.

5.1 General observations on induced representations

Let K be an S_3 extension of $\mathbb{Q}$ and let F be a cubic subfield of K. Define $\pi : G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q})$ to be the canonical projection. Suppose that p is an odd prime having inertial degree 3 in $K/\mathbb{Q}$, so that it is totally inert in $F/\mathbb{Q}$. Assume also that the class number of F is 1, and the ray class group of F modulo p is cyclic of order r with r dividing $(p^3 - 1)$, but not dividing $p^2 - 1$ or $p - 1$. There is then a ray class character modulo p

$$\chi : G_F \to \mathbb{F}_{p^3}$$

having order r. There are in fact $\varphi(r)$ such characters, χ^i where $1 \leq i \leq r$ and $(i, r) = 1$.

We will define

$$\rho_i : G_{\mathbb{Q}} \to \mathrm{GL}_3(\bar{\mathbb{F}}_3)$$

by

$$\rho_i = \mathrm{Ind}_{G_F}^{G_{\mathbb{Q}}} \chi^i,$$

for $1 \leq i \leq r$, and $(i, r) = 1$.

Theorem 5.1. *Let ψ be a power of χ as defined above, and let ρ be the representation induced from ψ, as above. Then ρ is an irreducible three-dimensional representation, with the following properties:*

1. *ρ is supersingular, and the image of $\rho|_{I_{p,0}}$ has order r,*
2. *If $K/\mathbb{Q}$ is ramified at a single odd prime q with ramification index 2, then the level of ρ is q and its nebentype is ϵ_q, the unique quadratic character modulo p ramified only at q,*
3. *If $g \in G_{\mathbb{Q}}$ with $\pi(g)$ having order 1, then $\rho(g)$ has eigenvalues $\psi(g_i^{-1} g g_i)$, where the g_i are coset representatives of G_F in $G_{\mathbb{Q}}$,*
4. *For $g \in G_{\mathbb{Q}}$ with $\pi(g)$ having order 2, some conjugate g' of g is in G_F, $Tr(\rho(g)) = \psi(g')$, and $T_2(\rho(g)) = \psi(g')^{-1} \det(\rho(g))$,*

5. For g in $G_{\mathbb{Q}}$ with $\pi(g)$ having order 3, $Tr(\rho(g)) = T_2(\rho(g)) = 0$.

Proof. Let ψ be the power of χ induced to obtain ρ, and let L/F be the field cut out by ψ. Then L/F is a cyclic extension of degree r, and is totally tamely ramified above p. Denote by M the Galois closure of $L/\mathbb{Q}$. M certainly contains K, and is in fact generated by the conjugates of KL over K, each of which is cyclic of order r. Hence, we see that $\mathrm{Gal}(M/K)$ is an abelian group of exponent r, and that it contains at least one element of order r (since the inertia group at p must be cyclic of order at least r). Now $\rho|_{G_F}$ contains ψ as an irreducible constituent, so that $G_F \cap \ker\rho$ is contained in $\ker\psi$. Hence, by normality, $\ker\rho$ fixes each conjugate of $L/\mathbb{Q}$, so that $\ker\rho$ fixes M. However, we see easily that ρ factors through $\mathrm{Gal}(M/\mathbb{Q})$, so that $\ker\rho = G_M$. This shows that the image of inertia at p under ρ is of order r (since inertia at p has image of order r in $\mathrm{Gal}(M/\mathbb{Q})$), and so we see that ρ is supersingular.

Let g_0, g_1, and g_2 be coset representatives of G_F in $G_{\mathbb{Q}}$. Define $\psi_0 : G_{\mathbb{Q}} \to \mathbb{F}_{p^3}$ by

$$\psi_0(g) = \begin{cases} \psi(g) & \text{if } g \in G_F, \\ 0 & \text{otherwise.} \end{cases}$$

Using the notation $g^{g_i} = g_i^{-1} g g_i$, we then have [FH91, pg. 34]

$$Tr(\rho(g)) = \sum_{i=0}^{2} \psi_0(g^{g_i}).$$

Suppose that $\pi(g)$ has order 1. Then $g \in G_K$, so g and all of its conjugates are in G_F. From the definition of an induced representation, and the fact that $g g_i = g_i(g_i^{-1} g g_i)$, we obtain the given eigenvalues for $\rho(g)$.

