

Algebra & Number Theory

Volume 20
2026
No. 3

**On the Frobenius fields of abelian varieties
over number fields**

Ashay A. Burungale, Haruzo Hida and Shilin Lai



On the Frobenius fields of abelian varieties over number fields

Ashay A. Burungale, Haruzo Hida and Shilin Lai

Let A be a non-CM simple abelian variety over a number field K . For a place v of K where A has good reduction, 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.

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 and 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 connectedness 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 (see [Theorem 1.3](#)).

Main results. Let K be a number field and Σ_K the set of its finite places. For \bar{K} an algebraic closure, let $G_K = \text{Gal}(\bar{K}/K)$ 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 g and conductor \mathfrak{N} . For a prime p , let $T_p A$ be the p -adic Tate module of A and

$$\rho_{A,p} : G_K \rightarrow \text{Aut}_{\mathbb{Z}_p} T_p A$$

MSC2020: 14K15.

Keywords: abelian varieties, Frobenius fields, Mumford–Tate groups.

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 $\rho_{A,p}(\text{Frob}_v)$. 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

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

When A is a CM abelian variety, the Frobenius fields are a subfield¹ of the corresponding CM field (cf. [35]). 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 $\text{ud}(S)$ is given by

$$\text{ud}(S) = \limsup_{X \rightarrow \infty} \frac{\#\{v \in \Sigma_K : N_{K/\mathbb{Q}}v \leq X, v \in S\}}{\#\{v \in \Sigma_K : N_{K/\mathbb{Q}}v \leq X\}},$$

where $N_{K/\mathbb{Q}}$ 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*

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

The connectivity Hypothesis 2.2 is satisfied by any abelian variety A over some 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, including hyperelliptic Jacobians [37, Theorem 1.2].

Remark 1.2. Theorem 1.1 gives a criterion for characterization 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 [12, §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}^{ss} be its semisimple quotient. Let

$$d = \dim \mathbf{G}^{\text{ss}}, \quad r = \text{rank } \mathbf{G}^{\text{ss}}$$

denote the dimension and (absolute) rank of \mathbf{G}^{ss} . Then our quantitative result is as follows.

¹More 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') .

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 for L -functions as in Remark 1.5. 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*

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

If A is generic — meaning that the associated adelic Galois representation has open image in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ — then $\mathbf{G}^{\mathrm{ss}} = \mathrm{PGSp}_{2g}$ for an integer $g \geq 1$. In this case $d = 2g^2 + g$ and $r = g$, so we obtain the following.

Corollary 1.4. *In the setting of Theorem 1.3 suppose further that A is generic and let $\mathbf{G}^{\mathrm{ss}} = \mathrm{PGSp}_{2g}$ for an integer $g \geq 1$. 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*

$$|\{v \in S_{A,M} \mid N_{K/\mathbb{Q}}v \leq X\}| \leq cX^{1-\frac{1}{6g^2+2g+2}+\varepsilon}.$$

Remark 1.5. Our approach to Theorem 1.3 is conditional on the GRH for two types of L -functions. The first is the Dedekind zeta function for a number field M . The second consists of L -functions of finite order Hecke characters appearing in the statement of Lemma 4.11, namely the characters attached to abelian subquotients of Galois extensions of the form $K(A[d])/K$, where d is a square-free product of rational primes.

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 [36] and Hui and Larsen [13] (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

$$\mathrm{Im}\left(\prod_p \rho_{A,p}\right) = \prod_p \mathrm{Im}(\rho_{A,p}), \tag{1-1}$$

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 and Odlyzko and the Selberg sieve. Some notable features:

- Without the Mumford–Tate conjecture, the p -adic monodromy groups can be different² 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 $N_{K/\mathbb{Q}v}$ (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 M. R. Murty, V. K. Murty and N. 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 above relies on a fundamental result of Deligne [10]: the Mumford–Tate group “contains” all p -adic monodromy groups (cf. [Theorem 4.16](#)).

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 [29, §7]. For elliptic curves, the result was first stated (without proof or explicit exponent) by Serre [29, §8.2]. Its various explicit forms have appeared in the work of Cojocaru, Fouvry and Murty [9], Cojocaru and David [6], Zywinia [38], and Kulkarni, Patankar and Rajan [17], among others. Cojocaru and 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.

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 generalizes 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](#)).

²Recall that the Mumford–Tate conjecture is not known in general.

Compared to previous works, our approach is closer in spirit to the square sieve method, which first appeared in [9]. 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 reductive groups³ and introduce the key notion of a bounding set (cf. [Definition 3.3](#)). In [Section 4](#) we prove the main theorems.

2. Backdrop

We describe some preliminaries regarding p -adic Galois representations associated to an abelian variety over a number field. The reader may refer to [13; 26; 36] 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 $\Delta_A = N_{K/\mathbb{Q}}\mathfrak{N}$, 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

$$\rho_p : G_K \rightarrow \text{Aut}_{\mathbb{Z}_p} T_p A$$

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 $\rho_p(\text{Frob}_v)$ has integral coefficients and is independent of p . Moreover, all of its roots have complex absolute value $(N_{K/\mathbb{Q}}v)^{\frac{1}{2}}$.*

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

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

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.

³As pointed out by the referee, these results may be well-known to specialists (cf. [15; 23]). Due to the lack of a precise reference in the literature (see [Remark 3.7](#)), we include details.

