COMPOSITIO MATHEMATICA

Height functions on Hecke orbits and the generalised André–Pink–Zannier conjecture

Rodolphe Richard and Andrei Yafaev

Compositio Math. **160** (2024), 2531–2584.

doi:10.1112/S0010437X2400722X

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY
EST. 1865

Check for updates

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Compositio Math. 160 (2024) 2531–2584
doi:10.1112/S0010437X2400722X

Height functions on Hecke orbits and the generalised André–Pink–Zannier conjecture

Rodolphe Richard and Andrei Yafaev

Abstract

We introduce and study the notion of a generalised Hecke orbit in a Shimura variety. We define a height function on such an orbit and study its properties. We obtain lower bounds for the sizes of Galois orbits of points in a generalised Hecke orbit in terms of this height function, assuming the 'weakly adelic Mumford–Tate hypothesis' and prove the generalised André–Pink–Zannier conjecture under this assumption, using Pila–Zannier strategy.

Contents

Received 14 December 2021, accepted in final form 24 January 2024, published online 19 November 2024.
2020 Mathematics Subject Classification 03C64, 11F80, 11G18, 11G50, 14G35 (primary), 14L30, 15A16, 20G35 secondary.
Keywords: Shimura varieties, Hecke orbits, Zilber–Pink, heights, Siegel sets, Mumford–Tate conjecture, Adelic linear groups.

1. Introduction

In this paper, we study the generalised André–Pink–Zannier conjecture for all Shimura varieties, whose statement is as follows.

Conjecture 1.1 (Generalised André–Pink–Zannier). Let S be a Shimura variety and Σ a subset of a generalised Hecke orbit in S. Then the irreducible components of the Zariski closure of Σ are weakly special subvarieties.

We refer to [Del71, Del79] for notions and notation concerning Shimura data and Shimura varieties. We refer to [UY11, Definition 2.1] for definitions and properties of weakly special subvarieties. We refer to Definition 2.1 or § 1.1 for the notion of *generalised* Hecke orbits.

1.1 Main result

Let (G, X) be a Shimura datum, let $K \leq G(\mathbb{A}_f)$ be a compact open subgroup, and let $S = Sh_K(G, X) = G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K$ be the associated Shimura variety. Let $x_0 \in X$ and denote by $M \leq G$ its Mumford–Tate group. Let $s_0 := [x_0, 1] \in S$.

The *generalised Hecke orbit of* x_0 *in* X (see § 2.1) is the set $\mathcal{H}(x_0)$ of the $\phi \circ x_0$, where $\phi : M \to G$ ranges through the morphisms of $\mathbb{Q}$-algebraic groups such that $\phi \circ x_0 \in X$. The *generalised Hecke orbit of* s_0 *in* S is $\mathcal{H}(s_0) := G(\mathbb{Q})\backslash\mathcal{H}(x_0) \times G(\mathbb{A}_f)/K \subseteq S$. For a sufficiently large field E of finite type over $\mathbb{Q}$ we have the following (see § 3.1): S and s_0 are defined over E and there exists a Galois representation $\rho_{x_0} : Gal(\overline{E}/E) \to M(\mathbb{A}_f) \cap K$ such that

$$\forall\, \sigma \in Gal(\overline{E}/E),\ g \in G(\mathbb{A}_f), \quad \sigma([x_0, g]) = [x_0, \rho_{x_0}(\sigma) \cdot g].$$

The main result of this paper is the following.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Theorem 1.2. *We consider the above situation. We assume the weakly adelic Mumford–Tate hypothesis (see § 6.3), which states that, with* $U := \rho_{x_0}(Gal(\overline{E}/E)) \subseteq M(\mathbb{A}_f) \cap K$*:*

$$\exists C > 0,\ \forall p,\ [K \cap M(\mathbb{Q}_p) : U \cap M(\mathbb{Q}_p)] \leq C. \tag{1}$$

Then, for any subset $\Sigma \subseteq \mathcal{H}(s_0)$*, every irreducible component of* $\overline{\Sigma}^{\mathrm{Zar}}$ *is weakly special.*

Our 'weakly adelic Mumford–Tate hypothesis' is weaker than the adelic form of the Mumford–Tate conjecture [Ser94b, 11.4?] stated by Serre. Here are some instances in which above Theorem 1.2 implies Conjecture 1.1 unconditionally.

Combining Theorem 1.2 with Lemma 6.12, one recovers the following.

Theorem 1.3 [EY03, KY14]. *Conjecture 1.1 is true if* Σ *contains a special point.*

Combining Theorem 1.2 with with [CM20, Theorem A (i)] we have the following, which strictly contains a 2005 result of Pink [Pin05, § 7] (and [CK16, Theorem B]).

Theorem 1.4. *Conjecture 1.1 is true if* S *is of abelian type, and* Σ *contains a point* s *which satisfies the Mumford–Tate conjecture (at some* ℓ*, in the sense of [UY13]).*

The assumptions of Theorem 1.4 are satisfied in the case where $S = \mathcal{A}_g$ and Σ contains a point $[A]$, where the abelian variety A satisfies the Mumford–Tate conjecture (at some prime ℓ). Examples of such abelian varieties are: when $\dim(A) \leq 3$; or when $\dim(A)$ is odd and $\mathrm{End}(A) \simeq \mathbb{Z}$. More examples were given in [Pin98], and many examples are mentioned in [Lom16, § 2.4].

The assumptions of Theorem 1.4 are also satisfied for 'most' points in $S(\overline{\mathbb{Q}})$ (with S of abelian type) in the following sense. The subset consisting of the $s \in S(\overline{\mathbb{Q}})$ such that s does not satisfy the Mumford–Tate conjecture is thin in the sense of [Ser97, § 9.1]: this uses a combination of [Ser94a, § 1], [Ser97, § 9] and [CM20, Theorem A (i)] and Theorem 6.18.

For arbitrary Shimura varieties, the hypotheses of Theorem 1.2 are satisfied in the situation of Theorem 6.18. In a sense, our results apply unconditionally to 'most' nonalgebraic points of a Shimura variety. The following are two special cases of Theorem 6.18.

Theorem 1.5. *Conjecture 1.1 is true if* Σ *contains a* $\overline{\mathbb{Q}}$*-Zariski generic point* s *of a special subvariety* $Z \subseteq S$*, namely: for every proper subvariety* $V \subsetneq Z$ *defined over* $\overline{\mathbb{Q}}$*, we have* $s \notin V(\mathbb{C})$*.*

Theorem 1.6. *Conjecture 1.1 is true if* M^{ad} *is* $\mathbb{Q}$*-simple and* Σ *contains a point* s *in* $S(\mathbb{C}) \smallsetminus S(\overline{\mathbb{Q}})$*.*

1.2 History of Conjecture 1.1

Conjecture 1.1 is a special case[1] of the Zilber–Pink conjecture, which has been and continues to be a subject of active research.

Conjecture 1.1 was first formulated (in a special case) in 1989 by André in [And89, Chapter X, § 4.5] (Problem 3). Zannier has considered questions of this type in the context of abelian schemes and tori in [Zan12]. It was then stated in the introduction to the second author's 2000 PhD thesis [Yaf00, bottom of p. 12],[2] following discussions with Bas Edixhoven. Pink, in his 2005 paper [Pin05], has formulated and studied this question.

These authors consider the classical Hecke[3] orbit as in Definition 2.14.

Pink proves the André–Pink–Zannier conjecture for 'Galois generic' points of $\mathcal{A}_g$. These points are Hodge generic, by [CK16, Proposition 6.2.1]. Pink's method uses equidistribution of Hecke

[1] We refer to [Orr15], proof of Lemma 2.2, for the argument, which applies to our generalised setting.

[2] The statement there uses the terminology 'totally geodesic subvarieties' instead of 'weakly special', but Moonen had proved in [Moo98] that the two notions are equivalent.

[3] Where André uses $G(\mathbb{Q})$, Pink uses $\mathrm{Aut}(G)(\mathbb{Q})$ instead of $G(\mathbb{Q})$ in Definition 2.14.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

points (by Clozel, Oh, and Ullmo: [COU01]; cf. also [EO06]). This was generalised to Galois generic points in arbitrary Shimura varieties in 2016 [CK16]. This was also contained in the first author's 2009 thesis under a weaker assumption [Ric09, Ch. III § 7, p. 59, Corollary 7.1].

In the case of generalised[4] Hecke orbits *of special points*, the articles [EY03, KY14] use a method of Edixhoven. This method is inapplicable in more general cases, for instance the case of the Hecke orbit of a *Hodge generic* point.

A real breakthrough on this problem was the introduction of the Pila–Zannier strategy which uses o-minimality and functional transcendence. It has now become the most powerful approach to all problems of Zilber–Pink type. This method was applied by Orr in [Orr15], who considered the case of curves in $\mathcal{A}_g$, the moduli space of principally polarised abelian varieties. His approach relies on Masser–Wüstholz isogeny estimates. Therefore, it is limited to Shimura varieties of abelian type, and cannot be applied to *generalised* Hecke orbits. For Shimura varieties of abelian type, Orr was able to prove the conjecture for 'S-adic Hecke orbits'[5] for a finite set of primes S, and for points which are Hodge generic (without the Galois generic assumption).

In the case of S-adic Hecke orbits, a stronger form of the conjecture, involving topological closure and equidistribution, was proved, in the abelian case, in [RY19] using ergodic theory approach relying on p-adic Ratner's theorems.

1.3 Main technical results

After choosing bases of the Lie algebras $\mathfrak{m}$ of M and $\mathfrak{g}$ of G, we associate to $\phi \in \mathrm{Hom}(M, G)$ its 'finite height' $H_f(\phi)$, defined as the lowest common multiple of the denominators of the coefficients of the matrix of $d\phi$. More generally, for $g \in G(\mathbb{A}_f)$, we define $H_f(g^{-1} \cdot \phi \cdot g)$ as the smallest $n \in \mathbb{Z}_{\geq 1}$ such that the matrix of $g^{-1} \cdot d\phi \cdot g$ has coefficients in $(1/n) \cdot \widehat{\mathbb{Z}}$.

1.3.1 A first crucial result is the following. We choose the bases of $\mathfrak{g}$ and $\mathfrak{m}$ constructed in § 4.3. Then the function

$$[\phi \circ x_0, g] \mapsto H_f(g^{-1} \cdot \phi \cdot g)$$

is well defined on the generalised Hecke orbit, and $Gal(\overline{E}/E)$-invariant.

1.3.2 Our most important technical result is an estimate on the size of Galois orbits in a generalised Hecke orbit.

The following definition is used throughout this article.

Definition 1.7. Let A be a set and $f, g : A \to \mathbb{R}_{\geq 0}$ two functions.

(i) We say that f *polynomially dominates* g, and write $g \preccurlyeq f$, if there exist $a, b, c \in \mathbb{R}_{>0}$ such that

$$\forall\, x \in A,\ g(x) \leq c + a f(x)^b.$$

(ii) We say that f and g are *polynomially equivalent*, and write $f \approx g$, if $f \preccurlyeq g$ and $g \preccurlyeq f$.

As functions on the generalised Hecke orbit $\mathcal{H}(s_0)$, we have the polynomial equivalence

$$\#Gal(\overline{E}/E) \cdot [\phi \circ x_0, g] \approx H_f(g^{-1} \cdot \phi \cdot g).$$

[4] They used a generalised notion of Hecke orbit, formulated using auxiliary linear representations; but using Proposition 2.15 and Theorem 2.4, this leads to a statement equivalent to our Conjecture 1.1.

[5] He considers Hecke correspondences whose level has only prime factors in S. This corresponds to isogenies of abelian varieties whose degree has prime factors only from S.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

1.3.3 Another essential technical result, from § 5, is the following. See the introduction in § 5 for the importance of this result in our approach to Conjecture 1.1.

Denote by ϕ_0 the inclusion monomorphism $M \hookrightarrow G$. Let W be the conjugacy class $G \cdot \phi_0 \subseteq \mathrm{Hom}(M, G)$, viewed as an algebraic variety over $\mathbb{Q}$. The usual height of the matrix of $d\phi$ defines an affine Weil height function H_W on $W(\mathbb{Q})$ (cf. (15) and (18)). Let $\mathfrak{S} \subseteq G(\mathbb{R})$ be a finite union of Siegel sets and $\mathfrak{S} \cdot \phi_0$ be its image in $W(\mathbb{R})$.

The main result 5.16 of § 5 is that, as functions of $\phi \in W(\mathbb{Q}) \cap \mathfrak{S} \cdot \phi_0$, we have

$$H_f(\phi) \approx H_W(\phi).$$

We note that every point of the geometric Hecke orbit can be written as $[\phi \circ x_0, g]$ with $g \in G(\mathbb{A}_f)$ and $\phi \in W(\mathbb{Q}) \cap \mathfrak{S} \cdot \phi_0$, provided $\mathfrak{S} \subseteq G(\mathbb{R})$ is a fundamental set.

1.4 Outline of the strategy

The proof of Theorem 1.2 is given in § 7. The technical results of § 1.3 play a crucial role in our approach. Let us outline our approach.

We reduce Conjecture 1.1 to the case where $V := \overline{\Sigma} = \overline{\{s_0; s_1; \ldots\}}$ is irreducible, G is adjoint and V is Hodge generic in S. We rely on functoriality properties (§ 2.2) of geometric and generalised Hecke orbits.[6] Theorem 2.4 allows us to use geometric and generalised Hecke orbits interchangeably. We also rely on the functoriality properties (see § 6.3) of the assumption (1).

The final objective of the proof is to apply the geometric part of the André–Oort conjecture [Ull14] (or [RU24]), and use induction on the number of simple factors of M^{ad}. For every n large enough, we construct a weakly special subvariety $Z_n \subseteq V$ of non-zero dimension such that $s_n \in Z_n$. Then [Ull14, RU24] describes $\overline{\bigcup Z_n}$, and we deduce Conjecture 1.1.

In order to construct the non-zero-dimensional Z_n, we use the Pila–Zannier strategy. By (3), we identify $\mathcal{H}(s_0)$ with a subset of $W(\mathbb{Q})$ where $W = G \cdot \phi_0 \simeq G/Z_G(M)$ is the algebraic variety of § 1.3.3.

Let $\pi : G(\mathbb{R}) \to X \to S$ be the uniformisation map, and $\mathfrak{S} \subseteq G(\mathbb{R})$ is a finite union of Siegel sets such that $S = \pi(\mathfrak{S})$. The goal is to apply the variant Theorem 7.1 of Pila–Wilkie theorem, after constructing many rational points of small height in the set

$$\tilde{V} = \big(\overset{-1}{\pi}(V) \cap \mathfrak{S}\big)/Z_{G(\mathbb{R})}(M) \subseteq W(\mathbb{R}),$$

which is definable in the o-minimal structure $\mathbb{R}_{an,\exp}$.

Let E be field of definition of V. Then V contains the Galois orbits $Gal(\overline{E}/E) \cdot s_n$.

We introduce

$$Q_n := \{\phi \in \mathfrak{S} \cdot \phi_0 \cap W(\mathbb{Q}) : [\phi \circ x_0 : 1] \in Gal(\overline{E}/E) \cdot s_n\} \subseteq \tilde{V}.$$

Denote by p the map $G(\mathbb{R}) \cdot \phi_0 \to X$, where $G(\mathbb{R}) \cdot \phi_0 \subseteq W(\mathbb{R})$. Each point $s' \in Gal(\overline{E}/E) \cdot s_n$ lifts to a rational point $\widetilde{s'} \in \tilde{V} \cap W(\mathbb{Q})$. We have surjections $Q_n \to p(Q_n) \to Gal(\overline{E}/E) \cdot s_n$. Thus, $\#Q_n \geq \#Gal(\overline{E}/E) \cdot s_n$.

By § 1.3.1, the value of H_f is constant as ϕ ranges through Q_n. By § 1.3.3, we also have $H_f(\phi) \approx H_W(\phi)$. By § 1.3.2, we have $\#Q_n \geq \#Gal(\overline{E}/E) \cdot s_n \approx H_f(\widetilde{s_n}) \approx H_W(\widetilde{s_n})$.

Thus, $\tilde{V}$ contains $\#Q_n \approx H_W(\widetilde{s_n})$ points of height $\approx H_W(\widetilde{s_n})$.

By Theorem 7.1, for sufficiently large n, there exist ϕ_n in Q_n such that $p(\phi_n) \in Z^{\mathrm{alg}}$, with $Z = p(\tilde{V})$. By the Ax–Lindemann–Weierstrass theorem [KUY16], it follows that $s'_n = [\phi_n, 1] \in Z_n \subseteq V$, for a non-zero-dimensional weakly special subvariety Z_n. Using Galois action, we may assume $s'_n = s_n$.

This concludes the proof of Theorem 1.2.

[6] This avoids one difficulty in the approach [Orr15] of Orr.

1.5 Summary of the sections

In § 2, we introduce and study generalised and geometric Hecke orbits. In § 3, we recall properties of the representations $\rho_{x_0} : Gal(\overline{E}/E) \to M(\mathbb{A}_f)$, and we relate Galois orbits to orbits of $U = \rho_{x_0}(Gal(\overline{E}/E))$. In § 4, we make precise and prove § 1.3.1. Section 5 deals with § 1.3.2. In § 6, we introduce and study the weakly adelic Mumford–Tate hypothesis, and establish the estimates from § 1.3.3. This relies on general estimates on adelic orbits, given in the appendices. The content of § 7 was outlined in § 1.4.

2. Generalised and geometric Hecke orbits

In this section we define the notions of *generalised Hecke orbit* and of *geometric Hecke orbit*, and study their properties. The heart of this section is Theorem 2.4, which implies, in particular, that generalised and geometric Hecke orbits can be used interchangeably in the statement of Conjecture 1.1.

These notions are naturally compatible with various operations on Shimura data. In particular, we prove several statements which will be important in reducing Conjecture 1.1 to the case where the Shimura variety is of adjoint type and Σ is Hodge generic in S.

Finally, § 2.5 compares our notions to different notions of generalised Hecke orbits found in the literature.

2.1 Definitions

Let (G, X) be a Shimura datum. We always assume, as in [UY14], that our Shimura datum is normalised so that G is the generic Mumford–Tate group of X.

Let x_0 be a point of X and let $M \leq G$ be the Mumford–Tate group of x_0. Recall that x_0 is a morphism $\mathbb{S} := \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(GL(1)) \longrightarrow G_{\mathbb{R}}$ and that $M = x_0(\mathbb{S})^{Zar,\mathbb{Q}}$ is the smallest $\mathbb{Q}$-algebraic subgroup of G containing $x_0(\mathbb{S})$. In the rest of the paper we denote the identity monomorphism $M \hookrightarrow G$ by ϕ_0.

In the following definition $\mathrm{Hom}(M, G)$ denotes the set of algebraic group morphisms *defined over* $\mathbb{Q}$.

Definition 2.1 (Generalised Hecke orbit). We define the *Generalised Hecke orbit* $\mathcal{H}(x_0)$ of x_0 *in* X as

$$\mathcal{H}(x_0) := X \cap \{\phi \circ x_0 : \phi \in \mathrm{Hom}(M, G)\}.$$

Let $X_M = M(\mathbb{R}) \cdot x_0 \subset X$. Then (M, X_M) is a Shimura datum, and $\phi \in \mathrm{Hom}(M, G)$ such that $\phi \circ x_0 \in X$ are precisely those giving rise to a morphism of Shimura data $(M, X_M) \to (G, X)$. In particular, $\phi(X_M) \subseteq X$.

Let K be a compact open subgroup of $G(\mathbb{A}_f)$ and $\mathrm{Sh}_K(G, X)$ be the Shimura variety associated to these data. There is a natural map

$$X \times G(\mathbb{A}_f) \longrightarrow \mathrm{Sh}_K(G, X)$$

and we denote the image of a point (x, g) by $[x, g]$.

Definition 2.2. We define the *generalised Hecke orbit* $\mathcal{H}([x_0, g_0])$ of $[x_0, g_0]$ *in* $\mathrm{Sh}_K(G, X)$ by

$$\mathcal{H}([x_0, g_0]) := \{[x, g] : x \in \mathcal{H}(x_0), g \in G(\mathbb{A}_f)\}.$$

Let $W = G \cdot \phi_0$ be the conjugacy class of ϕ_0 which we view as an algebraic variety defined over $\mathbb{Q}$. Denoting by $Z_G(M)$ the centraliser of M in G, we will identify $G/Z_G(M) \simeq W$. The

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

set $W(\overline{\mathbb{Q}})$ is the $G(\overline{\mathbb{Q}})$-conjugacy class of ϕ_0 in $\mathrm{Hom}(M_{\overline{\mathbb{Q}}}, G_{\overline{\mathbb{Q}}})$, and the points in $W(\mathbb{Q})$ are the $\mathbb{Q}$-defined homomorphisms $\phi \in \mathrm{Hom}(M, G)$ which are conjugated to ϕ_0 by elements of $G(\overline{\mathbb{Q}})$.

