Math. Res. Lett. **18** (2011), *no.* 01, 59–73

NEW PARTS OF HECKE RINGS

Benjamin Lundell and Ravi Ramakrishna

Abstract. In this note, we use the deformation theory of an absolutely irreducible Galois representation to study certain Hecke rings. Specifically, we investigate the variation in the rank of the new part of a completed Hecke ring as we vary the set of primes at which the deformations are allowed to ramify.

1. Introduction

Let $p \geq 5$ be a prime number. Consider the Galois representation

$$\bar{\rho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p), \text{ given by } \bar{\rho} = \begin{pmatrix} \bar{\chi} & 0 \\ 0 & 1 \end{pmatrix},$$

where $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is the absolute Galois group of the rationals and $\bar{\chi}$ is the mod p reduction of the p-adic cyclotomic character χ. Let

$$E_2(\tau) = 1 - 24\sum_{n=1}^{\infty} x^n \left(\sum_{d|n} d\right), \; x = e^{2\pi i \tau}$$

be the the weight two normalized non-holomorphic Eisenstein series. For any prime N, the weight two normalized Eisenstein series on $\Gamma_0(N)$, $E_{2,N} = E_2(\tau) - NE_2(N\tau)$, gives rise to a Galois representation lifting $\bar{\rho}$ which is unramified outside $\{N, p, \infty\}$. It is natural to ask when we can find such a lift of $\bar{\rho}$ which does not arise from an Eisenstein series.

When $N \equiv 1 \bmod p$, Mazur showed in [8] that there exists a weight two normalized cusp form f on $\Gamma_0(N)$, defined over $\bar{\mathbb{Q}}_p$, such that $\rho_f \equiv \bar{\rho} \bmod \mathfrak{p}$, where ρ_f is the Galois representation associated to f, and $\mathfrak{p}$ is the prime above p in the field of definition of f. That is, he showed that completion of the Hecke ring acting on the weight two cusp forms on $\Gamma_0(N)$ at the p-Eisenstein ideal, $\mathbb{T}_{\mathfrak{m}_{N,p}}$, has rank at least one as a $\mathbb{Z}_p$-algebra. This lead him to pose the question, "Is there anything general that can be said about [this rank]?" ([8], p. 140)

In [1], Calegari and Emerton approached this question by studying the deformation theory of the representation $\bar{\rho}$. They were able to prove an '$R = \mathbb{T}$' theorem and relate the rank of $\mathbb{T}_{\mathfrak{m}_{N,p}}$ to the p-part of the class group of $\mathbb{Q}(N^{1/p})$. See Theorem 1.2 and Corollary 1.6 of [1].

In this paper, we consider Mazur's question for *absolutely irreducible* representations. Let S be a finite set of places containing $\{p, \infty\}$ and G_S be the Galois

Received by the editors October 28, 2009.

2000 *Mathematics Subject Classification.* Primary: 11F80, 11F03.

Key words and phrases. Galois Representations, Deformation Theory, Modular Forms, Hecke Rings.

group over $\mathbb{Q}$ of the maximal algebraic extension of $\mathbb{Q}$ unramified outside S. Let $\bar{\rho} : G_S \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous, odd, absolutely irreducible representation that is weight two in the sense of [13]. Such a representation is necessarily modular by the work of Khare and Wintenberger on Serre's conjecture ([4], [5], [6]).

Like Calegari and Emerton, we obtain our results by studying the deformation theory of the representation $\bar{\rho}$. Let R_S be Mazur's weight two deformation ring associated to $\bar{\rho}$ and T any finite set of primes disjoint from S. Consider the weight two ring $R_{S\cup T}$ associated to the representation $G_{S\cup T} \twoheadrightarrow G_S \xrightarrow{\bar{\rho}} \mathrm{GL}_2(\mathbb{F}_p)$ which we also denote $\bar{\rho}$. Since in our setting deformation rings with suitable conditions at p are completed Hecke rings, we use the notation $\mathbb{T}$ for R.

Let $\mathrm{Ad}^0(\bar{\rho})$ be the 2×2 trace zero matrices over $\mathbb{F}_p$ with Galois acting via $\bar{\rho}$ and conjugation. In [11], it was proven that for a given $\bar{\rho}$ satisfying mild technical hypotheses, there exists a set of primes T such that $\mathbb{T}_{S\cup T}^{T-new} \simeq \mathbb{Z}_p$, where the superscript "$T-new$" indicates the quotient whose characteristic zero valued points correspond to cusp forms which are new at each of the primes in T. See Section 1 of [14] for the formulation of techniques used here. That $\mathbb{T}_{S\cup T}^{T-new} \simeq \mathbb{Z}_p$ is equivalent to the restriction map

$$H^1(G_{S\cup T}, \mathrm{Ad}^0(\bar{\rho})) \to \bigoplus_{v\in S\cup T} \frac{H^1(G_v, \mathrm{Ad}^0(\bar{\rho}))}{\mathcal{N}_v} \tag{1}$$

being an isomorphism. The subspace $\mathcal{N}_v$ of $H^1(G_v, \mathrm{Ad}^0(\bar{\rho}))$ arises from a surjection $R_v \twoheadrightarrow R_v^{sm}$, where R_v^{sm} is a suitable smooth quotient of the local deformation ring R_v associated to $\bar{\rho}|_{G_v}$. The kernel of an H^1 map as above is called a **Selmer group** and denoted $H^1_{\mathcal{N}}(G_{S\cup T}, \mathrm{Ad}^0(\bar{\rho}))$.

Throughout the remainder of the paper, we will make the following assumptions.

Hypothesis 1.

(1) $\bar{\rho} : G_S \to \mathrm{GL}_2(\mathbb{F}_p)$ is continuous, odd, weight two, and onto;
(2) $\dim H^1_{\mathcal{N}}(G_S, \mathrm{Ad}^0(\bar{\rho})) = 1$ (This is, $\mathbb{T}_S \simeq \mathbb{Z}_p[[X]]/A(X)$)); and
(3) $Ш^1_S(\mathrm{Ad}^0(\bar{\rho})) = 0$, where $Ш^1_S(\mathrm{Ad}^0(\bar{\rho}))$ denotes the kernel of the restriction map $H^1(G_S, \mathrm{Ad}^0(\bar{\rho})) \to \bigoplus_{v\in S} H^1(G_v, \mathrm{Ad}^0(\bar{\rho}))$.

Assumptions (2) and (3) are not too onerous. One can make a large Selmer group one dimensional following [11] and [14], while one can make a trivial Selmer group one dimensional following [2] or [12]. Assumption (3) can also be arranged by methods of [11] and [14]. All of these procedures involve adding primes to the ramification set.

Under the first assumption of this hypothesis, Lemma 1.2 of [14] constructs a Chebotarev set $\mathfrak{Q}$ (see Definition 2 below) such that, for any $q \in \mathfrak{Q}$, we have that $\mathbb{T}_{S\cup\{q\}}^{\{q\}-new} \simeq \mathbb{Z}_p$. It is worth noting that the results of [11] and [14] apply in far more general settings than Hypothesis 1. There, one starts with a representation satisfying only (1) (or not necessarily that: [11] also deals with even representations), and produces a finite set Q of primes such that $\mathbb{T}_{S\cup Q}^{Q-new} \simeq \mathbb{Z}_p$. The set Q has cardinality equal to $\dim H^1_{\mathcal{N}}(G_S, \mathrm{Ad}^0(\bar{\rho}))$. We will define a second set of Chebotarev set of primes $\mathfrak{L}$ (see Definition 15) and study the rank of $\mathbb{T}_{S\cup\{q,\ell\}}^{\{q,\ell\}-new}$ as ℓ varies for a fixed q.