Hypothesis 2.2. The group G_p is connected for a prime p .

Remark 2.3. A result of Serre [30, corollaire p. 15] shows that the component group G_p/G_p° 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^{conn} .

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

Theorem 2.4.

- (1) If p is sufficiently large, then 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 and Pink (cf. the proof of [22, Theorem 3.2]). Part (2) is another result of Serre [31, théorème p. 56] (see also [14; 33]). 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 and Larsen [13, Theorem 1.3]. An essentially equivalent result was obtained earlier by Wintenberger [36, théorème 2], but this formulation is more convenient for us.

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

Theorem 2.5. *Let A be an abelian variety over a number field K . Then there exists a constant $c_{A,K} \in \mathbb{Z}$ such that for any prime $p > c_{A,K}$, we have*

$$\text{Im}(G_p^{\text{sc}}(\mathbb{Z}_p) \rightarrow G_p^{\text{ss}}(\mathbb{Z}_p)) \subseteq \Gamma_p^{\text{ss}}.$$

Proof. The aforementioned result of Hui and Larsen is that for $p \gg 0$, the group $G_p(\mathbb{Q}_p)$ is unramified, and $\pi^{-1}(\Gamma_p^{\text{ss}})$ is a hyperspecial maximal compact subgroup of $G_p^{\text{sc}}(\mathbb{Q}_p)$.

It is not easy to extract the integral model directly from the proof, so we conclude in an indirect way. We have the inclusions

$$\pi^{-1}(\Gamma_p^{\text{ss}}) \subseteq \pi^{-1}(G_p^{\text{ss}}(\mathbb{Z}_p)) \subseteq G_p^{\text{sc}}(\mathbb{Z}_p)$$

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 $G_p^{\text{sc}}(\mathbb{Q}_p)$, and so all three groups above are equal. □

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

$$\bar{\rho}_p^{ss} : G_K \rightarrow \mathbf{G}_p^{ss}(\mathbb{F}_p),$$

Its image is also the image of Γ_p^{ss} under the reduction map $\mathbf{G}_p^{ss}(\mathbb{Z}_p) \rightarrow \mathbf{G}_p^{ss}(\mathbb{F}_p)$. Denote it by $\bar{\Gamma}_p^{ss}$. Put

$$I_p = \text{Im}(\mathbf{G}_p^{sc}(\mathbb{F}_p) \rightarrow \mathbf{G}_p^{ss}(\mathbb{F}_p)).$$

A simple consequence of [Theorem 2.5](#) is the following.

Corollary 2.7. *Let A be an abelian variety over a number field K and $c_{A,K} \in \mathbb{Z}$ be as in [Theorem 2.5](#). Then for any prime $p > c_{A,K}$, the image $\bar{\Gamma}_p^{ss}$ contains I_p .*

Remark 2.8. The lower bound $c_{A,K}$ in the above corollary and [Theorem 2.4](#) depends only on the number field K and the isogeny class of A . It seems likely that $c_{A,K}$ can be expressed as an explicit function of K and the conductor of A following the strategy outlined in [[36](#), Remarque 2.2].

2.2. A characterization of CM abelian varieties.

Proposition 2.9. *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 [[11](#)] (cf. [[28](#), 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 Faltings' 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 $W_{\mathbf{G}}$ be the absolute Weyl group of \mathbf{G} . It carries an action of the Galois group $\text{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. Let γ be the action corresponding to the Frobenius element. The general theory of forms gives a bijection

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

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 T under the above bijection. In particular, the γ -twisted class equation gives

$$\sum_T \frac{1}{|W(\mathbf{G}, T)|} = 1, \tag{3-1}$$

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 $W(\mathbf{G}, T)$ is nontrivial for any maximal torus T .*

Proof. By the class equation (3-1), if the lemma holds for one choice of T , then it holds for all choices of 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 T be its centralizer. This is a Levi subgroup of \mathbf{B} , and hence a maximal torus. In addition, $N_{\mathbf{G}}(\mathbf{S}) \subseteq N_{\mathbf{G}}(T)$, so the Weyl group $W(\mathbf{G}, T)$ contains the relative Weyl group $W(\mathbf{G}, \mathbf{S})$.⁴

Since \mathbf{G} is not abelian, its derived subgroup \mathbf{G}^{der} is nontrivial. By Lang’s theorem, \mathbf{G}^{der} has a Borel subgroup, which implies that \mathbf{G}^{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 nontrivial, so $W(\mathbf{G}, T)$ is also nontrivial for this choice of T . □

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

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

- (1) $\text{vol}(\mathbf{G}(\mathbb{F}_p)^{\text{reg}}) > 1 - Cp^{-1}$.
- (2) *If T is a maximal torus, then*

$$|\text{vol}(C_T^{\text{reg}}) - \frac{1}{|W(\mathbf{G}, T)|}| < Cp^{-1}.$$

Proof. Let T be a maximal torus. The map $\mathbf{G}/T \times T \rightarrow \mathbf{G}$, $(g, t) \mapsto gtg^{-1}$ is finite of degree $|W(\mathbf{G}, T)|$ 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 T , so $g^{-1}g' \in N_{\mathbf{G}}(T)$. On \mathbb{F}_p -points, the image of this map is exactly C_T , so

$$\text{vol}(C_T^{\text{reg}}) = \frac{1}{|W(\mathbf{G}, T)|} \cdot \frac{|T(\mathbb{F}_p)^{\text{reg}}|}{|T(\mathbb{F}_p)|}. \tag{3-2}$$

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

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

⁴We in fact have equality here, but this will not be needed.