In Definition 2.1, if we replace $\mathrm{Hom}(M, G)$ by its subset $W(\mathbb{Q})$, we obtain a more restrictive definition: that of a *geometric* Hecke orbit.

Definition 2.3. We define the *geometric Hecke orbit* $\mathcal{H}^g(x_0)$ of x_0 by

$$\mathcal{H}^g(x_0) = X \cap \{\phi \circ x_0 : \phi \in W(\mathbb{Q})\} \subset \mathcal{H}(x_0)$$

and the *geometric Hecke orbit* of $[x_0, g_0]$ by

$$\mathcal{H}^g([x_0, g_0]) = \{[x, g] : x \in \mathcal{H}^g(x_0), g \in G(\mathbb{A}_f)\}.$$

The main result of this section is the following.

Theorem 2.4. *The generalised Hecke orbit $\mathcal{H}(x_0)$ is a union of finitely many geometric Hecke orbits.*

Lemma 2.5. *Let $\phi, \phi' \in \mathrm{Hom}(M, G)$ (defined over $\mathbb{Q}$) be such that $\phi \circ x_0 = \phi' \circ x_0$. Then $\phi = \phi'$.*

Proof. One can check directly that

$$H := \{m \in M(\mathbb{C}) : \phi(m) = \phi'(m)\}$$

is a subgroup of $M(\mathbb{C})$ (it is the 'equaliser' of ϕ and ϕ'). It is algebraic and defined over $\mathbb{Q}$ because ϕ and ϕ' are. It contains the image $x_0(\mathbb{C})$ by hypothesis. But M is the Mumford–Tate group of x_0: there is no proper $\mathbb{Q}$-algebraic subgroup of M containing $x_0(\mathbb{C})$. Therefore, $H = M$. Thus, $\phi = \phi'$. □

The algebraic variety W is our central object in this article. We will use the notation

$$\begin{aligned} W(\mathbb{R})^+ &= G(\mathbb{R})/Z_G(M)(\mathbb{R}) \\ &= \{\phi \in W(\mathbb{R}) : \phi \circ x_0 \in X\} \end{aligned} \tag{2a}$$

and

$$\begin{aligned} W(\mathbb{Q})^+ &= W(\mathbb{R})^+ \cap W(\mathbb{Q}) \\ &= \{\phi \in W(\mathbb{Q}) : \phi \circ x_0 \in \mathcal{H}^g(x_0)\}. \end{aligned} \tag{2b}$$

The subset $W(\mathbb{R})^+ \subset W(\mathbb{R})$ is a union of some connected components of $W(\mathbb{R})$. With this notation, Lemma 2.5 implies that we have a bijection

$$\begin{aligned} W(\mathbb{Q})^+ &\xrightarrow{\sim} \mathcal{H}^g(x_0) \\ \phi &\mapsto \phi \circ x_0. \end{aligned} \tag{3}$$

2.2 Functoriality of generalised and geometric Hecke orbits

2.2.1 *Restriction to special subvarieties.* The following is a set-theoretic tautology.

Proposition 2.6. *Let (G', X') be a Shimura datum with $M \leq G' \leq G$ and $X_M \subset X' \subset X$, and define $K' = G'(\mathbb{A}_f) \cap K$.*

(i) *Let $\mathcal{H}'(x_0)$ be the generalised Hecke orbit of x_0 viewed as a point of X'. Then*

$$\mathcal{H}'(x_0) = \mathcal{H}(x_0) \cap X'.$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

(ii) *Let $\mathcal{H}'([x_0,1])$ be the generalised Hecke orbit of $[x_0,1]$ viewed as a point of $Sh_{K'}(G',X')$, and S' the image of*

$$f := Sh(\iota) : Sh_{K'}(G',X') \to Sh_K(G,X)$$

where $\iota : G' \to G$ is the inclusion. Then

$$\mathcal{H}([x_0,1]) \cap S' = f(\mathcal{H}'([x_0,1])) \text{ and } \mathcal{H}'([x_0,1]) = \overset{-1}{f}(\mathcal{H}([x_0,1])).$$

The following corollary can be deduced by combining Lemma 2.5 with Theorem 2.4 (it can also be deduced from [Ric67]).

Corollary 2.7. *We keep previous notation. Then*

$$\mathcal{H}^g(x_0) \cap X'$$

is a finite union of geometric Hecke orbits in X'.

Accordingly, $\overset{-1}{f}(\mathcal{H}^g([x_0,1]))$ is the image of finitely many geometric Hecke orbits in $Sh_{K'}(G',X')$.

2.2.2 *Compatibility to products.* A useful property of geometric Hecke orbits is the compatibility with respect to products of Shimura data.

Lemma 2.8. *Let (G,X) be an adjoint Shimura datum, and factor $G = G_1 \times \cdots \times G_f$ as a product of its $\mathbb{Q}$-defined simple normal subgroups, and assume $K = K_1 \times \cdots \times K_f$ for compact open subgroups $K_i \leq G_i(\mathbb{A}_f)$. We use $X = X_1 \times \cdots \times X_f$ to denote the corresponding factorisation, and choose $x_0 = (x_1, \ldots, x_f) \in X_1 \times \cdots \times X_f$. We use $\mathcal{H}^g(x_i)$ to denote the geometric Hecke orbit of x_i with respect to the Shimura datum (G_i, X_i).*

With respect to the corresponding factorisation of Shimura varieties

$$Sh_K(G,X) = Sh_{K_1}(G_1,X_1) \times \cdots \times Sh_{K_f}(G_f,X_f),$$

we have

$$\mathcal{H}^g(x_0) = \mathcal{H}^g(x_1) \times \cdots \times \mathcal{H}^g(x_f).$$

It follows from Lemma 2.8 that, at the level of Shimura varieties,

$$\mathcal{H}^g([x_0,1]) = \mathcal{H}^g([x_1,1]) \times \cdots \times \mathcal{H}^g([x_f,1]).$$

Proof. Since G is adjoint, we have a factorisation

$$X = X_1 \times \cdots \times X_f.$$

Let M be the Mumford–Tate group of x_0 and let $\phi_0 = (\phi_1, \ldots, \phi_f) : M \to G = G_1 \times \cdots \times G_f$ be the inclusion. As the conjugacy class in a product is the product of conjugacy classes, we have

$$G \cdot \phi_0 = G_1 \cdot \phi_1 \times \cdots \times G_f \cdot \phi_f.$$

The Mumford–Tate group of x_i is $M_i := \phi_i(M)$. Because $x_0(\mathbb{S})$ is Zariski dense over $\mathbb{Q}$ in M so is $x_i(\mathbb{S})$ in M_i. Let $\phi_i' : M_i \to G_i$ be the identity map. We can identify $G_i \cdot \phi_i \simeq G_i \cdot \phi_i'$, and have

$$\mathcal{H}^g(x_i) = \{g \cdot \phi_i' \circ x_i : g \in G_i\} \cap X_i = \{g \cdot \phi_i \circ x_i : g \in G_i\} \cap X_i.$$

The rest follows from the definition of geometric Hecke orbits. □

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

2.2.3 *Passing to the adjoint Shimura datum.* The following property is used to reduce the proof of Conjecture 1.1 and Theorem 1.2 to the case where G is adjoint.

LEMMA 2.9. *Let $ad : (G, X) \to (G^{\mathrm{ad}}, X^{\mathrm{ad}})$ be the map of Shimura data*[7] *induced by the natural morphism $ad : G \to G^{\mathrm{ad}}$ and choose a compact open subgroup $K^{\mathrm{ad}} \leq G^{\mathrm{ad}}(\mathbb{A}_f)$ containing $ad(K)$. Let $ad : x \mapsto x^{\mathrm{ad}} := ad \circ x$ be the map $X \to X^{\mathrm{ad}}$ and*

$$Sh(ad) : Sh_K(G, X) \to Sh_{K^{\mathrm{ad}}}(G^{\mathrm{ad}}, X^{\mathrm{ad}})$$

the corresponding morphism of Shimura varieties.

Let $x_0 \in X$. Recall that $\mathcal{H}^g(x_0)$ and $\mathcal{H}^g(x_0^{\mathrm{ad}})$ denote the geometric Hecke orbit of x_0 and x_0^{ad} with respect to G and G^{ad}.

We have

$$ad(\mathcal{H}^g(x_0)) \subseteq ad(X) \cap \mathcal{H}^g(x_0^{\mathrm{ad}}). \tag{4}$$

Lemma 2.9 implies the inclusion

$$ad(\mathcal{H}^g(x_0)) \times G(\mathbb{A}_f) \subseteq \mathcal{H}^g(x_0^{\mathrm{ad}}) \times G^{\mathrm{ad}}(\mathbb{A}_f).$$

Passing to the quotient, we obtain the following.

COROLLARY 2.10. *We have $Sh(ad)(\mathcal{H}^g([x_0, 1])) \subseteq \mathcal{H}^g([x_0^{\mathrm{ad}}, 1])$.*

We now prove Lemma 2.9.

Proof. Choose $x \in \mathcal{H}^g(x_0)$. Clearly $x' := ad(x) \in ad(X) \subset X^{\mathrm{ad}}$.

The Mumford–Tate group of $x_0' := ad(x_0)$ is $M' := ad(M)$. We denote by $\phi_0' \colon M' \to G^{\mathrm{ad}}$ the natural injection. We can write $x = \phi \circ x_0$ with $\phi = g\phi_0 g^{-1}$ and $g \in G(\overline{\mathbb{Q}})$. Then $\phi' := ad(g)\phi_0' ad(g)^{-1}$ is defined over $\mathbb{Q}$ because the map $G \cdot \phi_0 \to G^{\mathrm{ad}} \cdot \phi_0'$ between conjugacy classes is a morphism of varieties defined over $\mathbb{Q}$. One computes $x' = ad(gx_0g^{-1}) = ad(g)ad(x_0)ad(g)^{-1} = \phi' \circ x_0'$, where $x_0' \in X^{\mathrm{ad}}$, and ϕ is defined over $\mathbb{Q}$ and conjugated to ϕ_0' over $\overline{\mathbb{Q}}$; that is, $x' \in \mathcal{H}^g(x_0')$. □

Remarks. In (4), the reverse inclusion is also true, but it is not used in this paper, and its proof is left to the interested reader. The inclusion (4) and the proof we have given also applies to general morphisms of Shimura data $(G, X) \to (G', X')$ instead of just $(G, X) \to (G^{\mathrm{ad}}, X^{\mathrm{ad}})$.

2.3 Rational conjugacy of linear representations

The following notable fact will be used at several places in this article. We believe this property is also of independent interest.

THEOREM 2.11 [BT65, § 12.3, third paragraph]. *For any algebraic group M over $\mathbb{Q}$, any two representations $\phi, \phi' : M \to GL(n)$ which are defined over $\mathbb{Q}$ and conjugated under $GL(n, \overline{\mathbb{Q}})$ are actually conjugated under $GL(n, \mathbb{Q})$.*

It follows from the theory of linear representations for which references are for example [Hum75, Chapter XI] for $\overline{\mathbb{Q}}$ and [BT65, § 12] over $\mathbb{Q}$. We will only need the case where M is connected and reductive, and this case can be found, for instance, in [BT65, § 12.3, third paragraph]. They give a Galois cohomology argument, and the same Galois cohomology argument works in general with a reference to [Kne69, 1.7 Example 1, p. 16] instead. For reductive groups, it is also possible to reduce the result to Skolem–Noether theorem. For tori, it can be reduced to the fact that any matrix is rationally conjugated to its canonical companion form.

[7] Where $(G^{\mathrm{ad}}, X^{\mathrm{ad}})$ is as in [EY03, Proposition 2.2].

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

2.4 Proof of the finiteness Theorem 2.4

The strategy will combine an argument for semisimple groups and another for algebraic tori.

Proposition 2.12. *Let M be a semisimple algebraic group over $\mathbb{Q}$ (respectively, $\overline{\mathbb{Q}}$).*

(i) *For all $d \in \mathbb{Z}_{\geq 0}$, the set of linear representations defined over $\mathbb{Q}$ (respectively, $\overline{\mathbb{Q}}$)*

$$Hom(M, GL(d))$$

is a finite union of conjugacy classes under $GL(d, \mathbb{Q})$ (respectively, under $GL(d, \overline{\mathbb{Q}})$.)

(ii) *Let G be a reductive linear algebraic group over $\mathbb{Q}$ (respectively, $\overline{\mathbb{Q}}$). Then the set of homomorphisms defined over $\mathbb{Q}$ (respectively, $\overline{\mathbb{Q}}$)*

$$Hom(M, G)$$

is contained in (respectively, is equal to) a finite union of $G(\overline{\mathbb{Q}})$-conjugacy classes.

For simplicity, we will only give an argument which assumes M is Zariski connected, which is the case considered in the proof of Theorem 2.4.

Proof. We prove the first assertion. By virtue of Theorem 2.11, it is enough to treat the case where everything is defined over $\overline{\mathbb{Q}}$.

Because M is connected it is enough to prove that there are finitely many conjugacy classes of Lie algebra representations $\mathfrak{m} \to \mathfrak{gl}(d)$. Equivalently, there are finitely many isomorphisms classes of linear representations of $\mathfrak{m}$ of dimension d. For this,[8] we refer to [Hal03, § 7].

For the second assertion we treat the case where everything is defined over $\overline{\mathbb{Q}}$, which implies the case where everything is defined over $\mathbb{Q}$. It is deduced from the first part by using [Ric67, Theorem 3.1]. □

We prove Theorem 2.4 combining [UY14, Lemma 2.6] with Proposition 2.13.

Proof. We identify G with its image by a faithful representation $G \to GL(d)$, and we let $\Sigma = \{\phi \in \mathrm{Hom}(M, G) : \phi \circ x_0 \in X\}$.

Thanks[9] to [UY14, Lemma 2.6], we may use Proposition 2.13, and deduce that $\Sigma = \{\phi \in \mathrm{Hom}(M, G) : \phi \circ x_0 \in X\}$ is contained in finitely many $GL(d)$-conjugacy classes. Using [Ric67], we conclude that Σ is contained in finitely many $G(\overline{\mathbb{Q}})$-conjugacy classes, thus proving Theorem 2.4. □

Proposition 2.13 (Bounding conjugacy classes). *Let M be a connected reductive $\overline{\mathbb{Q}}$-group, M^{der} its derived subgroup and $T = Z_M(M)^0$ its connected centre.*

A subset $\Sigma \subseteq Hom(M, GL(d))$ is contained in finitely many $GL(d)$-conjugacy classes if and only if: there is a finite set of characters $F \subset X(T)$ such that for every $\rho \in \Sigma$, all the weights of the representation $\rho \restriction_T : T \to GL(d)$ belong to F.

Proof. Because the set of characters is invariant under conjugation, the condition is necessary. We prove that this condition is also sufficient.

We know that two representations of a torus T are conjugated if and only if they have the same weights, with same multiplicities. As the weights belongs to F, and the dimension d is fixed, there are only finitely many possibilities for these weights and multiplicities. Hence, $\{\rho \restriction_T : \rho \in \Sigma\}$

[8] These representations are sums of irreducible representations. By the theorem of the highest weight [Hal03, § 7.2, Theorem 7.15], the irreducible representations are parametrised by dominant weights. The dimension of irreducible representations are given by Weyl dimension formula [Hal03, § 7.6.3, Theorem 7.43], from which lower bounds for dimensions are easily derived: there are finitely many isomorphism classes of irreducible representations of bounded dimension.

[9] This is where the property $\phi \circ x_0 \in X$ is used. This also needs that the image of x_0 is $\mathbb{Q}$-Zariski dense in M.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

is contained in at most finitely many conjugacy classes $GL(d)\cdot\rho_1\upharpoonright_T,\dots,GL(d)\cdot\rho_c\upharpoonright_T$. Without loss of generality we may assume that there is only one conjugacy class, say $GL(d)\cdot\rho_1\upharpoonright_T$.

We want to prove that

$$\text{there are finitely many } \rho\in\Sigma, \text{ up to } GL(d)\text{-conjugation.} \tag{5}$$

Possibly after conjugating, we may assume $\rho\upharpoonright_T=\rho_1\upharpoonright_T$. Because M is connected, one has $M=M^{\mathrm{der}}\cdot T$. Thus,

$$\rho \text{ is determined by } \rho\upharpoonright_{M^{\mathrm{der}}} \text{ and } \rho\upharpoonright_T. \tag{6}$$

As M^{der} and T commute with each other, $\rho\upharpoonright_{M^{\mathrm{der}}}: M^{\mathrm{der}}\to GL(d)$ factors through $G':=Z_{GL(d)}(\rho_1(T))$. As T is reductive, so is G'.

By Proposition 2.12, these $\rho\upharpoonright_{M^{\mathrm{der}}}$ belong to finitely many conjugacy classes $G'\cdot\rho_{1,1}\upharpoonright_{M^{\mathrm{der}}},\dots,G'\cdot\rho_{1,e}\upharpoonright_{M^{\mathrm{der}}}$. Possibly after conjugating ρ by some $g\in G'$, which does not change $\rho\upharpoonright_T$, we have

$$\rho\upharpoonright_T=\rho_1\upharpoonright_T \text{ and } \rho\upharpoonright_{M^{\mathrm{der}}}\in\{\rho_{1,1}\upharpoonright_{M^{\mathrm{der}}};\dots;\rho_{1,e}\upharpoonright_{M^{\mathrm{der}}}\}.$$

In light of (6), this proves (5) and the conclusion follows. □

2.5 Relation to other notions of Hecke orbits

The following is not used in the rest of this article, however it clarifies the relation between different notions of Hecke orbits and we believe it to be of independent interest. We compare our generalised and geometric Hecke orbits to the classical Hecke orbits and another notion of 'generalised Hecke' orbit found in the literature.

2.5.1 *Relation to the classical definition of Hecke orbit.* Let us recall the notion of the classical Hecke orbit.

Definition 2.14 (classical Hecke orbit). Define the *classical Hecke orbit* of x_0 as follows:

$$\mathcal{H}^c(x_0)=\{\phi\circ x_0\in X:\phi\in G(\mathbb{Q})/Z_G(M)(\mathbb{Q})\}\subset\mathcal{H}(x_0)$$

and the *classical Hecke orbit* of $[x_0,1]$ as

$$\mathcal{H}^c(x_0)=\{[x,g]:x\in\mathcal{H}^c(x_0),g\in G(\mathbb{A}_f)\}.$$

We have a chain of inclusions:

$$\mathcal{H}^c(x_0)\subset\mathcal{H}^g(x_0)\subset\mathcal{H}(x_0) \tag{7}$$

$$\mathcal{H}^c(s_0)\subset\mathcal{H}^g(s_0)\subset\mathcal{H}(s_0). \tag{8}$$

In general, $\mathcal{H}^g(x_0)$ is not a finite union of classical Hecke orbits, even when G is of adjoint type.

Hecke correspondences. Recall that the classical Hecke orbit can be described using Hecke correspondences. For $g\in G(\mathbb{Q})$, the points $s_0=[x_0,1]$ and $s_g=[g\cdot x_0,1]$ have a common inverse image by the left, respectively, right, finite map in

$$Sh_K(G,X)\xleftarrow{Sh(Ad_1)}Sh_{K\cap gKg^{-1}}(G,X)\xrightarrow{Sh(Ad_g)}Sh_K(G,X),$$

where $Sh(Ad_g)$ the right map is the Shimura morphism associated to the map of Shimura data $AD_g:(G,X)\to(G,X)$ induced by the conjugation $AD_g:G\to G$ and $Sh(Ad_1)$ is induced by the identity map $AD_1:G\to G$.

Likewise generalised Hecke orbits can be interpreted using finite correspondences between Shimura varieties. For a point $\phi \circ x_0 \in \mathcal{H}(x_0)$, the point s_0 and $s_\phi = [\phi \circ x_0, 1]$ have a common inverse image in

$$\begin{tikzcd} Sh_K(G,X) & Sh_{K\cap \overset{-1}{\phi}(K)}(M,X_M) \arrow[l, "Sh(\phi_0)"'] \arrow[r, "Sh(\phi)"] & Sh_K(G,X). \end{tikzcd}$$

This time the correspondence is induced by a correspondence from the image of $Sh(\phi_0)$ to that of $Sh(\phi)$. These are also the smallest special subvarieties containing s_0, respectively, s_ϕ.