For each $q \in \mathfrak{Q}$, let $\mathfrak{L}_q = \left\{\ell \in \mathfrak{L} : \mathrm{rank}_{\mathbb{Z}_p}\left(\mathbb{T}_{S\cup\{q,\ell\}}^{\{q,\ell\}-new}\right) > 1\right\}$. We obtain the following density results.

Theorem A. *There exists a finite set $\mathfrak{G} \subset \mathfrak{Q}$ of cardinality at most $p-1$ such that for any $q \in \mathfrak{Q}\backslash\mathfrak{G}$*

$$\overline{\text{dens}}(\mathfrak{L}_q) \geq \frac{p!\,\text{dens}(\mathfrak{L})}{p^{p+1}}.$$

Theorem B. *There is a subset $\mathfrak{E}$ of $\mathfrak{Q}$ of cardinality at most $\sqrt{2p}+1$ such that for any $q \in \mathfrak{Q}\backslash\mathfrak{E}$ we have*

$$\underline{\text{dens}}(\mathfrak{L}_q) \leq \frac{2\sqrt{p}\,\text{dens}(\mathfrak{L})}{p}.$$

Theorem C. *If every element of the algebra of sets formed by the $\mathfrak{L}_q$ has natural density, then there exists a finite set $\mathfrak{G} \subset \mathfrak{Q}$ such that for any $q \in \mathfrak{Q}\backslash\mathfrak{G}$*

$$\text{dens}(\mathfrak{L}_q) \leq \frac{(2-\frac{1}{p})\,\text{dens}(\mathfrak{L})}{p}.$$

As a reminder, we give two definitions.

Definition 1. For a set of primes $\mathfrak{F}$ set

$$\overline{\text{dens}}(\mathfrak{F}) = \limsup_{x\to\infty} \frac{\mathfrak{F}\cap[1,x]}{\pi(x)} \text{ and } \underline{\text{dens}}(\mathfrak{F}) = \liminf_{x\to\infty} \frac{\mathfrak{F}\cap[1,x]}{\pi(x)}$$

and

$$\text{dens}(\mathfrak{F}) = \lim_{x\to\infty} \frac{(\mathfrak{F})\cap[1,x]}{\pi(x)}$$

when the limit exists.

Definition 2. A Chebotarev set is, up to finitely many elements, a set of prime numbers defined by an application of the Chebotarev density theorem in some extension of number fields L/K.

Theorem 1.3 of [7] shows that Chebotarev sets have density as in Definition 1.

Remark. Given a nice prime ℓ, it is not hard to find a nice prime q such that $H^1_{\mathcal{N}}(G_{S\cup\{q\}}, \text{Ad}^0(\bar{\rho})) = 0$ and $\text{rank}_{\mathbb{Z}_p}(\mathbb{T}^{\{q,\ell\}-new}_{S\cup\{q,\ell\}}) > 1$ or not as we wish. See Propositions 11 and 19. In [12], examples of Hecke rings $\mathbb{T}^{T-new}_{S\cup T}$ with arbitrarily large rank were produced, but in these cases the set T was very large. We are interested in how the rank changes when we add two primes to the level.

It is natural to compare the Hecke rings $\mathbb{T}^{\{q\}-new}_{S\cup\{q,\ell\}}$ and $\mathbb{T}^{\{q\}-new}_{S\cup\{q\}}$ via the ring homomorphism $\pi^{(q)}_\ell : \mathbb{T}^{\{q\}-new}_{S\cup\{q,\ell\}} \to \mathbb{T}^{\{q\}-new}_{S\cup\{q\}}$. The η-invariant for this map, denoted $\eta^{(q)}_\ell$, is defined to be the ideal $\pi^{(q)}_\ell(\text{Ann}_{\mathbb{T}^{\{q\}-new}_{S\cup\{q,\ell\}}}(\text{Ker}(\pi^{(q)}_\ell)))$ of $\mathbb{T}^{\{q\}-new}_{S\cup\{q\}}$ and is a device for comparing these rings (the analog of the η-invariant for N in the reducible setting discussed above is $p^{v_p(\frac{N-1}{12})}$). It is known in our setting that there is a power series $P^{(q)}_\ell(X)$ such that $\mathbb{T}^{\{q,\ell\}-new}_{S\cup\{q,\ell\}} \simeq \mathbb{Z}_p[[X]]/(P^{(q)}_\ell(X))$. Wiles has shown in general that deformation rings are finite and flat over $\mathbb{Z}_p$, so there is a distinguished polynomial $f^{(q)}_\ell(X)$ and a unit $u^{(q)}_\ell(X) \in \mathbb{Z}_p[[X]]^*$ such that $P^{(q)}_\ell(X) = f^{(q)}_\ell(X)u^{(q)}_\ell(X)$. It is not hard to see that $f^{(q)}_\ell(0) = \eta^{(q)}_\ell$ as ideals of $\mathbb{Z}_p$. It seems that η-invariants only give information about whether or not $\mathbb{T}^{\{q,\ell\}-new}_{S\cup\{q,\ell\}}$ is trivial, not about its rank when it is nontrivial.

We conclude by noting that we naively expect that

$$\mathrm{dens}(\mathfrak{L}_q) = \frac{\mathrm{dens}(\mathfrak{L})}{p}.$$

Our heuristic is as follows: $\mathbb{T}_{S\cup\{q,\ell\}}^{\{q,\ell\}-new} \simeq \mathbb{Z}_p[[X]]/(P_\ell^{(q)}(X))$ where $P_\ell^{(q)}(X)$ is a power series with constant term $\eta_\ell^{(q)}$ divisible by p, but $P_\ell^{(q)}(X)$ is *not* divisible by p. Write $P_\ell^{(q)}(X) = \eta_\ell^{(q)} + a_{1,\ell}^{(q)}X + a_{2,\ell}^{(q)}X^2 + a_{3,\ell}^{(q)}X^3 + \ldots$, and assume that the $a_{i,\ell}^{(q)} \in \mathbb{Z}_p$ are random with respect to the normalized Haar measure on $\mathbb{Z}_p$. Then, the probability that $a_{r,\ell}^{(q)}$ is the first $a_{i,\ell}^{(q)}$ not divisible by p is

$$\left(\frac{1}{p}\right)^{r-1}\frac{p-1}{p} = \frac{p-1}{p^r}.$$

This suggests $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}_{S\cup\{l,q\}}^{\{l,q\}-new}) > 1$ with probability $\frac{1}{p}$. This, in combination with Theorems A and B, leads to the following questions.

Question. Let $\bar{\rho} : G_S \to \mathrm{GL}_2(\mathbb{F}_p)$ be continuous, odd, surjective, and weight two. Suppose that $\mathbb{T}_S \simeq \mathbb{Z}_p$, and let $\mathfrak{V}$ be the Chebotarev set of primes such that $\bar{\rho}$ is unramified at v, $v \not\equiv \pm 1 \bmod p$, and $\bar{\rho}(Frob_v)$ has eigenvalues with ratio v. Let $\tilde{\mathfrak{V}} \subseteq \mathfrak{V}$ be those v such that $\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{T}_{S\cup\{v\}}^{v-new}) > 1$. Is $\tilde{\mathfrak{V}}$ a Chebotarev set? If not, is it still the case that $\tilde{\mathfrak{V}}$ has density as in Definition 1? Finally, if the density exists, is $\mathrm{dens}(\tilde{\mathfrak{V}}) = \dfrac{\mathrm{dens}(\mathfrak{V})}{p}$?

