ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 38, Number 3, 2008

DISTINGUISHING CONTRAGREDIENT GALOIS REPRESENTATIONS IN CHARACTERISTIC TWO

DARRIN DOUD

ABSTRACT. Recently, Ash, Pollack and Soares described Galois representations with image isomorphic to $\mathrm{GL}_3(\mathbf{F}_2)$, and computationally demonstrated a connection to arithmetic cohomology classes with predictable coefficient modules. In some cases, they did not distinguish between contragredient representations for which the predicted coefficient modules are different. In this paper, we distinguish between these representations, providing additional evidence for a conjecture relating Galois representations to cohomology.

1. Introduction. In [**3**], Ash and Sinnott describe a conjecture relating certain n-dimensional *niveau* one Galois representations to Hecke eigenclasses in certain arithmetic cohomology groups. Their conjecture also includes a method of determining the weight, level and nebentype of the arithmetic cohomology groups attached to a given representation. In [**1**] this conjecture is extended to apply to Galois representations of arbitrary *niveaux*. In [**2, 7**], the conjecture is refined slightly, to make more precise the prediction of which coefficient modules yield an appropriate Hecke eigenclass. All four papers give examples of Galois representations for which computational evidence for the conjecture is obtained.

In [**2**], Ash, Pollack and Soares refine the conjecture of [**1**] in characteristic two, give examples of Galois representations in characteristic two and computationally test the refined conjecture for these representations. In characteristic two, the predictions of [**1, 3**] for the weight claim only that there exist weights that should yield eigenclasses corresponding to certain Galois representations, but do not specify these weights. For *niveau* one representations, both [**2, 7**] specify which weights should work. The *niveau* one examples in [**2**] all support the refined conjecture of [**7**]; however, for some of the examples, the authors

2000 AMS *Mathematics subject classification.* Primary 11F75,11F80.
Received by the editors on January 30, 2006.

DOI:10.1216/RMJ-2008-38-3-835

of [**2**] do not distinguish between a representation and its contragredient, so that the refined conjecture of [**7**] is only checked up to duality. In other words, in a set of weights which are predicted by [**7**] for one of ρ and its contragredient, the appropriate eigenvalues are found to correspond to one of ρ and its contragredient. The purpose of this paper is to distinguish between these representations and their contragredients, thus giving evidence for the refined conjecture of [**7**], based on certain examples of [**2**]. This evidence is important because these representations are the first known examples of wildly ramified representations for which the refined conjecture involves a mixture of two different types (*très ramifiée* and *peu ramifiée*) of wild ramification.

2. The conjecture. In characteristic two and *niveau* one, the conjecture relating Galois representations and arithmetic cohomology is particularly simple; we briefly review the necessary notation here and refer to [**1**] for a more detailed version of the full conjecture. We note that many of the definitions used here are specific to the case of characteristic two representations; for full descriptions in arbitrary characteristic, see [**1**].

2.1. Level. Let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_3(\overline{\mathbf{F}}_2)$ be a Galois representation. For each rational prime ℓ, fix an embedding $G_{\mathbf{Q}_\ell} \to G_{\mathbf{Q}}$ arising from an embedding of $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_\ell$. The images of the lower numbering ramification groups in $G_{\mathbf{Q}_\ell}$ then yield a filtration of ramification groups $G_{\ell,0} \supset G_{\ell,1} \supset \cdots$ in $G_{\mathbf{Q}}$. Define $g_i = |\rho(G_{\ell,i})|$, and let $M = \overline{\mathbf{F}}_2^3$ be acted on by $G_{\ell,i}$ via ρ. Set

$$n_\ell = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \dim M/M^{G_{\ell,i}}.$$

This sum is easily seen to be finite, since $\rho(G_{\ell,i})$ is trivial for large enough i.

Definition 2.1. The level of ρ is

$$N(\rho) = \prod_{\ell \neq 2} \ell^{n_\ell}.$$

Note that $n_\ell = 0$ for unramified primes, so that the product defining $N(\rho)$ has only finitely many nontrivial factors.

