ON THE FROBENIUS FIELDS OF ABELIAN VARIETIES OVER NUMBER FIELDS

ASHAY A. BURUNGALE, HARUZO HIDA, AND SHILIN LAI

ABSTRACT. Let A be a non-CM simple abelian variety over a number field K. For a place v of K such that A has good reduction at v, let $F(A,v)$ denote the Frobenius field generated by the corresponding Frobenius eigenvalues. If A has connected monodromy groups, we show that the set of places v such that $F(A,v)$ is isomorphic to a fixed number field has upper Dirichlet density zero. Moreover, assuming the GRH, we give a power saving upper bound for the number of such places.

CONTENTS

1. INTRODUCTION

For an abelian variety over a number field and a place of good reduction, a basic invariant is the Frobenius field generated by the corresponding Frobenius eigenvalues. In this paper we study its connection with the arithmetic of the abelian variety.

For a CM abelian variety, in view of the CM theory of Shimura–Taniyama–Weil, the Frobenius fields are contained in a fixed number field and equal to it for a set of places of Dirichlet density one. A natural question: to explore the upper Dirichlet density of the set of places at which the Frobenius field of a non-CM abelian variety coincides with a given number field up to an isomorphism. The question has been studied in the literature in various low-dimensional cases, and the primary goal of this paper is to consider the general case via a uniform approach.

We show that the density is zero under a mild connected-ness hypothesis (see Theorem 1.1). Moreover, assuming the GRH, we provide a power saving upper bound on the size of the set of places with bounded norm at which the Frobenius field of a non-CM abelian variety coincides with a given number field.

Main results. Let K be a number field and Σ_K the set of its finite places. For $\overline{K}$ an algebraic closure, let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the corresponding absolute Galois group. For a place $v \in \Sigma_K$, let Frob_v be an associated geometric Frobenius.

Let A be an abelian variety defined over K of dimension d and conductor $\mathfrak{N}$. For a prime p, let T_pA be the p-adic Tate module of A and
$$\rho_{A,p} : G_K \to \mathrm{Aut}_{\mathbb{Z}_p} T_pA$$
the associated p-adic Galois representation. For $v \nmid p\mathfrak{N}$, it is unramified at v. Let $F(A,v)$ be the splitting field of the characteristic polynomial of $\rho_{A,p}(\mathrm{Frob}_v)$. As $(\rho_{A,p})_p$ is a compatible system of Galois representations, $F(A,v)$ is a number field independent of p, referred to as the Frobenius field associated to the pair (A,v).

Let M be a number field and $S_{A,M}$ a subset of finite places Σ_K of K given by

$$S_{A,M} = \{v \in \Sigma_K | v \nmid \mathfrak{N}, F(A,v) \cong M\}.$$

When A is a CM abelian variety, the Frobenius fields are a subfield[1] of the corresponding CM field (cf. [32]). Moreover, for a Dirichlet density one subset, the Frobenius fields equal a fixed subfield of the CM field.

In this paper, for non-CM abelian varieties A, we consider dependence of the Frobenius fields $F(A,v)$ on the place v. To state the results, we recall the following notion. For $S \subset \Sigma_K$, the upper Dirichlet density $\mathrm{ud}(S)$ is given by

$$\mathrm{ud}(S) = \limsup_{X \to \infty} \frac{\#\{v \in \Sigma_K : \mathbf{N}_{K/\mathbb{Q}} v \leq X, X \in S\}}{\#\{v \in \Sigma_K : \mathbf{N}_{K/\mathbb{Q}} v \leq X\}},$$

where $\mathbf{N}_{K/\mathbb{Q}}$ denotes the norm of the extension $K/\mathbb{Q}$.

Our first main result is the following.

Theorem 1.1. *Let A be an absolutely simple non-CM abelian variety defined over a number field K. Suppose that the monodromy groups associated to A over K are connected (cf. Hypothesis 2.2). Then for any number field M, we have*

$$\mathrm{ud}(S_{A,M}) = 0.$$

The connectivity Hypothesis 2.2 is satisfied by any abelian variety A over a finite extension of its field of definition (cf. Remark 2.3). Moreover, it is satisfied by a class of abelian varieties over their field of definition, for instance: most abelian varieties in a typical family (e.g. hyperelliptic Jacobians).

Remark 1.2. Theorem 1.1 gives a criterion for characterisation of CM/non-CM abelian varieties. For different criteria in the case of GL_2-type abelian varieties over $\mathbb{Q}$, the reader may refer to [13, §3.1.1].

In view of Theorem 1.1 it is natural to seek to estimate the size of subsets of $S_{A,M}$ with bounded norm. To state the result, we introduce some notation. Let $\mathbf{G}$ be the Mumford–Tate group associated to A. Let $\mathbf{G}^{\mathrm{ss}}$ be its semisimple quotient with dimension d, and let $r = \mathrm{rank}\,\mathbf{G}^{\mathrm{ss}}$ denote its absolute rank, namely the dimension of a maximal torus of $\mathbf{G}^{\mathrm{ss}}$. The quantitative result:

Theorem 1.3. *Let A be an absolutely simple non-CM abelian variety defined over a number field K. Suppose that the monodromy groups associated to A over K are connected (cf. Hypothesis 2.2), and that the generalized Riemann hypothesis (GRH) holds. Then for any $\varepsilon > 0$, there exists a constant c depending on (A, K, ε) such that for any number field M and $X \in \mathbb{R}_{>0}$, we have*

$$|\{v \in S_{A,M} \,|\, \mathbf{N}_{K/\mathbb{Q}} v \leq X\}| \leq cX^{1 - \frac{1}{3d-r+2} + \varepsilon}.$$

Corollary 1.4. *Suppose further that A is generic[2]. Then for any $\varepsilon > 0$, there exists a constant c depending on (A, K, ε) such that for any number field M and $X \in \mathbb{R}_{>0}$, we have*

$$|\{v \in \Sigma_K \,|\, \mathbf{N}_{K/\mathbb{Q}} v \leq X, v \text{ has Frobenius field } M\}| \leq cX^{1 - \frac{1}{6g^2 + 2g + 2} + \varepsilon}.$$

---

[1]More precisely, the Frobenius fields are a subfield of the CM endomorphism field K given by $\alpha^{\Phi'} \in K$ for some $\alpha \in K'$ for the reflex CM type (K', Φ').

[2]That is, the associated adelic Galois representation has open image in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$.

About the proof. Our approach is based on the compatible system of Galois representations associated to the abelian variety and some group theory. To begin, we recast the problem in terms of (a variant of) Frobenius tori in the algebraic monodromy group of the abelian variety. A volume computation of conjugacy classes arising from these tori and large Galois image results for A are keys of the proof.

We now describe the strategy in more detail. To begin, for primes p which split completely in M, we show that if $v \in S_{A,M}$, then the image of Frob_v in the associated mod p monodromy group lies in a $\mathbb{F}_p$-rational Borel subgroup. Then we give a volume upper bound for the union of all such subgroups (cf. Corollary 3.4), perhaps of independent interest. On the other hand, since A is non-CM, the associated Galois representations have large image, thanks to the work of Wintenberger [33] and Hui–Larsen [14] (cf. Theorem 2.5). In light of the image lower bound and the volume upper bound, the Chebotarev density theorem implies that $\mathrm{ud}(S_{A,M})$ is bounded above by a constant c less than 1, which is independent of the prime p. This deduction relies on basic properties of reductive groups, several of which require the group to be connected.

Next, we synthesise the analysis at different primes via the product Galois representation $\prod \rho_{A,p}$. Ideally, we expect

$$(1.1) \qquad \mathrm{Im}\left(\prod_p \rho_{A,p}\right) = \prod_p \mathrm{Im}(\rho_{A,p}),$$

which implies: for different choices of p, the events that $\rho_{A,p}(\mathrm{Frob}_v)$ lands in a $\mathbb{F}_p$-rational Borel subgroup are independent. Hence, Theorem 1.1 follows (recall that the density upper bound c is independent of p). Actually, Serre showed that the independence (1.1) holds upon replacing K with a finite extension (cf. Theorem 2.4(2)). This suffices for our argument.

As for Theorem 1.3, we quantify the above strategy with the aid of the effective Chebotarev theorem of Lagarias–Odlyzko and the Selberg sieve. Some notable features:

- Without the Mumford–Tate conjecture, the p-adic monodromy groups can be different[3] for each p. In order to control their sizes, we introduce a soft argument based on the Weil bound and the classification of reductive groups over algebraically closed fields (cf. the proof of Lemma 4.15).

- Since we are only sieving using primes which split completely in M, a lower bound on the number of such primes - independently of M - is necessary. This is achieved via a simple *a priori* upper bound on the discriminant of a Frobenius field $F(A, v)$ in terms of $\mathbf{N}_{K/\mathbb{Q}}v$ (cf. Lemma 4.18).

To refine exponents naturally appearing in the analysis, we make the following improvements:

- Instead of the p-adic monodromy group, we work with its semisimple quotient, reducing the sizes of the relevant Galois groups. This is a generalization of the PGL_2-reduction method used previously.

- Well-known results of Murty–Murty–Saradha give better error terms in the effective Chebotarev theorem when certain subgroups of the Galois group satisfy the Artin holomorphy conjecture (AHC) (cf. Theorem 4.8). In our case, the natural choice is a Borel subgroup of the monodromy group, and we make an elementary group-theoretic observation that it satisfies the AHC.

The prior work and prospects. Our study is inspired by the Lang–Trotter conjecture [20] and a consideration of Serre for Hecke eigenvalues of elliptic newforms [28, §7]. For elliptic curves, the result was first stated[4] by Serre [28, §8.2]. Its various explicit forms have appeared in the work of Cojocaru–Fouvry–Murty [8], Cojocaru–David [6], Zywina [34], and Kulkarni–Patankar–Rajan [17], among others. Cojocaru–David [7] consider the analogous question for Drinfeld modules.

For generic abelian varieties, Theorem 1.1 was first established by Bloom [1]. His method is different and does not seem amenable to quantitative refinements as in Theorem 1.3. As for general abelian varieties, the only known result seems to be that of Khare [16]: for a non-CM simple abelian variety, the set of places whose Frobenius fields equal a fixed number field cannot be the complement of a finite set of places.

---

[3]Recall that the Mumford–Tate conjecture is not known in general.

[4]albeit without proof or explicit exponent

Our result applies to any abelian variety up to a base change. In the generic case, no base change is needed, and it gives a better exponent than Bloom [1], assuming only the GRH. The qualitative part of the argument generalises to function fields, and we expect that a suitable modification yields the quantitative version. Moreover, our method seems to apply to any compatible system of Galois representations for which Frobenius semisimplicity holds (cf. Remark 2.6).

Compared to previous works, our approach is closer in spirit to the square sieve method, which first appeared in [8]. However, by working with abstract reductive groups, we replace all the work in estimating conjugacy class sizes with soft arguments, and we can identify power savings which are not apparent from the explicit matrix-based considerations. It would be interesting to see if our approach can be combined with the mixed Galois representation approach to obtain a further sharpening of Theorem 1.3.