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

Let $r = \text{rank } T$. The set of nonregular elements in $T(\mathbb{F}_p)$ is the \mathbb{F}_p -points of a variety T^{nr} of dimension $r - 1$. When base changed to $\overline{\mathbb{F}}_p$, it can be described as the subset of $G_{m, \overline{\mathbb{F}}_p}^r$ where at least two of the entries are equal. Let $E_{/\mathbb{Z}}$ be the subscheme of $G_{m, \mathbb{Z}}^r$ defined this way, then we see that T^{nr} is a form of $E \times_{\mathbb{Z}} \mathbb{F}_p$. It follows from the Weil bound⁵ that there exist a constant C (depending only on r) such that

$$\left| \frac{|T(\mathbb{F}_p)^{\text{reg}}|}{|T(\mathbb{F}_p)|} - 1 \right| \leq Cp^{-1} \tag{3-3}$$

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 (3-1), we see that

$$\text{vol}(G(\mathbb{F}_p)^{\text{reg}}) \geq \sum_T \frac{1}{|W(G, T)|} \cdot (1 - Cp^{-1}) = 1 - Cp^{-1}.$$

This proves (1). □

Definition 3.3. Let G be a reductive group over \mathbb{F}_p . Its *bounding set* is the set of elements in $G(\mathbb{F}_p)$ 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 G . There exists an integer N depending only on the rank of G such that if G is nonabelian and $p > N$, then*

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

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

$$\begin{aligned} \text{vol}(\mathcal{B}) &\leq \text{vol}(G(\mathbb{F}_p) - G(\mathbb{F}_p)^{\text{reg}}) + \text{vol}(C_T^{\text{reg}}) \\ &< 2Cp^{-1} + \frac{1}{|W(G, T)|} \end{aligned}$$

by Proposition 3.2. Lemma 3.1 shows that $W(G, T)$ is nontrivial, 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 $\frac{1}{2}$. □

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

⁵One may also proceed by an elementary argument: counting $T(\mathbb{F}_p)^{\text{reg}}$ using inclusion-exclusion, but the details are messy.

We have the following exact sequence of groups:

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

The final 1 in both rows comes from Lang’s theorem. A priori, the connecting morphisms are between pointed sets, but since Z is central, they are actually group homomorphisms (cf. [32, §I.5.6]).

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

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. This is also a special case of [2, Chapter V, Proposition 16.8]. \square

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:

Proposition 3.6. *Let \mathbf{G} be a nonabelian semisimple group. Let $I = \text{Im}(\mathbf{G}^{\text{sc}}(\mathbb{F}_p) \rightarrow \mathbf{G}(\mathbb{F}_p))$.*

(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*

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

(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 $n = [\mathbf{G}(\mathbb{F}_p) : I] = |\mathbf{H}^1(\mathbb{F}_p, Z)| = |Z(\mathbb{F}_p)|$. The group Z is a subgroup of the centre 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 $\mathbf{H}^1(\mathbb{F}_p, Z)$. Fix $g \in \mathbf{G}(\mathbb{F}_p)$, then we get

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

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

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

Therefore, we have

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

where C is the constant from (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

$$\frac{|\mathcal{B} \cap gI|}{|I|} \leq \frac{|\mathbf{G}(\mathbb{F}_p) - \mathbf{G}(\mathbb{F}_p)^{\text{reg}}|}{|I|} + \frac{|C_{\mathbf{T}}^{\text{reg}} \cap gI|}{|I|} < C(n+1)p^{-1} + \frac{1}{|W(\mathbf{G}, \mathbf{T})|}.$$

On the other hand,

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

The same argument as in Corollary 3.4 gives the desired bounds. □

Remark 3.7. Some versions of the above counting results for tori have previously appeared in literature (see [15, §3.4] and [23, §3]). For example, our Propositions 3.2(2) and 3.6(1) coincide respectively with Propositions 4.1 and 4.6 of [15]. However, the literature does not seem to contain finer results such as Corollary 3.4 and Proposition 3.6(2), which are necessary for our later arguments.

4. Proof of the 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 \mathfrak{N} be the conductor of A . Let M be a number field and

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

For X a positive real number, define

$$S_{A,M}(X) = \{v \in S_{A,M} \mid N_{K/\mathbb{Q}}v \leq X\}.$$

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 $2g$.

In view of [Corollary 2.7](#), 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 $\bar{\rho}_p^{\text{ss}}(\text{Frob}_v) \in \mathbf{G}_p^{\text{ss}}(\mathbb{F}_p)$ lives in a Borel subgroup defined over \mathbb{F}_p .*

Proof. Let $F_v = \rho_p^{\text{ss}}(\text{Frob}_v) \in \mathbf{G}_p^{\text{ss}}(\mathbb{Z}_p)$. By Faltings’ theorem, this is a semisimple element in $\mathbf{G}_p^{\text{ss}}(\mathbb{Q}_p)$. Our assumptions on p and v together imply that F_v lies in a split torus, and hence in a minimal parabolic subgroup of $\mathbf{G}_p^{\text{ss}}(\mathbb{Q}_p)$, which is necessarily a Borel subgroup since \mathbf{G}_p^{ss} is unramified. The scheme of Borel subgroups over \mathbb{Z}_p is proper [[34](#), 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 $\mathbf{G}_p^{\text{ss}}(\mathbb{F}_p)$ containing the reduction of F_v . \square