2. Background

Definition 3. For a finite place v of $\mathbb{Q}$, let G_v denote $\mathrm{Gal}(\bar{\mathbb{Q}}_v/\mathbb{Q})$, $I_v \subset G_v$ the inertia subgroup, and Frob_v the Frobenius element which topologically generates G_v/I_v. For a G_v-module M, denote the image of the inflation map

$$H^1(G_v/I_v, M^{I_v}) \to H^1(G_v, M)$$

by $H^1_{nr}(G_v, M)$. Now, let M be a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module and $h \in H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), M)$. We call h **unramified** at a prime v if $h|_{G_v} \in H^1_{nr}(G_v, M)$, otherwise we call h **ramified** at v.

Definition 4. Let M be a Galois module annihilated by m. Set $M^* = \mathrm{Hom}(M, \mu_m)$.

Facts 5 and 6 below are standard.

Fact 5. *There is a canonical isomorphism*

$$\mathrm{inv}_v : H^2(G_v, \mu_m) \to \frac{1}{m}\mathbb{Z}/\mathbb{Z}.$$

Fact 6. *Let M be a G_v-module annihilated by m. In the perfect pairing of local duality,*

$$H^1(G_v, M) \times H^1(G_v, M^*) \to H^2(G_v, \mu_m) \overset{\mathrm{inv}_v}{\to} \frac{1}{m}\mathbb{Z}/\mathbb{Z},$$

the groups $H^1_{nr}(G_v, M)$ and $H^1_{nr}(G_v, M^*)$ are exact annihilators of one another.

In this paper m will always be the prime p and we will always identify $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$ with $\mathbb{Z}/p\mathbb{Z}$.

Definition 7. Suppose $\bar{\rho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is given as in Hypothesis 1, (1). A prime v is nice (for $\bar{\rho}$) if

- $v \not\equiv \pm 1 \bmod p$
- $\bar{\rho}$ is unramified at v,
- the eigenvalues of $\bar{\rho}(\mathrm{Frob}_v)$ have ratio v.

Fact 8. *For $\bar{\rho}$ as in Hypothesis 1, (1), the nice primes form a Chebotarev set. Moreover, v is nice for $\bar{\rho}$ if and only if $a_v := \mathrm{Tr}(\bar{\rho}(\mathrm{Frob}_v)) \equiv (v+1)^2 \bmod p$.*

Proof. That the nice primes form a Chebotarev set is Fact 5 of [2]. To see the second part, one can compute directly the congruence (remembering that $\det \bar{\rho}$ is the mod p cyclotomic character). □

Let $\mathbb{Z}/p\mathbb{Z}(r)$ be the group $\mathbb{Z}/p\mathbb{Z}$ with Galois action via χ^r, the r-th power of the mod p cyclotomic character. Since the eigenvalues of $\bar{\rho}(\mathrm{Frob}_v)$ have ratio v, the eigenvalues of Frob_v acting on $\mathrm{Ad}^0(\bar{\rho})$ are v, 1 and v^{-1} so there are G_v-module isomorphisms

$$\begin{aligned} \mathrm{Ad}^0(\bar{\rho}) &= \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \oplus \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} \\ &\simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}(1) \oplus \mathbb{Z}/p\mathbb{Z}(-1) \end{aligned}$$

and

$$\begin{aligned} \mathrm{Ad}^0(\bar{\rho})^* &= \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}^* \oplus \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}^* \oplus \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}^* \\ &\simeq \mathbb{Z}/p\mathbb{Z}(1) \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}(2). \end{aligned}$$

Since $v \not\equiv \pm 1 \bmod p$ the elements v, 1 and v^{-1} of $\mathbb{Z}/p\mathbb{Z}$ are distinct. Thus, in each of the above decompositions the three terms are distinct.

Fact 9. *Let v be nice for $\bar{\rho}$. Then we have*

1. $H^1(G_v, \mathbb{Z}/p\mathbb{Z}(r)) = 0$ *for* $r \neq 0, 1$,
2. $H^i(G_v, \mathrm{Ad}^0(\bar{\rho})) \simeq H^i(G_v, \mathbb{Z}/p\mathbb{Z}) \oplus H^i(G_v, \mathbb{Z}/p\mathbb{Z}(1)) \simeq H^i(G_v, \mathrm{Ad}^0(\bar{\rho})^*)$,
3. $H^i(G_v, \mathrm{Ad}^0(\bar{\rho}))$ *and* $H^i(G_v, \mathrm{Ad}^0(\bar{\rho})^*)$ *have dimensions* 1, 2, *and* 1 *for* $i = 0, 1, 2$, *respectively, and*
4. $H^1_{nr}(G_v, \mathrm{Ad}^0(\bar{\rho}))$ *and* $H^1_{nr}(G_v, \mathrm{Ad}^0(\bar{\rho})^*)$ *correspond to* $H^1(G_v, \mathbb{Z}/p\mathbb{Z})$ *in the decomposition in (2).*

Moreover, there is a surjection from R_v, the local deformation ring at v, to $\mathbb{Z}_p[[X]]$ that induces a one dimensional subspace

$$\mathcal{N}_v = H^1(G_v, \mathbb{Z}/p\mathbb{Z}(1)) \subset H^1(G_v, \mathrm{Ad}^0(\bar{\rho})),$$

which, under local duality, is annihilated by the one dimensional space

$$\mathcal{N}_v^{\perp} = H^1(G_v, \mathbb{Z}/p\mathbb{Z}(1)) \subset H^1(G_v, \mathrm{Ad}^0(\bar{\rho})^*).$$

Therefore, if either

$$f \in H^1_{nr}(G_v, \mathrm{Ad}^0(\bar{\rho})) \text{ and } \psi \in H^1(G_v, \mathrm{Ad}^0(\bar{\rho})^*) \backslash H^1_{nr}(G_v, \mathrm{Ad}^0(\bar{\rho})^*)$$

or

$$f \in H^1(G_v, \mathrm{Ad}^0(\bar{\rho})) \backslash H^1_{nr}(G_v, \mathrm{Ad}^0(\bar{\rho})) \text{ and } \psi \in H^1_{nr}(G_v, \mathrm{Ad}^0(\bar{\rho})^*)$$

with $f, \psi \neq 0$, then $\mathrm{inv}_v(f \cup \psi) \neq 0$.

Proof. See Section 3 of [10] or Lemma 2 of [2] for the decomposition of the local Galois cohomology groups. The statement about the non-vanishing of the invariants follows from Fact 6. □

Definition 10. Let $\Psi \in H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mathrm{Ad}^0(\bar{\rho})^*)$ and v be a nice prime such that $\Psi|_{G_v}$ is unramified. Consider

$$H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mathrm{Ad}^0(\bar{\rho})^*) \stackrel{\mathrm{res}}{\to} H^1(G_v, \mathrm{Ad}^0(\bar{\rho})^*) \to H^1(G_v, \mathbb{Z}/p\mathbb{Z})$$

where the first map is restriction and the second arises from the decomposition of the G_v-module $\mathrm{Ad}^0(\bar{\rho})$ in Fact 9. By $\Psi(\mathrm{Frob}_v)$, we mean the evaluation at Frobenius at v of the image of Ψ under the composition above.

Proposition 11. *Let $\Psi \in H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mathrm{Ad}^0(\bar{\rho})^*)$, and let $\mathfrak{V}$ be the (Chebotarev) set of nice primes. Then the set of $v \in \mathfrak{V}$ such that $\Psi(\mathrm{Frob}_v) = \alpha$, for $\alpha \in \mathbb{Z}/p\mathbb{Z}$, is a Chebotarev set having density $\dfrac{\mathrm{dens}\,\mathfrak{V}}{p}$.*

Proof. Recall from the discussion following Definition 7 that $\mathrm{Ad}^0(\bar{\rho})^* \simeq \mathbb{Z}/p\mathbb{Z}(1) \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}(2)$ as G_v modules. The factor with trivial action is dual to the matrices which are zero except of the upper right hand entry.