Suppose that $\pi(g)$ has order 2. Then exactly one of the conjugates of g fixes F. Call this conjugate g'. Neither of the two conjugates of g' by g_1 or g_2 are in G_F, so

$$Tr(\rho(g)) = Tr(\rho(g')) = \psi(g').$$

The value of $T_2(\rho(g))$ is then easily derived from the fact that $Tr(\rho(g^{-1})) = \psi(g')^{-1}$ and the identity $T_2(\rho(g)) = Tr(\rho(g^{-1}))\det(\rho(g))$.

Suppose that $\pi(g)$ has order 3. Then neither g nor either of its conjugates is contained in G_F. Hence, we see that $Tr(\rho(g)) = 0$. In addition, g^{-1} and its conjugates are also not contained in G_F. Since $0 = Tr(\rho(g^{-1})) = T_2(\rho(g))/\det(\rho(g))$, we see that $T_2(\rho(g)) = 0$.

If $K/\mathbb{Q}$ is ramified only at q, with ramification index 2, let $\mathfrak{q}$ be the unique prime of F unramified over q, and let τ be a generator of the tame inertia group at $\mathfrak{q}$. Then $\pi(\tau) = 2$ and $\psi(\tau) = 1$ (since the ray class character is unramified at $\mathfrak{q}$), so $Tr(\rho(\tau)) = 1$. Hence, the eigenvalues of $\rho(\tau)$ must be 1, 1, and -1, so that ρ has level q and nebentype ϵ_q. $\square$

5.2 Induced representations of level 59 modulo 7

As described in [ADP02, Section 7.1], let $f = x^3 - 2x + 1$ and let α be a root of f. Then $F = \mathbb{Q}(\alpha)$ has ray class group modulo 7 of order 9, hence we may choose a ray class character $\chi : G_F \to \mathbb{F}_{7^3}$ of order 9, and get six distinct ρ_i. These ρ_i each have level 59 with nebentype ϵ_{59} (the unique quadratic character modulo 7 ramified only at 59). As mentioned in [ADP02], three of these have $m = 38$ and three have $m = 76$. For the three with $m = 38$, we see that with $p = 7$,

$$\begin{aligned} 38 &= 3 + 5p + 0p^2 \\ &\equiv 2 + 5p + 7p^2 \pmod{7^3 - 1} \\ &\equiv 9 + 4p + 7p^2 \pmod{7^3 - 1} \\ &\equiv 2 + 12p + 6p^2 \pmod{7^3 - 1} \\ &\equiv 8 + 4p + 14p^2 \pmod{7^3 - 1} \\ &\equiv 10 + 4p + 0p^2 \pmod{7^3 - 1}. \end{aligned}$$

The predicted weights are then $F(3, 2, 0)$, $F(5, 4, 2)$, $F(7, 6, 4)$, $F(10, 5, 2)$, $F(12, 7, 4)$, $F(8, 3, 0)$, and the extra weights $F(7, 4, 0)$, $F(9, 6, 2)$, and $F(11, 8, 4)$. Computations show that in all these weights there are eigenclasses with the correct eigenvalues (for $\ell < 50$) to correspond to each of the ρ_i with $m = 38$. Similarly for each of the three representations with $m = 76$ (which are contragredients of those with $m = 38$), we may compute the predicted weights, and we find that each of the predicted weights yields an eigenclass with the desired eigenvalues (for $\ell < 50$). In addition, computations in all other weights modulo 7 prove that the correct eigenvalues do not appear except in those weights predicted by Conjecture 2.10. Note that the original conjecture of [ADP02] predicted only the first three of the nine weights predicted here.

5.3 Induced representations of level 431 modulo 3

Let $f = x^3 - x + 8$, set $F = \mathbb{Q}(\alpha)$, where α is a root of f, and let K be a splitting field of f containing α. Note that $K/\mathbb{Q}$ is an S_3-extension ramified only at 431, and that 431 has ramification index 2 in $K/\mathbb{Q}$. In addition, 3 has inertial degree 3 in $F/\mathbb{Q}$, and the ray class group mod 3 in F is cyclic of order 13. Then the ray class field L has degree 13 over F, and $\mathrm{Gal}(L/F)$ is cyclic of order 13. We obtain 12 distinct representations $\rho_1, \ldots, \rho_{12}$ by inducing characters of the ray class group. These characters will take the form χ^i for some ray class character χ, and $1 \le i \le 12$, and we denote by ρ_i the representation induced from χ^i. Each ρ_i is of *niveau* 3, with m even, and has level 431 and nebentype ϵ_{431}, the unique quadratic character modulo 3 ramified only at 431.