2.5.2 *Relation to the usual definition of the generalised Hecke orbit.* We compare our notion of generalised Hecke to the 'generalised Hecke orbits' used in [KY14] and [EY03, Pin05, Orr15, UY13]. The latter is defined in terms of linear representations.

For any faithful representation $\rho : G \to GL(N)$ over $\mathbb{Q}$, let the 'ρ-Hecke orbit' be

$$\mathcal{H}^\rho(x_0) := \{\phi \circ x_0 \in X : \phi \in \mathrm{Hom}(M,G)(\mathbb{Q}), \rho \circ \phi \in GL(N,\mathbb{Q}) \cdot \rho \circ \phi_0\}.$$

By Theorem 2.11, we also have

$$\mathcal{H}^\rho(x_0) = \{\phi \circ x_0 \in X : \phi \in \mathrm{Hom}(M,G)(\mathbb{Q}), \rho \circ \phi \in GL(N,\overline{\mathbb{Q}}) \cdot \rho \circ \phi_0\}.$$

Proposition 2.15. *The ρ-Hecke orbit $\mathcal{H}^\rho(x_0)$ is contained in the generalised Hecke orbit $\mathcal{H}(x_0)$.*

The ρ-Hecke orbit $\mathcal{H}^\rho(x_0)$ is a finite union of geometric Hecke orbits $\mathcal{H}^g(x_0) \cup \cdots \cup \mathcal{H}^\rho(x_k)$.

The first statement is clear from the definition of $\mathcal{H}^\rho(x_0)$. The second statement follows from the second definition of $\mathcal{H}^\rho(x_0)$ and [Ric67].

The number of geometric Hecke orbits is bounded independently from ρ thanks to Theorem 2.4. It is unclear whether we can achieve $\mathcal{H}^\rho(x_0) = \mathcal{H}(x_0)$ for a sufficiently general representation ρ.

3. Galois functoriality on the generalised Hecke orbit

In §§ 3.1 and 3.2 we state known definitions and properties for the convenience of the reader. Details can be found, for instance, in [UY13]. In § 3.3 we relate cardinality of Galois orbits and cardinality of orbits in adelic groups. This is essential to our approach to the estimates of § 1.3.2 through adelic methods.

3.1 Galois representations

Our statements will use the following terminology.

Definition 3.1 (Galois representations). Let (M, X_M) be a Shimura datum, let x_0 be a point in X_M, and let $E \leq \mathbb{C}$ be a subfield containing the reflex field $E(M, X_M)$.

We say that a continuous homomorphism

$$\rho = \rho_{x_0} : \mathrm{Gal}(\overline{E}/E) \to M(\mathbb{A}_f) \tag{9}$$

is *a Galois representation (defined over E) for x_0 (in X_M)* if: for any compact open subgroup $K' \leq M(\mathbb{A}_f)$, denoting $[x_0, 1]'$ the image of $(x_0, 1)$ in $Sh_{K'}(M, X_M)$, we have $[x_0, 1]' \in Sh_{K'}(M, X_M)(\overline{E})$ and

$$\forall\, \sigma \in \mathrm{Gal}(\overline{E}/E), \sigma([x_0, 1]') = [x_0, \rho_{x_0}(\sigma)]'. \tag{10}$$

In the important case of moduli spaces of abelian varieties, a representation ρ_{x_0} can be directly constructed from the linear Galois action on the Tate module (see [UY13, CM20]).

Here we only need the existence of a ρ_{x_0}.

PROPOSITION 3.2 (Existence of Galois representations). *Let $[x_0, 1] \in Sh_{K_M}(M, X_M)(E')$ be a point defined over a field $E' \leq \mathbb{C}$ in a Shimura variety.*

Then there exist a finite extension E/E' and a Galois representation defined over E for x_0 in X_M.

The main ingredient in this proposition is the following, which is part of the definition of canonical models: for any $[x_0, m_0]$, any $m \in M(\mathbb{A}_f)$ and $\sigma \in Aut(\mathbb{C}/E(M, X_M))$,

$$\text{if } \sigma([x_0, m_0]) = [x', m'] \text{ then } \sigma([x_0, m_0 \cdot m]) = [x', m' \cdot m]. \tag{11}$$

The continuity of ρ_{x_0} is used in the following lemma.

LEMMA 3.3. *Let K be an open subgroup of $M(\mathbb{A}_f)$. Then, after possibly replacing E by a finite extension, we have*

$$\rho_{x_0}(\mathrm{Gal}(\overline{E}/E)) \leq K. \tag{12}$$

Proof. Such an extension corresponds to the open subgroup $\overset{-1}{\rho_{x_0}}(K) \leq \mathrm{Gal}(\overline{E}/E)$. □

Comments. If K is sufficiently small so that $K \cap Z_G(M_0)(\mathbb{Q}) = \{1\}$, for instance if K is *neat* then (see [KY14, § 4.1.4]) for any field $E \leq \mathbb{C}$, there is at most one Galois representation ρ_{x_0} satisfying (12).

3.2 Functoriality of the Galois representation

In the next statement we denote by $E(G, X)$ the *reflex field* of a Shimura datum (G, X). It is a number field over which $Sh(G, X)$ (and, hence, all the $Sh_K(G, X)$) admits a *canonical model*.

PROPOSITION 3.4 (Functoriality). *Let $\phi : (M, X_M) \to (G, X)$ be a morphism of Shimura data, and x_0 a point in X_M.*

If ρ_{x_0} is a Galois representation defined over a field E for x_0, then

$$\phi \circ \rho_{x_0}|_{Gal(\overline{E}/E \cdot E(G,X))}$$

is a Galois representation defined over $E \cdot E(G, X)$ for $\phi(x_0)$ in X.

This follows from the definition and the identity

$$\sigma([\phi \circ x, \phi(g)]) = [\phi \circ x', \phi(g')] \quad \text{for } [x', g'] = \sigma([x, g]),$$

which holds when $\sigma \in \mathrm{Aut}(\mathbb{C}/E(M, X_M)E(G, X))$. Equivalently, the Shimura morphisms induced by ϕ are defined over $E(M, X_M)E(G, X)$. (See [Del71, 1.14, 5.1].)

The compositum field $E \cdot E(G, X) \leq \mathbb{C}$ is a finite extension of E which does not depend on the morphism ϕ. With our definition, it also does not depend on the compact open subgroups. As a consequence, Galois representations for points in the same *generalised* Hecke orbit can be deduced from each other, after passing to the *same* finite extension $E \cdot E(G, X)/E$.

For future reference we summarise the above statements as follows.

PROPOSITION 3.5. *We keep the same notation. For any $\sigma \in Gal(\overline{E}/E \cdot E(G, X))$, any $g \in G(\mathbb{A}_f)$, and any $\gamma \in G(\mathbb{Q})$, we have*

$$\sigma([\gamma \cdot \phi(x_0), g]) = [\gamma \cdot \phi(x_0), \rho'(\sigma) \cdot g],$$

where

$$\rho' := Ad_\gamma \circ \phi \circ \rho_{x_0} : \sigma \mapsto \gamma \cdot \phi \circ \rho_{x_0}(\sigma) \cdot \gamma^{-1}$$

is a Galois representation defined over $E \cdot E(G, X)$ for $\gamma \cdot \phi(x_0)$ in X.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Proof. We may assume $g = 1$ by (11). This follows then from Proposition 3.4 applied to $Ad_\gamma \circ \phi_0 : M \to G \to G$. □

3.3 Galois orbits versus Adelic orbits

Let $U = \rho_{x_0}(Gal(\overline{E}/E))$. By definition, we have

$$\begin{aligned} Gal(\overline{E}/E) \cdot [\phi \circ x_0, g] &= [\phi \circ x_0, \phi \circ \rho_{x_0}(Gal(\overline{E}/E)) \cdot g] \\ &= G(\mathbb{Q}) \backslash G(\mathbb{Q}) \cdot \big(\{\phi \circ x_0\} \times \phi(U) \cdot g\big) \cdot K \cdot /K. \end{aligned}$$

The next proposition reduces the estimation of the size of the Galois orbit to that of the $\phi(U)$-orbit $\phi(U) \cdot g \cdot K \cdot /K$.

Proposition 3.6. *There is a real number $C \in \mathbb{R}_{>0}$ such that*

$$\forall\, (\phi \circ x_0, g) \in \mathcal{H}(x_0) \times G(\mathbb{A}_f), \quad \frac{1}{C} \leq \frac{|Gal(\overline{E}/E) \cdot [x_0, g]|}{[\phi(U) : \phi(U) \cap K]} \leq 1.$$

After possibly passing to a finite extension of E, we may choose $C = 1$.

Proof. We want to bound the cardinality of the fibres of the map

$$\phi(U) \cdot g \cdot K/K \to G(\mathbb{Q}) \backslash G(\mathbb{Q}) \cdot (\{\phi \circ x_0\} \times \phi(U) \cdot g) \cdot K \cdot /K. \tag{13}$$

We first describe the fibres. Let $Z_\phi := Z_G(\phi(M))$. The classical description of Hecke orbits gives an identity

$$\begin{aligned} G(\mathbb{Q}) \backslash G(\mathbb{Q}) \cdot \{\phi \circ x_0\} \times G(\mathbb{A}_f) &\simeq Z_\phi(\mathbb{Q}) \backslash \{\phi \circ x_0\} \times G(\mathbb{A}_f) \\ &\simeq \{\phi \circ x_0\} \times Z_\phi(\mathbb{Q}) \backslash G(\mathbb{A}_f). \end{aligned}$$

(This follows from $G(\mathbb{Q}) \cap Stab_{G(\mathbb{R})}(\phi \circ x_0) = Z_\phi(\mathbb{Q})$ in $G(\mathbb{R})$. We have embedded $Z_\phi(\mathbb{Q})$ in $G(\mathbb{A})$ in the first line, and in $G(\mathbb{A}_f)$ in the second line.)

Define

$$\Gamma = Z_\phi(\mathbb{Q}) \cap \phi(U).$$

The map (13) can be written as a quotient map

$$\phi(U) \cdot g \cdot K/K \to \Gamma \backslash (\phi(U) \cdot g \cdot K/K).$$

It will suffice to bound the order $|\Gamma|$.

The group $Z_\phi(\mathbb{Q})$ is discrete in $G(\mathbb{A}_f)$ because $Z_\phi(\mathbb{R})$ is compact modulo $Z(G)(\mathbb{R})$ and $Z(G)(\mathbb{Q})$ is discrete in $G(\mathbb{A}_f)$ (see [UY13, Appendix Lemma 5.13]), where $Z(G)$ is the centre of G. As usual, we assume that G is the generic Mumford–Tate group on X. Therefore, Γ is compact and discrete, and thus is finite.

We will realise Γ as a finite arithmetic group. We choose a faithful representation $G \to GL(N)$ defined over $\mathbb{Q}$, and identify M and G with their images in $GL(N)$.

We let $K[m] = \ker(GL(N, \widehat{\mathbb{Z}}) \to GL(N, \mathbb{Z}/(m))$ for $m \in \mathbb{Z}$.

There is a maximal compact subgroup K' of $GL(N, \mathbb{A}_f)$ which contains K. In $GL(N, \mathbb{A}_f)$ all maximal compact subgroups are conjugated: K' is of the form $h \cdot GL(N, \widehat{\mathbb{Z}}) \cdot h^{-1}$ with $h \in GL(N, \mathbb{A}_f)$. We may even choose $h \in GL(N, \mathbb{Q})$ (this is a consequence of the fact that the class number of $GL(N)/\mathbb{Q}$ is one).

Conjugating the representation by h^{-1} we may assume $h = 1$: we have

$$U \leq K \leq GL(N, \widehat{\mathbb{Z}}).$$

If $m = 3$ we pass to the finite extension of E corresponding to the subgroup $\overset{-1}{\rho_{x_0}}(U \cap K[m])$ of $\mathrm{Gal}(\overline{E}/E)$. In any case we may assume

$$U \leq K \cap K[m] \leq K[m].$$

From Proposition 3.5, we know that $\phi = \gamma\phi_0\gamma^{-1}$ for some $\gamma \in GL(N, \mathbb{Q})$. It follows that

$$\phi(U) \leq \gamma K[m]\gamma^{-1},$$

and, thus,

$$\Gamma = Z_\phi(\mathbb{Q}) \cap \phi(U) \leq GL(N, \mathbb{Q}) \cap \gamma K[m]\gamma^{-1}.$$

Conjugating by γ^{-1} yields

$$\begin{aligned} \gamma^{-1} \cdot \Gamma \cdot \gamma &\leq \gamma^{-1} GL(N, \mathbb{Q})\gamma \cap K[m] \\ &= GL(N, \mathbb{Q}) \cap K[m] \\ &= \begin{cases} GL(N, \mathbb{Z}) & \text{if } m = 1, \\ \ker(GL(N, \mathbb{Z}) \to GL(N, \mathbb{Z}/(3))) & \text{if } m = 3. \end{cases} \end{aligned}$$

Recall that $|\Gamma| = |\gamma^{-1}\Gamma\gamma|$. We may thus conclude by applying the following lemma to $\gamma^{-1} \cdot \Gamma \cdot \gamma$. It follows that for $m = 1$, $|\Gamma|$ is bounded independently of ϕ and for $m = 3$, $|\Gamma| = 1$. □

LEMMA 3.7. *For every N, there is a real number $C(N)$ such that, for every finite subgroup $\Gamma \leq GL(N, \mathbb{Z})$ we have*

$$|\Gamma| \leq C(N),$$

and if $\Gamma \leq \ker(GL(N, \mathbb{Z}) \to GL(N, \mathbb{Z}/(3)))$, then $\Gamma = 1$.

Proof. From [PR94, Lemma 4.19.(Minkowski), p. 232] the kernel has no nontrivial torsion. This implies the second assertion.

This also implies that the reduction map $GL(N, \mathbb{Z}) \to GL(N, \mathbb{Z}/(3))$ is injective on Γ, thus inducing an embedding of Γ in $GL(N, \mathbb{Z}/(3))$. The first conclusion follows with

$$C(N) = |GL(N, \mathbb{Z}/(3))| = \prod_{i=0}^{N-1} (3^N - 3^i).$$ □

4. Invariant heights on Hecke orbits

4.1 Height functions

4.1.1 *Local affine height functions over $\mathbb{R}$ or $\mathbb{Q}_p$.* Let W be an affine variety over $K = \mathbb{R}$ or $K = \mathbb{Q}_p$. For every affine embedding defined over K

$$\iota_K : W \to \mathbb{A}^N_K$$

there is an associated *affine local Weil height* function $H_{\iota_K} : W(K) \to \mathbb{R}_{\geq 0}$ given by

$$H_{\iota_K}(w) = \max\{1; |w_1|_K; \ldots; |w_N|_K\}, \tag{14}$$

where $|-|_K$ is the standard absolute value on K.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

4.1.2 *Affine height functions over $\mathbb{Q}$.* When W and $\iota := \iota_K$ are defined over $\mathbb{Q}$, we can define, for $w \in W(\mathbb{Q})$,

$$H_\iota(w) = H_{\iota\otimes\mathbb{R}}(w) \cdot H_{\iota,f}(w), \tag{15}$$

$$\text{with } H_{\iota,f}(w) = \prod_p H_{\iota\otimes\mathbb{Q}_p}(w). \tag{16}$$

We define more generally, for $w = (w_p)_p \in W(\mathbb{A}_f)$,

$$H_{\iota,f}(w) = \prod_p H_{\iota\otimes\mathbb{Q}_p}(w_p). \tag{17}$$

When W and the embedding $\iota_\mathbb{R}$, respectively, $\iota_{\mathbb{Q}_p}$, respectively, ι are clear from the context, we will simply write

$$H_\mathbb{R} = H_{\iota_\mathbb{R}}, \quad H_p = H_{\iota_{\mathbb{Q}_p}}, \quad H_W = H_\iota \text{ and } H_f = H_{\iota,f}. \tag{18}$$

Then (15) becomes

$$H_W = H_\mathbb{R} \cdot H_f. \tag{19}$$

4.2 Polynomial equivalence and functoriality of heights

We recall the *functoriality* properties of heights. See [Ser97] or [BG06] for corresponding statements about projective Weil heights. See Definition 1.7 for the symbols $\preccurlyeq$ and $\approx$.

THEOREM 4.1 (Functoriality of heights). *Let $\phi : V \to V'$ be a morphism of affine varieties over $\mathbb{R}$, respectively, $\mathbb{Q}_p$, respectively, $\mathbb{Q}$, and let*

$$\iota_\mathbb{R} : V \to \mathbb{A}^N_\mathbb{R}, \text{ respectively, } \iota_{\mathbb{Q}_p} : V \to \mathbb{A}^N_{\mathbb{Q}_p}, \text{ respectively, } \iota : V \to \mathbb{A}^N_\mathbb{Q}$$

be an affine embedding of V, and let $\iota'_\mathbb{R} : V' \to \mathbb{A}^{N'}_\mathbb{R}$, respectively, $\iota'_{\mathbb{Q}_p} : V' \to \mathbb{A}^{N'}_{\mathbb{Q}_p}$, respectively, $\iota' : V' \to \mathbb{A}^{N'}_\mathbb{Q}$ be an affine embedding of V'.

Then, as functions on $V(\mathbb{R})$, respectively, $V(\mathbb{Q}_p)$, respectively, $V(\mathbb{Q})$ and $V(\mathbb{A}_f)$,

$$H_{\iota'_\mathbb{R}} \circ \phi \preccurlyeq H_{\iota_\mathbb{R}}, \text{respectively, } H_{\iota'_{\mathbb{Q}_p}} \circ \phi \preccurlyeq H_{\iota_{\mathbb{Q}_p}},$$

$$\text{respectively, } H_{\iota'} \circ \phi \preccurlyeq H_\iota \text{ and } H_{\iota',f} \circ \phi \preccurlyeq H_{\iota,f}.$$

COROLLARY 4.2. *Let V be an affine algebraic variety over $\mathbb{R}$, respectively, $\mathbb{Q}_p$, respectively, $\mathbb{Q}$. Let*

$$\iota_\mathbb{R} : V \to \mathbb{A}^N_\mathbb{R} \text{ and } \iota'_\mathbb{R} : V \to \mathbb{A}^{N'}_\mathbb{R},$$

$$\text{respectively, } \iota_{\mathbb{Q}_p} : V \to \mathbb{A}^N_{\mathbb{Q}_p} \text{ and } \iota'_{\mathbb{Q}_p} : V \to \mathbb{A}^{N'}_{\mathbb{Q}_p},$$

$$\text{respectively, } \iota : V \to \mathbb{A}^N_\mathbb{Q} \text{ and } \iota : V' \to \mathbb{A}^{N'}_\mathbb{Q}$$

be affine embeddings of V'.

Then, as functions on $V(\mathbb{R})$, respectively, $V(\mathbb{Q}_p)$, respectively, $V(\mathbb{Q})$ and $V(\mathbb{A}_f)$,

$$H_{\iota'_\mathbb{R}} \approx H_{\iota_\mathbb{R}}, \text{respectively, } H_{\iota'_{\mathbb{Q}_p}} \approx H_{\iota_{\mathbb{Q}_p}}, \text{respectively, } H_{\iota'} \approx H_\iota \text{ and } H_{\iota',f} \approx H_{\iota,f}.$$

4.3 Galois invariant height on the Hecke orbit

Let $S = Sh_K(G,X)$ and x_0 be as in §1.1 and $\rho_{x_0} : \mathrm{Gal}(\overline{E}/E) \to M(\mathbb{A}_f)$ be as in (9). Let $W = G \cdot \phi_0 \subseteq \mathrm{Hom}(M,G)$ be the algebraic variety defined in §2.1. We have $W \simeq G/Z_G(M)$. Let $\mathrm{Hom}(\mathfrak{m},\mathfrak{g})$ be affine algebraic variety of linear maps $\mathfrak{m} \to \mathfrak{g}$. As M is connected, we have an

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

embedding

$$\phi \mapsto d\phi : W \hookrightarrow \mathrm{Hom}(\mathfrak{m}, \mathfrak{g}).$$

As M is reductive, the image is closed, by [Ric67].