Let $K = \mathbb{Q}(\mathrm{Ad}^0(\bar{\rho}), \mu_p)$, so that $\Psi|_{\mathrm{Gal}(\bar{K}/K)}$ is a homomorphism. Then the field cut out by Ψ, L_Ψ, is a Galois extension of K with (abelian) Galois group $\mathrm{Ad}^0(\bar{\rho})^*$. By Definition 10, $\Psi(\mathrm{Frob}_v) = \alpha$ is equivalent to Frob_v corresponding to the dual of a matrix with α in the upper right hand entry. Such matrices account for $\dfrac{1}{p}$ of all possibilities. The result follows. □

Recall a proposition of Wiles.

Fact 12. *Let $T \supseteq S$ be a finite set of places. For $v \in T$ let $\mathcal{L}_v \subset H^1(G_v, \mathrm{Ad}^0(\bar{\rho}))$ be a subspace with annihilator $\mathcal{L}_v^\perp \subset H^1(G_v, \mathrm{Ad}^0(\bar{\rho})^*)$. Define $H^1_{\mathcal{L}}(G_T, \mathrm{Ad}^0(\bar{\rho}))$ and $H^1_{\mathcal{L}^\perp}(G_T, \mathrm{Ad}^0(\bar{\rho})^*)$ to be, respectively, the kernels of the restriction maps*

$$H^1(G_T, \mathrm{Ad}^0(\bar{\rho})) \to \bigoplus_{v \in T} \frac{H^1(G_v, \mathrm{Ad}^0(\bar{\rho}))}{\mathcal{L}_v}$$

and

$$H^1(G_T, \mathrm{Ad}^0(\bar{\rho})^*) \to \bigoplus_{v \in T} \frac{H^1(G_v, \mathrm{Ad}^0(\bar{\rho})^*)}{\mathcal{L}_v^\perp}.$$

Then

$$\begin{aligned} \dim H^1_{\mathcal{L}}(G_T, \mathrm{Ad}^0(\bar{\rho})) &- \dim H^1_{\mathcal{L}^\perp}(G_T, \mathrm{Ad}^0(\bar{\rho})^*) \\ &= \dim H^0(G_T, \mathrm{Ad}^0(\bar{\rho})) - \dim H^0(G_T, \mathrm{Ad}^0(\bar{\rho})^*) \\ &+ \sum_{v \in T} \big(\dim(\mathcal{L}_v) - \dim H^0(G_v, \mathrm{Ad}^0(\bar{\rho}))\big) \end{aligned} \tag{2}$$

Proof. See Proposition 1.6 of [15] or Theorem 8.6.20 of [9]. □

The above groups are called the **Selmer** and **dual Selmer groups** for the set T and local conditions $\mathcal{L}_v$ and $\mathcal{L}_v^\perp$ respectively. The formula shows the difference in dimension between the Selmer and dual Selmer groups for a set of places T and local conditions $\mathcal{L}_v$ and $\mathcal{L}_v^\perp$ can be readily computed.

Corollary 13. *Let v_0 be nice, and set $U = T \cup \{v_0\}$. Then*

$$\begin{aligned}\dim H^1_{\mathcal{L}}(G_U, \mathrm{Ad}^0(\bar\rho)) - \dim H^1_{\mathcal{L}}(G_T, \mathrm{Ad}^0(\bar\rho)) &= \dim H^1_{\mathcal{L}^\perp}(G_U, \mathrm{Ad}^0(\bar\rho)^*) \\ &\quad - \dim H^1_{\mathcal{L}^\perp}(G_T, \mathrm{Ad}^0(\bar\rho)^*) \\ &\quad + \dim(\mathcal{L}_{v_0}) - 1. \end{aligned} \tag{3}$$

Proof. This follows immediately from Facts 9 and 12. □

3. Results

In [11] and [14] local conditions are prescribed for all deformation problems. These correspond to smooth quotients of the local deformation rings. These quotients give rise to subspaces $\mathcal{N}_v \subseteq H^1(G_v, \mathrm{Ad}^0(\bar\rho))$ as described in Fact 9.

Fact 14. *Let T be a finite set of primes and $\mathcal{N}_v \subset H^1(G_v, \mathrm{Ad}^0(\bar\rho))$ be as in* [11] *and* [14]. *Then*

$$\dim H^1_{\mathcal{N}}(G_{S\cup T}, \mathrm{Ad}^0(\bar\rho)) = \dim H^1_{\mathcal{N}^\perp}(G_{S\cup T}, \mathrm{Ad}^0(\bar\rho)^*).$$

If the Selmer group and dual Selmer group are both trivial, then we have that

$$R^{T-new}_{S\cup T} = \mathbb{T}^{T-new}_{S\cup T} = \mathbb{Z}_p.$$

Proof. For $v \in S$, the subspaces $\mathcal{N}_v$ defined in [11] and [14], give

$$\dim H^1_{\mathcal{N}}(G_S, \mathrm{Ad}^0(\bar\rho)) = \dim H^1_{\mathcal{N}^\perp}(G_S, \mathrm{Ad}^0(\bar\rho)^*).$$

The first statement now follows from the definition for $\mathcal{N}_v$ for the nice prime v given in Fact 9 and the formula in Fact 12. The second statement is Lemma 1.1 of [14]. □

For most $\bar\rho$, one can, following [11] and [14], add a nice prime to S to make the Selmer group one dimension smaller. Following [2] one can also add a finite number of nice primes to S to make the Selmer group larger.

Recall from Hypothesis 1 that

$$\dim H^1_{\mathcal{N}}(G_S, \mathrm{Ad}^0(\bar\rho)) = 1 = \dim H^1_{\mathcal{N}^\perp}(G_S, \mathrm{Ad}^0(\bar\rho)^*).$$

Let f and ϕ span $H^1_{\mathcal{N}}(G_S, \mathrm{Ad}^0(\bar\rho))$ and $H^1_{\mathcal{N}^\perp}(G_S, \mathrm{Ad}^0(\bar\rho)^*)$ respectively.

Definition 15. Let $\mathfrak{Q}$ be set of nice primes q satisfying $f|_{G_q} \neq 0$, $\phi|_{G_q} \neq 0$. Let $\mathfrak{L}$ be the set of nice primes ℓ satisfying $f|_{G_\ell} \neq 0$ and $\psi|_{G_\ell} = 0$ for all $\psi \in H^1(G_S, \mathrm{Ad}^0(\bar\rho)^*)$.

Fact 16. *The sets $\mathfrak{Q}$ and $\mathfrak{L}$ are Chebotarev sets. For $q \in \mathfrak{Q}$ we have that*

$$H^1_{\mathcal{N}}(G_{S\cup\{q\}}, \mathrm{Ad}^0(\bar\rho)) = 0.$$

Proof. That $\mathfrak{Q}$ and $\mathfrak{L}$ are Chebotarev sets is Lemma 8 of [3]. The second part comes from the fact that the primes $q \in \mathfrak{Q}$ are chosen to annihilate the dual Selmer group, $H^1_{\mathcal{N}^\perp}(G_S, \mathrm{Ad}^0(\bar\rho)^*)$ (see Lemmas 1.1 and 1.2 of [14] and the discussion there). Applying Fact 14 gives the desired result. □

Proposition 17. *For any $\ell \in \mathfrak{L}$,*

$$\dim H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})) = 1 = \dim H^1_{\mathcal{N}^\perp}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*),$$

$H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$ is not spanned by f and $H^1_{\mathcal{N}^\perp}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*)$ is spanned by ϕ.

Proof. As $\phi|_{G_\ell} = 0$, we have that $\phi \in H^1_{\mathcal{N}^\perp}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*)$. In particular, we may conclude that $\dim H^1_{\mathcal{N}^\perp}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*) \geq 1$.