Finally, to remove Hypothesis 2.2, we would need to study the structure of semisimple elements in a disconnected finite reductive group. We plan to return to this question in the near future.

Plan. In section 2 we describe preliminaries regarding Galois representations, monodromy groups, and large image theorems. In section 3 we present preliminaries regarding finite redcutive groups and introduce the key notion of a bounding set (cf. Definition 3.3). In section 4 we prove the main theorems.

Acknowledgments. We thank Brian Conrad, Chun-Yin Hui, Chandrashekhar Khare, Vijay Patankar, Will Sawin, and Victor Wang for helpful comments and suggestions.

2. BACKDROP

We describe some preliminaries regarding p-adic Galois representation associated to an abelian variety over a number field. The reader may refer to [14, 25, 33] for some details.

Let the setting be as in section 1. In particular, A is an abelian variety over a number field K of dimension g. Put $\Delta_A = \mathbf{N}_{K/\mathbb{Q}} \mathfrak{N}$, so A has good reduction away from places of K which lie above a prime dividing Δ_A.

2.1. **Galois representations.** For a prime p, let $T_p A$ be the p-adic Tate module of A. Let

$$\rho_p : G_K \to \mathrm{Aut}_{\mathbb{Z}_p} T_p A$$

be the associated p-adic Galois representation.

Theorem 2.1. *Let v be a finite place of K such that $v \nmid p\Delta_A$.*

(1) *(Serre–Tate) The Galois representation ρ_p is unramified at v.*

(2) *(Weil) The characteristic polynomial of $\rho_p(\mathrm{Frob}_v)$ has integral coefficients and is independent of p. Moreover, all of its roots have complex absolute value $(\mathbf{N}_{K/\mathbb{Q}} v)^{\frac{1}{2}}$.*

For a set T of primes, put

$$\rho^T = \prod_{p \notin T} \rho_p, \quad \rho_T = \prod_{p \in T} \rho_p.$$

For N a positive integer, put $\rho^N = \rho^{T(N)}$, $\rho_N = \rho_{T(N)}$, where $T(N)$ is the set of primes dividing N.

2.1.1. *Monodromy groups.* Let

$$\Gamma_p = \rho_p(G_K) \subseteq \mathrm{Aut}_{\mathbb{Z}_p} T_p A,$$

and $\mathbf{G}_p$ denote its Zariski closure. This is a linear algebraic group over $\mathbb{Z}_p$. The generic fibre of $\mathbf{G}_p$ is the usual p-adic monodromy group. Throughout this paper, we make the following assumption.

Hypothesis 2.2. *The group $\mathbf{G}_p$ is connected for a prime p.*

Remark 2.3. A result of Serre [29, Corollaire p. 15] shows that the component group $\mathbf{G}_p/\mathbf{G}_p^\circ$ is independent of the prime p. So the hypothesis holds for all primes p as soon as it holds for one prime. It is also proven in *op. cit.* that there exists a finite extension K^{conn}/K such that this hypothesis holds for the base change $A_{/K^{\mathrm{conn}}}$.

We will use the following key results on the monodromy group.

Theorem 2.4.

(1) *If p is sufficiently large, then $\mathbf{G}_p$ is reductive.*

(2) *There exists a finite Galois extension L/K and an integer N such that*

$$\rho^N(G_L) = \prod_{p \nmid N} \rho_p(G_L)$$

Part (1) is due to Larsen–Pink (cf. the proof of [22, Theorem 3.2]). Part (2) is another result of Serre [29, Théorème p. 56] (see also [15, 31]). The reference does not include the Galois requirement, but we can take the Galois closure, which preserves independence away from a finite set of primes.

2.1.2. *Galois image.* This subsection will recall some large image results for non-CM abelian varieties due to Hui–Larsen [14, Theorem 1.3]. An essentially equivalent result was obtained earlier by Wintenberger [33, Théorème 2], but this formulation is more convenient for us.

For a prime p such that $\mathbf{G}_p$ is reductive, let $\mathbf{G}_p^{\mathrm{ss}}$ denote the quotient of $\mathbf{G}_p$ by its radical, and Γ_p^{ss} the image of Γ_p in $\mathbf{G}_p^{\mathrm{ss}}$. Let $\pi : \mathbf{G}_p^{\mathrm{sc}} \to \mathbf{G}_p^{\mathrm{ss}}$ be the algebraic universal cover. This is a finite morphism.

Theorem 2.5. *For all sufficiently large p, we have*

$$\mathrm{Im}(\mathbf{G}_p^{\mathrm{sc}}(\mathbb{Z}_p) \to \mathbf{G}_p^{\mathrm{ss}}(\mathbb{Z}_p)) \subseteq \Gamma_p^{\mathrm{ss}}.$$

Proof. The cited result of Hui–Larsen is that for $p \gg 0$, the group $\mathbf{G}_p(\mathbb{Q}_p)$ is unramified, and $\pi^{-1}(\Gamma_p^{\mathrm{ss}})$ is a hyperspecial maximal compact subgroup of $\mathbf{G}_p^{\mathrm{sc}}(\mathbb{Q}_p)$. It is not easy to extract the integral model directly from the proof, so we conclude in an indirect way. We have the inclusions

$$\pi^{-1}(\Gamma_p^{\mathrm{ss}}) \subseteq \pi^{-1}(\mathbf{G}_p^{\mathrm{ss}}(\mathbb{Z}_p)) \subseteq \mathbf{G}_p^{\mathrm{sc}}(\mathbb{Z}_p)$$

The first is by definition. The second holds since π is finite, hence proper. The final group is also a hyperspecial maximal compact subgroup of $\mathbf{G}_p^{\mathrm{sc}}(\mathbb{Q}_p)$, and so all three groups above are equal. $\square$

Remark 2.6. If we have a compatible system of semisimple Galois representations coming from geometry, then Theorem 2.4 still holds. Larsen showed that Theorem 2.5 holds for a density one set of primes p [21, Theorem 3.17]. The exceptional set in that proof is again cut out using Chebotarev sets. Therefore, it's likely that our approach works in such generality, though we have not checked the details carefully.

Define the reduced residual representation

$$\overline{\rho}_p^{\mathrm{ss}} : G_K \to \mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p),$$

Its image is also the image of Γ_p^{ss} under the reduction map $\mathbf{G}_p^{\mathrm{ss}}(\mathbb{Z}_p) \to \mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p)$. Denote it by $\overline{\Gamma}_p^{\mathrm{ss}}$. A simple consequence of Theorem 2.5 is the following.

Corollary 2.7. *Let $I_p = \mathrm{Im}(\mathbf{G}_p^{\mathrm{sc}}(\mathbb{F}_p) \to \mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p))$, then for all sufficiently large p, $\overline{\Gamma}_p^{\mathrm{ss}}$ contains I_p.*

2.2. A characterisation of CM abelian varieties.

Proposition 2.8. *Let A be a simple abelian variety over a number field K. If the associated p-adic monodromy group $\mathbf{G}_{p/\mathbb{Q}_p}$ is abelian for one prime p, then it is so for all primes, and A has CM.*

Proof. Suppose that $\mathbf{G}_{p/\mathbb{Q}_p}$ is abelian. The p-adic Galois representation ρ_p is semisimple by Faltings, and rational by construction. Hence, this Galois representation arises from an arithmetic Hecke character over K by a result of Henniart [12] (cf. [27, Theorem 2 in III-13]). Considering infinity type of the Hecke character, it follows that ρ_p corresponds to a CM abelian variety A'. Note that A and A' are isogenous by Falting's isogeny theorem. Hence A has CM, and the assertion follows. $\square$

3. Results on finite reductive groups

Let $\mathbf{G}$ be a connected reductive group defined over $\mathbb{F}_p$. In this section we will give a volume upper bound for the union of certain conjugacy classes.

3.1. **Tori and Weyl groups.** We recall some basic results about maximal tori of $\mathbf{G}$. A detailed exposition can be found in [4, Section 3.3].

Let W_G be the absolute Weyl group of $\mathbf{G}$. It carries an action of the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Let γ be the action corresponding to the Frobenius element. The general theory of forms gives a bijection

$$\{\text{Conjugacy class of maximal tori defined over } \mathbb{F}_p\} \longleftrightarrow \{\gamma\text{-conjugacy classes in } W_G\}.$$

Let $\mathbf{T}$ be a maximal torus in $\mathbf{G}$. Define its Weyl group by

$$W(\mathbf{G}, \mathbf{T}) = N_{\mathbf{G}(\mathbb{F}_p)}(\mathbf{T})/\mathbf{T}(\mathbb{F}_p).$$

It can also be described as the stabilizer of the γ-conjugacy class corresponding to $\mathbf{T}$ under the above bijection. In particular, the γ-twisted class equation gives

$$\sum_{\mathbf{T}} \frac{1}{|W(\mathbf{G}, \mathbf{T})|} = 1 \tag{3.1}$$

where the sum is over a set of representatives for the conjugacy classes of maximal tori in $\mathbf{G}$.

Lemma 3.1. *If $\mathbf{G}$ is not abelian, then $W(\mathbf{G}, \mathbf{T})$ is non-trivial for any maximal torus $\mathbf{T}$.*

Proof. By the class equation (3.1), if the lemma holds for one choice of $\mathbf{T}$, then it holds for all choices of $\mathbf{T}$. Let $\mathbf{B}$ be a Borel subgroup of $\mathbf{G}$ defined over $\mathbb{F}_p$. Its existence is guaranteed by Lang's theorem [19]. Let $\mathbf{S}$ be a maximal $\mathbb{F}_p$-split torus contained in $\mathbf{B}$, and let $\mathbf{T}$ be its centralizer. This is a Levi subgroup of $\mathbf{B}$, and hence a maximal torus. In addition, $N_{\mathbf{G}}(\mathbf{S}) \subseteq N_{\mathbf{G}}(\mathbf{T})$, so the Weyl group $W(\mathbf{G}, \mathbf{T})$ contains the relative Weyl group $W(\mathbf{G}, \mathbf{S})$.[5]

Since $\mathbf{G}$ is not abelian, its derived subgroup $\mathbf{G}^{\mathrm{der}}$ is non-trivial. By Lang's theorem, $\mathbf{G}^{\mathrm{der}}$ has a Borel subgroup, which implies that $\mathbf{G}^{\mathrm{der}}$ has positive rank [3, Corollaire 4.17]. The second paragraph of the proof of [3, Théorème 5.3] then shows that the relative Weyl group $W(\mathbf{G}, \mathbf{S})$ is non-trivial, so $W(\mathbf{G}, \mathbf{T})$ is also non-trivial for this choice of $\mathbf{T}$. $\square$

3.2. **Conjugacy classes.** Given a maximal torus $\mathbf{T}$, let $C_{\mathbf{T}}$ denote the set of elements in $\mathbf{G}(\mathbb{F}_p)$ which are conjugate to an element of $\mathbf{T}(\mathbb{F}_p)$. We will also use the superscript "reg" to denote the subset of regular semisimple elements. The volume is the counting measure normalized so that $\mathrm{vol}(\mathbf{G}(\mathbb{F}_p)) = 1$.