2.2. Weight. The weights associated to a Galois representation ρ as above will be a certain set of irreducible $\mathbf{F}_2[\mathrm{GL}_3(\mathbf{F}_2)]$-modules. There are exactly four of these modules, which we will denote by $F(0,0,0), F(1,0,0), F(1,1,0)$ and $F(2,1,0)$. (The notation reflects the parametrization of irreducible $\mathbf{F}_2[\mathrm{GL}_3(\mathbf{F}_2)]$-modules by 2-restricted 3-tuples described in [**6**].)

2.3. Attached eigenvectors. Let $\Gamma_0(N)$ be the subgroup of matrices in $\mathrm{SL}_3(\mathbf{Z})$ whose first row is congruent to $(*,0,0)$ modulo N. Define S_N to be the subsemigroup of integral matrices in $\mathrm{GL}_3(\mathbf{Q})$ satisfying the same congruence condition and having positive determinant relatively prime to N. Denote by $\mathcal{H}(N)$ the $\overline{\mathbf{F}}_2$-algebra of double cosets $\Gamma_0(N)\backslash S_N/\Gamma_0(N)$. Then $\mathcal{H}(N)$ is a commutative algebra that acts on the cohomology of $\Gamma_0(N)$ with coefficients in any $\overline{\mathbf{F}}_2[S_N]$-module. For $0 \le k \le 3$ and ℓ a prime not dividing N, let $D(\ell,k)$ be the diagonal matrix with 1 on the diagonal $3-k$ times, followed by ℓ on the diagonal k times, and write $T(\ell,k)$ for the double coset $\Gamma_0(N)D(\ell,k)\Gamma_0(N)$.

Definition 2.2. Let V be an $\mathcal{H}(2N)$-module, and suppose that $v \in V$ is a simultaneous eigenvector for all $T(\ell,k)$ with $\ell \nmid 2N$ and $0 \le k \le n$. Denote the eigenvalue of $T(\ell,k)$ by $a(\ell,k) \in \overline{\mathbf{F}}_2$, so that $T(\ell,k)v = a(\ell,k)v$. Let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_3(\overline{\mathbf{F}}_2)$ be a representation unramified outside $2N$, and assume that

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

for all ℓ not dividing $2N$. Then we say that ρ is *attached* to v or that v corresponds to ρ.

Remark 2.3. In our examples, we will take the module V to be a cohomology group $H^3(\Gamma_0(N), W)$, with W an irreducible $\mathrm{GL}_3(\mathbf{F}_2)$-module. Our experimental confirmation that a Galois representation is attached to an eigenvector will consist of computing all the $a(\ell,k)$

for $\ell < 50$, and checking that they match the eigenvalues expected of ρ. We make the following definition:

Definition 2.4. Let ρ be a three-dimensional irreducible Galois representation in characteristic 2 with level N. We will say that a coefficient module W *yields eigenvalues attached to* ρ if there is an element

$$v \in H^3(\Gamma_0(N), W)$$

such that ρ is attached to v as in Definition 2.2.

2.4. Predictions. A Galois representation over $\overline{\mathbf{F}}_p$ is *niveau* one if its restriction to inertia at p is upper triangularizable with powers of the cyclotomic character on the diagonal. Since the mod 2 cyclotomic character is trivial, a Galois representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_3(\mathbf{F}_2)$ will be *niveau* one exactly when the inertia group at 2 is a 2-group. In this case, we will be able to conjugate ρ so that

$$\rho : G_{2,0} \to \mathrm{GL}_3(\mathbf{F}_2)$$

has its image in the upper triangular matrices. We will assume that ρ is conjugated in this way and define maps $\psi_1, \psi_2 : G_{2,0} \to \mathbf{F}_2$ by

$$\rho(\sigma) = \begin{bmatrix} 1 & \psi_1(\sigma) & * \\ 0 & 1 & \psi_2(\sigma) \\ 0 & 0 & 1 \end{bmatrix} \quad \text{for } \sigma \in G_{2,0}.$$