As f is a cohomology class for the group G_S, it is unramified at ℓ. Since $f|_{G_\ell} \neq 0$ (by definition of the set $\mathfrak{L}$), Fact 9 implies $f \notin H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$. Thus, any non-zero element of $H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$ is ramified at ℓ.

Let f_1 and f_2 be non-zero elements of $H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$. By Fact 9, there is a nontrivial linear combination of f_1 and f_2 which is unramified at ℓ. This linear combination is in $H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$ and therefore zero by the previous paragraph. Thus, f_1 and f_2 are linearly dependent, and $\dim H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})) \leq 1$. The proposition now follows from Fact 14. □

Proposition 18. *For any $\ell \in \mathfrak{L}$ the kernel of*

$$H^1(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})) \to \bigoplus_{v\in S} H^1(G_v, \mathrm{Ad}^0(\bar{\rho})) \tag{4}$$

is one dimensional. Moreover, for any nice prime v, the inflation map

$$H^1(G_S, \mathrm{Ad}^0(\bar{\rho})^*) \to H^1(G_{S\cup\{v\}}, \mathrm{Ad}^0(\bar{\rho})^*)$$

has one dimensional cokernel.

Proof. To prove the first statement, set

$$\mathcal{L}_r = 0,\ \mathcal{L}_r^\perp = H^1(G_r, \mathrm{Ad}^0(\bar{\rho})^*),\ \text{for } r \in S$$

and

$$\mathcal{L}_\ell = H^1(G_\ell, \mathrm{Ad}^0(\bar{\rho})),\ \mathcal{L}_\ell^\perp = 0,$$

so that

$$H^1_{\mathcal{L}^\perp}(G_S, \mathrm{Ad}^0(\bar{\rho})^*) = H^1(G_S, \mathrm{Ad}^0(\bar{\rho})^*).$$

As any $\psi \in H^1(G_S, \mathrm{Ad}^0(\bar{\rho})^*)$ satisfies $\psi|_{G_\ell} = 0$, we have that

$$H^1_{\mathcal{L}^\perp}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*) \supseteq H^1_{\mathcal{L}^\perp}(G_S, \mathrm{Ad}^0(\bar{\rho})^*),$$

and as $\mathcal{L}_\ell^\perp = 0$, all elements of $H^1_{\mathcal{L}^\perp}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*)$ are trivial (and therefore unramified) at ℓ, showing

$$H^1_{\mathcal{L}^\perp}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})^*) = H^1_{\mathcal{L}^\perp}(G_S, \mathrm{Ad}^0(\bar{\rho})^*).$$

Thus, Corollary 13 implies that

$$\dim H^1_{\mathcal{L}}(G_S, \mathrm{Ad}^0(\bar{\rho})) + 1 = \dim H^1_{\mathcal{L}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho})).$$

As $H^1_{\mathcal{L}}(G_S, \mathrm{Ad}^0(\bar{\rho})) = Ш^1_S(\mathrm{Ad}^0(\bar{\rho})) = 0$ by Hypothesis 1, the kernel of Equation (4) is $H^1_{\mathcal{L}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar{\rho}))$. The first part follows.

For the second part set $T = S \cup \{v\}$, and let

$$\mathcal{L}_r = 0,\ \mathcal{L}_r^\perp = H^1(G_v, \mathrm{Ad}^0(\bar{\rho})^*), \text{for } r \in T.$$

The Selmer groups for S and T are $Ш^1$s and the dual Selmer groups for S and T are the full H^1s. Then Corollary 13 gives

$$\dim(Ш^1_T(\mathrm{Ad}^0(\bar\rho))) - \dim(Ш^1_S(\mathrm{Ad}^0(\bar\rho))) = \dim(H^1(G_T, \mathrm{Ad}^0(\bar\rho)^*)) - \dim(H^1(G_S, \mathrm{Ad}^0(\bar\rho)^*)) - 1. \tag{5}$$

Hypothesis 1 guarantees that $Ш^1_S(\mathrm{Ad}^0(\bar\rho)) = 0$. Any element of $Ш^1_T(\mathrm{Ad}^0(\bar\rho))$ is trivial, and therefore unramified, at v, so $Ш^1_T(\mathrm{Ad}^0(\bar\rho)) \subseteq Ш^1_S(\mathrm{Ad}^0(\bar\rho)) = 0$. Thus, Equation (5) becomes

$$\dim(H^1(G_T, \mathrm{Ad}^0(\bar\rho)^*)) = \dim(H^1(G_S, \mathrm{Ad}^0(\bar\rho)^*)) + 1,$$

the desired result. □

The second part of Proposition 18 implies $H^1(G_{S\cup\{v\}}, \mathrm{Ad}^0(\bar\rho)^*)$ contains classes ramified at v, for all nice primes v. Fix $\Phi_v \in H^1(G_{S\cup\{v\}}, \mathrm{Ad}^0(\bar\rho)^*)$ ramified at v and normalized so that $\mathrm{inv}_v(f \cup \Phi_v) = 1$ (Recall invariants are normalized so they have values in $\mathbb{Z}/p\mathbb{Z}$). Note that f and any $\Psi \in H^1(G_S, \mathrm{Ad}^0(\bar\rho)^*)$ are unramified at v, so Fact 6 implies $\mathrm{inv}_v(f \cup \Psi) = 0$. Thus, though there is ambiguity in choosing Φ_v, the image of Φ_v in $H^1(G_{S\cup\{v\}}, \mathrm{Ad}^0(\bar\rho)^*)/H^1(G_S, \mathrm{Ad}^0(\bar\rho)^*)$ and $\mathrm{inv}_v(f \cup \Phi_v)$ are well-defined after this normalization.

The first part of Proposition 18 implies that the kernel of Equation (4) contains an element g_ℓ which is ramified at ℓ. By Proposition 17,

$$\dim H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar\rho)) = 1 \text{ and } f \notin H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar\rho)).$$

Let f_ℓ span $H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar\rho))$. As f_ℓ and g_ℓ are ramified at ℓ, we can argue as in the proof of Proposition 17. Fact 9 implies that some linear combination of f_ℓ and g_ℓ is unramified at ℓ. The coefficients of g_ℓ and f_ℓ in this linear combination are necessarily nonzero. As $f_\ell, g_\ell|_{G_v} \in \mathcal{N}_v$ for $v \in S$, this linear combination is locally in $\mathcal{N}_v$ for all $v \in S$ and so is in $H^1_{\mathcal{N}}(G_S, \mathrm{Ad}^0(\bar\rho))$; that is, it is a multiple of f. Thus, after suitably scaling f_ℓ, we have $f_\ell = a_\ell f + g_\ell$. Note that the coefficient a_ℓ is independent of the set $\mathfrak{Q}$.