Note that squares of the fundamental characters $\psi_{3,i}$ mod 3 factor through $\mathrm{Gal}(L/F)$. We will identify the $\psi_{3,i}^2$ with the characters that they induce on $\mathrm{Gal}(L/F)$ and G_F, and we will choose χ to equal $\psi_{3,1}^2$. Then ρ_1, ρ_3, ρ_9 will

$m = 2$	$F(1,1,1), F(1,0,0), F(3,2,0), F(3,3,1), F(5,3,1), F(2,1,0)$
$m = 4$	$F(1,0,0), F(2,1,0), F(3,2,0), F(4,2,1)$
$m = 8$	$F(1,1,1), F(2,2,1), F(3,1,1), F(4,2,1), F(5,3,1), F(2,1,0)$
$m = 14$	$F(2,2,1), F(2,1,0), F(3,2,0), F(4,2,1)$

Table 2: Predicted weights for a three dimensional supersingular representation modulo 3.

all have $m = 2$; ρ_2, ρ_6, ρ_5 will have $m = 4$; $\rho_4, \rho_{12}, \rho_{10}$ will have $m = 8$; and $\rho_7, \rho_8, \rho_{11}$ will have $m = 14$.

We are easily able to compute the predicted weights for each value of m. We list these weights in Table 2. Note that the last entry in the $m = 2$ and $m = 8$ rows is an extra weight, rather than one predicted directly from the value of m. Note also that for $m = 4$, $F(4,2,1)$ is predicted, but $F(2,2,1)$ (which is in $F(4,2,1)'$ but not in $F(4,2,1)^{\dagger}$) is not predicted.

We will now determine the traces and cotraces of Frobenius elements under each ρ_i.

We begin by determining $\zeta = \chi(\mathrm{Frob}_{\mathfrak{q}}) = \psi_{3,1}^2(\mathrm{Frob}_{\mathfrak{q}})$, where $\mathfrak{q}$ is the unique degree one prime of F lying over 7. To do this, we use the Hilbert Symbol from class field theory [Neu99, Chapter V.3] with $n = 13$. Since F has class number 1, we may find a generator a of $\mathfrak{q}$, and we note that 3 generates the unique prime $\mathfrak{p}$ of F lying over 3. We denote the completion of F at $\mathfrak{p}$ by $F_{\mathfrak{p}}$, and the completion of L at the unique prime of L lying over $\mathfrak{p}$ by $L_{\mathfrak{p}}$. Note that $F_{\mathfrak{p}}$ contains μ_{13}, and that $L_{\mathfrak{p}} = F_{\mathfrak{p}}(3^{1/13})$. The Hilbert symbol satisfies the relation [Neu99, V.3.1]

$$\left(\frac{a,3}{\mathfrak{p}}\right) = \frac{\sigma_a(3^{1/13})}{3^{1/13}} = \psi_{3,1}^2(\sigma_a),$$

where σ_a is given by the local norm residue symbol $(a, L_{\mathfrak{p}}/F_{\mathfrak{p}})$. Then by [Neu99, V.3.4], we see that

$$\left(\frac{a,3}{\mathfrak{p}}\right) \equiv \left(\frac{1}{a}\right)^2 \pmod{\mathfrak{p}}.$$

Hence, in order to determine $\psi_{3,1}^2(\mathrm{Frob}_{\mathfrak{q}})$, we need only determine the relationship between $\mathrm{Frob}_{\mathfrak{q}}$ and $(a, L_{\mathfrak{p}}/F_{\mathfrak{p}})$. By [Neu99, pp. 406–407], we see that $\mathrm{Frob}_{\mathfrak{q}} = (a, L_{\mathfrak{q}}/F_{\mathfrak{q}})$, where $F_{\mathfrak{q}}$ is the completion of F at $\mathfrak{q}$, and $L_{\mathfrak{q}}$ is the completion of L at some prime lying over $\mathfrak{q}$. By [Neu99, Cor. VI.5.7], we see that for the principal idele (a),

$$1 = ((a), L/F) = \prod_{\mathfrak{s}} (a, L_{\mathfrak{s}}/F_{\mathfrak{s}}) = (a, L_{\mathfrak{q}}/F_{\mathfrak{q}})(a, L_{\mathfrak{p}}/F_{\mathfrak{p}}),$$

where the product runs over all primes $\mathfrak{s}$ of F, and $L_{\mathfrak{s}}$ is the completion of L at some prime over $\mathfrak{s}$. Note that most of the terms drop out, since, for $\mathfrak{s} \neq \mathfrak{p}, \mathfrak{q}$, we have that $L_{\mathfrak{s}}/F_{\mathfrak{s}}$ is unramified and a is a unit in $F_{\mathfrak{s}}$. We see immediately that