Now, for $i = 1, 2$, we define $\rho_i : G_{2,0} \to \mathrm{GL}_2(\mathbf{F}_2)$ by

$$\rho_i = \begin{bmatrix} 1 & \psi_i \\ 0 & 1 \end{bmatrix}$$

and note that each ρ_i is a homomorphism. Each ρ_i can be either unramified, *très ramifiée*, or *peu ramifiée*, according to the definitions of Serre [**9**]. We then make the following conjecture (which is just the main conjecture of [**7**], in characteristic two):

Conjecture 2.5. *Let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_3(\mathbf{F}_2)$ be an irreducible niveau one Galois representation, with level $N(\rho)$. Define ρ_1 and ρ_2 as above. Then we make the following predictions*:

(1) *if neither* ρ_1 *nor* ρ_2 *is très ramifiée, then we predict that all four weights will yield eigenvalues attached to* ρ.

(2) *if only* ρ_1 *is très ramifiée, then we predict that* $F(1,0,0)$ *and* $F(2,1,0)$ *will yield eigenvalues attached to* ρ.

(3) *if only* ρ_2 *is très ramifiée, then we predict that* $F(1,1,0)$ *and* $F(2,1,0)$ *will yield eigenvalues attached to* ρ,

(4) *if both* ρ_1 *and* ρ_2 *are très ramifiée, then we predict that* $F(2,1,0)$ *will yield eigenvalues attached to* ρ.

Finally, we predict that any weight not predicted by the above for some conjugate of ρ *will not yield eigenvalues attached to* ρ.

Note that if there are several ways to conjugate ρ so that inertia has image in the upper triangular matrices, we may need to combine several of the cases described in the theorem. This situation does not occur in any of the examples found in [**2**]. Note also that, in certain cases, the predictions of [**2**] will differ slightly from those given above (for instance, the case where the image of inertia has order two, and the corresponding quadratic extension is *très ramifiée*). Unfortunately, we have no computational examples of representations for which the predicted weights differ.

Examples of cases (1) and (4) appear in [**2**] and will not be discussed further here. In [**2**], cases (2) and (3) are not distinguished. Instead, it is noted that if ρ falls into case (2), then the contragredient ρ^* of ρ (given by composing ρ with the outer automorphism of $\mathrm{GL}_3(\mathbf{F}_2)$ taking a matrix to its transpose-inverse) falls into case (3). Hence, in their examples, the authors of [**2**] look for eigenvalues of either ρ or ρ^*, making no distinction between the two. The main goal of this paper is to distinguish between these two representations and demonstrate that the weights predicted by Conjecture 2.5 for ρ and ρ^* yield eigenvalues (for $\ell < 50$) corresponding to ρ and ρ^*, respectively. Note that all four predictions for the weight in Conjecture 2.5 are specializations of a specific formulation for the weight in arbitrary characteristic [**7**].

3. $\mathrm{GL}_3(\mathbf{F}_2)$ as a permutation group. We begin by recording several facts about $\mathrm{GL}_3(\mathbf{F}_2)$ without proof. These facts are all either

well known, or can be verified quickly by using the MAGMA [**4**] computer algebra system.

Proposition 3.1. (1) $\mathrm{GL}_3(\mathbf{F}_2)$ *is a simple group of order* 168.

(2) *No proper subgroup of* $\mathrm{GL}_3(\mathbf{F}_2)$ *has order divisible by* 14.

(3) *Any subgroup of* $\mathrm{GL}_3(\mathbf{F}_2)$ *of order* 24 *is isomorphic to* S_4.

(4) $\mathrm{GL}_3(\mathbf{F}_2)$ *has two conjugacy classes of subgroups isomorphic to* S_4.

(5) $\mathrm{GL}_3(\mathbf{F}_2)$ *has a single conjugacy class of subgroups of order* 8.

(6) $\mathrm{GL}_3(\mathbf{F}_2)$ *has two inequivalent irreducible three-dimensional representations over* $\mathbf{F}_2$.