Proposition 19. *Let $q \in \mathfrak{Q}$ and $l \in \mathfrak{L}$. Then, $H^1_{\mathcal{N}}(G_{S\cup\{q,\ell\}}, \mathrm{Ad}^0(\bar\rho)) \neq 0$ if and only if $\mathrm{inv}_q(f_\ell \cup \Phi_q) = 0$.*

Proof. Recall that f_ℓ spans $H^1_{\mathcal{N}}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar\rho))$ and ϕ spans $H^1_{\mathcal{N}^\perp}(G_{S\cup\{\ell\}}, \mathrm{Ad}^0(\bar\rho)^*)$. The definition of $\mathfrak{Q}$ requires $\phi|_{G_q} \neq 0$, so Fact 9 implies $\phi|_{G_q} \notin \mathcal{N}_q^\perp$. The proof of Lemma 1.2 of [14] implies

$$H^1_{\mathcal{N}}(G_{S\cup\{q,\ell\}}, \mathrm{Ad}^0(\bar\rho)) \neq 0 \iff f_\ell|_{G_q} \in \mathcal{N}_q.$$

As f_ℓ is unramified at q and $\mathcal{N}_q$ consists of ramified classes, we see

$$f_\ell|_{G_q} \in \mathcal{N}_q \iff f_\ell|_{G_q} = 0.$$

But, Φ_q is ramified at q by definition, so

$$f_\ell|_{G_q} = 0 \iff \mathrm{inv}_q(f_\ell \cup \Phi_q) = 0$$

by Fact 9. □

Proposition 20. *Let $q \in \mathfrak{Q}$ and $l \in \mathfrak{L}$. Then $\mathrm{inv}_q(f_\ell \cup \Phi_q) = a_\ell - \mathrm{inv}_\ell(g_\ell \cup \Phi_q)$.*

Proof. Global reciprocity implies

$$\begin{aligned} 0 &= \sum_{v \in S \cup \{q,\ell\}} \mathrm{inv}_v(g_\ell \cup \Phi_q) \\ &= \mathrm{inv}_\ell(g_\ell \cup \Phi_q) + \mathrm{inv}_q(g_\ell \cup \Phi_q), \end{aligned}$$

since $g_\ell|_{G_v} = 0$ for all $v \in S$. Thus, we have that

$$\begin{aligned} \mathrm{inv}_q(f_\ell \cup \Phi_q) &= \mathrm{inv}_q((a_\ell f + g_\ell) \cup \Phi_q) \\ &= a_\ell \,\mathrm{inv}_q(f \cup \Phi_q) + \mathrm{inv}_q(g_\ell \cup \Phi_q) \\ &= a_\ell - \mathrm{inv}_\ell(g_\ell \cup \Phi_q), \end{aligned}$$

since $\mathrm{inv}_q(f \cup \Phi_q) = 1$. □

Definition 21. Fix $q \in \mathfrak{Q}$, and set $\mathfrak{L}_{q,\alpha} = \{l \in \mathfrak{L} | \,\mathrm{inv}_q(f_\ell \cup \Phi_q) = \alpha\}$. Note that $\mathfrak{L}_{q,0}$ is the $\mathfrak{L}_q$ in Theorems A, B, and C.

Theorem A′. *Let $\alpha \in \mathbb{Z}/p\mathbb{Z}$. There exists a finite set $\mathfrak{G} \subset \mathfrak{Q}$ of cardinality at most $p-1$ such that for any $q \in \mathfrak{Q}\backslash\mathfrak{G}$*

$$\overline{\mathrm{dens}}(\mathfrak{L}_{q,\alpha}) \geq \frac{p!\,\mathrm{dens}(\mathfrak{L})}{p^{p+1}}.$$

Proof. Let $\epsilon > 0$, and suppose there are p elements $q_i \in \mathfrak{Q}$ such that

$$\overline{\mathrm{dens}}(\mathfrak{L}_{q_i,\alpha}) < \frac{(p! - \epsilon)\,\mathrm{dens}(\mathfrak{L})}{p^{p+1}}.$$

Let $\mathfrak{C} = \cap_{i=1}^{p} \mathfrak{L}^c_{q_i,\alpha}$, where $\mathfrak{L}^c_{q,\alpha}$ denotes the complement in $\mathfrak{L}$ of $\mathfrak{L}_{q,\alpha}$. We immediately see that

$$\begin{aligned} \underline{\mathrm{dens}}(\mathfrak{C}) &\geq \left(1 - p\frac{p! - \epsilon}{p^{p+1}}\right)\mathrm{dens}(\mathfrak{L}) \\ &= \left(1 - \frac{p! - \epsilon}{p^p}\right)\mathrm{dens}(\mathfrak{L}). \end{aligned}$$

Next, consider the set

$$\mathfrak{D} = \{\ell \in \mathfrak{L} | \Phi_{q_i}(\mathrm{Frob}_\ell) \neq \Phi_{q_j}(\mathrm{Frob}_\ell) \text{ for } 1 \leq i < j \leq p\}.$$

Using Proposition 11, it is an exercise to see $\mathfrak{D}$ is a Chebotarev set with density $\frac{p!}{p^p}\,\mathrm{dens}(\mathfrak{L})$.

As $1 - \frac{p! - \epsilon}{p^p} + \frac{p!}{p^p} > 1$, we must have $\mathfrak{C} \cap \mathfrak{D} \neq \emptyset$; let $\ell \in \mathfrak{C} \cap \mathfrak{D}$. In particular, we have that

$$\mathrm{inv}_{q_i}(f_\ell \cup \Phi_{q_i}) = a_\ell - \mathrm{inv}_\ell(g_\ell \cup \Phi_{q_i}) \neq \alpha \tag{6}$$

for $i = 1, 2, \ldots, p$, since $\ell \in \mathfrak{C}$.

Next, for ℓ fixed, $\mathrm{inv}_\ell(g_\ell \cup \Phi_{q_i})$ depends only on the value of Φ_{q_i} at Frob_ℓ, since

$$\mathrm{inv}_\ell(g_\ell \cup \Phi_{v_1}) - \mathrm{inv}_\ell(g_\ell \cup \Phi_{v_2}) = 0$$

if and only if $(\Phi_{v_1} - \Phi_{v_2})(\mathrm{Frob}_\ell) = 0$, for any nice primes v_1, v_2. Since $\ell \in \mathfrak{D}$ the values $\Phi_{q_i}(\mathrm{Frob}_\ell)$ for $i = 1, 2, \ldots, p$ are all distinct. Combining this with Equation 6 gives a contradiction. Thus,

$$\overline{\mathrm{dens}}(\mathfrak{L}_{q_i,\alpha}) \geq \frac{(p! - \epsilon)\,\mathrm{dens}(\mathfrak{L})}{p^{p+1}}$$

for all but $p-1$ elements $q \in \mathfrak{Q}$. Since ϵ is arbitrary, the result follows. □

Remark. If we take $\alpha = 0$ in the previous theorem, we recover Theorem A from the introduction.

Now that we have established that the sets $\mathfrak{L}_{q,\alpha}$ are infinite (after possibly discarding some finite number of q), we turn our attention to showing that these sets are not too large.

Proposition 22. *Let $\alpha \in \mathbb{Z}/p\mathbb{Z}$ and $q_1, q_2 \in \mathfrak{Q}$ be distinct. Then*

$$\overline{\mathrm{dens}}(\mathfrak{L}_{q_1,\alpha} \cap \mathfrak{L}_{q_2,\alpha}) \leq \frac{\mathrm{dens}(\mathfrak{L})}{p}.$$

Proof. Observe that

$$\begin{aligned}
\mathfrak{L}_{q_1,\alpha} \cap \mathfrak{L}_{q_2,\alpha} &= \{\ell \in \mathfrak{L} |\, \mathrm{inv}_{q_1}(f_\ell \cup \Phi_{q_1}) = \alpha = \mathrm{inv}_{q_2}(f_\ell \cup \Phi_{q_2})\} \\
&\subseteq \{\ell \in \mathfrak{L} |\, \mathrm{inv}_{q_1}(f_\ell \cup \Phi_{q_1}) - \mathrm{inv}_{q_2}(f_\ell \cup \Phi_{q_2}) = 0\} \\
&= \{\ell \in \mathfrak{L} |\, \mathrm{inv}_\ell(g_\ell \cup (\Phi_{q_2} - \Phi_{q_1})) = 0\}, \text{ by Proposition 20,} \\
&= \{\ell \in \mathfrak{L} | (\Phi_{q_2} - \Phi_{q_1})(\mathrm{Frob}_\ell) = 0\}.
\end{aligned}$$