Lemma 4.2. *The image of the Galois representation*

$$\bar{\rho}_{\mathcal{P}}^{\text{ss}} : G_K \rightarrow \prod_{p \in \mathcal{P}} \mathbf{G}_p^{\text{ss}}(\mathbb{F}_p)$$

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

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

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

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

In other words, $\bar{\rho}_{\mathcal{P}}^{\text{ss}}(G_K)$ is a subgroup of $\prod_{p \in \mathcal{P}} \mathbf{G}_p^{\text{ss}}(\mathbb{F}_p)$ 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 $\bar{\rho}_d^{\text{ss}}(\text{Frob}_v)$ for $v \in S_{A,M}$ not dividing d .

By [Lemma 4.1](#), we have

$$\mathcal{F}_d \subseteq \left(\prod_{p|d} \mathcal{B}_p \right) \cap \bar{\rho}_d^{\text{ss}}(G_K),$$

where \mathcal{B}_p is the bounding set for \mathbf{G}_p^{ss} introduced in [Definition 3.3](#). The Chebotarev density theorem implies that

$$\text{ud}(S_{A,M}) \leq \frac{|\mathcal{F}_d|}{|\bar{\rho}_d^{\text{ss}}(G_K)|} \leq \frac{|(\prod_{p|d} \mathcal{B}_p) \cap \bar{\rho}_d^{\text{ss}}(G_K)|}{|\bar{\rho}_d^{\text{ss}}(G_K)|}. \tag{4-1}$$

To estimate the right-hand side, we utilise the following decomposition, given by [Lemma 4.2](#):

$$\bar{\rho}_d^{\text{ss}}(G_K) = \bigsqcup_{i=1}^s \left(g_i \prod_{p|d} I_p \right) = \bigsqcup_{i=1}^s \left(\prod_{p|d} g_{i,p} I_p \right).$$

In view of [Proposition 2.9](#), G_p^{ss} is nonabelian⁶. Therefore, [Proposition 3.6](#) can be applied, giving the upper bound

$$\left| \left(\prod_{p|d} \mathcal{B}_p \right) \cap \bar{\rho}_d^{ss}(G_K) \right| = \sum_{i=1}^s \left| \prod_{p|d} (\mathcal{B}_p \cap g_{i,p} I_p) \right| \leq s \prod_{p|d} \left(\frac{3}{4} |I_p| \right) = \left(\frac{3}{4} \right)^{\omega(d)} |\bar{\rho}_d^{ss}(G_K)|, \quad (4-2)$$

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

Combining [\(4-1\)](#) and [\(4-2\)](#), we get

$$\text{ud}(S_{A,M}) \leq \left(\frac{3}{4} \right)^{\omega(d)}$$

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

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

4.3. Proof of [Theorem 1.3](#). We will now use the effective Chebotarev theorem of Lagarias and 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 [\[29, §8.2\]](#).

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 $O(X/(\log X)^\alpha)$ 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 [Section 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 products 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 $G_d = \prod_{p|d} G_p^{ss}(\mathbb{F}_p)$, so we have a Galois representation

$$\bar{\rho}_d^{ss} : G_K \rightarrow G_d.$$

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

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

and K_d is the compositum of all K_p for $p|d$. Define H_d and L_d similarly using the restriction $\bar{\rho}_d^{ss}|_{G_L}$.

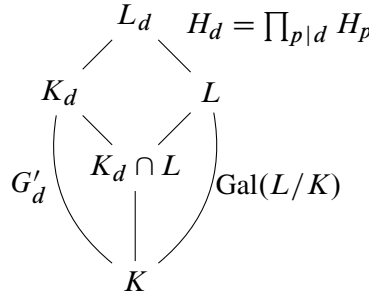
⁶The generic fibre is abelian if and if the special fibre is, since G_p^{ss} is reductive over \mathbb{Z}_p .

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 $\mathcal{I} = G'_\infty/H_\infty$. From the above diagram, $\mathcal{I} = \text{Gal}(K_\infty \cap L/K)$ is finite. Fix an integer d such that $K_d \cap L = K_\infty \cap L$, so if $d|d$, 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 $d|d$.

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

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

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

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

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

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

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*

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

where $\mathcal{P}^{(d)}$ consists of the primes in \mathcal{P} which do not divide 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. Section 3.3). The same argument works for the second term.

The containment is apparent: let $v \in S_{A,M}(X)$ and $g = (g_p)_{p \in \mathcal{P}} = \bar{\rho}_\infty^{\text{ss}}(\text{Frob}_v) \in G'_\infty$. Then there exists a unique $i \in \mathcal{I}$ such that $g \in g_i H_\infty$. 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 $(g_p)_{p|d} \in \mathcal{B}_d^{(i)}$, but it is not in $\mathcal{B}_d^{(i)} \times \mathcal{C}_p^{(i)}$ for any prime p . \square