Now, by Proposition 3.1 (2), $\mathrm{GL}_3(\mathbf{F}_2)$ is generated by the matrices

$$s = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad t = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

of orders 7 and 2. Let

$$H = \left\{ \begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{bmatrix} \right\},$$

and note that H is isomorphic to S_4. Then the cosets of H in $\mathrm{GL}_3(\mathbf{F}_2)$ are $s^k H$ with $1 \leq k \leq 7$. Identifying each coset with the exponent of s occurring in this representation, it is clear that s acts on the cosets as the seven cycle $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$. One checks easily that t acts on the cosets as the permutation $\tau = (1\ 2)(3\ 6)$. This gives a surjective homomorphism $\phi : \mathrm{GL}_3(\mathbf{F}_2) \to G$, where G is the subgroup of S_7 generated by σ and τ, and since $\mathrm{GL}_3(\mathbf{F}_2)$ is simple, this homomorphism must be an isomorphism.

Finally, we remark that H stabilizes the coset $s^7 H = H$, and is, in fact, the full stabilizer of $s^7 H$ in $\mathrm{GL}_3(\mathbf{F}_2)$.

We will be interested in three important subgroups of H, namely

$$D = \left\{ \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \right\},$$

$$V_1 = \left\{ \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \right\},$$

and

$$V_2 = \left\{ \begin{bmatrix} 1 & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}.$$

Note that D is a dihedral group with 8 elements, each V_i is a Klein four group, and that $V_1 \triangleleft H$.

4. Number fields of interest. We are interested in the Galois representations in [**2**] for which the predicted weights were not fully determined. These Galois representations corresponded to $\mathrm{GL}_3(\mathbf{F}_2)$-extensions K of $\mathbf{Q}$ in which 2 has inertia group D_8 (the dihedral group of order 8). Each of these number fields K is defined as the Galois closure of a degree seven polynomial having Galois group $\mathrm{GL}_3(\mathbf{F}_2)$. In fact, by Proposition 3.1 (3) and 3.1 (4), such a number field has two distinct isomorphism classes of subfields of degree seven. These subfields give rise to the "twin" polynomials described in [**2**]. We will use defining polynomials for each of the two classes of subfields–in cases where [**2**] did not give the "twin" polynomial, we have calculated it using a resolvent computation. Hence, for each case (2) $\mathrm{GL}_3(\mathbf{F}_2)$-extension $K/\mathbf{Q}$ given in [**2**] we have two polynomials, f_1 and f_2, with nonisomorphic root fields, both of which have splitting field K over $\mathbf{Q}$. These polynomials are given in Table 1. Each such number field K corresponds to a pair of surjective Galois representations ρ and ρ^* from $G_{\mathbf{Q}}$ to $\mathrm{GL}_3(\mathbf{F}_2)$ having the same level; we have labeled each pair of polynomials by the level of the related Galois representations. Note that the choice of which polynomial is f_1 is arbitrary; we could have switched the roles of f_1 and f_2. This choice does, however, affect our choice of ρ in the next section: swapping f_1 and f_2 would have the effect of swapping ρ and its contragredient.

5. Explicit Galois representations. For each of the polynomials f_1 listed in Table 1, we have used MAGMA [**4**] to compute the Galois group of f_1 as a permutation group on the roots. For each example,

TABLE 1. Table of defining polynomials.

Level	Defining Polynomials
181	$f_1 = x^7 - 5x^6 + 20x^5 - 12x^4 - 48x^3 + 176x^2 - 192x + 64$
	$f_2 = x^7 + 3x^6 - 2x^5 - 6x^4 - 80x^3 + 208x^2 - 192x + 64$
239	$f_1 = x^7 - 3x^6 + 12x^4 - 15x^3 - 7x^2 + 24x - 8$
	$f_2 = x^7 - 4x^5 - 8x^4 + 13x^3 + 4x^2 - 10x - 4$
307	$f_1 = x^7 + 6x^6 + 8x^5 + 48x^4 - 48x^3 + 96x^2 - 384x + 256$
	$f_2 = x^7 + 18x^6 + 124x^5 + 568x^4 + 2176x^3 + 3328x^2 - 2560x + 1024$
389	$f_1 = x^7 - 12x^6 - 16x^5 + 384x^4 + 320x^3 - 5376x^2 + 9216x - 4096$
	$f_2 = x^7 - 36x^6 + 400x^5 - 1088x^4 - 4096x^3 + 81920x + 196608$
421	$f_1 = x^7 - 6x^6 + 17x^5 - 30x^4 + 24x^3 - 24x + 16$
	$f_2 = x^7 - 18x^6 + 142x^5 - 668x^4 + 2113x^3 - 4514x^2 + 5828x - 3368$
443	$f_1 = x^7 + 3x^6 - 20x^5 - 28x^4 + 108x^3 - 116x^2 + 64x - 16$
	$f_2 = x^7 + 9x^6 - 13x^5 - 333x^4 - 704x^3 + 2384x^2 + 10688x + 11072$