By Proposition 11, the set of $\ell \in \mathfrak{L}$ satisfying $(\Phi_{q_2} - \Phi_{q_1})(\mathrm{Frob}_\ell) = 0$ is a Chebotarev set with density $\dfrac{\mathrm{dens}(\mathfrak{L})}{p}$. □

Remark. The moral of Proposition 22 is that while we do not know how to control $\mathfrak{L}_{q,\alpha}$ by a Chebotarev condition, we can control the 'difference' between $\mathfrak{L}_{q_i,\alpha}$ and $\mathfrak{L}_{q_j,\alpha}$. Moreover, suppose for some q_0 that $\mathrm{inv}_{q_0}(f_\ell \cup \Phi_{q_0}) = \alpha$ for all $\ell \in \mathfrak{L}$; that is, suppose that $\mathfrak{L} = \mathfrak{L}_{q_0,\alpha}$. Then, for any $q \in \mathfrak{Q}$, $q \neq q_0$, $\mathrm{inv}_q(f_\ell \cup \Phi_q) = \alpha$ if and only if $\mathrm{inv}_\ell(g_\ell \cup (\Phi_q - \Phi_{q_0})) = 0$, which happens on a set of density $\dfrac{1}{p}\,\mathrm{dens}(\mathfrak{L})$ by Proposition 11. Thus, the largest deviation from what we expect for q_0 implies the expected distribution for all other primes of $\mathfrak{Q}$.

Proposition 23. *Let X_i be sets of primes. Then,*

$$\overline{\mathrm{dens}}\left(\cup_{i=1}^M X_i\right) \geq \left(\sum_{i=1}^M \underline{\mathrm{dens}}(X_i)\right) - \sum_{1 \leq i < j \leq M} \overline{\mathrm{dens}}(X_i \cap X_j).$$

Proof. Let $\epsilon > 0$ be given. Set $b_i = \underline{\mathrm{dens}}(X_i)$ and $y = \overline{\mathrm{dens}}(\cup_{i=1}^M X_i)$. For large x,

$$\begin{aligned}
(y + \epsilon)\pi(x) &\geq \#\left(\left(\cup_{i=1}^M X_i\right) \cap [1, x]\right), \\
\#\left(X_i \cap [1, x]\right) &\geq (b_i - \epsilon)\pi(x), \text{ and} \\
(\overline{\mathrm{dens}}(X_i \cap X_j) + \epsilon)\pi(x) &\geq \#\left(X_i \cap X_j\right) \cap [1, x].
\end{aligned}$$

From inclusion-exclusion, we have for all x

$$\#\left(\left(\cup_{i=1}^{M} X_i\right) \cap [1,x]\right) \geq \left(\sum_{i=1}^{M} \#\left(X_i \cap [1,x]\right)\right) - \left(\sum_{1\leq i<j\leq M} \#\left((X_i \cap X_j) \cap [1,x]\right)\right),$$

so for large x

$$(y+\epsilon)\pi(x) \geq \left(\sum_{i=1}^{M}(b_i-\epsilon)\right)\pi(x) - \left(\sum_{1\leq i<j\leq M}(\overline{\text{dens}}\,(X_i\cap X_j)+\epsilon)\right)\pi(x),$$

and the result follows. □

Theorem B′. *Let $\alpha \in \mathbb{Z}/p\mathbb{Z}$. There are at most $\sqrt{2p}$ primes q_i such that $\underline{\text{dens}}(\mathfrak{L}_{q_i,\alpha}) \geq \frac{\sqrt{2p}\,\text{dens}(\mathfrak{L})}{p}$.*

Proof. Suppose there are $M \geq \sqrt{2p}+1$ such q_i, namely $q_1,\ldots,q_M$. Proposition 23 implies

$$\overline{\text{dens}}\left(\cup_{i=1}^{M}\mathfrak{L}_{q_i,\alpha}\right) \geq \left(\sum_{i=1}^{M}\frac{\sqrt{2p}\,\text{dens}(\mathfrak{L})}{p}\right) - \left(\sum_{1\leq i<j\leq M}\overline{\text{dens}}(\mathfrak{L}_{q_i,\alpha}\cap\mathfrak{L}_{q_j,\alpha})\right).$$

Proposition 22 and the fact that $\mathfrak{L}_{q_i,\alpha} \subseteq \mathfrak{L}$ imply

$$\text{dens}(\mathfrak{L}) \geq \overline{\text{dens}}\left(\cup_{i=1}^{M}\mathfrak{L}_{q_i,\alpha}\right) \geq \binom{M}{1}\frac{\sqrt{2p}\,\text{dens}(\mathfrak{L})}{p} - \binom{M}{2}\frac{\text{dens}(\mathfrak{L})}{p}. \tag{7}$$

The right hand side of Equation (7) is a quadratic in M that is maximized at $M = \sqrt{2p}+\frac{1}{2}$. At $M = \sqrt{2p}+\frac{1}{2}-\frac{1}{2} = \sqrt{2p}$, the inequality becomes $\text{dens}(\mathfrak{L}) \geq \left(1+\frac{1}{\sqrt{2p}}\right)\text{dens}(\mathfrak{L})$. This would lead to a contradiction if $\sqrt{2p}$ were an integer. As quadratics are symmetric about their extrema, we get the same inequality for $M = \sqrt{2p}+\frac{1}{2}+\frac{1}{2} = \sqrt{2p}+1$. Plugging the integer in the interval $[\sqrt{2p}, \sqrt{2p}+1]$ into Equation (7) gives a contradiction. □

Remark. If we take $\alpha = 0$ in the previous theorem, we recover Theorem B from the introduction.

It remains to prove Theorem C. We begin with a generalization of Proposition 22.

Proposition 24. *Let $\alpha \in \mathbb{Z}/p\mathbb{Z}$ and $q_1,\ldots,q_r \in \mathfrak{Q}$ be distinct. Then*

$$\overline{\text{dens}}(\cap_{i=1}^{r}\mathfrak{L}_{q_i,\alpha}) \leq \frac{\text{dens}(\mathfrak{L})}{p^{r-1}}.$$

Proof. The proof is similar to that of Proposition 22, except here

$$\cap_{i=1}^{r}\mathfrak{L}_{q_i,\alpha} \subseteq \{\ell \in \mathfrak{L} | (\Phi_{q_i}-\Phi_{q_1})(\text{Frob}_\ell) = 0,\ i = 2,\ldots,r\}.$$

The conditions $(\Phi_{q_i}-\Phi_{q_1})(\text{Frob}_\ell) = 0$ are independent Chebotarev conditions as the cohomology class $\Phi_{q_i}-\Phi_{q_1}$ is ramified at q_i. Thus, the set $\{\Phi_{q_2}-\Phi_{q_1},\ldots,\Phi_{q_r}-\Phi_{q_1}\}$

gives $r-1$ independent Chebotarev conditions by Lemma 8 of [3]. The result follows from Proposition 11. □

For the remainder of the paper we will assume:

Hypothesis 2. All subsets of $\mathfrak{L}$ in the algebra formed by the sets $\mathfrak{L}_{q,\alpha}$ have density.