We choose a lattice $\mathfrak{g}_{\mathbb{Z}} \leq \mathfrak{g}$ such that

$$\mathfrak{g}_{\mathbb{Z}} \otimes \widehat{\mathbb{Z}} \leq \mathfrak{g} \otimes \mathbb{A}_f$$

is stable under the action of $K \leq G(\mathbb{A}_f)$. We define $\mathfrak{m}_{\mathbb{Z}} = \mathfrak{g}_{\mathbb{Z}} \cap \mathfrak{m}$. We choose a basis of $\mathfrak{g}$ which generates $\mathfrak{g}_{\mathbb{Z}}$ and a basis of $\mathfrak{m}$ which generates $\mathfrak{m}_{\mathbb{Z}}$. This choice induces an isomorphism

$$j : \mathrm{Hom}(\mathfrak{m}, \mathfrak{g}) \xrightarrow{\sim} \mathbb{Q}^{\dim(M)\cdot\dim(G)}.$$

This induces an affine embedding

$$\iota := j \circ d : W = G \cdot \phi_0 \hookrightarrow \mathrm{Hom}(\mathfrak{m}, \mathfrak{g}) \to \mathbb{A}_{\mathbb{Q}}^{\dim(M)\cdot\dim(G)}$$

by first mapping ϕ to $d\phi$ and then to its matrix with respect to the bases we have chosen.

We denote by $H_f : W(\mathbb{A}_f) \to \mathbb{Z}_{\geq 1}$ and $H'_f : \mathrm{Hom}(\mathfrak{m}_{\mathbb{A}_f}, \mathfrak{g}_{\mathbb{A}_f}) \to \mathbb{Z}_{\geq 1}$ the functions given by (17) with respect to the embeddings ι and j.

PROPOSITION 4.3 (Galois invariance). *Let $\phi_1, \phi_2 \in W(\mathbb{Q})$ be such that $s_1 = [\phi_1 \circ x_0, g_1]$ and $s_2 = [\phi_2 \circ x_0, g_2]$ define points in $\mathcal{H}^g(s_0)$, where $g_1, g_2 \in G(\mathbb{A}_f)$, and assume that there exists a $\sigma \in \mathrm{Gal}(\overline{E}/E)$ such that*

$$\sigma(s_1) = s_2. \tag{20}$$

Then

$$H_f({g_1}^{-1}\phi_1 g_1) = H_f({g_2}^{-1}\phi_2 g_2).$$

We first remark, from the formula

$$\forall\, \psi \in \mathrm{Hom}(\mathfrak{m}_{\mathbb{A}_f}, \mathfrak{g}_{\mathbb{A}_f}),\ H'_f(\psi) = \min\{n \in \mathbb{Z}_{\geq 1} : n \cdot \psi(\mathfrak{m}_{\widehat{\mathbb{Z}}}) \subset \mathfrak{g}_{\widehat{\mathbb{Z}}}\}, \tag{21}$$

that for every $\widehat{\mathbb{Z}}$-module automorphism $u : \mathfrak{m}_{\widehat{\mathbb{Z}}} \to \mathfrak{m}_{\widehat{\mathbb{Z}}}$ and $k : \mathfrak{g}_{\widehat{\mathbb{Z}}} \to \mathfrak{g}_{\widehat{\mathbb{Z}}}$, we have

$$H'_f(k \circ \psi \circ u) = H'_f(\psi). \tag{22}$$

When $\psi = d\phi$, and $k = ad_{k'} : \mathfrak{g} \to \mathfrak{g}$ with $k' \in K$ and $u = ad_{u'} : \mathfrak{m} \to \mathfrak{m}$ with $u' \in K \cap M(\mathbb{A}_f)$, this gives, with $AD_{k'} \circ \phi \circ AD_{u'} : m \mapsto k'\phi(u'mu'^{-1})k'^{-1}$,

$$H_f(AD_{k'} \circ \phi \circ AD_{u'}) = H_f(\psi). \tag{23}$$

Proof of Proposition 4.3. We define $u = \rho_{x_0}(\sigma) \in M(\mathbb{A}_f) \cap K$. From (20) and the functoriality of Galois action Propositions 3.4 and 3.5, we have

$$[\phi_1 \circ x_0, \phi_1(u) \cdot g_1] = [\phi_2 \circ x_0, g_2].$$

Hence, there exists $\gamma \in G(\mathbb{Q})$ and $k \in K$ such that

$$(\gamma \cdot \phi_1 \circ x_0, \gamma \cdot \phi_1(u) g_1 k) = (\phi_2 \circ x_0, g_2).$$

By Lemma 2.5, we also have $\gamma \cdot \phi_1 \cdot \gamma^{-1} = \phi_2$. Thus,

$$\begin{aligned} {g_2}^{-1}\phi_2 g_2 &= (k^{-1}{g_1}^{-1}\phi_1(u)^{-1}\gamma^{-1}) \cdot (\gamma \cdot \phi_1 \cdot \gamma^{-1}) \cdot (\gamma \cdot \phi_1(u) g_1 k) \\ &= k^{-1}{g_1}^{-1}\phi_1(u^{-1}) \cdot \phi_1 \cdot \phi_1(u) g_1 k. \end{aligned}$$

We have

$$\forall\, m \in M(\mathbb{A}_f), \phi_1(u)^{-1} \cdot \phi_1(m) \cdot \phi_1(u) = \phi_1(u^{-1}mu) = \phi_1 \circ AD_{u^{-1}}(m)$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

and, hence,

$$k^{-1}{g_1}^{-1}\phi_1(u)^{-1}\cdot\phi_1\cdot\phi_1(u)g_1k = AD_{k^{-1}}\circ({g_1}^{-1}\cdot\phi_1\cdot g_1)\circ AD_{u^{-1}}.$$

We finally have, using (23),

$$H_f({g_2}^{-1}\phi_2 g_2) = H_f(AD_{k^{-1}}\circ({g_1}^{-1}\cdot\phi_1\cdot g_1)\circ AD_{u^{-1}}) = H_f({g_1}^{-1}\phi_1 g_1). \qquad \square$$

4.3.1 *Height function on the generalised Hecke orbit* $\mathcal{H}([x_0, 1])$. The function H'_f on $\mathrm{Hom}(\mathfrak{m}_{\mathbb{A}_f}, \mathfrak{g}_{\mathbb{A}_f})$ induces, at the level of the $Sh_K(G, X)$, a function H_{s_0} on the generalised Hecke orbit $\mathcal{H}(s_0)$ of $s_0 := [x_0, 1]$, given as follows. For $\phi \in \mathrm{Hom}(\mathfrak{m}_{\mathbb{Q}}, \mathfrak{g}_{\mathbb{Q}})$ such that $\phi\circ x_0 \in X$ and $g \in G(\mathbb{A}_f)$, we define

$$H_{s_0}([\phi\circ x_0, g]) = H'_f(d(g^{-1}\phi g)).$$

The function H_{s_0} depends on the choices we have made, but different choices will produce the same function, up to a bounded factor.

The case $\sigma = 1$ of Proposition 4.3 implies that H_{s_0} is well defined. Proposition 4.3 can then be rephrased as follows.

Lemma 4.4. *For every* $\sigma \in \mathrm{Gal}(\overline{E}/E)$ *and* $s \in \mathcal{H}(s_0)$ *we have*

$$H_{s_0}(\sigma(s)) = H_{s_0}(s). \tag{24}$$

5. Height comparison on Siegel sets

The main result of this section, Theorem 5.16, compares, for rational points of $W = G/Z_G(M)$ contained in a given Siegel set (as in Definition 5.11), the global height H_W of (4.1.2), with its factor H_f in (19) (coming from the finite places). The height H_W is that appearing in our variant (Theorem 7.1) of the theorem of Pila–Wilkie, and H_f is the height appearing in our Galois bounds (see Theorem 6.4).

Our Theorem 5.16 extends a result of Orr, in [Orr18], which is only applicable to elements in $G(\mathbb{Q})$. We work with elements of $W(\mathbb{Q})$ instead. This is crucial to us as, in our strategy § 1.4, we are working with geometric Hecke orbits.[10]

This section develops different arguments than those of [Orr18]. They are more flexible, which allows us to obtain a more general result.

5.1 Polynomial equivalence and archimedean height

We use Definition 1.7.

Lemma 5.1. *Let* $A \subset \mathbb{R}^n$ *be a semialgebraic subset, and let* $f, g\colon A \longrightarrow \mathbb{R}_{\geq 0}$ *be semialgebraic and continuous functions. Assume that* f *is a proper map.*

Then

$$g \preccurlyeq f.$$

Proof. We claim that the following function

$$h\colon \left]\inf_A(f), \infty\right[\to \mathbb{R}_{\geq 0}$$
$$t \mapsto \sup\{g(a) : a \in A, f(a) \leq t\}$$

[10] In general, when $Z_G(M) \neq \{1\}$, the height of an element $g \in G(\mathbb{Q})$ is not bounded by the height of its image $g\phi_0 g^{-1}$ in $W(\mathbb{Q})$ and not every element of $W(\mathbb{Q})$ is the image of an element of $G(\mathbb{Q})$.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

is well defined. Fix an arbitrary t be in $]\inf_A(f), \infty[$. The set $\{a \in A : f(a) \leq t\}$ is compact since f is proper. It is nonempty since $t > \inf_A(f)$. As g is continuous, $\{g(a) : a \in A, f(a) \leq t\}$ is compact and nonempty, and its maximum belongs to $\mathbb{R}_{\geq 0}$, which proves the claim.

The function h is also semialgebraic (see [BCR98, Proposition 2.2.4.]). By [vdDri98, § 4.1 'Notes and comments' and references therein], h is polynomially bounded. The conclusion follows. □

The following uses Lemma 5.1 for f and g, and again after swapping f and g.

Corollary 5.2. *On a semialgebraic subset $A \subset \mathbb{R}^n$, two proper semialgebraic continuous functions $f, g : A \to \mathbb{R}$ are polynomially equivalent.*

We will also encounter the following situation.

Lemma 5.3. *Let $A \subset \mathbb{R}^n$ and $B \subset \mathbb{R}^m$ be semialgebraic subsets, and $f \colon A \to \mathbb{R}_{\geq 0}$ and $g \colon B \to \mathbb{R}_{\geq 0}$ be two proper semialgebraic continuous functions, and $p \colon A \to B$ be a proper and continuous semialgebraic function. Then $g \circ p \approx f$.*

Proof. We note that $g \circ p$ is proper and continuous because g and p are. We can apply the Corollary 5.2 to f and $g \circ p$. □

Lemma 5.4. *Let V be an affine algebraic variety over $\mathbb{R}$. Let $\phi : V \to \mathbb{A}^N$, and $\phi' : V \to \mathbb{A}^M$ be two closed embeddings, and let H_ϕ and $H_{\phi'}$ be defined as in (14).*

Then H_ϕ and $H_{\phi'}$ are semialgebraic continuous proper functions, and

$$H_\phi \approx H_{\phi'}.$$

Proof. The real algebraic map $V(\mathbb{R}) \to \mathbb{R}^N$ induced by the Zariski-closed embedding ϕ is a closed embedding for the real topology. The functions $\| \, \|_\infty : \mathbb{R}^N \to \mathbb{R}_{\geq 0}$ and $t \mapsto \max\{1; t\} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ are semialgebraic continuous proper maps. The composite map H_ϕ, and likewise $H_{\phi'}$, are thus semialgebraic continuous and proper on $V(\mathbb{R})$. We conclude with Corollary 5.2. □

Lemma 5.5. *Let $p : U \to V$ be a morphism of affine algebraic varieties over $\mathbb{R}$, and $\phi_U : U \to \mathbb{A}^N_{\mathbb{R}}$ and $\phi_V : V \to \mathbb{A}^M_{\mathbb{R}}$ be closed embeddings. Let H_{ϕ_U} and H_{ϕ_V} be defined as in (14).*

Let $A \subset U(\mathbb{R})$ be a semialgebraic subset such that $p|_A : A \to V(\mathbb{R})$ is proper. Then, as functions $A \to \mathbb{R}_{\geq 0}$,

$$H_{\phi_U}|_A \approx H_{\phi_V} \circ p|_A.$$

Proof. We know that H_{ϕ_U} and H_{ϕ_V} are proper continuous and semialgebraic. As $p|_A$ is proper, $\iota : A \hookrightarrow U(\mathbb{R})$ is closed. It follows that $H_{\phi_U}|_A = H_{\phi_U} \circ \iota$ is continuous, proper and semialgebraic. We apply Lemma 5.3 with $A = U(\mathbb{R})$, $B = V(\mathbb{R})$, and $p|_A$ as p, and $f = H_{\phi_U}|_A$ and $g = H_{\phi_V}$. □

5.2 Comparison of archimedean and finite height

Lemma 5.6. *Let $\iota : V \to \mathbb{A}^M$ be a closed embedding with $V = {\mathbb{G}_m}^N$. Then $H_{\iota,\mathbb{R}} \preccurlyeq H_{\iota,f}$ on $\mathbb{Q}^{\times N}$, where $H_\mathbb{R}$ and H_f are as in § 4.1.2 (see (18)).*

Proof. Thanks to Corollary 4.2, we may substitute ι with the closed embedding

$$\iota_N : {\mathbb{G}_m}^N \xrightarrow{(t_1,\ldots,t_N)\mapsto(t_1,{t_1}^{-1},\ldots,t_N,{t_N}^{-1})} \mathbb{A}^{2N}. \tag{25}$$

We start with the case $N = 1$. We write an element $t \in \mathbb{Q}^\times$ as a reduced fraction n/m. We can compute

$$H_{\iota_1 \otimes \mathbb{R}}(t) = \max\{|t|; |1/t|\} \text{ and } H_{\iota_1, f}(t) = |n \cdot m|.$$

It follows $H_{\iota_1 \otimes \mathbb{R}}(t) \leq H_{\iota_1, f}(t)$.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

For general $\vec{t} = (t_1, \ldots, t_N) \in \mathbb{Q}^{\times N}$ there is some $1 \leq i \leq N$ such that

$$H_{\iota_N \otimes \mathbb{R}}(\vec{t}) = \max\{|t_1|; |1/t_1|; \ldots; |t_N|; |1/t_N|\} = \max\{|t_i|; |1/t_i|\}.$$

By the previous computation we have

$$H_{\iota_N \otimes \mathbb{R}}(\vec{t}) = H_{\iota_1 \otimes \mathbb{R}}(t_i) \leq H_{\iota_1, f}(t_i).$$

We conclude by observing that

$$H_{\iota_1, f}(t_i) \leq H_{\iota_N, f}(\vec{t}),$$

as can be seen prime by prime. □

Lemma 5.7. *For $V = \mathbb{G}_m^N \subset W = \mathbb{A}^N$, and affine embeddings $\iota_V : V \to \mathbb{A}^M$, respectively, $\iota_W : W \to \mathbb{A}^{M'}$, we have $H_{\iota_V, f} \preccurlyeq H_{\iota_W}$ on $\mathbb{Q}^{\times N}$.*

Proof. By Corollary 4.2, we may assume that ι_V is ι_N of (25), and that ι_W is the identity map. We can again reduce the problem to the case $N = 1$. We write $t_i = n/m$ as an irreducible fraction and then we have

$$H_{\iota_V, f}(n/m) = |n \cdot m| \leq \max\{|n|, |m|\}^2 = H_{\iota_W}(n/m)^2. \qquad \square$$

Corollary 5.8. *Let $C \in \mathbb{R}_{>0}$. We have*

$$H_{\iota_V, f} \preccurlyeq H_{\iota_W, f} \text{ on } (\mathbb{Q}^\times \cap [-C; C])^N.$$

Proof. In Lemma 5.7, we decompose $H_{\iota_W} = H_{\iota_W \otimes \mathbb{R}} \cdot H_{\iota_W, f}$. By hypothesis, $H_{\iota_W \otimes \mathbb{R}} \leq C$, hence $H_{\iota_W} \preccurlyeq H_{\iota_W, f}$ on $(\mathbb{Q}^\times \cap [-C; C])^N$ which allows us to conclude. □

We establish the following.

Proposition 5.9. *Let W be an affine variety over $\mathbb{Q}$ and let $p \colon W \longrightarrow \mathbb{A}^r$ be an algebraic map and $\mathfrak{S} \subset W(\mathbb{R})$ be a semialgebraic closed subset such that:*

(i) *we have $p(\mathfrak{S}) \subseteq (\mathbb{R}^\times)^r$;*
(ii) *the restriction $p|_{\mathfrak{S}} \colon \mathfrak{S} \longrightarrow \mathbb{R}^{\times r}$ is a proper map;*
(iii) *the image $p(\mathfrak{S})$ is bounded in $\mathbb{R}^r$.*

We fix an affine embedding ι of W and use notation (18). Then

$$H_{\mathbb{R}}|_{\mathfrak{S} \cap W(\mathbb{Q})} \preccurlyeq H_f|_{\mathfrak{S} \cap W(\mathbb{Q})}.$$

In particular,

$$H_W|_{\mathfrak{S} \cap W(\mathbb{Q})} \approx H_f|_{\mathfrak{S} \cap W(\mathbb{Q})}.$$

Proof. We denote by ${\mathbb{G}_m}^r \subset \mathbb{A}^r$ the affine open subset on which every coordinate is invertible.

We fix affine embeddings ι_W of W, and $\iota_{{\mathbb{G}_m}^r}$ of ${\mathbb{G}_m}^r$ and $\iota_{\mathbb{A}^r}$ of $\mathbb{A}^r$.

Because $p|_{\mathfrak{S}}$ is continuous real algebraic, and (as a function to $\mathbb{R}^r$) is proper, by Lemma 5.5 we have

$$H_{\iota_W \otimes \mathbb{R}}|_{\mathfrak{S}} \approx H_{\iota_{{\mathbb{G}_m}^r} \otimes \mathbb{R}} \circ p|_{\mathfrak{S}}. \tag{26}$$

By functoriality of heights, Theorem 4.1, we have, on $W(\mathbb{Q})$,

$$H_{\iota_{\mathbb{A}^r}, f} \circ p \preccurlyeq H_{\iota_W, f}. \tag{27}$$

As $p(\mathfrak{S})$ is bounded in $\mathbb{R}^r$, we have, by Lemma 5.6,

$$H_{\iota_{{\mathbb{G}_m}^r} \otimes \mathbb{R}} \preccurlyeq H_{\iota_{{\mathbb{G}_m}^r}, f}. \tag{28}$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

By hypothesis (iii) we can use Corollary 5.8 and get

$$H_{\iota_{\mathbb{G}_m{}^r},f}|_{p(\mathfrak{S})\cap\mathbb{Q}^{\times r}} \preccurlyeq H_{\iota_{\mathbb{A}^r},f}|_{p(\mathfrak{S})\cap\mathbb{Q}^{\times r}}. \tag{29}$$

Combining these we get, using (26), (28), (29), and then (27),

$$\begin{aligned} H_{\iota_W\otimes\mathbb{R}}|_{\mathfrak{S}\cap W(\mathbb{Q})} &\approx H_{\iota_{\mathbb{G}_M{}^r}\otimes\mathbb{R}}\circ p|_{\mathfrak{S}\cap W(\mathbb{Q})} \\ &\preccurlyeq H_{\iota_{\mathbb{G}_M{}^r},f}\circ p|_{\mathfrak{S}\cap W(\mathbb{Q})} \preccurlyeq H_{\iota_{\mathbb{A}^r},f}\circ p|_{\mathfrak{S}\cap W(\mathbb{Q})} \preccurlyeq H_{\iota_W,f}|_{\mathfrak{S}\cap W(\mathbb{Q})}. \qquad \square \end{aligned}$$

5.3 Construction of Siegel sets

We start by recalling some facts about parabolic subgroups and Siegel sets. A general reference is [BJ06].

Let $G_{\mathbb{Q}}$ be a semisimple $\mathbb{Q}$-algebraic group of adjoint type. We fix a minimal $\mathbb{Q}$-defined parabolic[11] subgroup $P_{\mathbb{Q}}$. Let $G_{\mathbb{R}}$ and $P_{\mathbb{R}}$ be the corresponding $\mathbb{R}$-algebraic groups.

Let X be the associated symmetric space,[12] and choose $x \in X$ and let $\Theta : G_{\mathbb{R}} \to G_{\mathbb{R}}$ be the Cartan involution associated with x. The orbit map $g \mapsto g \cdot x$ induces the identification $G(\mathbb{R})/K \simeq X$ where K is the maximal compact subgroup $\{g \in G(\mathbb{R}) : g = \Theta(g)\}$. We denote by $K_\infty = K^+$ the neutral component.