MAGMA returned the result that the Galois group was the subgroup of S_7 generated by the permutations

$$\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7) \quad \text{and} \quad \tau = (1\ 2)(3\ 6).$$

Of course this representation depends on the ordering of the roots. In Table 2 we give the ordering of the roots of f_1 used by MAGMA and denote the roots by $r_1, \ldots, r_7$ in the given order.

We are now able to explicitly construct the Galois representations that we will study. We have a canonical projection $\pi : G_{\mathbf{Q}} \to \mathrm{Gal}\,(f_1)$, and we have identified $\mathrm{Gal}\,(f_1)$ with the subgroup $G \subset S_7$ generated by σ and τ. We also have an isomorphism $\phi^{-1} : G \to \mathrm{GL}_3(\mathbf{F}_2)$. We define

$$\rho = \phi^{-1} \circ \pi : G_{\mathbf{Q}} \to \mathrm{GL}_3(\mathbf{F}_2).$$

We remark that by defining $F_1 = \mathbf{Q}(r_7) = K^{\phi(H)}$, we have that $\mathrm{Gal}\,(K/F_1) = \phi(H) \cong S_4$. Define $L = K^{\phi(D)}$ and $M_i = K^{\phi(V_i)}$. We see easily that M_1 is the Galois closure of L over F_1, and that $\mathrm{Gal}\,(M_1/F_1) \cong S_3$.

TABLE 2. Details of the computations, including an ordering of the roots of f_1, the predicted weight of ρ and the trace of $\rho(\mathrm{Frob}_\ell)$ for the smallest prime ℓ having inertial degree 7.

Level	approximate roots of f_1		predicted weight	ℓ	$\mathrm{Tr}\,(\rho(\mathrm{Fr}_\ell))$
181	$1.00+1.50i$,	$1.00-1.50i$,	$F(1,0,0)$	3	0
	$1.80+3.50i$,	0.900,			
	-2.10,	$1.80-3.50i$,			
	0.700				
239	$1.18+1.23i$,	$1.18-1.23i$,	$F(1,1,0)$	3	1
	$1.61-0.563i$,	0.413,			
	-1.55,	$1.61+0.563i$			
	-1.46				
307	$0.014+2.56i$,	$0.014-2.56i$,	$F(1,1,0)$	3	1
	$-0.936-2.23i$,	-6.25,			
	0.854,	$-0.936+2.23i$,			
	1.24				
389	$1.89+0.425i$,	$1.89-0.425i$,	$F(1,1,0)$	5	0
	$-4.40+1.99i$,	6.53,			
	9.75,	$-4.40-1.99i$			
	0.732				
421	$0.814+1.16i$,	$0.814-1.16i$,	$F(1,0,0)$	3	1
	$0.791-1.85i$,	2.74,			
	-0.823,	$0.791+1.85i$,			
	0.869				
443	$0.358+0.567i$,	$0.358-0.567i$,	$F(1,1,0)$	3	0
	$0.748-0.141i$,	3.35,			
	-3.91,	$0.749+0.141i$,			
	-4.65				

6. Ramification at 2 in $\mathrm{GL}_3(\mathbf{F}_2)$-extensions. For the extensions $K/\mathbf{Q}$ defined by polynomials in Table 1, Ash, Pollack and Soares [**2**] have shown that the decomposition and inertia groups at primes above 2 are isomorphic to D. Since $\mathrm{GL}_3(\mathbf{F}_2)$ contains only one conjugacy class of groups of order 8, we may choose a prime $\mathfrak{P}$ of K lying above 2 with decomposition and inertia groups equal to $\phi(D)$. Then $L = K^{\phi(D)}$ is the inertia field of $\mathfrak{P}|2$, and we will define $\mathfrak{p} = \mathfrak{P} \cap L$. Note that $\mathfrak{p}$ is a prime of L lying over 2, with inertial degree and ramification index 1. Hence, we may identify the completions $\mathbf{Q}_2$ and $L_\mathfrak{p}$. In particular, we

note that these completions have the same inertia group, which we can identify with $G_{2,0}$ in $G_{\mathbf{Q}}$.