Each term in the disjoint 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 A be a finite set. For each $p \in \mathcal{P}$, let $A_p \subseteq A$. For $d \in \mathcal{R}$, define $A_d = \bigcap_{p|d} A_p$. If $d = 1$, set $A_1 = A$. Suppose that, for all d , we can write

$$|A_d| = \beta_d c \text{Li}(X) + R_d,$$

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

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

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

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

Proof. This follows from a minor refinement to the proof of [8, Theorem 7.2.1], and we borrow their notations, with the obvious modification that their X is $c \text{Li}(X)$ in our case. It is easy to compute that $f(d) = \beta_d^{-1}$, $f_1(d) = \prod_{p|d} (1 - \beta_p) / \beta_p$, 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 the 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

$$|V(z)\lambda_d| \leq \prod_{p|d} \frac{1}{1-\beta_p} \cdot \sum_{\substack{t \leq \frac{z}{d} \\ t \in \mathcal{R}}} \frac{\mu^2(t)}{f_1(t)} \tag{4-3}$$

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

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

The same argument can be applied to the first term of (4-3). Therefore,

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

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

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

This concludes the proof. □

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

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

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

$$\pi(X, C, l/k) := |\{p \mid p \text{ is unramified in } l, \text{Frob}_p \in C, N_{k/\mathbb{Q}}p \leq X\}|.$$

We are interested in the error term

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

The following result is equation (20_R) in [29, §2.4], which is an improvement to Lagarias and Odlyzko’s original result [18].

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

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

Assuming the truth of the Artin holomorphy conjecture, Murty, Murty and Saradha obtained the following improvement [24, 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*

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

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 [24, 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,

$$|E_{d_1 d_2}(\mathcal{B}_{d_1}^{(i)} \times \mathcal{C}_{d_2}^{(i)})| = \frac{1}{[G'_{d_1 d_2} : H_{d_1 d_2}]} \alpha_{d_1}^{(i)} \beta_{d_2}^{(i)} \text{Li}(X) + R(X, \mathcal{B}_{d_1}^{(i)} \times \mathcal{C}_{d_2}^{(i)}, K_{d_1 d_2}/K). \quad (4-4)$$

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 $|E_d(\mathcal{B}_d^{(i)})|$ 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 $B_p \subseteq G_p^{\text{ss}}$, and let

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

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 $gbg^{-1} \in \mathcal{B}'_p$, where $g \in G_p$. Let $T_p \subseteq B_p$ be a maximal torus. Then the commutative diagram appearing Section 3.3 shows that $T_p(\mathbb{F}_p)$ intersects all cosets of I_p . Choose $t \in T_p(\mathbb{F}_p)$ 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 . \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 [27, 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 G_p^{ss} is actually split over \mathbb{F}_p . Indeed, by a result of Serre (cf. [5, Corollary 3.8]), the element $\rho_p(\text{Frob}_v) \in G_p(\mathbb{Q}_p)$ 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 G_p over \mathbb{Q}_p , which also implies G_p^{ss} is split.

Fix a faithful representation $G_p^{ss} \hookrightarrow \text{GL}_N$ 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 $\text{GL}_N(\mathbb{F}_p)$. Write the derived series of R_N as

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

Then a standard calculation shows that

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

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

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

Then we have a normal series $S_k \triangleright S_{k,1} \triangleright \cdots \triangleright S_{k,k-1} = S_{k-1}$ 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. \square

Proposition 4.12. *For each prime p , let*

$$N_p = |\mathbf{G}_p^{ss}(\mathbb{F}_p)| \cdot |\mathbf{B}_p(\mathbb{F}_p)|^{-\frac{1}{2}}. \tag{4-5}$$

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

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

Proof. Applying [Theorem 4.8](#) to the extension $l/k = K_d/K$ with the subgroup $H = B'_d$ gives the error term

$$\begin{aligned} |R(X, \mathcal{B}_d^{(i)}, K_d/K)| &\ll (|\mathcal{B}_d^{(i)}| \cdot [G'_d : B'_d])^{\frac{1}{2}} n_K X^{\frac{1}{2}} (\log X + \log M(K_d/K)) \\ &\leq (|G_d| \cdot [G_d : B_d])^{\frac{1}{2}} n_K X^{\frac{1}{2}} (\log X + \log M(K_d/K)) \\ &= \prod_{p|d} N_p \cdot n_K X^{\frac{1}{2}} (\log X + \log M(K_d/K)). \end{aligned}$$

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

$$\begin{aligned} \log M(K_d/K) &= \log|G'_d| + \frac{\log(\Delta_K)}{n_K} + \sum_{p|d} \log p + \sum_{p|\Delta_A} \log p \\ &\leq \sum_{p|d} \log|\mathbf{G}_p^{\text{ss}}(\mathbb{F}_p)| + \log d + O_{A,K}(1) \\ &\ll_{A,K} \log d, \end{aligned}$$

where in the final estimate we used the trivial bound $|\mathbf{G}_p^{\text{ss}}(\mathbb{F}_p)| \leq |\text{GSp}_{2g}(\mathbb{F}_p)|$. □

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 \mathfrak{d} , then*

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

Proof. We have the equality

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

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 $E_{\mathfrak{d}}(\mathcal{B}_{\mathfrak{d}}^{(i)})$ already forces the Frobenius element to be in this coset (cf. [Remark 4.4](#)).

The principle of inclusion-exclusion now gives

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

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 $\text{Li}(X)$ is given by

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

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

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}^{ss} its semisimple quotient. Put*

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

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 ,*

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

Proof. In view of Lemma 3.5 we may replace \mathbf{G}_p^{ss} with \mathbf{G}_p^{sc} in the definition of N_p . The base change $(\mathbf{G}_p^{\text{sc}})_{/\mathbb{F}_p}$ 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, and each of them is obtained from a Chevalley group over \mathbb{Z} by base change.