We let $N_{\mathbb{Q}}$ be the unipotent radical of $P_{\mathbb{Q}}$: thus $P_{\mathbb{Q}}/N_{\mathbb{Q}}$ is the maximal reductive quotient of $P_{\mathbb{Q}}$. The $\mathbb{R}$-algebraic group

$$L := P_{\mathbb{R}} \cap \Theta(P_{\mathbb{R}})$$

is a maximal $\mathbb{R}$-algebraic reductive subgroup of $P_{\mathbb{R}}$ (cf. [BJ06, § III.1.9]), not necessarily defined over $\mathbb{Q}$, and the map $L \to P_{\mathbb{R}} \to (P_{\mathbb{Q}}/N_{\mathbb{Q}})_{\mathbb{R}}$ is an isomorphism. We denote by $A'_{\mathbb{Q}}$ the maximal central $\mathbb{Q}$-split torus of $P_{\mathbb{Q}}/N_{\mathbb{Q}}$, and define $A \leq L$ as the inverse image of $A_{\mathbb{R}}$ in L. We denote by $A^+ = A(\mathbb{R})^+$ the neutral component as a real Lie group.

We denote by Φ the set of non-zero weights of the adjoint action of A on $\mathfrak{g} \otimes \mathbb{R}$ (the '(relative) roots'), and Φ^+ the subset of weights of the action on $\mathfrak{n} \otimes \mathbb{R}$ (the 'positive' ones). The eigenspaces are not necessarily defined over $\mathbb{Q}$. There exists a unique subset $\Delta = \{\alpha_1; \ldots; \alpha_r\} \subset \Phi^+$ such that $\alpha_1, \ldots, \alpha_r$ is a basis of $X(A) = \mathrm{Hom}(A, \mathbb{G}_{m\mathbb{R}})$ and $\Phi^+ \subset \alpha_1 \cdot \mathbb{Z}_{\geq 0} + \cdots + \alpha_r \cdot \mathbb{Z}_{\geq 0}$. The α_i are known as the (relative) simple roots, and r is equal to the $\mathbb{Q}$-rank of $G_{\mathbb{Q}}$.

The positive Weyl chamber in A^+ is

$$A^+_{\geq 0} = \{a \in A^+ : \forall\, 1 \leq i \leq r,\ \alpha_i(a) \geq 1\}. \tag{30}$$

We define

$$H_P := \bigcap_{\chi \in X(P_{\mathbb{Q}})} \ker(\chi^2). \tag{31}$$

We note that, for every one-dimensional representation $\mathbb{Q} \cdot \eta$ of H_P, we have

$$\forall\, h \in H_P(\mathbb{R}),\ h \cdot \eta \in \{+\eta; -\eta\}. \tag{32}$$

We first define Siegel sets in $G_{\mathbb{Q}}(\mathbb{R})$.

Definition 5.10 (Siegel set). A *$\mathbb{Q}$-Siegel set $\mathfrak{S}$ in $G_{\mathbb{Q}}(\mathbb{R})$ with respect to $P_{\mathbb{Q}}$ and x* is a subset $\mathfrak{S} \subseteq G(\mathbb{R})$ of the following form.

[11] Non-necessarily proper: we have $P_{\mathbb{Q}} = G_{\mathbb{Q}}$ when $G_{\mathbb{Q}}$ is of $\mathbb{Q}$-rank zero.

[12] The space X in this section is of the form $G(\mathbb{R})/K$ with K a *non-necessarily connected* maximal compact subgroup. This $G(\mathbb{R})/K$ is connected and is a quotient of the space $X = G(\mathbb{R})/K_\infty$ from other sections of this article: when x is the image of $x_0 \in G(\mathbb{R})/K_\infty$, we have $K_\infty = K^+$, where for simplicity we assume G is of adjoint type. The point x_0 determines and is determined by a Hodge cocharacter $h : \mathbb{S} \to G_{\mathbb{R}}$, and the image point $x \in G(\mathbb{R})/K$ determines and is determined by the corresponding Cartan involution $\Theta = Ad_{h(i)}$.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

There is a nonempty open and relatively compact subset $\Omega \subseteq P_{\mathbb{Q}}(\mathbb{R})$ and an element $a \in A^+$ such that

$$\mathfrak{S} = \Omega \cdot A^+_{\geq 0} \cdot a \cdot K_\infty.$$

We will always assume that $\Omega \subseteq H_{\mathbb{Q}}(\mathbb{R})$ and that Ω is semialgebraic.

Usually Siegel sets are defined in $G_{\mathbb{Q}}(\mathbb{R})$ or in $X = G_{\mathbb{Q}}(\mathbb{R})/K$. Working with geometric Hecke orbits as defined in Definition 2.3, we use the variety $W(\mathbb{R})^+ = G(\mathbb{R})/Z_G(M)(\mathbb{R})$. We can view $W(\mathbb{R})^+$ as an intermediary space in the sequence of maps $G(\mathbb{R}) \to W = G(\mathbb{R})/Z_G(M)(\mathbb{R}) \to X$. The following definition allows us to work with Siegel sets in a greater generality.

Definition 5.11. Let Z be a compact subgroup of K, and $W = G_{\mathbb{R}}/Z$. We define *a $\mathbb{Q}$-Siegel set $\mathfrak{S}_W$ with respect to $P_{\mathbb{Q}}$ and x in $W^+ := G_{\mathbb{R}}(\mathbb{R})/Z(\mathbb{R})$* to be the image of $\mathbb{Q}$-Siegel set $\mathfrak{S}$ in $G_{\mathbb{Q}}(\mathbb{R})$ with respect to $P_{\mathbb{Q}}$ and x.

We note that if Z is defined over $\mathbb{Q}$ then so is W and we can consider the subset $W^+(\mathbb{Q}) \cap \mathfrak{S}_W$.

5.4 Divergence in Siegel sets

In the rest of this section we use the notation $G = G_{\mathbb{Q}}$.

5.4.1 We say that an infinite sequence, in an appropriate topological space, is *divergent* if it does not contain an infinite convergent subsequence. A continuous map is *proper* if it maps divergent sequences to divergent sequences.

5.4.2 We will use the closure of a Siegel set.

Proposition 5.12. *Consider $\mathfrak{S} = \Omega \cdot A^+_{\geq 0} \cdot a \cdot K_\infty$ as in Definition 5.10.*

Then its closure in $G(\mathbb{R})$ is given by

$$\overline{\mathfrak{S}} = \overline{\Omega} \cdot A^+_{\geq 0} \cdot a \cdot K_\infty. \tag{33}$$

and $\overline{\mathfrak{S}}$ is contained in a $\mathbb{Q}$-Siegel set $\mathfrak{S}'$ in $G(\mathbb{R})$ with respect to P and x.

Proof. The set $\mathfrak{S}$ is obviously dense in the right-hand side of (33). It is the image of the proper map in Lemma 5.13, and thus it is a closed subset in $G(\mathbb{R})$. This proves the first assertion. Let U be a nonempty relatively compact semialgebraic open neighbourhood of 1 in $H(\mathbb{R})$, for instance a small euclidean open ball in a faithful representation $H \to GL(N)$. Then $\Omega' = U \cdot \overline{\Omega}$ is an open relatively compact semialgebraic open neighbourhood of $\overline{\Omega}$ in $H(\mathbb{R})$, and the Siegel set $\Omega' \cdot A^+_{\geq 0} \cdot a \cdot K$ contains $\overline{\mathfrak{S}}$. □

We used the following.

Lemma 5.13. *The map*

$$(\omega, a, k) \mapsto \omega \cdot a \cdot k : \overline{\Omega} \times A^+_{\geq 0} \cdot a \times K \to G(\mathbb{R})$$

is proper.

Proof. It suffices to prove that the image of every divergent sequence in the left-hand side is not a convergent sequence in the right-hand side. We prove the contrapositive.

Let $(\omega_n, a_n, k_n)_{n \in \mathbb{Z}_{\geq 1}}$ be a sequence in the left-hand side such that $(\omega_n \cdot a_n \cdot k_n)_{n \in \mathbb{Z}_{\geq 1}}$ is a convergent sequence in $G(\mathbb{R})$. Because $\overline{\Omega}$ and K are compact, after possibly extracting a subsequence we may assume that $(\omega_n)_{n \in \mathbb{Z}_{\geq 1}}$ and $(k_n)_{n \in \mathbb{Z}_{\geq 1}}$ are convergent sequences. It follows that $(a_n)_{n \in \mathbb{Z}_{\geq 1}}$

is a convergent subsequence. We recall that $(\alpha_1, \dots, \alpha_r) : A^+ \to {\mathbb{R}_{>0}}^r$ is an isomorphism. It follows that $A^+_{\geq 0}$ is closed in A^+. Because $A(\mathbb{R})$ is a closed subgroup of $G(\mathbb{R})$, that A^+ is a closed subgroup of $A(\mathbb{R})$, this $A^+_{\geq 0}$ is closed in $G(\mathbb{R})$. One deduces that $A^+_{\geq 0} \cdot a$ is closed in $G(\mathbb{R})$ and that the limit of $(a_n)_{n \in \mathbb{Z}_{\geq 1}}$ in $G(\mathbb{R})$ belongs to $A^+_{\geq 0} \cdot a$.

We proved that the original sequence $(\omega_n, a_n, k_n)_{n \in \mathbb{Z}_{\geq 1}}$ contains a convergent infinite subsequence. Thus, it is not a divergent sequence. □

These results have the following consequence.

COROLLARY 5.14. *A sequence $(\omega_n \cdot a_n \cdot k_n)_{n \in \mathbb{Z}_{\geq 1}}$ is divergent in $\overline{\mathfrak{S}}$ if and only if a_n is divergent in $A^+_{\geq 0}$.*

Proof. Because $\overline{\mathfrak{S}}$ is closed, $(\omega_n \cdot a_n \cdot k_n)_{n \in \mathbb{Z}_{\geq 1}}$ is also divergent in $G(\mathbb{R})$. It follows that the sequence $(\omega_n, a_n, k_n)_{n \in \mathbb{Z}_{\geq 1}}$ contains no convergent subsequence. Because $\overline{\Omega}$ and K are compact, the projection map

$$\overline{\Omega} \times A^+_{\geq 0} \cdot a \times K \to A^+_{\geq 0} \cdot a$$

is proper. It follows that the image sequence $(a_n)_{n \in \mathbb{Z}_{\geq 1}}$ is divergent in $A^+_{\geq 0} \cdot a$. □

5.4.3 Let $P_1, \dots, P_r$ be the maximal $\mathbb{Q}$-defined proper[13] parabolic subgroups of G containing P. We denote by N_i their unipotent radicals, and $\mathfrak{n}_i$ the ($\mathbb{Q}$-linear) Lie algebra of N_i. The adjoint representation of G induces an action of G on the $\mathbb{Q}$-vector space $V_i = \bigwedge^{\dim(N_i)} \mathfrak{g}$. Then the $\mathbb{Q}$-vector subspace $\bigwedge^{\dim(N_i)} \mathfrak{n}_i \leq V_i$ is of dimension 1, and we choose a generator η_i of this $\mathbb{Q}$-line.

Then the $\mathbb{R}$-line $\mathbb{R} \cdot \eta_i$ is an eigenspace of A acting on $V_i \otimes \mathbb{R}$, and this eigenspace is defined over $\mathbb{Q}$. Let χ_i be the corresponding eigencharacters of A: we have

$$\forall\, a \in A(\mathbb{R}),\ \forall\, 1 \leq i \leq r,\ \forall a \cdot \eta_i = \chi_i(a) \cdot \eta_i. \tag{34}$$

For $1 \leq i \leq r$ the χ_i are positive multiples $k_1 \cdot \omega_1, \dots, k_r \cdot \omega_r$ of the (relative) fundamental weights[14] $\omega_1, \dots, \omega_r \in X(A) \otimes \mathbb{Q}$. In particular,

$$\forall\, \alpha \in A^+_{\geq 0}, \forall\, 1 \leq i \leq r, \quad \chi_i(\alpha)^{-1} \leq 1. \tag{35}$$

One knows that the fundamental weights are positive $\mathbb{Q}$-linear combinations of α_i and that they form a basis of $X(A) \otimes \mathbb{Q}$. The same holds for χ_i. We deduce the following.

LEMMA 5.15. *Let $(a_n)_{n \in \mathbb{Z}_{\geq 0}}$ be a sequence in $A^+_{\geq 0} \cdot a$. Then the sequence is divergent (no infinite subsequence is convergent) if and only if*

$$\lim_{n \to \infty} \min_{1 \leq i \leq r} \chi_i(a_n)^{-1} = 0. \tag{36}$$

Proof. If $(a_n)_{n \in \mathbb{Z}_{\geq 0}}$ contains a convergent infinite subsequence, then the sequence $(\min_{1 \leq i \leq r} \chi_i(a_n)^{-1})_{n \in \mathbb{Z}_{\geq 0}}$ contains a convergent infinite subsequence in $\mathbb{R}_{>0}$ and we cannot have (36).

This proves one implication and we now prove the other.

Assume that (36) fails. Equivalently,

$$L := \limsup_{n \to \infty} \min_{1 \leq i \leq r} \chi_i(a_n)^{-1} > 0.$$

[13] There are none if $r = 0$.

[14] The 'weights lattice' $\omega_1 \cdot \mathbb{Z} + \cdots + \omega_r \cdot \mathbb{Z} \supset X(A)$ can be identified with $X(\tilde{A})$ where $\tilde{A}$ is the torus in a simply connected cover $\tilde{G}_{\mathbb{R}} \to G_{\mathbb{R}}$ which maps onto A.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

After possibly extracting a subsequence, we have

$$\lim_{n\to\infty} \min_{1\leq i\leq r} \chi_i(a_n)^{-1} = L \neq 0. \tag{37}$$

Because the a_n belong to $A^+_{\geq 0}\cdot a$ we have $\sup_{n\in\mathbb{Z}_{\geq 0}} \alpha_i(a_n)^{-1} \leq \alpha_i(a)^{-1}$ for every $1\leq i\leq r$. Because the χ_i are positive linear combination of the α_i, the $\chi_i(a_n)^{-1}$ are bounded above. According to (37) they are bounded below in $\mathbb{R}_{>0}$. Because the χ_i form a basis of $X(A)\otimes\mathbb{Q}$, the α_i are linear combination of the χ_i. Hence, the $\alpha_i(a_n)$ are bounded above and below in $\mathbb{R}_{>0}$. Equivalently $(a_n)_{n\in\mathbb{Z}_{\geq 0}}$ is bounded in A^+. Hence $(a_n)_{n\in\mathbb{Z}_{\geq 0}}$ is not divergent.

This proves the other implication. □

5.5 Height on Siegel sets

The following statement is the main objective of § 5.

Theorem 5.16. *Let $\mathfrak{S}_W$ as in Definition 5.11 with Z defined over $\mathbb{Q}$, let $\iota : G/Z \to \mathbb{A}^N_{\mathbb{Q}}$ be an affine embedding and let $H_W = H_{\mathbb{R}}\cdot H_f$ be as in (19). Then, as functions $\overline{\mathfrak{S}_W}\cap W(\mathbb{Q})\to\mathbb{R}_{\geq 0}$ we have*

$$H_W \approx H_f.$$

This will be deduced from Proposition 5.9. We first construct the map p to which we apply the proposition, and then verify the assumptions of the proposition.

5.5.1 *Construction of the morphism p.* Let $\eta_i \in V_i = \bigwedge^{\dim \mathfrak{n}_i}\mathfrak{g}$ and χ_i be as in § 5.4.3. For each $1\leq i\leq r$, we choose a positive-definite quadratic form

$$Q_i' \colon V_i \longrightarrow \mathbb{Q}.$$

We denote by dz the Haar probability measure on $Z(\mathbb{R})$ we define the real quadratic form

$$Q_i(v) = \int_{Z(\mathbb{R})} Q_i'(z\cdot v)\, dz : V_i\otimes\mathbb{R}\to\mathbb{R}. \tag{38}$$

The following is central in our argument.

Lemma 5.17. *The quadratic form Q_i is invariant under $Z(\mathbb{R})$, is positive definite, and is defined over $\mathbb{Q}$.*

Proof. The two first properties are immediate from (38). We prove that Q_i is defined over $\mathbb{Q}$. Let V be the $\mathbb{Q}$-vector space of quadratic forms, as a representation of Z, and V^Z be the subspace of elements fixed by Z. As $Z(\mathbb{R})$ is compact, the $\mathbb{Q}$-group Z is reductive, and there is a Z-stable $\mathbb{Q}$-subspace W such that we can decompose

$$V = V^Z \oplus W.$$

Let us write correspondingly

$$Q_i' = Q_Z' + Q_W'$$

with Q_Z' in V^Z and Q_W' in W.

Because Q_Z is invariant under $Z(\mathbb{R})$ and $W\otimes\mathbb{R}$ is stable under $Z(\mathbb{R})$,

$$\int_{Z(\mathbb{R})} z\cdot Q_Z\, dz = Q_Z \quad\text{and}\quad \int_{Z(\mathbb{R})} z\cdot Q_W\, dz \in W\otimes\mathbb{R}.$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

By construction, $\int_{Z(\mathbb{R})} z \cdot Q_W \, dz$ is fixed by $Z(\mathbb{R})$ and, thus, it belongs to $W \otimes \mathbb{R} \cap V^Z \otimes \mathbb{R} = \{0\}$. We compute

$$Q_i = \int_{Z(\mathbb{R})} z \cdot Q_i' \, dz = \int_{Z(\mathbb{R})} z \cdot Q_Z \, dz + \int_{Z(\mathbb{R})} z \cdot Q_W \, dz = Q_Z + 0.$$

Because Q_Z is defined over $\mathbb{Q}$, so is Q_i. □

We can now define $p : W \to \mathbb{A}^r_{\mathbb{Q}}$ by

$$p(gZ) = (Q_1(g^{-1} \cdot \eta_1), \ldots, Q_r(g^{-1} \cdot \eta_r)). \tag{39}$$

As the Q_i are defined over $\mathbb{Q}$ so is p, and as the Q_i are Z-invariant, p is well defined.

5.5.2 *Properties of the morphism p.* Our next task is to verify the assumptions of Proposition 5.9.

(i) We have $p(\overline{\mathfrak{S}_W}) \subset (\mathbb{R}^\times)^r$.
(ii) As a map $\overline{\mathfrak{S}_W} \to (\mathbb{R}^\times)^r$, $p|_{\overline{\mathfrak{S}_W}}$ is proper with respect to the real topologies.
(iii) The image $p(\overline{\mathfrak{S}})$ is bounded in $\mathbb{R}^r$.

Proof of assumption (i). Every point of $\overline{\mathfrak{S}_W}$ is of the form gZ with $g \in G(\mathbb{R})$. The vector $g \cdot \eta_i$ is thus in $V_i \otimes \mathbb{R}$. As $\eta_i \neq 0$ and g is invertible, $g^{-1} \cdot \eta_i \neq 0$. As Q_i is positive definite by Lemma 5.17, we have $p_i(g) := Q_i(g^{-1}\eta_i) \in \mathbb{R}_{>0}$. □

We will use that there exists $C \in \mathbb{R}_{>0}$ such that for every $1 \leq i \leq r$,

$$\forall\, (h, \alpha, k) \in H_P \times A^+_{\geq 0} \times K_\infty, \quad 0 \leq p_i(h \cdot a \cdot \alpha \cdot k) \leq C \cdot \chi_i(\alpha)^{-2}. \tag{40}$$

Proof of (40). We write $\sigma = h \cdot a \cdot \alpha \cdot k$. By (32), we have $h^{-1} \cdot \eta_i = \pm\eta_i$. Thus,

$$\sigma^{-1} \cdot \eta_i = \pm k^{-1} \cdot \alpha^{-1} \cdot a^{-1} \cdot \eta_i = \pm k^{-1} \cdot \chi_i(\alpha)^{-1} \cdot \eta_i.$$

Because K is compact there exists a K-invariant euclidean norm $\|{-}\|$ on $V_i \otimes \mathbb{R}$. The two norms $\sqrt{Q_i}$ and $\|{-}\|$ on $V_i \otimes \mathbb{R}$ are comparable: there is $C_i \in \mathbb{R}_{>0}$ such that for any $v \in V_i \otimes \mathbb{R}$,

$$Q_i(v) \leq C_i \cdot \|v\|^2.$$

We deduce (40) with $C = \max_{i \in \{1;\ldots;r\}} C_i \cdot \|a^{-1} \cdot \eta_i\|^2$ from

$$\begin{aligned} p_i(\sigma) &= Q_i(\sigma^{-1} \cdot \eta_i) \\ &\leq C_i \cdot \|\pm k^{-1} \cdot \chi_i(\alpha)^{-1} \cdot a^{-1} \cdot \eta_i\|^2 \\ &= C_i \cdot \|\pm \chi_i(\alpha)^{-1} \cdot a^{-1} \cdot \eta_i\|^2 \\ &= C_i \cdot \chi_i(\alpha)^{-2} \cdot \|a^{-1} \cdot \eta_i\|^2 \geq 0. \end{aligned}$$ □

Proof of assumption (ii). For a divergent sequence $\sigma_n = \omega_n a \cdot \alpha_n k_n$ in $\overline{\mathfrak{S}_W}$, Corollary 5.14 and Lemma 5.15 imply that $\min_{1 \leq i \leq r} \chi_i(\alpha_n) \to 0$. Using (40), we deduce that

$$\min_{1 \leq i \leq r} p_i(\omega_n a_n a k_n) \to 0 \tag{41}$$

and, thus, $p(\omega_n a_n k_n)$ is divergent in $\mathbb{R}^{\times r}$. This proves the properness. □

Proof of assumption (iii). For $\sigma = h \cdot \alpha \cdot a \cdot k \in \overline{\mathfrak{S}}$, we have $0 \leq \chi_1(\alpha), \ldots, \chi_r(\alpha) \leq 1$ by (35), and deduce from (40) that

$$\max_{1 \leq i \leq r} |p_i(\omega_n a_n a k_n)| \leq C.$$ □

We now use Proposition 5.9 with $\mathfrak{S} = \overline{\mathfrak{S}_W}$. This concludes the proof of Theorem 5.16.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

6. Weak adelic Mumford–Tate hypothesis and lower bounds on Galois orbits

This section is central to the proof of the André–Pink–Zannier conjecture under our assumptions (Theorem 1.2). In this section, we state a precise form of the 'weak adelic Mumford–Tate hypothesis'.