Recall the definition of ρ_1 and ρ_2 from subsection 2.4. Examining $\rho_1 : G_{2,0} \to \mathrm{GL}_2(\mathbf{F}_2)$, we see that it is a composition of $\rho : G_{2,0} \to \mathrm{GL}_3(\mathbf{F}_2)$ with a map $\theta : D \to \mathrm{GL}_2(\mathbf{F}_2)$ having kernel V_1. Hence ρ_1 cuts out a quadratic extension of $L_{\mathfrak{p}}$ inside $K_{\mathfrak{P}}$; defining $\mathfrak{p}_1 = \mathfrak{P} \cap M_1$, we see that this quadratic extension is $(M_1)_{\mathfrak{p}_1}/L_{\mathfrak{p}}$. Hence, we may study the ramification of ρ_1 by studying the ramification of $\mathfrak{p}_1|\mathfrak{p}$. Similarly, letting $\mathfrak{p}_2 = \mathfrak{P} \cap M_2$, we may study the ramification of ρ_2 by studying the ramification of $\mathfrak{p}_2|\mathfrak{p}$. In order to study this ramification, we factor the polynomial f_2 over the field F_1.

Lemma 6.1. *Let f_1 and f_2 be defining polynomials for nonconjugate degree seven subfields F_1 and F_2 of $K/\mathbf{Q}$, where $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathrm{GL}_3(\mathbf{F}_2)$. Then, when considered as a polynomial in $F_1[x]$, f_2 factors into an irreducible cubic factor and an irreducible quartic factor.*

Proof. Note that the splitting field of f_2 over F_1 is the degree 24 extension K/F_1 and $\mathrm{Gal}(K/F_1) \cong S_4$. Hence, any irreducible factors of f_2 over F_1 have degree dividing 24. There can be no irreducible factors of degree 1, since F_2 and F_1 are nonconjugate fields, hence there can be no irreducible factors of degree 6. Therefore, the only possible degrees of irreducible factors are 2, 3 and 4. Since all the quadratic and cubic extensions of F_1 inside K are contained in a common S_3 extension of F_1, it cannot be the case that all of the degrees are less than 4. Hence, f_2 must factor as an irreducible cubic times an irreducible quartic polynomial. □

We will denote the cubic factor of f_2 over F_1 by f_3 and the quartic factor by f_4. Note that the splitting fields of f_3 and f_4 over F_1 are M_1 and K, respectively.

Let $\mathfrak{q} = \mathfrak{P} \cap F_1$, and note that M_1/F_1 is an S_3 extension, with three primes lying over $\mathfrak{q}$, each having ramification index 2 and inertial degree 1. We see that in L, the prime $\mathfrak{q}$ factors as $\mathfrak{p}\mathfrak{s}^2$. It is clear that the ramification of $\mathfrak{s}|\mathfrak{q}$ is of the same type as that of $\mathfrak{p}_1|\mathfrak{p}$. In addition, the polynomial f_3 factors in $(F_1)_{\mathfrak{q}}$ into a linear and a quadratic factor, corresponding to $\mathfrak{p}$ and $\mathfrak{s}$, respectively. We may

compute the ramification of $\mathfrak{s}|\mathfrak{q}$ by studying the quadratic factor: if the $\mathfrak{q}$-adic valuation of its discriminant is odd, then $\mathfrak{s}|\mathfrak{q}$ is *très ramifiée*, otherwise $\mathfrak{s}|\mathfrak{q}$ is *peu ramifiée*, [**7**].