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

$$|\mathbf{G}_p^{\text{sc}}(\mathbb{F}_p)| = \sum_{i=0}^{2 \dim \mathbf{G}_p^{\text{sc}}} (-1)^i \text{Tr}(F, H_c^i((\mathbf{G}_p^{\text{sc}})_{/\mathbb{F}_p}, \mathbb{Q}_\ell))$$

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

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

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

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

for all primes p .

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

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 have⁷ $G_{p/\mathbb{Q}_p} \subseteq G \times_{\mathbb{Q}} \mathbb{Q}_p$.*

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

$$\dim G_p^{ss} - \frac{1}{2} \dim B_p \leq \frac{1}{4} (3 \dim G^{ss} - \text{rank } G^{ss}).$$

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 B_p is a Borel subgroup of G_p^{ss} . Let N_p be its unipotent radical. We have the relations

$$\dim G_p^{ss} = 2 \dim B_p - \text{rank } G_p^{ss} = \dim B_p + \dim N_p.$$

Rearranging this, we get

$$\dim G_p^{ss} - \frac{1}{2} \dim B_p = \frac{1}{4} (3 \dim G_p^{ss} - \text{rank } G_p^{ss}) = \frac{1}{2} \dim G_p^{ss} + \frac{1}{2} \dim N_p.$$

It remains to show that $\dim G_p^{ss} \leq \dim G^{ss}$ and $\dim N_p \leq \dim N$.

The previous theorem gives an embedding $G_p \subseteq G$ of reductive groups, and hence the inclusion of the derived subgroups $G_p^{\text{der}} \subseteq G^{\text{der}}$. 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 N_p is again a unipotent subgroup, so it lies in a conjugate of N . \square

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 \mathfrak{N} , then*

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

Proof. Let $P(T) \in \mathbb{Z}[T]$ be the characteristic polynomial of $\rho_p(\text{Frob}_v)$. Let $\alpha_1, \dots, \alpha_{2g}$ be the roots of $P(T)$, then $F(A, v)$ is the compositum 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 $q = N_{K/\mathbb{Q}v}$. Then all the roots of $P(T)$ have complex absolute value $q^{\frac{1}{2}}$, so

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

Combining the two inequalities above gives the claim. \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 $\gamma = \frac{1}{4} (3 \dim G^{ss} - \text{rank } G^{ss})$ from [Proposition 4.14](#).

⁷Recall that we are assuming all monodromy groups are connected.

Proof. Fix $\varepsilon > 0$; then [Proposition 4.5](#) gives an equality

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

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 $\mathcal{P}^{(d)}$, and excluded subsets $\mathcal{A}_p = E_{dp}(\mathcal{B}_d^{(i)} \times \mathcal{C}_p^{(i)})$. By combining [Propositions 4.13](#) and [4.14](#), we get the estimate

$$\begin{aligned} |\mathcal{A}_d| &= \left| \bigcap_{p|d} E_{dp}(\mathcal{B}_d^{(i)} \times \mathcal{C}_p^{(i)}) \right| = \frac{1}{|\mathcal{I}|} \alpha_d^{(i)} \beta_d^{(i)} \text{Li}(X) + O_{A,K}((2C)^{\omega(d)} d^\gamma X^{\frac{1}{2}} (\log X + \log d)) \\ &= \frac{1}{|\mathcal{I}|} \alpha_d^{(i)} \beta_d^{(i)} \text{Li}(X) + O_{A,K,\varepsilon}(d^{\gamma+\varepsilon} X^{\frac{1}{2}} (\log X + \log d)). \end{aligned}$$

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

$$\begin{aligned} &\left| E_d(\mathcal{B}_d^{(i)}) - \bigcup_{p \in \mathcal{P}^{(d)}} E_{dp}(\mathcal{B}_d^{(i)} \times \mathcal{C}_p^{(i)}) \right| \\ &\ll_{A,K,\varepsilon} \frac{1}{|\mathcal{I}|} \alpha_d^{(i)} \cdot \frac{\text{Li}(X)}{\pi_{\mathcal{P}^{(d)}}(z)} + \left(\frac{z^{1+\varepsilon}}{\pi_{\mathcal{P}^{(d)}}(z)} \right)^2 X^{\frac{1}{2}} \sum_{\substack{d_1, d_2 \leq z \\ d_1, d_2 \in \mathcal{R}^{(d)}}} \frac{[d_1, d_2]^{\gamma+\varepsilon}}{d_1 d_2} (\log X + \log[d_1, d_2]). \end{aligned}$$

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,

$$\begin{aligned} \sum_{\substack{d_1, d_2 \leq z \\ d_1, d_2 \in \mathcal{R}^{(d)}}} \frac{[d_1, d_2]^{\gamma+\varepsilon}}{d_1 d_2} (\log X + \log[d_1, d_2]) &\leq \sum_{d_1, d_2 \leq z} (d_1 d_2)^{\gamma-1+\varepsilon} (\log X + 2 \log z) \\ &= (\log X + 2 \log z) \left(\sum_{d \leq z} d^{\gamma-1+\varepsilon} \right)^2 \\ &\ll_\gamma z^{2\gamma+2\varepsilon} (\log X + \log z), \end{aligned}$$

which gives

$$\left| E_d(\mathcal{B}_d^{(i)}) - \bigcup_{p \in \mathcal{P}^{(d)}} E_{dp}(\mathcal{B}_d^{(i)} \times \mathcal{C}_p^{(i)}) \right| \ll_{A,K,\varepsilon} \frac{X}{\pi_{\mathcal{P}^{(d)}}(z)} + \left(\frac{z^{1+\varepsilon}}{\pi_{\mathcal{P}^{(d)}}(z)} \right)^2 X^{\frac{1}{2}} z^{2\gamma+2\varepsilon} \log(Xz). \quad (4-6)$$