Proposition 3.2. *There exists a constant C depending only on the (absolute) rank of the group $\mathbf{G}$ such that the following holds for all p*

(1) $\mathrm{vol}(\mathbf{G}(\mathbb{F}_p)^{\mathrm{reg}}) > 1 - Cp^{-1}$,

(2) If $\mathbf{T}$ is a maximal torus, then

$$\left| \mathrm{vol}(C_{\mathbf{T}}^{\mathrm{reg}}) - \frac{1}{|W(\mathbf{G}, \mathbf{T})|} \right| < Cp^{-1}.$$

Proof. Let $\mathbf{T}$ be a maximal torus. The map $\mathbf{G}/\mathbf{T} \times \mathbf{T} \to \mathbf{G}$, $(g, t) \mapsto gtg^{-1}$ is finite of degree $|W(\mathbf{G}, \mathbf{T})|$ above the regular elements in its image. Indeed, if $gtg^{-1} = g't'(g')^{-1}$, then $g^{-1}g'$ conjugates t' to t, so it conjugates $Z_{\mathbf{G}}(t')$ to $Z_{\mathbf{G}}(t)$. If t is regular, then the centralizer is just $\mathbf{T}$, so $g^{-1}g' \in N_{\mathbf{G}}(\mathbf{T})$. On $\mathbb{F}_p$-points, the image of this map is exactly $C_{\mathbf{T}}$, so

$$\mathrm{vol}(C_{\mathbf{T}}^{\mathrm{reg}}) = \frac{1}{|W(\mathbf{G}, \mathbf{T})|} \cdot \frac{|\mathbf{T}(\mathbb{F}_p)^{\mathrm{reg}}|}{|\mathbf{T}(\mathbb{F}_p)|}. \tag{3.2}$$

---

[5]We in fact have equality here, but this will not be needed.

Summing over a set of representatives of conjugacy classes of maximal tori, we get

$$\mathrm{vol}(\mathbf{G}(\mathbb{F}_p)^{\mathrm{reg}}) = \sum_{\mathbf{T}} \frac{1}{|W(\mathbf{G},\mathbf{T})|} \cdot \frac{|\mathbf{T}(\mathbb{F}_p)^{\mathrm{reg}}|}{|\mathbf{T}(\mathbb{F}_p)|}.$$

We now give a coarse estimate for the right hand side.

Let $r = \mathrm{rank}\,\mathbf{T}$. The set of non-regular elements in $\mathbf{T}(\mathbb{F}_p)$ is the $\mathbb{F}_p$-points of a variety $\mathbf{T}^{\mathrm{nr}}$ of dimension $r - 1$. When base changed to $\overline{\mathbb{F}}_p$, it can be described as the subset of $\mathbf{G}^r_{m,\overline{\mathbb{F}}_p}$ where at least two of the entries are equal. Let $E_{/\mathbb{Z}}$ be the subscheme of $\mathbf{G}^r_{m,\mathbb{Z}}$ defined this way, then we see that $\mathbf{T}^{\mathrm{nr}}$ is a form of $E \times_{\mathbb{Z}} \mathbb{F}_p$. It follows from the Weil bound[6] that there exist a constant C (depending only on r) such that

$$(3.3) \qquad \left| \frac{|\mathbf{T}(\mathbb{F}_p)^{\mathrm{reg}}|}{|\mathbf{T}(\mathbb{F}_p)|} - 1 \right| \le Cp^{-1}$$

for all p (cf. the proof of Lemma 4.15).

This estimate together with equation (3.2) immediately gives part (2) of the proposition. Using equation (3.1), we see that

$$\mathrm{vol}(\mathbf{G}(\mathbb{F}_p)^{\mathrm{reg}}) \ge \sum_{\mathbf{T}} \frac{1}{|W(\mathbf{G},\mathbf{T})|} \cdot (1 - Cp^{-1}) = 1 - Cp^{-1}.$$

This proves (1). $\qquad\qquad\square$

Definition 3.3. Let $\mathbf{G}$ be a reductive group over $\mathbb{F}_p$. Its *bounding set* is the set of elements in $\mathbf{G}(\mathbb{F}_p)$ which lie in a Borel subgroup defined over $\mathbb{F}_p$.

A consequence of Proposition 3.2 is the following.

Corollary 3.4. *Let $\mathcal{B}$ be the bounding set of $\mathbf{G}$. There exists an integer N depending only on the rank of $\mathbf{G}$ such that if $\mathbf{G}$ is non-abelian and $p > N$, then*

$$\mathrm{vol}(\mathcal{B}) < \frac{3}{4}.$$

Proof. Let $\mathbf{T}$ be a maximal torus in a Borel subgroup $\mathbf{B}$. Let $x \in \mathcal{B}$ be regular semisimple. We will show that x is conjugate to an element of $\mathbf{T}$. Indeed, all Borel subgroups are conjugate [3, Théorème 4.13(b)], so we may assume $x \in \mathbf{B}$. Any maximal torus of $\mathbf{B}$ containing x is a Levi component, so it is conjugate to $\mathbf{T}$ [3, Proposition 4.7]. It follows that $\mathcal{B}$ is contained in the union of non-regular semisimple elements and $C_{\mathbf{T}}$. Therefore,

$$\mathrm{vol}(\mathcal{B}) \le \mathrm{vol}(\mathbf{G}(\mathbb{F}_p) - \mathbf{G}(\mathbb{F}_p)^{\mathrm{reg}}) + \mathrm{vol}(C^{\mathrm{reg}}_{\mathbf{T}}) < 2Cp^{-1} + \frac{1}{|W(\mathbf{G},\mathbf{T})|}$$

by Proposition 3.2. Lemma 3.1 shows that $W(\mathbf{G},\mathbf{T})$ is non-trivial, so its order is at least 2. By taking p sufficiently large, the right hand side can be made smaller than any real number greater than $\frac{1}{2}$. $\qquad\square$

3.3. **Central isogeny.** This subsection refines Proposition 3.2 and Corollary 3.4. This refinement is the key ingredient which allows us to apply the large image results of Theorem 2.5 and Corollary 2.7.

Suppose $\mathbf{G}$ is semisimple, then it has an algebraic universal cover $\pi : \mathbf{G}^{\mathrm{sc}} \to \mathbf{G}$. Its kernel, denoted by Z, is a finite group scheme over $\mathbb{F}_p$ and contained in the centre of $\mathbf{G}^{\mathrm{sc}}$. Let $\mathbf{T}$ be a maximal torus of $\mathbf{G}$, then $\mathbf{T}^{\mathrm{sc}} := \pi^{-1}(\mathbf{T})$ is a maximal torus in $\mathbf{G}^{\mathrm{sc}}$ containing Z.

We have the following exact sequence of groups

$$\begin{array}{ccccccccc}
1 & \longrightarrow & Z(\mathbb{F}_p) & \longrightarrow & \mathbf{T}^{\mathrm{sc}}(\mathbb{F}_p) & \longrightarrow & \mathbf{T}(\mathbb{F}_p) & \longrightarrow & H^1(\mathbb{F}_p, Z) & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \| \\
1 & \longrightarrow & Z(\mathbb{F}_p) & \longrightarrow & \mathbf{G}^{\mathrm{sc}}(\mathbb{F}_p) & \longrightarrow & \mathbf{G}(\mathbb{F}_p) & \xrightarrow{\ \delta\ } & H^1(\mathbb{F}_p, Z) & \longrightarrow & 1.
\end{array}$$

---

[6]One may also proceed by an elementary argument: counting $\mathbf{T}(\mathbb{F}_p)^{\mathrm{reg}}$ using inclusion-exclusion, but the details are messy.

The final 1 in both rows are by Lang's theorem. Note that *a priori*, the connecting morphisms are between pointed sets, but since Z is central, they are actually group homomorphisms (cf. [30, §I.5.6]).

Lemma 3.5. *We have* $|\mathbf{G}^{\mathrm{sc}}(\mathbb{F}_p)| = |\mathbf{G}(\mathbb{F}_p)|$.

Proof. Since $Z(\overline{\mathbb{F}}_p)$ is finite, its Herbrand quotient is 1. Hence the assertion follows by considering the bottom row of the above diagram. We remark that this is also a special case of [2, Chapter V, Proposition 16.8]. □

The main result of this section is that the various conjugacy classes we have considered are approximately equally distributed in the fibres of δ. More precisely, we have the following.

Proposition 3.6. *Let* $\mathbf{G}$ *be a non-abelian semisimple group. Let* $I = \mathrm{Im}(\mathbf{G}^{\mathrm{sc}}(\mathbb{F}_p) \to \mathbf{G}(\mathbb{F}_p))$.

(1) *There exists a constant* C *depending only on the rank of* $\mathbf{G}$ *such that for any maximal torus* $\mathbf{T}$ *and* $g \in \mathbf{G}(\mathbb{F}_p)$, *we have*

$$\left| \frac{|C_{\mathbf{T}}^{\mathrm{reg}} \cap gI|}{|I|} - \frac{1}{|W(\mathbf{G}, \mathbf{T})|} \right| < Cp^{-1}.$$

(2) *There exists an integer* N *depending only on the rank of* $\mathbf{G}$ *such that for all* $p > N$, *we have*

$$\frac{1}{2|W(\mathbf{G}, \mathbf{T})|} < \frac{|\mathcal{B} \cap gI|}{|I|} < \frac{3}{4}$$

where $\mathcal{B}$ *is the bounding set for* $\mathbf{G}$.

Proof. Let $n = [\mathbf{G}(\mathbb{F}_p) : I] = |\mathrm{H}^1(\mathbb{F}_p, Z)| = |Z(\mathbb{F}_p)|$. The group Z is a subgroup of the center of a semisimple simply connected group over $\overline{\mathbb{F}}_p$. Since the rank is fixed, there are a finite number of such groups, so n is bounded from above, independently of $\mathbf{G}$.