Note that f_4 is $\mathfrak{q}$-adically irreducible, since a degree 4 extension of F_1 inside K must be totally ramified. Identifying $(F_1)_{\mathfrak{q}}$ with $\mathbf{Q}_2$, we see that the $\mathfrak{q}$-adic quadratic factor of f_3 is in fact the unique 2-adic quadratic factor of f_2. Hence, we may determine the ramification type of ρ_1 by determining the discriminant of the unique 2-adic quadratic factor of f_2. Ash, Pollack, and Soares have already shown that, for the extensions $K/\mathbf{Q}$ defined by polynomials in Table 1, the representations ρ_1 and ρ_2 have opposite ramification types. We have then proven the following theorem:

Theorem 6.2. *Given f_1 and f_2 as in Table* 1*, let ρ be the Galois representation defined in Section* 5*.*

(1) *If the* 2*-adic valuation of the discriminant of the quadratic* 2*-adic factor of f_2 is odd, then ρ satisfies case* (2) *of Conjecture* 2.5*, and the predicted weights for ρ are $F(1,0,0)$ and $F(2,1,0)$.*

(2) *If the* 2*-adic valuation of the discriminant of the quadratic* 2*-adic factor of f_2 is even, then ρ satisfies case* (3) *of Conjecture* 2.5*, and the predicted weights for ρ are $F(1,1,0)$ and $F(2,1,0)$.*

For each of the examples in which we are interested, we have 2-adically factored f_2 (using GP/PARI [**10**]) and determined which of $F(1,0,0)$ and $F(1,1,0)$ is predicted for ρ. This determination is indicated in Table 2.

7. Computing Frobenius elements. A simple exercise using the rational canonical form shows that $\mathrm{GL}_3(\mathbf{F}_2)$ has two distinct conjugacy classes of elements of order 7; one consists of elements of trace 1 and the other consists of elements of trace 0. For a rational prime ℓ with Frobenius of order seven in K, it will be necessary for us to determine which conjugacy class contains the Frobenius. We do this using a technique of Serre, mentioned by Buhler [**5**, page 53] and described in detail by Roberts [**8**].

Proposition 7.1. *Let $f_1 \in \mathbf{Z}[x]$ be a monic degree 7 polynomial with Galois group $\mathrm{GL}_3(\mathbf{F}_2)$, let $r_1, r_2, \ldots, r_7$ be the set of roots of f_1, considered in a specific order, and let $\sigma \in S_7$ be a permutation of the roots arising from an element of $\mathrm{Gal}(f_1)$. Suppose that σ has order 7. Let $\ell > 2$ be a rational prime such that the Frobenius of ℓ has order 7 in $\mathrm{Gal}(f_1)$ and $\ell \nmid \mathrm{disc}(f_1)$. Define*

$$D = D(\sigma) = \prod_{1 \le i < j \le 7} (\sigma^i(r_1) - \sigma^j(r_1)).$$

Then, since the Galois group is a subgroup of A_7, D is an integer with $D^2 = \mathrm{disc}(f)$. Let $\overline{D} \in \mathbf{F}_\ell$ be the reduction of D modulo ℓ.

We note that f_1 is irreducible mod ℓ*, and set*

$$d = \prod_{1 \le i < j \le 7} (x^{\ell^i} - x^{\ell^j})$$

in $\mathbf{F}_\ell[x]/(f_1)$. Then $d \in \mathbf{F}_\ell$, and $d = \overline{D}$ if and only if σ is a Frobenius at ℓ.