We then translate lower and upper bounds on adelic orbits of Appendices B and C into estimates for sizes of the Galois orbits in terms of the height functions of § 4 (when the Mumford–Tate hypothesis holds).

For simplicity in the following we refer to the 'Mumford–Tate hypothesis' or simply 'MT hypothesis'.

Finally, we provide some natural functoriality properties of the Mumford–Tate hypothesis, which will be needed for the reduction steps in the proof of our main theorem.

6.1 The Mumford–Tate hypothesis

We start with a property applicable in more general situations.

Definition 6.1. Let M be a linear algebraic group over $\mathbb{Q}$, let $K_M \leq M(\mathbb{A}_f)$ be a compact open subgroup, and let $U \leq M(\mathbb{A}_f)$ be a compact subgroup.

We say that U is *MT in* M if the indices

$$[K_M \cap M(\mathbb{Q}_p) : U \cap K_M \cap M(\mathbb{Q}_p)] \tag{42}$$

are finite and uniformly bounded as p ranges through primes, where $M(\mathbb{Q}_p) \leq M(\mathbb{A}_f)$ is understood as a factor subgroup of $M(\mathbb{A}_f)$.

Note that the definition does not depend on the choice of K_M, as any two compact open subgroups are commensurable. We may always enlarge K_M so that it takes the product form $K_M = \prod_p K_p$ in which case the indices become

$$[K_p : U \cap K_p].$$

Likewise if $U' \leq M(\mathbb{A}_f)$ is a compact subgroup commensurable to U, then U is MT in M if and only if U' is MT in M. Note (and this is very important) that the condition that U is MT in M *does not imply* that U is open in $M(\mathbb{A}_f)$.

The following observation is an immediate consequence of the definition.

Lemma 6.2. *In the Definition 6.1, let*

$$U_p := U \cap K_M \cap M(\mathbb{Q}_p) \text{ and } U' = \prod_p U_p \leq \prod_p M(\mathbb{Q}_p). \tag{43}$$

Then U is MT in M if and only if U' is MT in M.

We specialise the above definition to the context of images of Galois representations.

Definition 6.3. Let (G, X) be a Shimura datum, let $x_0 \in X$ and let M be the Mumford–Tate group of x_0, let ρ_{x_0} be a Galois representation for x_0 defined over a field E in the sense of Definition 3.1, and let $U = \rho_{x_0}(Gal(\overline{E}/E)) \leq M(\mathbb{A}_f)$ be the image of ρ_{x_0}.

(i) We say that x_0 *satisfies the MT hypothesis*, if U is MT in M.

(ii) Let $K \leq G(\mathbb{A}_f)$ be a compact open subgroup, and $s_0 = [x_0, 1] \in Sh_K(G, X)$. We say that s_0 *satisfies the MT hypothesis* if U is MT in M.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

6.2 Lower bounds for Galois orbits in terms of finite heights under the MT hypothesis

The following statement is an essential ingredient in the proof of the main theorem (see § 7). We also believe it to be of independent interest.

Theorem 6.4. *Let M be a connected reductive group over $\mathbb{Q}$ and $U \leq M(\mathbb{A}_f)$ be a compact subgroup which is MT in M in the sense of Definition 6.1. We use the notation of Definition 1.7.*

(i) *Let $\phi_0 : M \to GL(N)$ be a representation over $\mathbb{Q}$, and let W be the $GL(N)$-conjugacy class of ϕ_0. We consider an affine embedding $\iota : W \to \mathbb{A}^N_{\mathbb{Q}}$ and the corresponding function $H_f : W(\mathbb{Q}_f) \to \mathbb{Z}_{\geq 1}$ defined by (17). Then, as ϕ ranges through $W(\mathbb{A}_f)$, we have*

$$[\phi(U) : \phi(U) \cap GL(N, \widehat{\mathbb{Z}})] \approx H_f(\phi). \tag{44}$$

(ii) *Let $\phi_0 : M \to G$ be a morphism of algebraic groups over $\mathbb{Q}$ and let W be the G-conjugacy class of ϕ_0. We consider an affine embedding $\iota : W \to \mathbb{A}^N_{\mathbb{Q}}$ and the corresponding function $H_f : W(\mathbb{Q}_f) \to \mathbb{Z}_{\geq 1}$ defined by (17). We also consider an open compact subgroup $K \leq G(\mathbb{A}_f)$. Then, as ϕ ranges through $W(\mathbb{A}_f)$, we have*

$$[\phi(U) : \phi(U) \cap K] \approx H_f(\phi). \tag{45}$$

First, let us reduce the second assertion to the first.

Proof. We identify G with its image by a faithful representation $G \to GL(N)$. We may replace K by a commensurable group, and assume K is a maximal compact subgroup of $G(\mathbb{A}_f)$. For any maximal compact subgroup K' of $GL(N, \mathbb{A}_f)$ such that $K \leq K' \leq GL(N, \mathbb{A}_f)$, we then have

$$K = K' \cap G(\mathbb{A}_f). \tag{46}$$

We choose such a K', and, possibly conjugating by an element of $GL(N, \mathbb{Q})$, we may assume $K' = GL(N, \widehat{\mathbb{Z}})$.

Consider $\phi : M \to G$ in (45). From $\phi(U) \leq G(\mathbb{A}_f)$ and (46), we deduce

$$[\phi(U) : \phi(U) \cap K] = [\phi(U) : \phi(U) \cap K'] = [\phi(U) : \phi(U) \cap GL(N, \widehat{\mathbb{Z}})]. \tag{47}$$

We have identified the left-hand side of (47) with the left-hand side of (45).

It will be enough to identify the right-hand sides. We will show that a height function H_f on the $GL(N)$-conjugacy class of ϕ, when restricted to the G-conjugacy class, is a height function on this G-conjugacy class.

If $H_f : GL(N, \mathbb{A}_f) \cdot \phi \to \mathbb{Z}_{\geq 1}$ is associated to $\iota : GL(N) \cdot \phi \to \mathbb{A}^N_{\mathbb{Q}}$, then its restriction to $GL(N, \mathbb{A}_f) \cdot \phi$ is associated to $\iota' : G \cdot \phi \to GL(N) \cdot \phi \to \mathbb{A}^N_{\mathbb{Q}}$, *provided ι' is a closed embedding.*

It is equivalent to proving that $G \cdot \phi \subseteq GL(N, \mathbb{A}_f) \cdot \phi$ is Zariski closed.

To do this, we choose the map

$$\iota : GL(N) \cdot \phi \xrightarrow{\phi' \mapsto d\phi'} \mathrm{Hom}(\mathfrak{m}, \mathfrak{gl}(N)).$$

By assumption, M is Zariski connected. This map is thus injective. As M is reductive, according to [Ric88, Theorem 3.6], the image of $G \cdot \phi$ is closed in $\mathrm{Hom}(\mathfrak{m}, \mathfrak{gl}(N))$, and thus $G \cdot \phi \subseteq GL(N, \mathbb{A}_f) \cdot \phi$ is Zariski closed. □

We now reduce the first assertion to Corollary B.2, Theorems B.1 and B.4.

Proof. Writing $K = GL(N, \widehat{\mathbb{Z}})$ for short, we may rewrite the left-hand side of (44) as

$$[\phi(U) : \phi(U) \cap K] = |\phi(U) \cdot K/K| = |U/ \overset{-1}{\phi} (K)| = [U : \overset{-1}{\phi} (K)].$$

Theorem C.1 implies $[\phi(U) : \phi(U) \cap K] \preccurlyeq H_f(\phi)$. We now prove $H_f(\phi) \preccurlyeq [\phi(U) : \phi(U) \cap K]$.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

It is enough to obtain a lower bound after replacing U by the smaller group $U' \leq U$ as in Lemma 6.2: without loss of generality we may assume $U = U'$. We thus assume that $U = \prod_p U_p$ as in (43).

The left-hand side is the product of $K_p = GL(N, \mathbb{Z}_p)$, hence we have

$$[\phi(U) : \phi(U) \cap K] = \prod_p [\phi(U_p) : \phi(U_p) \cap K_p].$$

We apply Definition 6.1 for $K_M = M(\widehat{\mathbb{Z}}) = M(\mathbb{A}_f) \cap GL(d, \widehat{\mathbb{Z}})$: the upper bound $C = \sup_p [M(\mathbb{Z}_p) : U_p]$ is finite. Using (B.6) we have

$$[\phi(M(U_p)) : \phi(M(U_p)) \cap GL(N, \mathbb{Z}_p)] \geq \frac{H_p(d\phi)}{c \cdot C}. \tag{48}$$

As in the proof of (B.1) of Theorem B.1, we can deduce

$$[\phi(U) : \phi(U) \cap GL(N, \widehat{\mathbb{Z}})] \geq \frac{1}{(c \cdot C)^{\omega(H_f(d\phi))}} \cdot H_f(d\phi). \tag{49}$$

Arguing as in the proof of (B.2) and (B.3) of Corollary B.2, we obtain

$$H_{W,f}(\phi) \approx H_f(d\phi) \preccurlyeq [\phi(U) : \phi(U) \cap GL(N, \widehat{\mathbb{Z}})]. \tag{50}$$

□

6.3 Functoriality properties of the MT hypothesis

The following uses general properties of adelic topologies on algebraic groups. A good reference is [PR94].

Lemma 6.5. *Let $\phi : M \to G$ be a morphism of connected linear algebraic groups over $\mathbb{Q}$, and let $U \leq M(\mathbb{A}_f)$ be a compact subgroup.*

(i) *If U is MT in M, then $\phi(U)$ is MT in $\phi(M)$.*

(ii) *If ϕ is an isogeny onto its image (i.e. $\ker(\phi)$ is finite), then U is MT in M if $\phi(U)$ is MT in $\phi(M)$.*

(iii) *We assume M is reductive. Let $ad_M : M \to M^{\mathrm{ad}} = M/Z_M(M)$ be the adjoint map, and $ab_M : M \to M^{\mathrm{ab}} = M/[M, M]$ be the abelianisation map. Then U is MT in M if and only if $ad_M(U)$ is MT in M^{ad} and $ab_M(U)$ is MT in M^{ab}.*

The proof of Lemma 6.5 will rely on the following.

Theorem 6.6. *Let $\phi : H \to G$ be an epimorphism of $\mathbb{Q}$-algebraic groups and C be the number of components of* $\ker(\phi)$ *for the Zariski topology.*

(i) *Let $K \leq H(\mathbb{A}_f)$ and $K' \leq G(\mathbb{A}_f)$ be compact open subgroups of the form $\prod_p K_p$ and $\prod_p K'_p$. Then*

$$\forall\, p \gg 0, \phi(K_p) \leq K'_p \text{ and } [K'_p : \phi(K_p)] \leq C.$$

(ii) *If $C = 1$, then the map $p : H(\mathbb{A}_f) \to G(\mathbb{A}_f)$ is open: for any open subgroup $K \leq H(\mathbb{A}_f)$, the image $\phi(K)$ is open in $G(\mathbb{A}_f)$.*

The second assertion, which is [PR94, p. 296, § 6.2, Proposition 6.5], is a corollary of the first assertion. The first assertion follows from [PR94, p. 296, § 6.2, Proposition 6.4] and [PR94, p. 296, § 6.2, Proposition 6.5] (using their exact sequence (6.9) under conditions of their Lemma 6.6).

Let us prove Lemma 6.5(i).

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Proof. We choose a maximal compact subgroup $K_M \leq M(\mathbb{A}_f)$, and a maximal compact subgroup $K' \leq \phi(M)(\mathbb{A}_f)$ containing $\phi(K_M)$. By maximality, they have a product form $K_M = \prod_p K_p$ and $K' = \prod_p K'_p$. According to Definition 6.1, there exists $c \in \mathbb{R}_{>0}$ such that for all primes p, we have $c \geq [K_p : U_p \cap K_p]$. Applying ϕ we deduce

$$c \geq [\phi(K_p) : \phi(U_p \cap K_p)] \geq [\phi(K_p) : \phi(U_p) \cap \phi(K_p)].$$

Let $C \in \mathbb{R}_{>0}$ be given by Theorem 6.6. Using natural inclusions $\phi(U_p) \subseteq \phi(U)_p$ and $\phi(K_p) \subseteq K'_p$, we have

$$\begin{aligned}[K'_p : \phi(U)_p \cap K'_p] &\leq [K'_p : \phi(U_p) \cap \phi(K_p)] \\ &= [K'_p : \phi(K_p)] \cdot [\phi(K_p) : \phi(U_p) \cap \phi(K_p)] \leq C \cdot [\phi(K_p) : \phi(U_p) \cap \phi(K_p)]. \quad (51)\end{aligned}$$

Thus, for every prime p, we have $[K'_p : \phi(U)_p \cap K'_p] \leq c \cdot C$. □

We now prove Lemma 6.5(ii).

Proof. We write $K_M = \prod K_p$ and $K' = \prod K'_p$ as before.

We choose a set of generators $\phi(u_1), \ldots, \phi(u_k)$ for $\phi(U)_p$ and let $U' \leq U$ be the compact subgroup topologically generated by u_i. Let us prove that k can be chosen independently of p. □

Proof. For a fixed p we use assertion (i) of Lemma 6.8 with $V = \phi(U)_p$. For large p, the group $V' := \exp(p\phi(\mathfrak{m}_{\mathbb{Z}_p}))$ and the reduction map $M(\mathbb{Z}_p) \to M(\mathbb{F}_p)$ are well defined and, by assertion (iii) of Lemma 6.8, we have $V' \leq V \leq M(\mathbb{Z}_p)$. Applying the remark from the proof of Proposition 6.7 to the exact sequence $1 \to V' \to V \to M(\mathbb{F}_p)$, it follows from Proposition 6.7 for the image of V and assertion (ii) of Lemma 6.8 for V'. □

Let F be the kernel of ϕ. This is a finite algebraic group by hypothesis. We define $U'_p = U' \cap M(\mathbb{Q}_p)$. Then U'_p is also the kernel of the map

$$\begin{aligned} U' \hookrightarrow \overset{-1}{\phi}\left(\phi(M(\mathbb{A}_f))\right) \to \overset{-1}{\phi}\left(\phi(M(\mathbb{Q}_p))\right) \\ \to \overset{-1}{\phi}\left(\phi(M(\mathbb{Q}_p))\right)/M(\mathbb{Q}_p) \xleftarrow{\sim} F(\mathbb{A}_f)/(F \cap M)(\mathbb{Q}_p). \quad (52)\end{aligned}$$

The last group is a commutative group isomorphic to a subgroup of $(\mathbb{Z}/(C))^{\infty}$ where $C = |F(\overline{\mathbb{Q}})|$. Because U' is generated by k elements, the size of the image of U' is bounded by C^k.

We deduce

$$[\phi(U)_p : \phi(U_p)] \leq [\phi(U') : \phi(U_p)] \leq [\phi(U') : \phi(U'_p)] \leq [U' : U'_p] \leq C^k. \quad (53)$$

□

PROPOSITION 6.7. *For all $N \in \mathbb{Z}_{\geq 0}$ there exists $k = k(N)$ such that for every prime p and every subgroup $U \leq GL(N, \mathbb{F}_p)$, there exist $u_1, \ldots, u_k$ in U which generate U.*

Proof. We fix N. There exists $p(N) \in \mathbb{Z}_{\geq 0}$ such that $p \geq p(N)$, so that Nori applies [Nor87].

For $p \leq p(N)$ we have $\#U \leq \#GL(N, \mathbb{F}_p) \leq p(N)^{N^2}$ and we take $k(N) = p(N)^{N^2}$.

We assume that $p \geq p(N)$ and apply Nori theory [Nor87].

According to Jordan theorem [Nor87, Theorem C] there exist normal subgroups $U^+ \leq U' \leq U$ with U^+ generated by the unipotent elements of U, and U'/U^+ abelian of order prime to p, and $[U : U'] \leq d(N)$, where $d(N)$ is as in [Nor87, Theorem C]. According to [Nor87], there exists $\tilde{U} \leq GL(N)_{\mathbb{F}_p}$ such that $\tilde{U}(\mathbb{F}_p)^+ = U^+$. Define $U'' = \tilde{U}(\mathbb{F}_p) \cap U$. Moreover, one knows[15] that there exists an injective morphism $U'/U'' \hookrightarrow GL(N', \mathbb{F}_p)$, where N' is bounded in terms of N.

[15] See [Ser98, no. 134, p. 25 and no. 137, p. 38–39, bottom of p. 44].

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

We will use the following remark. For every exact sequence $1 \to K \to G \to Q \to 1$, if K and Q are generated by k_N and k_Q elements, then G is generated by $k_K + k_Q$ elements. Thus, in order to bound the size of a generating subset of G, it suffices to do it for K and for Q.

Using the remark, it will be enough to prove that U/U', U'/U'', U''/U^+ and U^+ can be generated by $k_1(N), k_2(N), k_3(N), k_4(N)$ elements. Then the proposition will be satisfied with $k(N) = \max\{k_1(N) + k_2(N) + k_3(N) + k_4(N); p(N)^{N^2}\}$.

As $\#U/U' \leq d(N)$, we can take $k_1(N) = d(N)$.

As $\tilde{U}$ is generated by unipotent subgroups, we can write $\tilde{U} = \tilde{S} \cdot \tilde{N}$ where $\tilde{S}$ is semisimple and $\tilde{N}$ is the unipotent radical. According to [Nor87, Remark 3.6, 3.6(v)], we have $\tilde{S}(\mathbb{F}_p)/\tilde{S}(\mathbb{F}_p)^+ \leq 2^N$. We deduce that $\#U''/U^+ \leq \#\tilde{U}(\mathbb{F}_p)/\tilde{U}(\mathbb{F}_p)^+ = \#\tilde{S}(\mathbb{F}_p)/\tilde{S}(\mathbb{F}_p)^+ \leq 2^N$.

We can thus take $k_3(N) = 2^N$.

The factor U'/U'' is isomorphic to an abelian subgroup of $GL(N', \mathbb{F}_p)$ of order prime to p. It is thus diagonalisable over some extension $\mathbb{F}_q$. Because ${\mathbb{F}_q}^\times$ is cyclic, every subgroup of $({\mathbb{F}_q}^\times)^{N'}$ is generated by at most N' elements.

We can thus take $k_2(N) = N'$.