From the above diagram, $I = \ker \delta$ is a normal subgroup with an abelian quotient, so if two elements of $\mathbf{G}(\mathbb{F}_p)$ are conjugate, then they lie in the same coset of I. Moreover, δ is still surjective when restricted to $\mathbf{T}(\mathbb{F}_p)$, so it identifies $\mathbf{T}(\mathbb{F}_p)/(\mathbf{T}(\mathbb{F}_p) \cap I)$ with $\mathrm{H}^1(\mathbb{F}_p, Z)$. Fix $g \in \mathbf{G}(\mathbb{F}_p)$, then we get

$$|\mathbf{T}(\mathbb{F}_p) \cap gI| = \frac{|\mathbf{T}(\mathbb{F}_p)|}{|\mathrm{H}^1(\mathbb{F}_p, Z)|}.$$

The conjugation action $\mathbf{G}/\mathbf{T} \times \mathbf{T} \to \mathbf{G}$, $(x, t) \mapsto xtx^{-1}$, as in the proof of Proposition 3.2, restricts to an action on the coset gI, so

$$|C_{\mathbf{T}}^{\mathrm{reg}} \cap gI| = \frac{1}{|W(\mathbf{G}, \mathbf{T})|} \cdot \frac{|\mathbf{G}(\mathbb{F}_p)|}{|\mathbf{T}(\mathbb{F}_p)|} \cdot |\mathbf{T}(\mathbb{F}_p)^{\mathrm{reg}} \cap gI|$$

$$= \frac{|I|}{|W(\mathbf{G}, \mathbf{T})|} \cdot \frac{|\mathbf{T}(\mathbb{F}_p)^{\mathrm{reg}} \cap gI|}{|\mathbf{T}(\mathbb{F}_p) \cap gI|}.$$

Therefore, we have

$$\left| \frac{|C_{\mathbf{T}}^{\mathrm{reg}} \cap gI|}{|I|} - \frac{1}{|W(\mathbf{G}, \mathbf{T})|} \right| = \frac{|(\mathbf{T}(\mathbb{F}_p) - \mathbf{T}(\mathbb{F}_p)^{\mathrm{reg}}) \cap gI|}{|\mathbf{T}(\mathbb{F}_p) \cap gI|} \leq \frac{|\mathbf{T}(\mathbb{F}_p) - \mathbf{T}(\mathbb{F}_p)^{\mathrm{reg}}|}{|\mathbf{T}(\mathbb{F}_p)|/n} \leq nCp^{-1}$$

where C is the constant from the equation (3.3).

For the second part, take $\mathbf{T}$ to be the maximal torus in a Borel subgroup as before. Let C be the constant in Proposition 3.2, then

$$\frac{|\mathcal{B} \cap gI|}{|I|} \leq \frac{|\mathbf{G}(\mathbb{F}_p) - \mathbf{G}(\mathbb{F}_p)^{\mathrm{reg}}|}{|I|} + \frac{|C_{\mathbf{T}}^{\mathrm{reg}} \cap gI|}{|I|}$$

$$< C(n+1)p^{-1} + \frac{1}{|W(\mathbf{G}, \mathbf{T})|}.$$

On the other hand,

$$\frac{|\mathcal{B} \cap gI|}{|I|} \geq \frac{|C_{\mathbf{T}}^{\mathrm{reg}} \cap gI|}{|I|} \geq \frac{1}{|W(\mathbf{G}, \mathbf{T})|} - nCp^{-1}$$

The same argument as in Corollary 3.4 gives the desired bounds. $\square$

4. Proof of Main Theorem

We now prove the main results. The first subsection sets up some notation. Then the second contains a short proof of the qualitative version (cf. Theorem 1.1). Finally, the third subsection is dedicated to the quantitative version (cf. Theorem 1.3).

4.1. **Preliminaries.**

4.1.1. *Setting.* Let A be a simple abelian variety of dimension g defined over a number field K such that $A_{/\bar{K}}$ does not have CM. Let Δ_A be the norm of the conductor of A. Let M be a number field and

$$S_{A,M} = \{v \in \Sigma_K | v \nmid \Delta_A, F(A, v) \cong M\}.$$

For X a positive real number, define

$$S_{A,M}(X) = \{v \in S_{A,M} \,|\, \mathbf{N}_{K/\mathbb{Q}} v \leq X\}.$$

Our goal is to bound $S_{A,M}(X)$ from above, supposing Hypothesis 2.2.

Let L be a finite Galois extension of K such that the conclusion of Theorem 2.4(2) holds, and let N be the bound given therein. Increase N so that for all $p > N$, the following holds:

(1) The monodromy group $\mathbf{G}_p$ is reductive, cf. Theorem 2.4(1).

(2) The large image result in Corollary 2.7 holds for $A_{/L}$

(3) The density estimate in Proposition 3.6(2) holds for all groups of rank at most $2g$.

This N depends only on A and K. Let $\mathcal{P}$ be the set of all primes greater than N which split completely in M.

4.1.2. *Preliminary lemmas.*

Lemma 4.1. *Pick $p \in \mathcal{P}$ and $v \in S_{A,M}$ which does not lie above p. Then the Frobenius $\overline{\rho}_p^{\mathrm{ss}}(\mathrm{Frob}_v) \in \mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p)$ lives in a Borel subgroup defined over $\mathbb{F}_p$.*

Proof. Let $F_v = \rho_p^{\mathrm{ss}}(\mathrm{Frob}_v) \in \mathbf{G}_p^{\mathrm{ss}}(\mathbb{Z}_p)$. By Faltings' theorem, this is a semisimple element in $\mathbf{G}_p^{\mathrm{ss}}(\mathbb{Q}_p)$. Moreover, our assumptions on p and v together imply that F_v lies in a split torus, and hence in a minimal parabolic subgroup of $\mathbf{G}_p^{\mathrm{ss}}(\mathbb{Q}_p)$, which is necessarily a Borel subgroup since $\mathbf{G}_p^{\mathrm{ss}}$ is unramified. The scheme of Borel subgroups over $\mathbb{Z}_p$ is proper [11, XXII, 5.8.3(i)], so we can extend this Borel subgroup to one defined over $\mathbb{Z}_p$. Its fibre over $\mathbb{F}_p$ is a Borel subgroup of $\mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p)$ containing the reduction of F_v. $\square$

Lemma 4.2. *The image of the Galois representation*

$$\overline{\rho}_{\mathcal{P}}^{\mathrm{ss}} : G_K \to \prod_{p \in \mathcal{P}} \mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p)$$

is a union of cosets of $\prod_{p \in \mathcal{P}} I_p$, where I_p is defined as in Corollary 2.7.

Proof. By the choice of L, we have

$$\overline{\rho}_{\mathcal{P}}^{\mathrm{ss}}(G_L) = \prod_{p \in \mathcal{P}} \overline{\rho}_p^{\mathrm{ss}}(G_L) \subseteq \prod_{p \in \mathcal{P}} \mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p).$$

Item (2) of the choice of $\mathcal{P}$ implies that $\overline{\rho}_p^{\mathrm{ss}}(G_L)$ contains the subgroup I_p for all $p \in \mathcal{P}$. Therefore,

$$\overline{\rho}_{\mathcal{P}}^{\mathrm{ss}}(G_K) \supseteq \overline{\rho}_{\mathcal{P}}^{\mathrm{ss}}(G_L) \supseteq \prod_{p \in \mathcal{P}} I_p.$$

In other words, $\overline{\rho}_{\mathcal{P}}^{\mathrm{ss}}(G_K)$ is a subgroup of $\prod_{p \in \mathcal{P}} \mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p)$ which contains the subgroup $\prod_{p \in \mathcal{P}} I_p$. $\square$

4.2. **Proof of Theorem 1.1.** Let d be a square-free product of primes in $\mathcal{P}$. Let $\mathcal{F}_d$ be the union of all conjugacy classes $\overline{\rho}_d^{\mathrm{ss}}(\mathrm{Frob}_v)$ for $v \in S_{A,M}$ not dividing d.

By Lemma 4.1, we have

$$\mathcal{F}_d \subseteq \Big(\prod_{p|d} \mathcal{B}_p \Big) \cap \overline{\rho}_d^{\mathrm{ss}}(G_K)$$

where $\mathcal{B}_p$ is the bounding set for $\mathbf{G}_p^{\mathrm{ss}}$ introduced in Definition 3.3. The Chebotarev density theorem implies that

$$(4.1) \qquad \mathrm{ud}(S_{A,M}) \leq \frac{|\mathcal{F}_d|}{|\overline{\rho}_d^{\mathrm{ss}}(G_K)|} \leq \frac{\big| \big(\prod_{p|d} \mathcal{B}_p \big) \cap \overline{\rho}_d^{\mathrm{ss}}(G_K) \big|}{|\overline{\rho}_d^{\mathrm{ss}}(G_K)|}.$$

To estimate the right hand side, we utilise the following decomposition

$$\overline{\rho}_d^{\mathrm{ss}}(G_K) = \bigsqcup_{i=1}^{s} \Big(g_i \prod_{p|d} I_p \Big) = \bigsqcup_{i=1}^{s} \Big(\prod_{p|d} g_{i,p} I_p \Big)$$

given by Lemma 4.2. In view of Proposition 2.8, $\mathbf{G}_p^{\mathrm{ss}}$ is non-abelian[7]. Therefore, Proposition 3.6 can be applied, giving the upper bound

$$(4.2) \qquad \Big| \Big(\prod_{p|d} \mathcal{B}_p \Big) \cap \overline{\rho}_d^{\mathrm{ss}}(G_K) \Big| = \sum_{i=1}^{s} \Big| \prod_{p|d} \big(\mathcal{B}_p \cap g_{i,p} I_p \big) \Big| \leq s \prod_{p|d} \Big(\frac{3}{4} |I_p| \Big) = \Big(\frac{3}{4} \Big)^{\omega(d)} |\overline{\rho}_d^{\mathrm{ss}}(G_K)|$$

where $\omega(d)$ is the number of prime divisors of d.

Combining equations (4.1) and (4.2), we get

$$\mathrm{ud}(S_{A,M}) \leq \Big(\frac{3}{4} \Big)^{\omega(d)}$$

for any d which is a square-free product of primes in $\mathcal{P}$. Since $\mathcal{P}$ is infinite, this implies that

$$\mathrm{ud}(S_{A,M}) = 0.$$

4.3. **Proof of Theorem 1.3.** We will now use the effective Chebotarev theorem of Lagarias–Odlyzko and the Selberg sieve to obtain a power saving upper bound for the number of places with a given Frobenius field M. This is possibly the approach suggested by Serre in [28, §8.2].

In this section we will write $f(X) = O(g(X))$ or $f(X) \ll g(X)$ to mean the existence of an absolute constant c such that $|f(X)| \leq c |g(X)|$ for all X. If the constant is allowed to depend on some other object, we will indicate so in the subscripts. All constants are in fact effectively computable.

Remark 4.3. This section will be conditional on the GRH. Unconditionally, we expect that the standard methods lead to an upper bound of the form $O\big(\frac{X}{(\log X)^{\alpha}} \big)$ for some explicit $\alpha > 1$, but we have not worked out the details.

4.3.1. *Sieving setup.* In this subsection, we recast the problem into a form where the Selberg sieve can be directly applied. There are notational complications since we are only assuming potential independence of the Galois images at different primes p. No important idea is lost if one assumes $L = K$, i.e. the family of Galois representations over K has independent image.

Fix a positive real number X. Let $\Sigma_K(X)$ be the set of all finite places of K of norm at most X where A has good reduction. Recall that in §4.1, we have chosen a finite Galois extension L/K and an infinite set of primes $\mathcal{P}$ defined by a splitting condition.

Let $\mathcal{R}$ be the set of square-free product of primes in $\mathcal{P}$. Let $d \in \mathcal{R} \cup \{\infty\}$. In the infinite case, the condition "$p|d$" should be interpreted as "$p \in \mathcal{P}$". Let $G_d = \prod_{p|d} \mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p)$, so we have a Galois representation

$$\overline{\rho}_d^{\mathrm{ss}} : G_K \to G_d.$$

---

[7]The generic fibre is abelian if and if the special fibre is, since $\mathbf{G}_p^{\mathrm{ss}}$ is reductive over $\mathbb{Z}_p$.