Proof. If σ is a Frobenius at ℓ, then for some prime $\mathfrak{P}$ of K lying over ℓ,

$$\sigma^i(\alpha) \equiv \alpha^{\ell^i} \pmod{\mathfrak{P}}$$

for all $\alpha \in K$. Hence, the reduction modulo $\mathfrak{P}$ of D is equal to d, and we see that $d \in \mathbf{F}_\ell$ and $\overline{D} = d$. If σ is not a Frobenius at p, then σ^3 is. One notes that $D(\sigma) = -D(\sigma^3)$, so that $D(\sigma)$ and $D(\sigma^3)$ are not congruent modulo ℓ. In particular, if σ is not a Frobenius at ℓ so that σ^3 is a Frobenius at ℓ, then $\overline{D} = -d \neq d$. □

For each of our examples, we have determined the primes ℓ which have Frobenius of order 7 in K, checked that they do not divide $\mathrm{disc}(f_1)$ and determined whether $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ is a Frobenius at ℓ, using the ordering of the roots of f given in Table 2. If σ is a Frobenius, then the trace of the image of the Frobenius under ρ is 1, otherwise the trace is 0. Note that the trace of the image of the Frobenius under ρ^* takes exactly the opposite values. For each extension, the smallest values of ℓ and the trace of the image of the Frobenius under ρ at this ℓ are given in Table 2.

Note that $\mathrm{GL}_3(\mathbf{F}_2)$ has only one conjugacy class of elements of a given order different than 7. For such conjugacy classes, the traces of ρ and ρ^* are equal. Hence, for primes ℓ with Frobenius of order different from 7, the trace of the image of the Frobenius is easy to compute and is the same for both ρ and ρ^*.

8. Cohomology computations. For each of the levels N in Table 1 and each of the four possible weights W, we have duplicated the computations of [**2**] in computing the arithmetic cohomology. We note that the programs that we use, which were developed for [**1**], compute $H^3(\Gamma_0(N), W)$ by computing the space $H_3(\Gamma_0(N), W)$ to which it is naturally dual. Also, in characteristic two the techniques we use actually compute the $\Gamma_0(N)$-invariants of $H_3(\Delta, W)$ for $\Delta \subset \Gamma_0(N)$ a subgroup of finite index in $\Gamma_0(N)$. For each weight we also computed the action of the Hecke operators for prime $2 < \ell < 50$. For each level, we found an eigenclass with the correct eigenvalues (for $\ell < 50$) to correspond to ρ exactly when W was one of the two weights predicted for ρ by Conjecture 2.5. In addition, we found an eigenclass with the correct eigenvalues (for $\ell < 50$) to correspond to ρ^* exactly when W was one of the two weights predicted for ρ^* by Conjecture 2.5.

For example, when $N = 181$, the predicted weights for ρ are $F(1,0,0)$ and $F(2,1,0)$ and the predicted weights for ρ^* are $F(1,1,0)$ and $F(2,1,0)$. Computations in the predicted weights for ρ yield eigenvalues (for $\ell < 50$) corresponding to ρ (in particular, for $\ell = 3$, $a(\ell, 1) = 0$). Computations in the two weights $F(0,0,0)$ and $F(1,0,0)$, on the other hand, do not yield eigenvalues corresponding to ρ. Similarly, we note that computations in weights $F(1,1,0)$ and $F(2,1,0)$ yield eigenvalues (for $\ell < 50$) corresponding to ρ^*, while computations in weights $F(0,0,0)$ and $F(1,0,0)$ do not. Note that although computing eigenvalues for only small ℓ would suffice to distinguish between ρ and ρ^*, we have duplicated the work of [**2**] in computing all eigenvalues for $\ell < 50$. Similar computations were done for all the levels in Table 2.

In all cases, our computational data fully supports the refined conjecture of [**7**]. This is the first such evidence involving Galois representations ρ for which ρ_1 and ρ_2 have different ramification types.

REFERENCES

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

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

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

4. Wieb Bosma, John Cannon and Catherine Playoust, *The MAGMA algebra system*, I: *The user language*, J. Symbolic Comp. **24** (1997), 235–265.

5. Joe Buhler, *Icosahedral Galois representations*, Lect. Notes Math. **654**, Springer-Verlag, Berlin, 1978.

6. 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*, J. Algebra **147** (1992), 411–441.

7. Darrin Doud, *Wildly ramified Galois representations and a generalization of a conjecture of Serre*, Experiment. Math. **14** (2005), 119–127.

8. David Roberts, *Frobenius classes in alternating groups*, Rocky Mountain J. Math. **34** (2004), 1–15.

9. Jean-Pierre Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}\,(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179–230.

10. 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
Email address: doud@math.byu.edu