Proposition 25. *Let $\alpha \in \mathbb{Z}/p\mathbb{Z}$ and $s > 0$. For each $1 \le t \le p^s$, let*

$$\mathfrak{D}_t = \mathfrak{L}_{q_1} \cap \cdots \cap \mathfrak{L}_{q_s},$$

where $\{q_1, \ldots, q_s\} \subset \mathfrak{Q}$ and no $\mathfrak{L}_q$ occurs in more than one intersection $\mathfrak{D}_t$. Fix $\epsilon \ge 0$ and suppose $\operatorname{dens}(\mathfrak{D}_t) \ge \dfrac{2+\epsilon}{p^s}\operatorname{dens}(\mathfrak{L})$ for all $1 \le t \le p^s$. Then for at least one pair (t,u),

$$\operatorname{dens}(\mathfrak{D}_t \cap \mathfrak{D}_u) \ge \frac{2+2\epsilon+\frac{2}{p^s}}{p^{2s}}\operatorname{dens}(\mathfrak{L}).$$

Proof. Suppose $\operatorname{dens}(\mathfrak{D}_t \cap \mathfrak{D}_u) < \dfrac{2+2\epsilon+\frac{2}{p^s}}{p^{2s}}\operatorname{dens}(\mathfrak{L})$ for all $1 \le t < u \le p^s$. Proposition 23 implies

$$\operatorname{dens}(\mathfrak{L}) \ge \operatorname{dens}(\cup_{j=1}^{p^s}\mathfrak{D}_j) \ge \left(\sum_{j=1}^{p^s}\operatorname{dens}(\mathfrak{D}_j)\right) - \left(\sum_{1\le t<u\le p^s}\operatorname{dens}(\mathfrak{D}_t\cap\mathfrak{D}_u)\right).$$

This becomes

$$\operatorname{dens}(\mathfrak{L}) > \binom{p^s}{1}\frac{2+\epsilon}{p^s}\operatorname{dens}(\mathfrak{L}) - \binom{p^s}{2}\frac{2+2\epsilon+\frac{2}{p^s}}{p^{2s}}\operatorname{dens}(\mathfrak{L}).$$

Simplifying,

$$\operatorname{dens}(\mathfrak{L}) > \left(1+\frac{1}{p^{2s}}+\frac{\epsilon}{p^s}\right)\operatorname{dens}(\mathfrak{L}),$$

a contradiction. □

Theorem C′. *Let $\alpha \in \mathbb{Z}/p\mathbb{Z}$. There are only finitely many $q \in \mathfrak{Q}$ with $\operatorname{dens}(\mathfrak{L}_{q,\alpha}) > \dfrac{(2-\frac{1}{p})\operatorname{dens}(\mathfrak{L})}{p}$.*

Proof. Suppose there are infinitely many such q_i. Let $\mathfrak{G} \subseteq \mathfrak{Q}$ be this exceptional set.

Let $\{q_1, \ldots, q_p\} \subset \mathfrak{G}$. We will show some that for some $1 \le i_0 < j_0 \le p$ that $\operatorname{dens}(\mathfrak{L}_{q_{i_0},\alpha} \cap \mathfrak{L}_{q_{j_0},\alpha}) \ge \dfrac{2}{p^2}\operatorname{dens}(\mathfrak{L})$. Suppose otherwise; that is, assume

$$\operatorname{dens}(\mathfrak{L}_{q_i,\alpha} \cap \mathfrak{L}_{q_j,\alpha}) < \frac{2}{p^2}\operatorname{dens}(\mathfrak{L}) \tag{8}$$

for all $1 \le i < j \le p$. Proposition 23 implies

$$\operatorname{dens}(\mathfrak{L}) \ge \operatorname{dens}(\cup_{i=1}^{p}\mathfrak{L}_{q_i,\alpha}) \ge \left(\sum_{i=1}^{p}\operatorname{dens}(\mathfrak{L}_{q_i,\alpha})\right) - \left(\sum_{1\le i<j\le p}\operatorname{dens}(\mathfrak{L}_{q_i,\alpha}\cap\mathfrak{L}_{q_j,\alpha})\right).$$

Using Equation 8 and simplifying, this becomes

$$\operatorname{dens}(\mathfrak{L}) > \binom{p}{1}\frac{\left(2-\frac{1}{p}\right)\operatorname{dens}(\mathfrak{L})}{p} - \binom{p}{2}\frac{2}{p^2}\operatorname{dens}(\mathfrak{L}) = \operatorname{dens}(\mathfrak{L}),$$

a contradiction. Thus, given p elements $q_1, \ldots, q_p$ of $\mathfrak{G}$ there are i_0, j_0 with $1 \leq i_0 < j_0 \leq p$ and $\operatorname{dens}(\mathfrak{L}_{q_i,\alpha} \cap \mathfrak{L}_{q_j,\alpha}) \geq \dfrac{2}{p^2}\operatorname{dens}(\mathfrak{L})$.

Using the hypothesis that $\mathfrak{G}$ is infinite and grouping $\mathfrak{G}$ into disjoint subsets of p elements, we get infinitely many 2-fold intersections with density at least $\dfrac{2}{p^2}\operatorname{dens}(\mathfrak{L})$ and no repeated q_i among the indices. Applying Proposition 25 with $s = 2$ and $\epsilon = 0$, we get infinitely many 4-fold intersections with density at least $\dfrac{2+\frac{2}{p^2}}{p^4}\operatorname{dens}(\mathfrak{L})$ and no repeated q_i among the indices.

Now repeatedly apply Proposition 25 starting with 4-fold intersections and $\epsilon_0 = \dfrac{2}{p^2}$. The key point is that the the 'discrepancy from 2' more than doubles in Proposition 25. For $m > 2$ there are infinitely many 2^m-fold intersections with density greater than $\dfrac{2+2^{m-2}\epsilon_0}{p^{2^m}}\operatorname{dens}(\mathfrak{L})$ and each $\mathfrak{L}_{q_i}$ occurring in at most one 2^m-fold intersection. Note for large enough m that $2 + 2^{m-2}\epsilon_0 > p$. Thus, there is a 2^m-fold intersection with density greater than $\dfrac{p}{p^{2^m}}\operatorname{dens}(\mathfrak{L})$. This contradicts Proposition 24.

The original supposition that the exceptional set $\mathfrak{G}$ is infinite is false. □

Remark. If we take $\alpha = 0$ in the previous theorem, we recover Theorem C from the introduction.

References

[1] F. Calegari and M. Emerton, *On the ramification of Hecke algebras at Eisenstein primes*, Invent. Math. **160** (2005), no. 1, 97–144.

[2] C. Khare, M. Larsen, and R. Ramakrishna, *Constructing semisimple p-adic Galois representations with prescribed properties*, Amer. J. Math. **127** (2005), no. 4, 709–734.

[3] C. Khare and R. Ramakrishna, *Finiteness of Selmer groups and deformation rings*, Invent. Math. **154** (2003), no. 1, 179–198.

[4] C. Khare and J.-P. Wintenberger, *On Serre's conjecture for 2-dimensional mod p representations of* $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, Ann. of Math. (2) **169** (2009), no. 1, 229–253.

[5] ———, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504.

[6] ———, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586.

[7] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem*, in Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), 409–464, Academic Press, London (1977).

[8] B. Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques de l'IHES **47** (1977) 33–186.

[9] J. Neukirch, A. Schmidt, and K. Wingberg, Cohomology of Number Fields, Springer, Berlin (2000).

[10] R. Ramakrishna, *Lifting Galois representations*, Invent. Math. **138** (1999), no. 3, 537–562.

[11] ———, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur*, Ann. of Math. (2) **156** (2002), no. 1, 115–154.

[12] ———, *Constructing Galois representations with very large image*, Canad. J. Math. **60** (2008), no. 1, 208–221.

[13] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* Gal($\overline{\mathbf{Q}}/\mathbf{Q}$), Duke Math. J. **54** (1987), no. 1, 179–230.
[14] R. Taylor, *On icosahedral Artin representations. II*, Amer. J. Math. **125** (2003), no. 3, 549–566.
[15] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

Department of Mathematics, Cornell University, Malott Hall, Ithaca, NY 14853.
E-mail address: blundell@math.cornell.edu

Department of Mathematics, Cornell University, Malott Hall, Ithaca, NY 14853.
E-mail address: ravi@math.cornell.edu