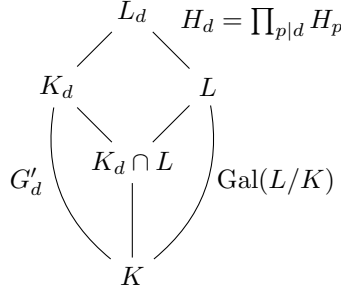Denote its image by G'_d and the fixed field of its kernel by K_d, so we have an isomorphism

$$\mathrm{Gal}(K_d/K) \simeq G'_d,$$

and K_d is the compositum of all K_p for $p|d$. Define H_d and L_d similarly using the restriction $\overline{\rho}^{\mathrm{ss}}_d|_{G_L}$. By the choice of L, we have $H_d = \prod_{p|d} H_p$. In these notations, we have

$$I_d := \prod_{p|d} I_p \subseteq H_d \subseteq G'_d \subseteq G_d$$

where the first inclusion is due to Corollary 2.7.

Here is a summary of the above definitions

Let $\mathcal{I} = G'_\infty/H_\infty$, then from the above diagram, $\mathcal{I} = \mathrm{Gal}(K_\infty \cap L/K)$ is finite. Fix an integer $\mathtt{d}$ such that $K_\mathtt{d} \cap L = K_\infty \cap L$, so if $\mathtt{d}|d$, then $G'_d/H_d \simeq \mathcal{I}$. Write down a coset decomposition

$$G'_\infty = \bigsqcup_{i \in \mathcal{I}} g_i H_\infty = \bigsqcup_{i \in \mathcal{I}} \prod_{p \in \mathcal{P}} g_{i,p} H_p.$$

For any d as above, define $g_{i,d} = (g_{i,p})_{p|d} \in G'_d$, so we have a decomposition $G'_d = \bigcup_{i \in \mathcal{I}} g_{i,d} H_d$. By comparing indices, this is a disjoint union if $\mathtt{d}|d$.

For each $p \in \mathcal{P}$, let $\mathcal{B}_p \subseteq G_p$ be the bounding set as in the previous section (cf. Definition 3.3). Let $\mathcal{C}_p = G_p - \mathcal{B}_p$. For a general $d \in \mathcal{R} \cup \{\infty\}$, define $\mathcal{C}_d$ and $\mathcal{B}_d$ as a product of the corresponding sets for p dividing d. Let $\mathcal{C}'_d = \mathcal{C}_d \cap G'_d$ and $\mathcal{B}'_d = \mathcal{B}_d \cap G'_d$. For an index $i \in \mathcal{I}$, define

$$\mathcal{B}^{(i)}_d = \mathcal{B}_d \cap \prod_{p|d} g_{i,p} H_p.$$

So we have $\mathcal{B}^{(i)}_d = \prod_{p|d} \mathcal{B}^{(i)}_p$. Moreover, $\mathcal{B}'_d = \bigcup_{i \in \mathcal{I}} \mathcal{C}^{(i)}_B$. Define the subset $\mathcal{C}^{(i)}_d$ similarly. If p is a prime, then $g_{i,p} H_p = \mathcal{B}^{(i)}_p \sqcup \mathcal{C}^{(i)}_p$.

Remark 4.4. It could be the case that $\mathcal{B}^{(i)}_d = \mathcal{B}^{(i')}_d$ even though $i \neq i'$ in $\mathcal{I}$. However, this cannot happen if $\mathtt{d}|d$, in which case $\mathcal{B}'_d = \bigsqcup_{i \in \mathcal{I}} \mathcal{B}^{(i)}_d$. In other words, the purpose of the auxiliary $\mathtt{d}$ will play is to identify the correct coset.

Let C be any union of conjugacy classes in G'_d. Define

$$E_d(C) = \left\{ v \in \Sigma_K(X) \,\middle|\, v \text{ does not lie above any } p|d, \ \overline{\rho}^{\mathrm{ss}}_d(\mathrm{Frob}_v) \in C \right\}.$$

The proof of Theorem 1.1 in the previous subsection then implies $S_{A,M}(X) \subseteq E_d(\mathcal{B}'_d)$. This form does not immediately yield a power saving upper bound. Instead, we re-write it in a different way.

Proposition 4.5. *We have an inclusion*

$$S_{A,M}(X) \subseteq \bigsqcup_{i \in \mathcal{I}} \left(E_\mathtt{d}(\mathcal{B}^{(i)}_\mathtt{d}) - \bigcup_{p \in \mathcal{P}^{(\mathtt{d})}} E_{\mathtt{d}p}(\mathcal{B}^{(i)}_\mathtt{d} \times \mathcal{C}^{(i)}_p) \right)$$

where $\mathcal{P}^{(\mathtt{d})}$ consists of the primes in $\mathcal{P}$ which do not divide $\mathtt{d}$.

Proof. Implicit in the statement is that $\mathcal{B}_d^{(i)}$ is a union of conjugacy classes in G_d' for all d. To see this, observe that $\mathcal{B}_d'$ is a union of conjugacy classes, and $\mathcal{B}_d^{(i)}$ is its intersection with a coset of H_d in G_d'. It remains to observe that H_d is a normal subgroup of G_d', and the quotient is abelian, since it is a subquotient of the abelian group G_d/I_d (cf. §3.3). The same argument works for the second term.

The containment is apparent: let $v \in S_{A,M}(X)$ and $g = (g_p)_{p \in \mathcal{P}} = \overline{\rho}_\infty^{\mathrm{ss}}(\mathrm{Frob}_v) \in G_\infty'$. Then there exists a unique $i \in \mathcal{I}$ such that $g \in g_i H_\infty$. Moreover, we know that $g_p \in \mathcal{B}_p'$ for all $p \in \mathcal{P}$, so $g_p \notin \mathcal{C}_p'$. It follows that $(g_p)_{p|\mathtt{d}} \in \mathcal{B}_\mathtt{d}^{(i)}$, but it is not in $\mathcal{B}_\mathtt{d}^{(i)} \times \mathcal{C}_p^{(i)}$ for any prime p. $\qquad\square$

Each term in the disjoin union in Proposition 4.5 is a sieving problem. We now recall a form of the Selberg sieve.

Theorem 4.6. *Let $\mathcal{P}$ be a set of primes, and let $\mathcal{R}$ be the set of square-free products of primes in $\mathcal{P}$.*

Let $\mathcal{A}$ be a finite set. For each $p \in \mathcal{P}$, let $\mathcal{A}_p \subseteq \mathcal{A}$. For $d \in \mathcal{R}$, define $\mathcal{A}_d = \bigcap_{p|d} \mathcal{A}_p$. If $d = 1$, set $\mathcal{A}_1 = \mathcal{A}$. Suppose for all d, we can write

$$|\mathcal{A}_d| = \beta_d c \operatorname{Li}(X) + R_d$$

where R_d is some real number, the function $d \mapsto \beta_d$ is multiplicative, and there exists constants $0 < \underline{\beta} < \overline{\beta} < 1$ such that $\underline{\beta} < \beta_p < \overline{\beta}$ for all $p \in \mathcal{P}$.

Under these assumptions, for any positive real numbers z and ε, we have

$$\left| \mathcal{A} - \bigcup_{p \in \mathcal{P}} \mathcal{A}_p \right| \ll_{\underline{\beta}, \overline{\beta}, \varepsilon} \frac{c \operatorname{Li}(X)}{\pi_{\mathcal{P}}(z)} + \left(\frac{z^{1+\varepsilon}}{\pi_{\mathcal{P}}(z)} \right)^2 \sum_{\substack{d_1, d_2 \leq z \\ d_1, d_2 \in \mathcal{R}}} \frac{R_{[d_1, d_2]}}{d_1 d_2}$$

where $\pi_{\mathcal{P}}(z) = |\{p \in \mathcal{P} \mid p \leq z\}|$.

Proof. This follows from a minor refinement to the proof of [9, Theorem 7.2.1], and we borrow their notations, with the obvious modification that their X is $c \operatorname{Li}(X)$ in our case. It is easy to compute that $f(d) = \beta_d^{-1}$, $f_1(d) = \prod_{p|d} \frac{1 - \beta_p}{\beta_p}$, and

$$V(z) = \sum_{\substack{d \leq z \\ d | P(z)}} \frac{\mu^2(d)}{f_1(d)} \geq \sum_{\substack{p \leq z \\ p \in \mathcal{P}}} \frac{1}{f_1(p)} = \sum_{\substack{p \leq z \\ p \in \mathcal{P}}} \frac{\beta_p}{1 - \beta_p} \geq \frac{\underline{\beta}}{1 - \underline{\beta}} \pi_{\mathcal{P}}(z).$$

The first term in the upper bound is the main term of the conclusion in *loc. cit.*. For second term, we start from the third displayed equation on page 122 and improve on the estimate $|\lambda_d| \leq 1$. From the second to last displayed equation on page 122, we have

(4.3) $$|V(z)\lambda_d| \leq \prod_{p|d} \frac{1}{1 - \beta_p} \cdot \sum_{\substack{t \leq \frac{z}{d} \\ t \in \mathcal{R}}} \frac{\mu^2(t)}{f_1(t)}$$

Fix an $\varepsilon > 0$, then for all $t \in \mathcal{R}$,

$$\frac{1}{f_1(t)} = \prod_{p|t} \frac{\beta_p}{1 - \beta_p} \leq \left(\frac{\overline{\beta}}{1 - \overline{\beta}} \right)^{\omega(t)} \ll_{\overline{\beta}, \varepsilon} t^\varepsilon$$

The same argument can be applied to the first term of equation (4.3). Therefore,

$$|V(z)\lambda_d| \ll_{\overline{\beta}, \varepsilon} d^\varepsilon \sum_{\substack{t \leq \frac{z}{d} \\ t \in \mathcal{R}}} t^\varepsilon \leq d^{-1} z^{1+\varepsilon}$$

Combined with the above lower bounds for $V(z)$, we get

$$|\lambda_d| \ll_{\underline{\beta}, \overline{\beta}, \varepsilon} d^{-1} \frac{z^{1+\varepsilon}}{\pi_{\mathcal{P}}(z)}$$

This concludes the proof. $\qquad\square$

In our applications, we will take $\mathscr{P} = \mathcal{P}^{(\mathsf{d})}$, $\mathcal{A} = E_{\mathsf{d}}(\mathcal{B}_{\mathsf{d}}^{(i)})$, and $\mathcal{A}_p = E_{\mathsf{d}p}(\mathcal{B}_{\mathsf{d}}^{(i)} \times \mathcal{C}_p^{(i)})$. Let $\mathcal{R}^{(\mathsf{d})}$ be the subset of $\mathcal{R}$ which are coprime to d, then for all $d \in \mathcal{R}^{(\mathsf{d})}$, we have

$$\mathcal{A}_d = \bigcap_{p|d} E_{\mathsf{d}p}(\mathcal{B}_{\mathsf{d}}^{(i)} \times \mathcal{C}_p^{(i)}) = E_{\mathsf{d}d}(\mathcal{B}_{\mathsf{d}}^{(i)} \times \mathcal{C}_d^{(i)})$$

The sizes of $\mathcal{A}_d$ will be estimated using versions of the effective Chebotarev theorem, which we now recall.