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

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

By the effective Chebotarev theorem ([Theorem 4.7](#), also cf. [[29](#), equation (14_R)]), we have

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

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

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

Substituting this in (4-6) and summing over all $i \in \mathcal{I}$ gives the desired result. \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 nonabelian Lie-extensions $\{K_d/K\}$. There are some works when the Galois group is fixed (cf. [[25](#)]), but we are not aware of any work in our setting.

Acknowledgements

We thank Brian Conrad, Chun-Yin Hui, Chandrashekhara Khare, Vijay Patankar, Will Sawin and Victor Wang for helpful communications. We are grateful to the referee for valuable comments and suggestions.

References

- [1] S. Bloom, “The square sieve and a Lang–Trotter question for generic abelian varieties”, *J. Number Theory* **191** (2018), 119–157. [MR](#)
- [2] A. Borel, *Linear algebraic groups*, 2nd ed., Graduate Texts in Mathematics **126**, Springer, 1991. [MR](#)
- [3] A. Borel and J. Tits, “Groupes réductifs”, *Inst. Hautes Études Sci. Publ. Math.* **27** (1965), 55–150. [MR](#)
- [4] R. W. Carter, *Finite groups of Lie type: Conjugacy classes and complex characters*, Wiley, New York, 1985. [MR](#)
- [5] W. C. Chi, “ l -adic and λ -adic representations associated to abelian varieties defined over number fields”, *Amer. J. Math.* **114**:2 (1992), 315–353. [MR](#)
- [6] A. C. Cojocaru and C. David, “Frobenius fields for Drinfeld modules of rank 2”, *Compos. Math.* **144**:4 (2008), 827–848. [MR](#)
- [7] A. C. Cojocaru and C. David, “Frobenius fields for elliptic curves”, *Amer. J. Math.* **130**:6 (2008), 1535–1560. [MR](#)
- [8] A. C. Cojocaru and M. R. Murty, *An introduction to sieve methods and their applications*, London Math. Soc. Student Texts **66**, Cambridge University Press, 2006. [MR](#)
- [9] A. C. Cojocaru, E. Fouvry, and M. R. Murty, “The square sieve and the Lang–Trotter conjecture”, *Canad. J. Math.* **57**:6 (2005), 1155–1177. [MR](#)
- [10] P. Deligne, “Hodge cycles on abelian varieties”, pp. 9–100 in *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Math. **900**, Springer, 1982.
- [11] G. Henniart, “Représentations l -adiques abéliennes”, pp. 107–126 in *Seminar on Number Theory* (Paris, 1980/1981), Progr. Math. **22**, Birkhäuser, Boston, 1982. [MR](#)