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$o(\pi(\mathrm{Frob}_p))$	1	*	3	2	3	2	2	3	3	3	2	2	1	2	2
$Tr(\rho_1(\mathrm{Frob}_p))$	α	*	0	ζ	0	ζ^9	ζ^8	0	0	0	ζ^{11}	ζ^7	γ	ζ^{12}	ζ^3
$T_2(\rho_1(\mathrm{Frob}_p))$	β	*	0	$-\zeta^{12}$	0	$-\zeta^4$	$-\zeta^5$	0	0	0	$-\zeta^2$	$-\zeta^6$	δ	$-\zeta$	$-\zeta^{10}$

Table 3: Traces and cotraces: $\alpha = \zeta^5+\zeta^{10}+\zeta^{11}$, $\beta = \zeta^2+\zeta^3+\zeta^8$, $\gamma = \zeta^6+\zeta^6+\zeta$, $\delta = \zeta^7 + \zeta^7 + \zeta^{12}$.

$(a, L_{\mathfrak{p}}/F_{\mathfrak{p}}) = \mathrm{Frob}_{\mathfrak{q}}^{-1}$, so that

$$\zeta = Tr(\rho_1(\mathrm{Frob}_{\mathfrak{q}})) = \chi(\mathrm{Frob}_{\mathfrak{q}}) = \psi_{3,1}^2(\mathrm{Frob}_{\mathfrak{q}}) \equiv a^2 \pmod{\mathfrak{p}}.$$

Using GP/PARI to do computations in F, we find that ζ is a root of the cubic polynomial $x^3 + 2x + 2$ over $\mathbb{F}_3$. Note that $Tr(\rho_3(\mathrm{Frob}_{\mathfrak{q}})) = \zeta^3$ and $Tr(\rho_9(\mathrm{Frob}_{\mathfrak{q}})) = \zeta^9$ are also roots of this same polynomial.

We now use the canonical isomorphism from $\mathrm{Gal}(L/F)$ to the ray class group which, for any prime $\mathfrak{r}$ of F not dividing (3), takes $\mathrm{Frob}_{\mathfrak{r}}$ to the class of $\mathfrak{r}$. Hence, we may determine the image of $\mathrm{Frob}_{\mathfrak{r}}$ in terms of the image of $\mathrm{Frob}_{\mathfrak{q}}$ by finding $\mathfrak{r}$ as a power of $\mathfrak{q}$ in the ray class group. This is easily done using GP/PARI's facilities for computation in ray class groups (or we could do calculations using the Hilbert symbol, as above).

We find that the primes $\ell \in \{7, 13, 17, 31, 37, 43, 47\}$ each have inertial degree 2 in $K/\mathbb{Q}$. Hence, each has a unique degree one prime lying over it in F, which we will denote by $\mathfrak{q}_\ell$. We have then defined $\zeta = \chi(\mathrm{Frob}_{\mathfrak{q}_7})$. Using the `bnrisprincipal` command in GP/PARI, we find that $\chi(\mathrm{Frob}_{\mathfrak{q}_{13}}) = \zeta^9$, since $\mathfrak{q}_{13}$ is a ninth power of $\mathfrak{q}_7$ in the ray class group. Similarly, $\chi(\mathrm{Frob}_{\mathfrak{q}_{17}}) = \zeta^8$, $\chi(\mathrm{Frob}_{\mathfrak{q}_{31}}) = \zeta^{11}$, $\chi(\mathrm{Frob}_{\mathfrak{q}_{37}}) = \zeta^7$, $\chi(\mathrm{Frob}_{\mathfrak{q}_{43}}) = \zeta^{12}$, and $\chi(\mathrm{Frob}_{\mathfrak{q}_{47}}) = \zeta^3$. Using the fact that the determinant of ρ_i is $\omega^{2i}\epsilon_{431} = \epsilon_{431}$, and that $\epsilon_{431}(\mathrm{Frob}_\ell) = -1$ for these primes, we may use Theorem 5.1 to compute the trace and cotrace of $\rho_1(\mathrm{Frob}_\ell)$ for each of these primes.

Note that the primes $\ell \in \{3, 5, 11, 19, 23, 29\}$ each have inertial degree of order 3 in $K/\mathbb{Q}$. We see immediately by Theorem 5.1 that for all i, the trace and cotrace of $\rho_i(\mathrm{Frob}_\ell)$ for any of these primes are both 0.