4.3.2. *Background on effective Chebotarev.* For any number field k, let $n_k = [k : \mathbb{Q}]$ and Δ_k be its absolute discriminant. Given a finite extension l/k, let $\mathcal{D}(l/k)$ denote the set of rational primes that lie below the ramified finite places of l/k. Define

$$M(l/k) = |G| \Delta_k^{\frac{1}{n_k}} \prod_{p \in \mathcal{D}(l/k)} p.$$

Suppose that l/k is Galois with Galois group G. Let $C \subseteq G$ be a union of conjugacy classes. For any positive real number X, define

$$\pi(X, C, l/k) := |\{\mathfrak{p} \,|\, \mathfrak{p} \text{ is unramified in } l, \ \mathrm{Frob}_{\mathfrak{p}} \in C, \ \mathbf{N}_{k/\mathbb{Q}}\mathfrak{p} \le X\}|.$$

We are interested in the error term

$$R(X, C, l/k) := \pi(X, C, l/k) - \frac{|C|}{|G|} \mathrm{Li}(X).$$

The following result is equation (20_{R}) in [28, §2.4], which is an improvement to Lagarias–Odlyzko's original result [18].

Theorem 4.7. *Assume the GRH holds for the Artin L-functions of irreducible representations of l/k, then*

$$|R(X, C, l/k)| \ll |C| \, n_k X^{\frac{1}{2}} \big(\log X + \log M(l/k) \big).$$

Assuming the AHC, Murty–Murty–Saradha obtained the following improvement [23, Corollary 3.10].

Theorem 4.8. *Let H be a subgroup of G such that the GRH and AHC hold for the Artin L-functions of the irreducible characters of H. Suppose H meets every conjugacy class contained in C, then*

$$R(X, C, l/k) \ll |C|^{\frac{1}{2}} [G : H]^{\frac{1}{2}} n_k X^{\frac{1}{2}} \big(\log X + \log M(l/k) \big).$$

If $|C|$ is of roughly the same size as $|G|$, then this estimate saves a factor of $|H|^{\frac{1}{2}}$ compared to Theorem 4.7. We therefore want to take $|H|$ as large as possible.

Remark 4.9. This theorem is a corollary of a precise result [23, Proposition 3.9]. While it suffices for our purpose, we expect that a finer analysis of centralizers in finite reductive groups can give a better exponent.

4.3.3. *Applications.* We now apply the above results to the various terms appearing in Theorem 4.6. Fix $i \in \mathcal{I}$. For each $d \in \mathcal{R}$, define

$$\alpha_d^{(i)} = \frac{|\mathcal{B}_d^{(i)}|}{|H_d|}, \quad \beta_d^{(i)} = \frac{|\mathcal{C}_d^{(i)}|}{|H_d|}.$$

Then we have the relations

$$\alpha_d^{(i)} = \prod_{p|d} \alpha_p^{(i)}, \quad \beta_d^{(i)} = \prod_{p|d} \beta_p^{(i)}, \quad \alpha_p^{(i)} + \beta_p^{(i)} = 1$$

for all $p \in \mathcal{P}$ and $d \in \mathcal{R}$. If d_1, d_2 are coprime numbers in $\mathcal{R}$, then in the above notations,

$$(4.4) \qquad \left| E_{d_1 d_2}(\mathcal{B}_{d_1}^{(i)} \times \mathcal{C}_{d_2}^{(i)}) \right| = \frac{1}{[G'_{d_1 d_2} : H_{d_1 d_2}]} \alpha_{d_1}^{(i)} \beta_{d_2}^{(i)} \mathrm{Li}(X) + R(X, \mathcal{B}_{d_1}^{(i)} \times \mathcal{C}_{d_2}^{(i)}, K_{d_1 d_2}/K).$$

Using Theorem 4.7 alone, this error term is of the order $|G_{d_1 d_2}| X^{\frac{1}{2}+\varepsilon}$.

In this subsection, we show that the error term for $\left| E_d(\mathcal{B}_d^{(i)}) \right|$ can be improved using Theorem 4.8. This yields the required estimate for (4.4) using the principle of inclusion-exclusion. The main result is Proposition 4.13.

For each prime p, fix a Borel subgroup $\mathbf{B}_p \subseteq \mathbf{G}_p^{\mathrm{ss}}$, and let

$$B_p = \mathbf{B}_p(\mathbb{F}_p).$$

Define $B_d = \prod_{p|d} B_p$ and $B_d' = B_d \cap G_d'$. This is a subgroup of G_d'. The next two lemmas verify that it satisfies the conditions in Theorem 4.8.

Lemma 4.10. *All conjugacy classes in $\mathcal{B}_d^{(i)}$ intersect B_d'.*

Proof. By the Borel conjugacy theorem [3, Théorème 4.13(b)], this result holds in G_d. To conclude, we will show that the conjugating element can be chosen to lie in I_d. It is enough to do this for $d = p$, a prime.

Suppose $b \in \mathcal{B}_p'$ and $gbg^{-1} \in B_p'$, where $g \in G_p$. Let $\mathbf{T}_p \subseteq \mathbf{B}_p$ be a maximal torus. Then the commutative diagram appearing §3.3 shows that $\mathbf{T}_p(\mathbb{F}_p)$ intersects all cosets of I_p. Choose $t \in \mathbf{T}_p(\mathbb{F}_p)$ so that t and g are in the same coset, then $t^{-1}g$ is an element of I_p conjugating b to B_p'. $\qquad\square$

Lemma 4.11. *All irreducible representations of B_d' are induced from abelian characters. Consequently, the AHC holds for $K_d/K_d^{B_d'}$, and the GRH holds provided it holds for all Hecke L-functions.*

Proof. We will show that if $p \in \mathcal{P}$, then B_p is supersolvable. The group B_d' is a subquotient of their product, so it is also supersolvable. The first claim of the lemma is an elementary group theory fact [26, Theorem 12.8.5]. The second part of the lemma is a standard consequence of class field theory.

Let $p \in \mathcal{P}$. We first observe that $\mathbf{G}_p^{\mathrm{ss}}$ is actually split over $\mathbb{F}_p$. Indeed, by a result of Serre (cf. [5, Corollary 3.8]), the element $\rho_p(\mathrm{Frob}_v) \in \mathbf{G}_p(\mathbb{Q}_p)$ generates a maximal torus for a density one set of places v. On the other hand, p splits completely in M, so this element lies in a split torus. Therefore, we have constructed a split maximal torus of $\mathbf{G}_p$ over $\mathbb{Q}_p$, which also implies $\mathbf{G}_p^{\mathrm{ss}}$ is split.

Fix a faithful representation $\mathbf{G}_p^{\mathrm{ss}} \hookrightarrow \mathrm{GL}_N$ defined over $\mathbb{F}_p$, we see that B_p is isomorphic to a subgroup of R_N, the group of upper triangular matrices in $\mathrm{GL}_N(\mathbb{F}_p)$. Write the derived series of R_N as

$$R_N \rhd S_N \rhd S_{N-1} \rhd \cdots \rhd S_0 = \{1\}.$$

Then a standard calculation shows that

$$S_k = \{g \in R_N \,|\, g_{ii} = 1, \ g_{ij} = 0 \text{ if } 0 < j - i \leq N - k\}.$$

For $v = 1, \cdots, k-1$, let

$$S_{k,v} = \{g \in S_k \,|\, g_{i,i+N-k} = 0 \text{ if } i \leq v\}.$$

Then we have a normal series $S_k \rhd S_{k,1} \rhd \cdots \rhd S_{k,k-1} = S_{k-1}$ where each quotient is isomorphic to $\mathbb{F}_p$. Conjugation by a diagonal matrix preserves $S_{k,v}$, so all of the groups are normal in R_N. This normal series shows that R_N is a supersolvable group, which completes the proof. $\qquad\square$

Proposition 4.12. *For each prime p, let*

(4.5) $$N_p = \left| \mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p) \right| \cdot \left| \mathbf{B}_p(\mathbb{F}_p) \right|^{-\frac{1}{2}}.$$

Assume the GRH for Hecke L-functions. Then for all $d \in \mathcal{R}$, we have

$$\left| E_d(\mathcal{B}_d^{(i)}) \right| = \frac{1}{[G_d' : H_d]} \alpha_d^{(i)} \mathrm{Li}(X) + O_{A,K}\Big(\prod_{p|d} N_p \cdot X^{\frac{1}{2}} (\log X + \log d) \Big).$$

Proof. Applying Theorem 4.8 to the extension $l/k = K_d/K$ with the subgroup $H = B_d'$ gives the error term

$$\left| R(X, \mathcal{B}_d^{(i)}, K_d/K) \right| \ll (|\mathcal{B}_d^{(i)}| \cdot [G_d' : B_d'])^{\frac{1}{2}} n_K X^{\frac{1}{2}} \big(\log X + \log M(K_d/K) \big)$$

$$\leq (|G_d| \cdot [G_d : B_d])^{\frac{1}{2}} n_K X^{\frac{1}{2}} \big(\log X + \log M(K_d/K) \big)$$

$$= \prod_{p|d} N_p \cdot n_K X^{\frac{1}{2}} \big(\log X + \log M(K_d/K) \big).$$

For the terms beside N_p, recall that K_d/K is unramified away from the places of K dividing $d\Delta_A$, so

$$\log M(K_d/K) = \log|G'_d| + \frac{\log(\Delta_K)}{n_K} + \sum_{p|d}\log p + \sum_{p|\Delta_A}\log p$$

$$\leq \sum_{p|d}\log\left|\mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p)\right| + \log d + O_{A,K}(1)$$

$$\ll_{A,K} \log d$$

where for the final estimate, we used the trivial bound $\left|\mathbf{G}_p^{\mathrm{ss}}(\mathbb{F}_p)\right| \leq \left|\mathrm{GSp}_{2g}(\mathbb{F}_p)\right|$. $\qquad\square$

We now apply this to calculate the intersection terms in the Selberg sieve.

Proposition 4.13. *Assume the GRH for Hecke L-functions. If $d \in \mathcal{R}$ is coprime to $\mathtt{d}$, then*

$$\left|\bigcap_{p|d}E_{\mathtt{d}p}(\mathcal{B}_{\mathtt{d}}^{(i)}\times\mathcal{C}_p^{(i)})\right| = \frac{1}{|\mathcal{I}|}\alpha_{\mathtt{d}}^{(i)}\beta_d^{(i)}\mathrm{Li}(X) + O_{A,K}\left(2^{\omega(d)}\prod_{p|\mathtt{d}d}N_p \cdot X^{\frac{1}{2}}\left(\log X + \log(\mathtt{d}d)\right)\right).$$

Proof. We have the equality

$$\bigcap_{p|d}E_{\mathtt{d}p}(\mathcal{B}_{\mathtt{d}}^{(i)}\times\mathcal{C}_p^{(i)}) = E_{\mathtt{d}}(\mathcal{B}_{\mathtt{d}}^{(i)}) - \bigcup_{p|d}E_{\mathtt{d}p}(\mathcal{B}_{\mathtt{d}p}^{(i)}).$$

To see this, observe that $\mathcal{B}_p^{(i)} \sqcup \mathcal{C}_p^{(i)}$ is the coset of $g_{i,p}H_p$, and the condition defining the set $E_{\mathtt{d}}(\mathcal{B}_{\mathtt{d}}^{(i)})$ already forces the Frobenius element to be in this coset (cf. Remark 4.4).