Let $\tilde{U} \leq GL(N)_{\mathbb{F}_p}$ be the algebraic group associated to U and let $\tilde{\mathfrak{u}} \leq \mathfrak{gl}(N, \mathbb{F}_p)$ be its Lie algebra. By [Nor87], $\tilde{\mathfrak{u}} \leq \mathfrak{gl}(N, \mathbb{F}_p)$ is linearly generated by nilpotents. Let $X_1, \ldots, X_d$, with $d \leq N^2$ be a linear basis of nilpotent elements. Denote by $U' = \langle \exp(X_1), \ldots, \exp(X_d) \rangle$ the group generated by their exponentials, and consider the associated $\tilde{\mathfrak{u}}' \leq \tilde{\mathfrak{u}}$ and $\tilde{U}' \leq \tilde{U}$. We have $X_1, \ldots, X_d \in \tilde{\mathfrak{u}}'$. Thus, $\tilde{\mathfrak{u}}' = \tilde{\mathfrak{u}}$ and $\tilde{U}' = \tilde{U}$. From [Nor87, Theorem B], we get $U = U^+ = \tilde{U}(\mathbb{F}_p)^+ = \tilde{U}'(\mathbb{F}_p)^+ = U'^+ = U'$. Thus, U is generated by at most N^2 elements $\exp(X_1), \ldots, \exp(X_d)$.

We can thus take $k_4(N) = N^2$. □

We used the following.

Lemma 6.8. *Let $M \leq GL(N)$ be an algebraic subgroup defined over $\mathbb{Q}_p$ and let $\mathfrak{m} \leq \mathfrak{gl}(N, \mathbb{Q}_p)$ be its Lie algebra.*

(i) *Let $V \leq GL(N, \mathbb{Z}_p)$ a compact subgroup. Then V is topologically finitely generated.*
(ii) *Then $V' := \exp(\mathfrak{m} \cap 2p\mathfrak{gl}(N, \mathbb{Z}_p))$ is topologically generated by at most N^2 elements if p is large enough.*
(iii) *Let $M(\mathbb{Z}_p) := M(\mathbb{Q}_p) \cap GL(N, \mathbb{Z}_p)$ and $V \leq M(\mathbb{Z}_p)$ an open subgroup such that $C := [M(\mathbb{Z}_p) : V] \in \mathbb{Z}_{\geq 1}$. Then for $p > C$, we have*

$$V' \leq V.$$

Proof. The first assertion is [Ser64, Proposition 2].

Let $G = \exp(2p\mathfrak{gl}(N, \mathbb{Z}_p)) = 1 + 2p\mathfrak{gl}(N, \mathbb{Z}_p)$ and $H = V' \leq G$. According to [DSMS99, Theorem 5.2] the pro-p group is powerful and $d(G) = N^2$, where $d(G)$ is the minimal cardinality of a set of generators for G as in [DSMS99, p. 41]. We can, thus, apply [DSMS99, Theorem 2.9]. This proves the second assertion.

As G is a pro-p group, by [PR94, Lemma 4.8, p. 138], V' is a pro-p group. We also have

$$[V' : V' \cap V] \leq [M(\mathbb{Z}_p) : V] = C.$$

Assume $p > C$ and assume, by contradiction, that there exists $w \in V' \smallsetminus V$. We denote by $w^{\mathbb{Z}}$ the subgroup generated by w. Then $c := [w^{\mathbb{Z}} : w^{\mathbb{Z}} \cap V] \neq 1$ and $c \leq C$. But c is a power of p because V' is a pro-p group: thus, $c \geq p$. We deduce that $C \geq c \geq p$. This contradicts our assumptions. □

We prove assertion (iii) of Lemma 6.5. We will make use of Goursat's lemma.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Proof. As M is reductive, the map $(ad_M, ab_M) : M \to M' := M^{\mathrm{ad}} \times M^{\mathrm{ab}}$ is an isogeny. From assertion (ii) of Lemma 6.5 it follows that it is enough to prove that the image V of U in $M'(\mathbb{A}_f)$ is MT in M'. We may thus assume $M = M^{\mathrm{ad}} \times M^{\mathrm{ab}}$.

Using Lemma 6.2 we may assume $U = \prod_p U_p$. Let

$$K_M = \prod K_{M,p} = \prod_p K_{M^{\mathrm{ad}},p} \times K_{M^{\mathrm{ab}},p} \leq M(\mathbb{A}_f)$$

be a maximal compact subgroup containing U.

By assumption, there is an upper bound $C \in \mathbb{Z}_{\geq 1}$ for $[K_{M^{\mathrm{ab}},p} : ab_M(U_p)]$ and $[K_{M^{\mathrm{ad}},p} : ad_M(U_p)]$, independent of p.

Let $H_1 = ad_M(U_p)$ and $H_2 = ab_M(U_p)$ and $\Gamma = (ad_M, ab_M)(U_p) \leq H_1 \times H_2$. Let $N_1 = \Gamma \cap H_1$ and $N_2 = \Gamma \cap H_2$. By Goursat's lemma, N_1 and N_2 are normal subgroups in H_1 and H_2 and there is an isomorphism (whose graph is $\Gamma/(N_1 \times N_2)$)

$$H_1/N_1 \xrightarrow{\sim} H_2/N_2. \tag{54}$$

Because H_2 is abelian, N_1 contains the derived subgroup $[H_1, H_1]$.

By the first part of Lemma 6.9, $[H_1 : N_1]$ is finite for every prime p, and by the second part of Lemma 6.9, $[H_1 : N_1]$ is bounded by $C(M^{\mathrm{ad}})$ for almost every prime p.

As a result there exists $C' \in \mathbb{Z}_{\geq 1}$ such that $[H_1 : N_1] \leq C'$ for every prime p. Using (54), we also have $[H_2 : N_2] \leq C'$ for every prime p.

Recall that $N_1 \times N_2 \leq \Gamma$. It follows

$$[H_1 \times H_2 : \Gamma] \leq [H_1 : N_1] \cdot [H_2 : N_2] = C'^2.$$

By the definition of C,

$$[K_{M,p} : H_1 \times H_2] \leq C^2.$$

We deduce

$$[K_{M,p} : (ad_M, ab_M)(U_p)] = [K_p : H_1 \times H_2] \cdot [H_1 \times H_2 : \Gamma] \leq C^2 C'^2.$$

The bound is independent of p, which concludes. □

LEMMA 6.9. *Let G be a semisimple algebraic group over $\mathbb{Q}$, and for every prime p, let $U_p, K_p \leq G(\mathbb{Q}_p)$ be compact open subgroups such that $K = \prod_p K_p \leq G(\mathbb{A}_f)$ is open. Let $[U_p, U_p]$ be the subgroup generated by commutators.*

(i) *For every prime p, the quotient $U_p/[U_p, U_p]$ is finite.*
(ii) *There exists $C(G) \in \mathbb{Z}_{\geq 1}$ such that, for almost all p, if $[K_p : U_p \cap K_p] < p$ then $U_p/[U_p, U_p] < C(G)$.*

Proof. The first assertion follows from the fact that $[U_p, U_p]$ is open, because G is semisimple.

We prove the second assertion. We may replace U_p by $K_p \cap U_p$ and assume $U_p = K_p \cap U_p \leq K_p$. Thus, $[K_p : K_p \cap U_p] = [K_p : U_p] < p$.

Let us identify G with its image by a faithful linear representation $G \to GL(N)$. For p large enough, we have $K_p = G(\mathbb{Z}_p) := G(\mathbb{Q}_p) \cap GL(N, \mathbb{Z}_p)$.

Let $G(\mathbb{Z}_p)^+$ and $G(\mathbb{F}_p)^+$ be as in Lemma 6.10 below.

Then $U_p \cap G(\mathbb{Z}_p)^+$ is an open subgroup of $G(\mathbb{Z}_p)^+$ and,

$$[G(\mathbb{Z}_p)^+ : U_p \cap G(\mathbb{Z}_p)^+] \leq [G(\mathbb{Z}_p) : U_p] < p.$$

(Recall the assumption $[K_p : U_p] < p$.)

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

As $G(\mathbb{Z}_p)^+$ is generated by pro-p-groups, we have, for every subgroup $L \leq G(\mathbb{Z}_p)^+$,

$$[G(\mathbb{Z}_p)^+ : L] > 1 \Rightarrow [G(\mathbb{Z}_p)^+ : L] \geq p.$$

Therefore, with $L = U_p$,

$$[G(\mathbb{Z}_p)^+ : U_p \cap G(\mathbb{Z}_p)^+] = 1.$$

At the level of derived subgroups, we have

$$[G(\mathbb{Z}_p)^+, G(\mathbb{Z}_p)^+] \subseteq [U_p, U_p].$$

We deduce

$$[G(\mathbb{Z}_p) : [U_p, U_p]] \leq [G(\mathbb{Z}_p) : G(\mathbb{Z}_p)^+] \cdot [G(\mathbb{Z}_p)^+ : [G(\mathbb{Z}_p)^+, G(\mathbb{Z}_p)^+]].$$

We note that $G(\mathbb{Z}_p)^+ \leq G(\mathbb{Z}_p)$ is an open subgroup of index prime to p. It follows that the image of $G(\mathbb{Z}_p)^+$ in $G(\mathbb{F}_p)$ contains $G(\mathbb{F}_p)^+$. Thus,

$$[G(\mathbb{Z}_p) : G(\mathbb{Z}_p)^+] \leq [G(\mathbb{F}_p) : G(\mathbb{F}_p)^+].$$

We have, by [Nor87, p. 270],

$$[G(\mathbb{F}_p) : G(\mathbb{F}_p)^+] \leq 2^N. \tag{55}$$

For p large enough we have:

– $G(\mathbb{F}_p) = \tilde{G}(\mathbb{F}_p)$ for a connected semisimple $\mathbb{F}_p$-algebraic subgroup $\tilde{G} \leq GL(N)_{\mathbb{F}_p}$;
– $[\tilde{G}(\mathbb{F}_p)^+, \tilde{G}(\mathbb{F}_p)^+] = [\tilde{G}, \tilde{G}](\mathbb{F}_p)^+ = \tilde{G}(\mathbb{F}_p)^+$, using Lemma 6.11.

Thus, $[G(\mathbb{Z}_p)^+, G(\mathbb{Z}_p)^+]$ maps surjectively onto

$$[G(\mathbb{F}_p)^+, G(\mathbb{F}_p)^+] = G(\mathbb{F}_p)^+.$$

We apply Lemma 6.10 to $H = [G(\mathbb{Z}_p)^+, G(\mathbb{Z}_p)^+]$. We deduce

$$[G(\mathbb{Z}_p)^+, G(\mathbb{Z}_p)^+] = G(\mathbb{Z}_p)^+.$$

This implies

$$[G(\mathbb{Z}_p)^+ : [G(\mathbb{Z}_p)^+, G(\mathbb{Z}_p)^+]] = 1. \tag{56}$$

The second assertion of Lemma 6.9 follows from (55) and (56). □

Lemma 6.10 [CK16, Fact 2.4 and its proof]. *Let $G \leq GL(N)_{\mathbb{Q}}$ be a connected semisimple algebraic subgroup. For every prime p, define $G(\mathbb{Z}_p) := G(\mathbb{Q}_p) \cap GL(N, \mathbb{Z}_p)$ and denote by $G(\mathbb{F}_p)$ the image of $G(\mathbb{Z}_p)$ in $GL(N, \mathbb{F}_p)$. We denote by $G(\mathbb{F}_p)^+ \leq G(\mathbb{F}_p)$ and $G(\mathbb{Z}_p)^+ \leq G(\mathbb{Z}_p)$ the subgroups generated by p-Sylow subgroups, respectively, pro-p-Sylow.*

Then, for p large enough: if $H \leq G(\mathbb{Z}_p)^+$ maps surjectively onto $G(\mathbb{F}_p)^+$, then $H = G(\mathbb{Z}_p)$.

We used the following in the proof of Lemma 6.9.

Lemma 6.11. *For every $n \in \mathbb{Z}_{\geq 0}$, there exists $c(n)$ such that the following holds. Let $p \geq c(n)$ be a prime, and let $G \leq GL(n)$ be a semisimple algebraic group over $\mathbb{F}_p$.*

Then $[G(\mathbb{F}_p)^+, G(\mathbb{F}_p)^+] = G(\mathbb{F}_p)^+$.

Proof. Let $\pi : G^{\mathrm{sc}} \to G$ be the simply connected cover. According to [MT11, 24.15], we have $G^{\mathrm{sc}}(\mathbb{F}_p)^+ = G^{\mathrm{sc}}(\mathbb{F}_p)$.

It follows that $\pi(G^{\mathrm{sc}}(\mathbb{F}_p)) \leq G(\mathbb{F}_p)^+$. Since $G(\mathbb{F}_p)^+$ is generated by elements of order a power of p, we have the following alternative:

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

- either $\pi(G^{\mathrm{sc}}(\mathbb{F}_p)) = G(\mathbb{F}_p)^+$;
- or $\#G(\mathbb{F}_p)^+/\pi(G^{\mathrm{sc}}(\mathbb{F}_p)) \geq p$.

Let $Z = \ker(\pi : G^{\mathrm{sc}}(\overline{\mathbb{F}_p}) \to G(\overline{\mathbb{F}_p}))$.

By [MT11, 24.21], we have $\#G(\mathbb{F}_p)^+/\pi(G^{\mathrm{sc}}(\mathbb{F}_p)) \leq \#Z$.

On the other hand, there exists an integer $c(n)$ (depending only on n) such that we have $\#Z \leq c(n)$. Thus, for $p > c(n)$, the second case of the alternative does not happen.

By [MT11, 24.17], for $p \geq 4$, the group $G^{\mathrm{sc}}(\overline{\mathbb{F}_p})$ is perfect. It implies that its quotient $\pi(G^{\mathrm{sc}}(\mathbb{F}_p)) = G(\mathbb{F}_p)^+$ is perfect, namely, that $[G(\mathbb{F}_p)^+, G(\mathbb{F}_p)^+] = G(\mathbb{F}_p)^+$. □

6.4 MT hypothesis for Images of Galois representations

We use the notation of Definition 6.3. We assume furthermore that E is of finite type over $\mathbb{Q}$. In this case, we have the following.

Lemma 6.12. *If x_0 is a special point (i.e. $M = M^{\mathrm{ab}}$), then x_0 satisfies the MT hypothesis.*

The Galois representation $Gal(\overline{E}/E) \to M^{\mathrm{ab}}(\mathbb{A}_f)$ is prescribed by Deligne–Shimura reciprocity law, which is part of the definition of a canonical model [Del79, 2.2.5]. In this case, we know that $M = M^{\mathrm{ab}}$ is the Zariski closure of the image of x_0. It follows that the morphism [Del79, 2.2.2.1] is an epimorphism, and we can apply Theorem 6.6.[16]

Using Lemmas 6.12 and of 6.5(iii) we have the following.

Lemma 6.13. *The point x_0 satisfies the MT hypothesis if and only if $ad_M(x_0)$ satisfies the MT hypothesis.*

The following is not needed but can help relate our MT hypothesis to other notions found in literature.

Theorem 6.14. *Assume M is a semisimple and simply connected algebraic group over $\mathbb{Q}$. Then a compact subgroup $U \leq M(\mathbb{A}_f)$ is MT in M if and only if it is an open subgroup.*

Theorem 6.14 is a consequence of the following.

Lemma 6.15. *Let $M \leq GL(n)_{\mathbb{Q}}$ be a simply connected semisimple $\mathbb{Q}$-algebraic subgroup, and, for every prime p, define $M(\mathbb{Z}_p) := M(\mathbb{Q}_p) \cap GL(n, \mathbb{Z}_p)$.*

There exists C such that for every prime $p \geq C$, every $U \leq M(\mathbb{Z}_p)$ satisfies

$$U = M(\mathbb{Z}_p) \text{ or } [M(\mathbb{Z}_p) : U] \geq p.$$

Proof. This is a consequence of the following claim: for $p \gg 0$, the group $M(\mathbb{Z}_p)$ is generated by topologically p-nilpotent elements.

Let us prove the claim. For every prime p, every element in the kernel of the morphisms $red_p : M(\mathbb{Z}_p) \to GL(n, \mathbb{F}_p)$ belongs to $1 + p\mathfrak{gl}(\mathfrak{n}, \mathbb{Z}_{\mathfrak{p}})$ and is topologically p-nilpotent. It will be enough to prove that $red_p(M(\mathbb{Z}_p))$ is generated by elements of order power of p. For $p \gg 0$, the group $M(\mathbb{Z}_p)$ is hyperspecial and the model of M induced by $GL(n)_{\mathbb{Z}}$ is smooth over $\mathbb{Z}_p$ with semisimple fibre $M_{\mathbb{F}_p}$. This implies that the map $M(\mathbb{Z}_p) \to M_{\mathbb{F}_p}(\mathbb{F}_p)$ is surjective. For $p \gg 0$ the algebraic group $M_{\mathbb{F}_p}$ is semisimple and simply connected.[17] By [MT11, 24.15] we have $M(\mathbb{F}_p) = M(\mathbb{F}_p)^+$. This proves the claim. □

[16] If the kernel of $\mu_h : GL(1)_E \to T_E$ is connected, then the Galois image is actually open for the topology induced by the adelic topology on $T(\mathbb{A}_f)$. This is also the H-maximality condition. See [CM20].

[17] This is [MVW84, § 6.5] and here is an argument. Passing to a finite extension of $\mathbb{Q}$ we may assume that M is simply connected and hyperspecial at p. Applying [Tit79, § 3.5.4], we deduce that the special fibre is simply connected. The case $C - BC_n$ of [Tit79, p. 61] is excluded in the hyperspecial case.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

This relies on strong approximation, Hasse principle, and Kneser–Tits properties for M. See [Del71] for related discussions.

6.4.1 For moduli spaces of abelian varieties or, more generally, for Shimura varieties of abelian type, a Galois representation associated to a point $x_0 \in X$ can be deduced from the Galois representation on the Tate module of an abelian variety.

We have the following.

Theorem 6.16 [CM20, Theorem A(i)] and [HR16, Theorem 10.1]. *Let S be a Shimura variety of Hodge type, let $s \in S$ be a point.*

If the abelian variety A associated to s satisfies the classical Mumford–Tate conjecture at some prime ℓ, then s satisfies the weakly adelic Mumford–Tate hypothesis.

Using Lemma 6.13 we can deduce the following.

Theorem 6.17. *Let S be a Shimura variety of abelian type, let $s \in S$ be a point.*

If s satisfies the Mumford–Tate conjecture at some prime ℓ in the sense of [UY13], then s satisfies the weakly adelic Mumford–Tate hypothesis.

6.4.2 As observed in [Bal20], the combination of a theorem of Deligne and André and with a theorem of Weisfeiler [MVW84] and Nori [Nor87] produces, in *any* Shimura variety, *many* examples of (non-algebraic) points for which the MT hypothesis is satisfied. With our terminology it is stated as follows.

Theorem 6.18 [Bal20, Theorem 1.2]. *Let M be the Mumford–Tate group of a point $x_0 \in X$ for a Shimura datum (G, X). We decompose the adjoint datum $(M^{\mathrm{ad}}, X_{M^{\mathrm{ad}}})$ of $(M, X_M) := (M, M(\mathbb{R}) \cdot x_0)$ as a product*

$$(p_1, \dots, p_f) : (M^{\mathrm{ad}}, X_{M^{\mathrm{ad}}}) \simeq (M_1, X_1) \times \cdots \times (M_f, X_f)$$

with respect to the $\mathbb{Q}$-simple factors M_i of M^{ad}.

Assume that for some compact open subgroups $K_i \leq M_i(\mathbb{A}_f)$

$$\forall\, i \in \{1; \dots; f\},\ [p_i \circ ad_M(x_0)] \in Sh_{K_i}(M_i, X_i)(\mathbb{C}) \smallsetminus Sh_{K_i}(M_i, X_i)(\overline{\mathbb{Q}}).$$

Then x_0 satisfies the MT hypothesis.

7. Proof of the main result

In this section we prove the Theorem 1.2, following the strategy outlined in § 1.4. We then give in § 7.3 a variant of the Pila–Wilkie theorem.

7.1 Reduction steps

We put ourselves in the situation of Theorem 1.2 and Conjecture 1.1.

Let Z be an irreducible component of $\overline{\Sigma}^{\mathrm{Zar}}$. The aim is to prove that Z is weakly special. We may replace Σ by $\mathcal{H}(x_0) \cap Z$.

7.1.1 *Reduction to the Hodge generic case.* We will reduce the theorem to the case where Z is Hodge generic in $Sh_K(G, X)$. For convenience, we will assume that $s_0 = [x_0, 1] \in Z$. We choose a Hodge generic point z in Z. One knows that one can choose a lift $\tilde{z}$ of z in X such that the

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Mumford–Tate group G' of $\tilde{z}$ contains M. We write $X' = G'(\mathbb{R}) \cdot \tilde{z}$. We have a Shimura morphism

$$\Psi : Sh_{K \cap G'(\mathbb{A}_f)}(G', X') \to Sh_K(G, X).$$

(The smallest special subvariety of $Sh_K(G, X)$ containing Z is the image of one component of $Sh_{K \cap G'(\mathbb{A}_f)}(G', X')$.) Let Z' be the inverse image of Z by Ψ. It is known that Z is weakly special if and only if any component of Z' is weakly special.