The primes 2 and 41 each split completely in $K/\mathbb{Q}$. Hence, for $p = 2$ or $p = 41$, there are three primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ above p in F. The three conjugacy classes $\mathrm{Frob}_{\mathfrak{p}_i}$ are conjugate in $G_{\mathbb{Q}}$, but not in G_F. Hence using the coset representatives e, g_1, g_2 of G_F in $G_{\mathbb{Q}}$ as in Theorem 5.1, we may obtain the three character values $\chi(\mathrm{Frob}_{\mathfrak{p}_i})$, $\chi(\mathrm{Frob}_{\mathfrak{p}_i}^{g_1})$, and $\chi(\mathrm{Frob}_{\mathfrak{p}_i}^{g_2})$ by computing the classes of $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$ in the ray class group in terms of $\mathfrak{q}_7$. We find for $p = 2$ that these three character values are ζ^5, ζ^{10}, and ζ^{11}. Hence $Tr(\rho_1(\mathrm{Frob}_2)) = \zeta^5 + \zeta^{10} + \zeta^{11}$, and $T_2(\rho_1(\mathrm{Frob}_2)) = \zeta^2 + \zeta^3 + \zeta^8$. For $p = 41$, we find $Tr(\rho_1(\mathrm{Frob}_{41})) = \zeta^6 + \zeta^6 + \zeta$, and $T_2(\rho_1(\mathrm{Frob}_{41})) = \zeta^7 + \zeta^7 + \zeta^{12}$.

We summarize our computations for ρ_1 in Table 3. We note that we may read the traces and cotraces of Frobenius elements under ρ_i directly from Table 3 by replacing ζ by ζ^i.

We have done the homology calculations in level 431 with quadratic nebentype for all weights modulo 3. In each of the weights predicted for $m = 2$, we found three eigenclasses, conjugate over $\mathbb{F}_3$, with the correct eigenvalues (for $\ell < 50$) to correspond to ρ_1, ρ_3, and ρ_9. In all of the weights not predicted for $m = 2$, no such eigenclasses were found.

Similarly, in exactly the weights predicted for $m = 4$, we found eigenclasses corresponding to ρ_2, ρ_6, and ρ_5, in exactly the weights predicted for $m = 8$ we found eigenclasses corresponding to ρ_4, ρ_{12}, ρ_{10}, and in exactly the weights predicted for $m = 14$, we found eigenclasses corresponding to ρ_7, ρ_8, and ρ_{11}. These computations exactly match what we expect from Conjecture 2.10.

6 Acknowledgements

The author thanks BYU's Ira and Mary Lou Fulton Supercomputing Center for the generous allocation of resources that made the computations in this paper possible. He also thanks David Pollack and Avner Ash for their comments. Finally, he thanks the referee for suggesting the use of the Hilbert symbol in Section 5.3.

References

[AAC98] Gerald Allison, Avner Ash, and Eric Conrad. Galois representations, Hecke operators, and the mod-p cohomology of $\mathrm{GL}(3, \mathbf{Z})$ with twisted coefficients. *Experiment. Math.*, 7(4):361–390, 1998.

[ADP02] Avner Ash, Darrin Doud, and David Pollack. Galois representations with conjectural connections to arithmetic cohomology. *Duke Math. J.*, 112(3):521–579, 2002.

[APS04] Avner Ash, David Pollack, and Dayna Soares. $\mathrm{SL}_3(\mathbb{F}_2)$-extensions of $\mathbb{Q}$ and arithmetic cohomology modulo 2. *Experiment. Math.*, 13:297–307, 2004.

[AS86] Avner Ash and Glenn Stevens. Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues. *J. Reine Angew. Math.*, 365:192–220, 1986.

[AS00] Avner Ash and Warren Sinnott. An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod p cohomology of $\mathrm{GL}(n,\mathbb{Z})$. *Duke Math. J.*, 105(1):1–24, 2000.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The MAGMA algebra system, I: The user language. *J. Symb. Comp.*, 24:235–265, 1997.

[DW92] Stephen R. Doty and Grant Walker. The composition factors of $F_p[x_1, x_2, x_3]$ as a $\mathrm{GL}(3,p)$-module. *Journal of Algebra*, 147:411–441, 1992.

[FH91] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.

[Gre80] James A. Green. *Polynomial representations of* GL_n, volume 830 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1980.

[Her06] Florian Herzig. *The weight in a Serre-type conjecture for tame n-dimensional Galois representations*. PhD thesis, Harvard University, 2006.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser87] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[Sim04] Glen Simpson. PSL(2,7)-extensions of $\mathbb{Q}$ with certain ramification at two primes. Master's thesis, Brigham Young University, 2004.

[The00] The PARI-Group, Bordeaux. *PARI/GP, Version 2.1.5*, 2000. available from `http://www.parigp-home.de`.