The principle of inclusion-exclusion now gives

$$\left|\bigcap_{p|d}E_{\mathtt{d}p}(\mathcal{B}_{\mathtt{d}}^{(i)}\times\mathcal{C}_p^{(i)})\right| = \sum_{d'|d}\mu(d')\left|E_{\mathtt{d}d'}(\mathcal{B}_{\mathtt{d}d'}^{(i)})\right|.$$

Apply the previous proposition to the right hand side. There are $2^{\omega(d)}$ terms in the above sum, so the error term has the required form by the triangle inequality. In the main term, the coefficient in front of $\mathrm{Li}(X)$ is given by

$$\sum_{d'|d}\mu(d') \cdot \frac{1}{|\mathcal{I}|}\alpha_{\mathtt{d}d'}^{(i)} = \frac{1}{|\mathcal{I}|}\alpha_{\mathtt{d}}^{(i)}\prod_{p|d}(1-\alpha_p^{(i)}) = \frac{1}{|\mathcal{I}|}\alpha_{\mathtt{d}}^{(i)}\beta_d^{(i)}$$

where we used the observation that $[G'_d : H_d] = [G'_\infty : H_\infty] = |\mathcal{I}|$ for $\mathtt{d}|d$. $\qquad\square$

4.3.4. *Point counting.* We will now estimate N_p, defined in (4.5).

Proposition 4.14. *Let $\mathbf{G}$ be the Mumford–Tate group of $A_{/K}$ and $\mathbf{G}^{\mathrm{ss}}$ its semisimple quotient. Put*

$$\gamma = \frac{1}{4}(3\dim\mathbf{G}^{\mathrm{ss}} - \mathrm{rank}\,\mathbf{G}^{\mathrm{ss}}).$$

There exists a constant C depending only on g such that

$$N_p \leq Cp^\gamma$$

for all primes p.

The key feature of this proposition is that neither C nor γ depend on the prime p, even though the monodromy groups $\mathbf{G}_p$ are not assumed to interpolate into a group over $\mathbb{Q}$. The proposition follows by combining Lemma 4.15 and Corollary 4.17 below.

Lemma 4.15. *There exists a constant C depending only on g such that for all prime p,*

$$N_p \leq Cp^{\dim\mathbf{G}_p^{\mathrm{ss}} - \frac{1}{2}\dim\mathbf{B}_p}.$$

Proof. In view of Lemma 3.5 we may replace $\mathbf{G}_p^{\mathrm{ss}}$ with $\mathbf{G}_p^{\mathrm{sc}}$ in the definition of N_p. The base change $(\mathbf{G}_p^{\mathrm{sc}})_{/\overline{\mathbb{F}}_p}$ is a simply connected semisimple group, so it is a product of simply connected split simple groups. These are classified by Dynkin diagrams. Since the rank is bounded (say by $2g$), there are only a finite number of possibilities. Moreover, each of them is obtained from a Chevalley group over $\mathbb{Z}$ by base change.

Now, $\mathbf{G}_p^{\mathrm{sc}}(\mathbb{F}_p)$ is the set of fixed points of the Frobenius operator F acting on $\mathbf{G}_p^{\mathrm{sc}}(\overline{\mathbb{F}}_p)$. The Grothendieck–Lefschetz trace formula gives

$$\left|\mathbf{G}_p^{\mathrm{sc}}(\mathbb{F}_p)\right| = \sum_{i=0}^{2\dim\mathbf{G}_p^{\mathrm{sc}}} (-1)^i \mathrm{Tr}\left(F, \mathrm{H}_c^i\left((\mathbf{G}_p^{\mathrm{sc}})_{/\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell\right)\right)$$

The top degree term is $p^{\dim\mathbf{G}_p^{\mathrm{sc}}}$ since $\mathbf{G}_p^{\mathrm{sc}}$ is geometrically connected. Deligne's Weil bound gives an upper bound for the Frobenius eigenvalues on each of the remaining terms. In particular, it implies

$$\left|p^{-\dim\mathbf{G}_p^{\mathrm{sc}}}\left|\mathbf{G}_p^{\mathrm{sc}}(\mathbb{F}_p)\right| - 1\right| \leq bp^{-\frac{1}{2}}$$

where b is the sum of the dimensions of all lower degree cohomology groups. The argument in the previous paragraph gives a finite list of possibilities for b independently of p. Therefore, we get positive constants $c_1(g), c_2(g)$ depending only on g such that

$$c_1 p^{\dim\mathbf{G}_p^{\mathrm{sc}}} \leq \left|\mathbf{G}_p^{\mathrm{sc}}(\mathbb{F}_p)\right| \leq c_2 p^{\dim\mathbf{G}_p^{\mathrm{sc}}}$$

for all primes p.

By applying the exact same argument to the term $|\mathbf{B}_p(\mathbb{F}_p)|$, the assertion follows. $\square$

Let $\mathbf{G}$ be the Mumford–Tate group of A. For our purpose, it suffices to know that this is a reductive group over $\mathbb{Q}$ which "contains" all p-adic monodromy groups, made precise by the following theorem of Deligne [10].

Theorem 4.16. *For all primes p, we have[8] $\mathbf{G}_{p/\mathbb{Q}_p} \subseteq \mathbf{G} \times_{\mathbb{Q}} \mathbb{Q}_p$.*

Corollary 4.17. *Let $\mathbf{G}^{\mathrm{ss}}$ denote the semisimple quotient of $\mathbf{G}$, then for all primes p,*

$$\dim\mathbf{G}_p^{\mathrm{ss}} - \frac{1}{2}\dim\mathbf{B}_p \leq \frac{1}{4}\left(3\dim\mathbf{G}^{\mathrm{ss}} - \mathrm{rank}\,\mathbf{G}^{\mathrm{ss}}\right)$$

Proof. Fix a prime p. For simplicity, we base change the pertinent groups to $\overline{\mathbb{Q}}_p$. This does not change its dimension or rank.

Recall that $\mathbf{B}_p$ is a Borel subgroup of $\mathbf{G}_p^{\mathrm{ss}}$. Let $\mathbf{N}_p$ be its unipotent radical. We have the relations

$$\dim\mathbf{G}_p^{\mathrm{ss}} = 2\dim\mathbf{B}_p - \mathrm{rank}\,\mathbf{G}_p^{\mathrm{ss}} = \dim\mathbf{B}_p + \dim\mathbf{N}_p$$

Rearranging this, we get

$$\dim\mathbf{G}_p^{\mathrm{ss}} - \frac{1}{2}\dim\mathbf{B}_p = \frac{1}{4}\left(3\dim\mathbf{G}_p^{\mathrm{ss}} - \mathrm{rank}\,\mathbf{G}_p^{\mathrm{ss}}\right) = \frac{1}{2}\dim\mathbf{G}_p^{\mathrm{ss}} + \frac{1}{2}\dim\mathbf{N}_p$$

It remains to show that $\dim\mathbf{G}_p^{\mathrm{ss}} \leq \dim\mathbf{G}^{\mathrm{ss}}$ and $\dim\mathbf{N}_p \leq \dim\mathbf{N}$.

The previous theorem gives an embedding $\mathbf{G}_p \subseteq \mathbf{G}$ of reductive groups, and hence the inclusion of the derived subgroups $\mathbf{G}_p^{\mathrm{der}} \subseteq \mathbf{G}^{\mathrm{der}}$. Moreover, the derived subgroup is isogenous to the semisimple quotient, so they have the same dimension and rank. The first inequality follows. For the second part, the image of $\mathbf{N}_p$ is again a unipotent subgroup, so it lies in a conjugate of $\mathbf{N}$. $\square$

---

[8]Recall that we are assuming all monodromy groups are connected.

4.3.5. *Conclusion of the proof.* We now assemble the pieces to conclude the proof.

Lemma 4.18. *If v is a finite place of K not dividing Δ_A, then*

$$\log |\Delta_{F(A,v)}| \ll_g \log \mathbf{N}_{K/\mathbb{Q}} v.$$

Proof. Let $P(T) \in \mathbb{Z}[T]$ be the characteristic polynomial of $\rho_p(\mathrm{Frob}_v)$. Let $\alpha_1, \cdots, \alpha_{2g}$ be the roots of $P(T)$, then $F(A, v)$ is the compostium of the fields $\mathbb{Q}(\alpha_i)$. Therefore,

$$\frac{\log |\Delta_{F(A,v)}|}{[F(A,v):\mathbb{Q}]} \leq \sum_{i=1}^{2g} \frac{\log |\Delta_{\mathbb{Q}(\alpha_i)}|}{[\mathbb{Q}(\alpha_i):\mathbb{Q}]}.$$

Let $q = \mathbf{N}_{K/\mathbb{Q}} v$, then all the roots of $P(T)$ have complex absolute value $q^{\frac{1}{2}}$, so

$$\log \left|\Delta_{\mathbb{Q}(\alpha)}\right| \leq \log |\mathrm{disc}\, P(T)| = \sum_{i \neq j} \log |\alpha_i - \alpha_j| \leq ((2g)^2 - 2g) \log \left(2q^{\frac{1}{2}}\right).$$

Combining the above two inequalities gives the claim. $\qquad \square$

Theorem 4.19. *Assume the GRH. For any $\varepsilon > 0$, we have*

$$|S_{A,M}(X)| \ll_{A,K,\varepsilon} X^{1 - \frac{1}{4\gamma+2} + \varepsilon},$$

where $\gamma = \frac{1}{4}(3 \dim \mathbf{G}^{\mathrm{ss}} - \mathrm{rank}\, \mathbf{G}^{\mathrm{ss}})$ from Proposition 4.14.