- [12] H. Hida, *Elliptic curves and arithmetic invariants*, Springer, 2013. [MR](#)
- [13] C. Y. Hui and M. Larsen, “Maximality of Galois actions for abelian and hyper-Kähler varieties”, *Duke Math. J.* **169**:6 (2020), 1163–1207. [MR](#)
- [14] L. Illusie, “Independence of families of l -adic representations and uniform constructibility (after J.-P. Serre)”, prenotes for talks at the University of Tokyo, 2010, available at <https://tinyurl.com/Illusie-Independence>.
- [15] J. Jouve, K. Kowalski, and D. Zywinia, “Splitting fields of characteristic polynomials of random elements in arithmetic groups”, *Israel J. Math.* **193**:1 (2013), 263–307.
- [16] C. Khare, “ F -split Galois representations are potentially abelian”, *Proc. Amer. Math. Soc.* **131**:10 (2003), 3021–3023. [MR](#)
- [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** (2016), 87–102. [MR](#)
- [18] J. C. Lagarias and A. M. Odlyzko, “Effective versions of the Chebotarev density theorem”, pp. 409–464 in *Algebraic number fields: L -functions and Galois properties* (Durham, 1975), Academic Press, 1977. [MR](#)
- [19] S. Lang, “Algebraic groups over finite fields”, *Amer. J. Math.* **78** (1956), 555–563. [MR](#)
- [20] S. Lang and H. Trotter, *Frobenius distributions in GL_2 -extensions*, Lecture Notes in Mathematics **504**, Springer, 1976. [MR](#)
- [21] M. Larsen, “Maximality of Galois actions for compatible systems”, *Duke Math. J.* **80**:3 (1995), 601–630. [MR](#)
- [22] M. Larsen and R. Pink, “Abelian varieties, l -adic representations, and l -independence”, *Math. Ann.* **302**:3 (1995), 561–579. [MR](#)
- [23] A. Lubotzky and L. Rosenzweig, “The Galois group of random elements of linear groups”, *Amer. J. Math.* **136**:5 (2014), 1347–1383. [MR](#)
- [24] M. R. Murty, V. K. Murty, and N. Saradha, “Modular forms and the Chebotarev density theorem”, *Amer. J. Math.* **110**:2 (1988), 253–281. [MR](#)
- [25] 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 (2020), 701–778. [MR](#)
- [26] R. Pink, “ l -adic algebraic monodromy groups, cocharacters, and the Mumford–Tate conjecture”, *J. Reine Angew. Math.* **495** (1998), 187–237. [MR](#)
- [27] W. R. Scott, *Group theory*, Prentice-Hall, Englewood Cliffs, NJ, 1964. [MR](#)
- [28] J.-P. Serre, *Abelian l -adic representations and elliptic curves*, W. A. Benjamin, 1968. [MR](#)
- [29] J.-P. Serre, “Quelques applications du théorème de densité de Chebotarev”, *Publications Mathématiques de l’IHÉS* **54** (1981), 123–201. [MR](#)
- [30] J.-P. Serre, “Lettres à Ken Ribet du 1/1/1981 et du 29/1/1981”, item 133, pp. 1–20 in *Œuvres = Collected papers*, vol. IV, 1985–1998, Springer, 2000. [MR](#)
- [31] J.-P. Serre, “Lettre à Ken Ribet du 7/3/1986”, item 138, pp. 56–65 in *Œuvres = Collected papers*, vol. IV, 1985–1998, Springer, 2000. [MR](#)
- [32] J.-P. Serre, *Galois cohomology*, Springer, 2002. [MR](#)
- [33] J.-P. Serre, “Un critère d’indépendance pour une famille de représentations ℓ -adiques”, *Comment. Math. Helv.* **88**:3 (2013), 541–554. [MR](#)
- [34] M. Demazure and A. Grothendieck, *Schémas en groupes, II: Groupes de type multiplicatif, et structure des schémas en groupes généraux* (Séminaire de Géométrie Algébrique du Bois Marie 1962–1964), Lecture Notes in Math. **152**, Springer, 1970. [MR](#)
- [35] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series **46**, Princeton University Press, 1998. [MR](#)
- [36] J.-P. Wintenberger, “Démonstration d’une conjecture de Lang dans des cas particuliers”, *J. Reine Angew. Math.* **553** (2002), 1–16. [MR](#)
- [37] Y. Zarhin, “Two-dimensional families of hyperelliptic Jacobians with big monodromy”, *Trans. Amer. Math. Soc.* **368**:5 (2016), 3651–3672. [MR](#)

- [38] D. Zywina, “[Bounds for the Lang–Trotter conjectures](#)”, pp. 235–256 in *SCHOLAR—a scientific celebration highlighting open lines of arithmetic research*, Contemp. Math. **655**, Amer. Math. Soc., 2015. [MR](#)

Communicated by Philippe Michel

Received 2024-06-22 Revised 2025-01-14 Accepted 2025-03-03

ashayburungale@gmail.com

*Department of Mathematics, University of Texas at Austin, Austin, TX,
United States*

hharuzo@gmail.com

*Department of Mathematics, University of California, Los Angeles,
Los Angeles, CA, United States*

shilinl@umich.edu

*Department of Mathematics, University of Michigan, Ann Arbor, MI,
United States*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Antoine Chambert-Loir
Université Paris-Diderot
France

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Jason P. Bell	University of Waterloo, Canada	Philippe Michel	École Polytechnique Fédérale de Lausanne
Bhargav Bhatt	University of Michigan, USA	Martin Olsson	University of California, Berkeley, USA
Frank Calegari	University of Chicago, USA	Irena Peeva	Cornell University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Saclay, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	Duke University, USA	Bjorn Poonen	Massachusetts Institute of Technology, USA
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	SUNY Buffalo, USA
Wee Teck Gan	National University of Singapore	Shunsuke Takagi	University of Tokyo, Japan
Andrew Granville	Université de Montréal, Canada	Pham Huu Tiep	Rutgers University, USA
Ben J. Green	University of Oxford, UK	Ravi Vakil	Stanford University, USA
Christopher Hacon	University of Utah, USA	Akshay Venkatesh	Institute for Advanced Study, USA
Roger Heath-Brown	Oxford University, UK	Melanie Matchett Wood	Harvard University, USA
János Kollár	Princeton University, USA	Shou-Wu Zhang	Princeton University, USA
Michael J. Larsen	Indiana University Bloomington, USA		

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2026 is US \$590/year for the electronic version, and \$865/year (+\$75, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 2000 Allston Way # 59, Berkeley, CA 94701-4004, is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2026 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 20 No. 3 2026

Ramified descent and transcendental Brauer–Manin obstruction	419
JULIAN LAWRENCE DEMEIO	
Logarithmic base change theorem and smooth descent of positivity of log canonical divisor	445
SUNG GI PARK	
Chevalley formulae for motivic Chern classes of Schubert cells and for stable envelopes	477
LEONARDO C. MIHALCEA, HIROSHI NARUSE and CHANGJIAN SU	
The Mahler measure of exact polynomials in three variables	525
TRIEU THU HA	
On the Frobenius fields of abelian varieties over number fields	577
ASHAY A. BURUNGALE, HARUZO HIDA and SHILIN LAI	
Galois groups of reciprocal polynomials and the van der Waerden–Bhargava theorem	603
THERESA C. ANDERSON, ADAM BERTELLI and EVAN M. O’DORNEY	