Proof. Fix $\varepsilon > 0$, then Proposition 4.5 gives an equality

$$|S_{A,M}(X)| = \sum_{i \in \mathcal{I}} \left| E_{\mathsf{d}}(\mathcal{B}_{\mathsf{d}}^{(i)}) - \bigcup_{p \in \mathcal{P}^{(\mathsf{d})}} E_{\mathsf{d}p}(\mathcal{B}_{\mathsf{d}}^{(i)} \times \mathcal{C}_p^{(i)}) \right|.$$

Fix an index $i \in \mathcal{I}$. We will apply Theorem 4.6 to the corresponding term in the above sum. Take $\mathcal{A} = E_\infty(g_i H_\infty)$, sieving primes $\mathcal{P}^{(\mathsf{d})}$, and excluded subsets $\mathcal{A}_p = E_{\mathsf{d}p}(\mathcal{B}_{\mathsf{d}}^{(i)} \times \mathcal{C}_p^{(i)})$. By combing Proposition 4.13 and Proposition 4.14, we get the estimate

$$|\mathcal{A}_d| = \left| \bigcap_{p|d} E_{\mathsf{d}p}(\mathcal{B}_{\mathsf{d}}^{(i)} \times \mathcal{C}_p^{(i)}) \right| = \frac{1}{|\mathcal{I}|} \alpha_{\mathsf{d}}^{(i)} \beta_d^{(i)} \mathrm{Li}(X) + O_{A,K}\left((2C)^{\omega(d)} d^\gamma X^{\frac{1}{2}} (\log X + \log d)\right)$$

$$= \frac{1}{|\mathcal{I}|} \alpha_{\mathsf{d}}^{(i)} \beta_d^{(i)} \mathrm{Li}(X) + O_{A,K,\varepsilon}\left(d^{\gamma+\varepsilon} X^{\frac{1}{2}} (\log X + \log d)\right).$$

By definition, the function $d \mapsto \beta_d^{(i)}$ is multiplicative. Let $p \in \mathcal{P}^{(\mathsf{d})}$, then

$$\beta_p^{(i)} = \frac{|\mathcal{C}_p \cap g_{i,p} H_p|}{|H_p|} = 1 - \frac{|\mathcal{B}_p \cap g_{i,p} H_p|}{|H_p|}.$$

Recall that H_p contains I_p, so each $g_{i,p} H_p$ is a union of cosets of I_p. Over each such coset, Proposition 3.6 gives uniform upper and lower bounds for its intersection with $\mathcal{B}_p$. It follows that $\beta_p^{(i)}$ is uniformly bounded away from 0 and 1, and the bounds only depend on the dimension g.

Having verified all of the hypotheses, Theorem 4.6 gives the estimate

$$\left| E_{\mathsf{d}}(\mathcal{B}_{\mathsf{d}}^{(i)}) - \bigcup_{p \in \mathcal{P}^{(\mathsf{d})}} E_{\mathsf{d}p}(\mathcal{B}_{\mathsf{d}}^{(i)} \times \mathcal{C}_p^{(i)}) \right|$$

$$\ll_{A,K,\varepsilon} \frac{1}{|\mathcal{I}|} \alpha_{\mathsf{d}}^{(i)} \cdot \frac{\mathrm{Li}(X)}{\pi_{\mathcal{P}^{(\mathsf{d})}}(z)} + \left(\frac{z^{1+\varepsilon}}{\pi_{\mathcal{P}^{(\mathsf{d})}}(z)}\right)^2 X^{\frac{1}{2}} \sum_{\substack{d_1,d_2 \leq z \\ d_1,d_2 \in \mathcal{R}^{(\mathsf{d})}}} \frac{[d_1,d_2]^{\gamma+\varepsilon}}{d_1 d_2} (\log X + \log[d_1,d_2]).$$

In the sum for the second term, use the trivial bound $[d_1, d_2] \leq d_1 d_2$ and extend the sum to all pairs $d_1, d_2 \leq z$. In particular, $\log[d_1, d_2] \leq \log(z^2)$. Therefore,

$$\sum_{\substack{d_1, d_2 \leq z \\ d_1, d_2 \in \mathcal{R}^{(\mathsf{d})}}} \frac{[d_1, d_2]^{\gamma+\varepsilon}}{d_1 d_2}(\log X + \log[d_1, d_2]) \leq \sum_{d_1, d_2 \leq z} (d_1 d_2)^{\gamma-1+\varepsilon}(\log X + 2\log z)$$

$$= (\log X + 2\log z)\Big(\sum_{d \leq z} d^{\gamma-1+\varepsilon}\Big)^2$$

$$\ll_\gamma z^{2\gamma+2\varepsilon}(\log X + \log z).$$

which gives

$$(4.6) \qquad \left| E_{\mathsf{d}}(\mathcal{B}_{\mathsf{d}}^{(i)}) - \bigcup_{p \in \mathcal{P}^{(\mathsf{d})}} E_{\mathsf{d}p}(\mathcal{B}_{\mathsf{d}}^{(i)} \times \mathcal{C}_p^{(i)}) \right| \ll_{A, K, \varepsilon} \frac{X}{\pi_{\mathcal{P}^{(\mathsf{d})}}(z)} + \left(\frac{z^{1+\varepsilon}}{\pi_{\mathcal{P}^{(\mathsf{d})}}(z)}\right)^2 X^{\frac{1}{2}} z^{2\gamma+2\varepsilon} \log(Xz).$$

It remains to bound $\pi_{\mathcal{P}^{(\mathsf{d})}}(z)$ from below. By definition,

$$\pi_{\mathcal{P}^{(\mathsf{d})}}(z) = \pi(z, \{1\}, M/\mathbb{Q}) - O_{A,K}(1)$$

By the effective Chebotarev theorem (Theorem 4.7, also cf. [28, Equation (14_R)]), we have

$$\pi(z, \{1\}, M/\mathbb{Q}) = \frac{1}{[M:\mathbb{Q}]}\mathrm{Li}(z) + O_g\big(z^{\frac{1}{2}}(\log z + \log|\Delta_M|)\big).$$

We may assume $\log|\Delta_M| \ll_g \log X$, since otherwise $S_{A,M}(X) = \emptyset$ by Lemma 4.18. Now choose $z = X^\beta$, where $\beta = \frac{1}{4\gamma+2}$, then

$$\pi_{\mathcal{P}^{(\mathsf{d})}}(z) = \frac{1}{[M:\mathbb{Q}]}\mathrm{Li}(X^\beta) + O_{g,\beta}(X^{\frac{\beta}{2}}\log X) - O_{A,K}(1) \gg_{A,K,\varepsilon} X^{\beta-\varepsilon}.$$

Substituting this in equation 4.6 and summing over all $i \in \mathcal{I}$ gives the desired result. $\qquad\square$

Remark 4.20. We only needed the error term in the effective Chebotarev theorem on average. The situation is analogous to the Bombieri–Vinogradov theorem, except that it deals with the family of abelian extensions $\{\mathbb{Q}(\zeta_q)/\mathbb{Q}\}$, and we have a family of non-abelian Lie-extensions $\{K_d/K\}$. There are some works when the Galois group is fixed (cf. [24]), but we are not aware of any work in our setting.

REFERENCES

[1] S. Bloom. The square sieve and a Lang-Trotter question for generic abelian varieties. *J. Number Theory*, 191:119–157, 2018.

[2] A. Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[3] A. Borel and J. Tits. Groupes réductifs. *Inst. Hautes Études Sci. Publ. Math.*, 27:55–150, 1965.

[4] R. W. Carter. *Finite groups of Lie type: Conjugacy classes and complex characters*. Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York, 1985.

[5] W. C. Chi. *l*-adic and λ-adic representations associated to abelian varieties defined over number fields. *Amer. J. Math.*, 114(2):315–353, 1992.

[6] A. C. Cojocaru and C. David. Frobenius fields for Drinfeld modules of rank 2. *Compos. Math.*, 144(4):827–848, 2008.

[7] A. C. Cojocaru and C. David. Frobenius fields for elliptic curves. *Amer. J. Math.*, 130(6):1535–1560, 2008.

[8] A. C. Cojocaru, E. Fouvry, and M. R. Murty. The square sieve and the Lang-Trotter conjecture. *Canad. J. Math.*, 57(6):1155–1177, 2005.

[9] A. C. Cojocaru and M. R. Murty. *An introduction to sieve methods and their applications*, volume 66 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2006.

[10] P. Deligne. Hodge cycles on abelian varieties. In *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Math., pages 9–100. Springer, Berlin, 1982.

[11] M. Demazure and A. Grothendieck. *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*, volume 152 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1970. (SGA 3).

[12] G. Henniart. Représentations *l*-adiques abéliennes. In *Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981)*, volume 22 of *Progr. Math.*, pages 107–126. Birkhäuser Boston, Boston, MA, 1982.

[13] H. Hida. *Elliptic curves and arithmetic invariants*. Springer Monographs in Mathematics. Springer, New York, 2013.

[14] C. Y. Hui and M. Larsen. Maximality of Galois actions for abelian and hyper-Kähler varieties. *Duke Math. J.*, 169(6):1163–1207, 2020.

[15] L. Illusie. Independence of families of l-adic representations and uniform constructibility (after J.-P. Serre). Available at http://www.math.u-psud.fr/~illusie, 2010.

[16] C. Khare. F-split Galois representations are potentially abelian. *Proc. Amer. Math. Soc.*, 131(10):3021–3023, 2003.

[17] M. Kulkarni, V. M. Patankar, and C. S. Rajan. Locally potentially equivalent two dimensional Galois representations and Frobenius fields of elliptic curves. *J. Number Theory*, 164:87–102, 2016.

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

[19] S. Lang. Algebraic groups over finite fields. *Amer. J. Math.*, 78:555–563, 1956.

[20] S. Lang and H. Trotter. *Frobenius distributions in* GL_2-*extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[21] M. Larsen. Maximality of Galois actions for compatible systems. *Duke Math. J.*, 80(3):601–630, 1995.

[22] M. Larsen and R. Pink. Abelian varieties, l-adic representations, and l-independence. *Math. Ann.*, 302(3):561–579, 1995.

[23] M. R. Murty, V. K. Murty, and N. Saradha. Modular forms and the Chebotarev density theorem. *Amer. J. Math.*, 110(2):253–281, 1988.

[24] L. B. Pierce, C. L. Turnage-Butterbaugh, and M. M. Wood. An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups. *Invent. Math.*, 219(2):701–778, 2020.

[25] R. Pink. l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture. *J. Reine Angew. Math.*, 495:187–237, 1998.

[26] W. R. Scott. *Group theory*. Prentice-Hall, Inc., Englewood Cliffs, NJ, 1964.

[27] J.-P. Serre. *Abelian l-adic representations and elliptic curves*. W. A. Benjamin, Inc., New York-Amsterdam, 1968. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute.

[28] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publications Mathématiques de l'IHÉS*, 54:123–201, 1981.

[29] J.-P. Serre. *Œuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000. 1985–1998.

[30] J.-P. Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[31] J.-P. Serre. Un critère d'indépendance pour une famille de représentations ℓ-adiques. *Comment. Math. Helv.*, 88(3):541–554, 2013.

[32] G. Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998.

[33] J.-P. Wintenberger. Démonstration d'une conjecture de Lang dans des cas particuliers. *J. Reine Angew. Math.*, 553:1–16, 2002.

[34] D. Zywina. Bounds for the Lang-Trotter conjectures. In *SCHOLAR—a scientific celebration highlighting open lines of arithmetic research*, volume 655 of *Contemp. Math.*, pages 235–256. Amer. Math. Soc., Providence, RI, 2015.

DEPARTMENT OF MATHEMATICS, UT AUSTIN, AUSTIN, TX 78712

Email address: ashayburungale@gmail.com

DEPARTMENT OF MATHEMATICS, UCLA, LOS ANGELES, CA 90095-1555, USA

Email address: hharuzo@gmail.com

DEPARTMENT OF MATHEMATICS, UT AUSTIN, AUSTIN, TX 78712

Email address: shilin.lai@math.utexas.edu