In the notation of Proposition 2.6, we have

$$\Sigma' := \overset{-1}{\Psi}(\Sigma) = \mathcal{H}'([x_0, 1]) \cap Z'.$$

Because $Sh_{K \cap G'(\mathbb{A}_f)}(G', X') \to \Psi(Sh_{K \cap G'(\mathbb{A}_f)}(G', X'))$ is flat, and because Z is in the image of Ψ, we deduce that Σ' is dense in Z' and, hence, dense in every component of Z'.

Thus, in proving the conclusion of the theorem we may replace Z by a component of Z', and (G, X) by (G', X'), and K by $K \cap G'(\mathbb{A}_f)$.

On the other hand, the Mumford–Tate hypothesis depends only on M, and thus is insensitive to such substitutions.

In other words, *we can, and will, assume that Z is Hodge generic in $Sh_K(G, X)$.*

7.1.2 *Reduction to the adjoint datum.* We will reduce the theorem to the case where $G = G^{\mathrm{ad}}$ is of adjoint type. Here we use geometric Hecke orbits.

Using Theorem 2.4, we write our generalised Hecke orbit

$$\mathcal{H}([x_0, 1]) = \mathcal{H}^g([x_0, 1]) \cup \cdots \cup \mathcal{H}^g([x_k, 1])$$

as a finite union of geometric Hecke orbits. We define accordingly

$$\Sigma_i = Z \cap \mathcal{H}^g([x_i, 1]).$$

As Z is irreducible there at least one $i \in \{0; \ldots; k\}$ such that Σ_i is Zariski dense in Z.

Because the Galois representations $\rho_{x_1}, \ldots, \rho_{x_k}$ of $x_1, \ldots, x_k$ can be deduced from ρ_{x_0} using § 3, the Mumford–Tate hypothesis will still be valid even if we replace x_0 by x_i. We assume, for simplicity, that $x_i = x_0$.

We choose an open compact subgroup $K' \leq G^{\mathrm{ad}}(\mathbb{A}_f)$ so that we can consider the Shimura morphism

$$\Psi : Sh_K(G, X) \to Sh_{K'}(G^{\mathrm{ad}}, X^{\mathrm{ad}}).$$

Let Z' be the image of Z. One knows that Z is weakly special in $Sh_K(G, X)$ if and only if Z' is weakly special in $Sh_{K'}(G^{\mathrm{ad}}, X^{\mathrm{ad}})$.

Then $\Psi(\Sigma_0)$ is dense in Z'. Denote x_0^{ad} the image of x_0 in X^{ad}, and define

$$\Sigma' := \mathcal{H}^g([x_0^{\mathrm{ad}}, 1]).$$

Using § 2.2.3, we get

$$\Psi(\Sigma_0) \subset \Sigma' \subset Z'$$

and, thus, Σ' is Zariski dense in Z'.

Let M' be the image of M by $ad_G : G \to G^{\mathrm{ad}}$. Then $M^{\mathrm{ad}} \simeq M'^{\mathrm{ad}}$ because $\ker(ad_G)$ is commutative and central in G. In view of § 6, the Mumford–Tate hypothesis will still hold for $x_0^{\mathrm{ad}} \in X^{\mathrm{ad}}$.

Thus, *we can, and will, assume $G = G^{\mathrm{ad}}$.*

7.1.3 *Induction argument for factorisable subvarieties.* The following reduction will be useful at the very end of the whole proof.

We recall that G is a direct product $G_1 \times \cdots \times G_f$ of its $\mathbb{Q}$-simple subgroups.

It can be easily proved that in the Theorem 1.2 we can replace K by any other compact open subgroup. After possibly replacing K by the open subgroup $\prod_{i=1}^{f} K_i := \prod_{i=1}^{f} K \cap G_i(\mathbb{A}_f)$, there are factorisations $X = \prod_{i=1}^{f} X_i$ and

$$Sh_K(G,X) = \prod_{i=1}^{f} Sh_{K_i}(G_i, X_i). \tag{57}$$

The factorisation (57) is defined over the reflex field $E(G,X)$, hence over E. Consider a nontrivial partition $\{1;\dots;f\} = I \sqcup J$ and the corresponding nontrivial factorisation of Shimura data

$$(G,X) \xrightarrow{(p_I,p_J)} (G_I,X_I) \times (G_J,X_J)$$

with

$$(G_I,X_I) = \prod_{i\in I}(G_i,X_i) \quad \text{and} \quad (G_J,X_J) = \prod_{i\in I}(G_j,X_j).$$

By functoriality (§ 3.2) for $\phi = p_I \circ \phi_0$ (respectively, $\phi = p_J \circ \phi_0$), we will have

$$\rho_{p_I(x_0)} = p_I \circ \rho_{x_0} \quad \text{and} \quad \rho_{p_J(x_0)} = p_J \circ \rho_{x_0}.$$

As explained in § 6, the Mumford–Tate hypothesis will hold for $p_I(x_0)$ and for $p_J(x_0)$.

Suppose that Z factors as a Cartesian product

$$Z_I \times Z_J \subseteq Sh_{K_I}(G_I,X_I) \times Sh_{K_J}(G_J,X_J) \tag{58}$$

in the corresponding factorisation of Shimura varieties. From § 2.2.2, we have

$$\mathcal{H}^g(x_0) = \mathcal{H}^g(p_I(x_0)) \times \mathcal{H}^g(p_J(x_0))$$

and

$$\mathcal{H}^g([x_0,1]) = \mathcal{H}^g([p_I(x_0,1)]) \times \mathcal{H}^g([p_J(x_0),1]).$$

Recall that the partition $\{1;\dots;f\} = I \sqcup J$ is not trivial. Arguing by induction on f, we can assume that Theorem 1.2 is proven for Z_I and Z_J. Then $Z_I \times Z_J$ is also a weakly special subvariety and we are done.

Henceforth, we assume that for every nontrivial partition $\{1;\dots;f\} = I \sqcup J$, the variety Z is not a product of the form (58).

7.2 Central arguments

Let us recollect some of the notation and notions we will be using.

We have an irreducible subvariety Z of $\mathrm{Sh}_K(G,X)$ containing a Zariski-dense subset Σ contained in the generalised Hecke orbit $\mathcal{H}([x_0,1])$ of the point $[x_0,1]$. Let E be a field of finite type over $\mathbb{Q}$ such that Z and $[x_0,1]$ are defined over E, and passing to a finite extension we have a Galois representation $\rho : \mathrm{Gal}(\overline{E}/E) \to M(\mathbb{A}_f) \cap K$ as in Definition 3.1 and our main hypothesis is that its image $U := \rho(\mathrm{Gal}(\overline{E}/E))$ satisfies Definition 6.3. Passing to a finite extension we also assume that E is a field of definition for every geometric component of $Sh_K(G,X)$.

We reduce Theorem 1.2 to the case where Σ is contained in a single geometric Hecke orbit. According to Theorem 2.4 the generalised Hecke orbit is a finite union of geometric orbit, with

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

$\phi_0 : M \to G$ the identity map,

$$\mathcal{H}([x_0,1]) = \mathcal{H}^g([x_0,1]) \cup \mathcal{H}^g([\phi_1 \circ x_0, 1]) \cup \cdots \cup \mathcal{H}^g([\phi_k \circ x_0, 1]). \tag{59}$$

As Z is irreducible, at least one of the intersections $Z \cap \mathcal{H}^g([\phi_i \circ x_0, 1])$ is Zariski dense in Z. From § 3.2, we obtain $\rho_{\phi_i \circ x_0} = \phi_i \circ \rho_{x_0}$ and the MT hypothesis is still valid for $\phi(U)$ in $\phi(M) = M_{\phi_i \circ x_0}$. Without loss of generality, we may assume $\phi_i = \phi_0$, that is $\phi_i \circ x_0 = x_0$.

We may also assume that $[x_0, 1] \in Z$ and, thus, that Z is contained in the image of $X \times \{1\}$ in $Sh_K(G,X)$.

7.2.1 *Covering by Siegel sets.* We choose a minimal $\mathbb{Q}$-parabolic subgroup P of G and a maximal compact subgroup K_∞ of $G(\mathbb{R})^+$, for instance $K_{x_0} = Z_{G(\mathbb{R})}(x_0)$. We define

$$X^+ = G(\mathbb{R})^+ \cdot x_0 \subset X$$

and denote by

$$S^+ \subset Sh_K(G,X)$$

the geometric component of $Sh_K(G,X)$ which is the image of $X^+ \times \{1\}$.

See Definition 5.10 for the definition of a Siegel set associated to P and K_∞. It is known that there is a finite set $\{g_1; \ldots ; g_c\} \subseteq G(\mathbb{Q})$ and Siegel sets $\mathfrak{S}_1, \ldots, \mathfrak{S}_c$ associated to $g_1 P {g_1}^{-1}, \ldots, g_c P {g_c}^{-1}$ and K_∞ such that S^+ is the image of $\mathfrak{S} := \mathfrak{S}_1 \cup \cdots \cup \mathfrak{S}_c$.

For each $\mathfrak{S}_i$, it is assumed that Ω from Definition 5.10 is a bounded *semialgebraic* subset.

Let $\mathfrak{S}_W = \mathfrak{S}/Z_{G(\mathbb{R})}(M)$ be the image of $\mathfrak{S}$ in $W^+(\mathbb{R})$.

The maps

$$G(\mathbb{R}) \xrightarrow{g \mapsto g Z_{G(\mathbb{R})}(M)} G(\mathbb{R})/Z_{G(\mathbb{R})}(M) \xrightarrow{g Z_{G(\mathbb{R})}(M) \mapsto g K_\infty} X = G(\mathbb{R})/K_\infty$$

are real algebraic and, thus, semialgebraic. It follows that $\mathfrak{S}_W$ is semialgebraic, that its image $\mathfrak{S}_X$ in X is semialgebraic and that the map

$$p_{W,X} : \mathfrak{S}_W \to \mathfrak{S}_X \tag{60}$$

is semialgebraic.

7.2.2 *o-minimality.* We use the theory of o-minimal structures and recall that the map

$$\pi_{\mathfrak{S},X} : \mathfrak{S}_X \to S^+$$

is definable in the o-minimal structure $\mathbb{R}_{an,\exp}$ by [KUY16]. As (60) is semialgebraic, it is definable in $\mathbb{R}_{an,\exp}$, and the following is definable in $\mathbb{R}_{an,\exp}$ as well

$$\pi_{\mathfrak{S},W} := p_{W,X} \circ \pi_{\mathfrak{S},X} : \mathfrak{S}_W \to \mathfrak{S}_X \to S^+.$$

The algebraic variety Z is definable in $\mathbb{R}_{an,\exp}$ and its inverse image

$$\tilde{Z}_W = \overset{-1}{\pi_{\mathfrak{S},W}}(Z)$$

is definable in $\mathbb{R}_{an,\exp}$ as well.

Because E is a field of definition for Z, for every $\sigma \in Gal(\overline{E}/E)$ and $z \in Z(\overline{E})$ we have $\sigma(z) \in Z$ and, finally,

$$Gal(\overline{E}/E) \cdot z \subset Z.$$

Assume now that z also belongs to $\mathcal{H}^g(x_0)$. For every

$$z' \in Gal(\overline{E}/E) \cdot z$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

we have $z' \in Z \subset S^+$ and we can find $\phi_{z'} \in W(\mathbb{Q})$ such that

$$z' = [\phi_{z'} \circ x_0, 1].$$

Because $\mathfrak{S}_X$ maps onto S^+ we may assume that $\phi_{z'} \circ x_0 \in \mathfrak{S}_X$. Equivalently, we have

$$\phi_{z'} \in \mathfrak{S}_W.$$

The set

$$Q(z) = W(\mathbb{Q}) \cap \overset{-1}{\pi_{\mathfrak{S},W}} (Gal(\overline{E}/E) \cdot z)$$

maps onto $Gal(\overline{E}/E) \cdot z$ and we deduce

$$|Q(z)| \geq |Gal(\overline{E}/E) \cdot z|. \tag{61}$$

7.2.3 *Height bounds.* We consider the affine embedding $\iota : W \to \mathbb{A}^{\dim(M) \cdot \dim(G)}$ of § 4.3. Let H_W and H_f be as in (18).

We can, of course, assume that Z is infinite, and because

$$\Sigma := Z \cap \mathcal{H}^g(x_0)$$

is Zariski dense, it is infinite as well, and we can choose an infinite sequence $(z_n)_{n \in \mathbb{Z}_{\geq 1}}$ of pairwise distinct $z_n \in \Sigma$. We also assume that this sequence is Zariski generic in Z.

By hypothesis, Definitions 6.1 and 6.3 apply, and thus we invoke Theorem 6.4 and, by Proposition 3.6, use it for Galois orbits. We have

$$H_f(\phi) \preccurlyeq |Gal(\overline{E}/E) \cdot [\phi \circ x_0, 1]| \quad \text{on } W(\mathbb{Q}).$$

Thanks to the height comparison Theorem 5.16, we have

$$H_W(\phi) \preccurlyeq H_f(\phi) \text{ on } W(\mathbb{Q}) \cap \mathfrak{S}_W. \tag{62}$$

It follows

$$H_W(\phi) \preccurlyeq |Gal(\overline{E}/E) \cdot [\phi \circ x_0, 1]| \quad \text{on } W(\mathbb{Q}) \cap \mathfrak{S}_W.$$

More precisely, there are $a, b \in \mathbb{R}_{>0}$ such that

$$\forall\, \phi \in W(\mathbb{Q}) \cap \mathfrak{S}_W, \quad a + H_W(\phi)^b \leq |Gal(\overline{E}/E) \cdot [\phi \circ x_0, 1]|.$$

Using (61) we deduce

$$a + H_W(\phi_{z_n})^b \leq |Q(z_n)|. \tag{63}$$

From Proposition 4.3 we have

$$\forall\, z' \in Gal(\overline{E}/E) \cdot z_n, \quad H_f(\phi_{z'}) = H_f(\phi_{z_n})$$

and because $H_f(\phi)$ only depends on $[\phi \circ x_0, 1]$ we have

$$\forall\, \phi \in Q(z_n),\ H_f(\phi) = H_f(\phi_{z_n}).$$

We make (62) precise by choosing a', b' such that

$$\forall\, \phi \in W(\mathbb{Q}) \cap \mathfrak{S}_W, H_W(\phi) \leq a' + H_f(\phi)^{b'}. \tag{64}$$

For $\phi \in Q(z_n) \subset W(\mathbb{Q}) \cap \mathfrak{S}_W$ we get

$$H_W(\phi) \leq a' + H_f(\phi)^{b'} = a' + H_f(\phi_{z_n})^{b'}.$$

Writing $k(n) = H_f(\phi_{z_n})$, we deduce from the above that the subset $Q(z_n) \subseteq \tilde{Z} \cap W(\mathbb{Q})$ contains at least $a + k(n)^b$ points of H_W-height at most $a' + k(n)^{b'}$.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Because the z_n are distinct, so are the inverse images ϕ_{z_n}, and by the Northcott theorem we deduce that $H_W(\phi_{z_n}) \to +\infty$ and, thus, $k(n) \to +\infty$.

We are ready to use the Pila–Wilkie theorem.

7.2.4 *Pila–Wilkie theorem.* We use the form Theorem 7.1 of the Pila–Wilkie theorem. We denote $K_\infty^{\mathbb{R}}$ the real algebraic group corresponding to K_∞, and $X_{\mathbb{R}}$ the algebraic variety $G_{\mathbb{R}}/K_\infty^{\mathbb{R}}$ over $\mathbb{R}$ (we have $X \subset X_{\mathbb{R}}(\mathbb{R})$). We apply Theorem 7.1 to the morphism $p : W = G_{\mathbb{R}}/Z_{G_{\mathbb{R}}}(M) \to X_{\mathbb{R}} = G_{\mathbb{R}}/K_\infty^{\mathbb{R}}$ and the definable subset

$$\tilde{Z}_X := \overset{-1}{\pi_{\mathfrak{S},X}}(Z) \subset X \subset X_{\mathbb{R}}(\mathbb{R}).$$

We deduce for every n that

$$|Q(z_n) \cap (\tilde{Z}_X \smallsetminus \tilde{Z}_X^{\mathrm{alg}})| = (a' + H_f(\phi_{z_n})^{b'})^{o(1)} = o(|Q(z_n)|).$$

Thus, for $n \gg 0$, we have

$$Q(z_n) \cap \tilde{Z}_X^{\mathrm{alg}} \neq \emptyset.$$

In other terms, for almost every n, there exist $\phi \in Q(z_n)$, and a non-zero-dimensional semialgebraic subset $A_n \subset \tilde{Z}_X$, such that $\phi \circ x_0 \in A_n$.

We will now use the hyperbolic Ax–Lindemann–Weierstrass theorem.

7.2.5 *Functional transcendence.* According to Ax–Lindemann–Weierstrass theorem (see [KUY16]), that for $n \gg 0$, there exists a weakly special subvariety S_n' of S^+ such that

$$z_n' \in \pi_{\mathfrak{S},X}(A_n) \subset S_n' \subset Z.$$

One can check that a weakly special subvariety containing a $\overline{E}$-valued point is defined over $\overline{E}$. It follows that this S_n' is defined over $\overline{E}$, and applying $\sigma \in Gal(\overline{E}/E)$ such that $\sigma(z_n') = z_n$, the conjugated subvariety $S_n = \sigma(S_n')$ will be: weakly special, contained in Z and containing z_n.

Because the sequence z_n is generic in Z, the family $(S_n)_{n\geq 0}$ is Zariski dense in Z.

Because A_n has non-zero semialgebraic dimension, and $\pi_{\mathfrak{S},X}$ has finite fibers, the image $\pi_{\mathfrak{S},X}(A_n)$ has non-zero semialgebraic dimension, and S_n' has non-zero dimension as a variety, and S_n also.

We are ready to use the so-called geometric part of André–Oort conjecture.

7.2.6 *Geometric André–Oort.* We reuse the notation of § 7.1.3

From the geometric part of the André–Oort conjecture from [Ull14, RU24], there exists a partition $\{1; \ldots; c\} = I \sqcup J$, with $I \neq \emptyset$, but possibly $J = \emptyset$, such that we have a factorisation

$$Z = S_1 \times Z_J \subset Sh_{K_I}(G_I, X_I) \times Sh_{K_J}(G_J, X_J),$$

where S_1 is a geometric component of $Sh_{K_I}(G_I, X_I)$, and Z_J is a subvariety of $Sh_{K_J}(G_J, X_J)$.

Because we assumed that Z has no nontrivial factorisation, the partition $\{1; \ldots; c\} = I \sqcup J$ is trivial. We must have $J = \emptyset$, $I = \{1; \ldots; c\}$. Equivalently, $Z = S_1$. In other words, Z is special and, in particular, is weakly special.

This finishes the proof of Theorem 1.2.

7.3 Refined Pila–Wilkie theorem

The following is a variant of Pila–Wilkie Theorem, which replaces the 'block version' of the Pila–Wilkie theorem used by Orr. We believe this variant is easier to understand and use, and will be of independent interest.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

We deduce the following from [Pil09, Theorem 1.7].

Theorem 7.1. *Let W be an affine algebraic variety defined over $\mathbb{Q}$, let X be an affine algebraic variety over $\mathbb{R}$ and let $p : W_{\mathbb{R}} \to X$ be a morphism of algebraic varieties defined over $\mathbb{R}$.*

Let $Z \subset X(\mathbb{R})$ be a definable subset, and denote Z^{alg} be the union of the semialgebraic subsets of $X(\mathbb{R})$ which are contained in Z and of non-zero dimension.

We consider a height function H_W on $W(\mathbb{Q})$ associated to some affine embedding. Then

$$|(Z \smallsetminus Z^{\mathrm{alg}}) \cap p(\{w \in W(\mathbb{Q}) : H_W(w) \leq T\})| = T^{o(1)}.$$

Explicitly, for every $\epsilon \in \mathbb{R}_{>0}$, there exists $C(\epsilon, Z) \in \mathbb{R}_{>0}$, such that

$$\forall T \gg 0,\ |(Z \smallsetminus Z^{\mathrm{alg}}) \cap p(\{w \in W(\mathbb{Q}) : H_W(w) \leq T\})| \leq C(\epsilon, Z) \cdot T^{\epsilon}.$$

Comment. The theorem still holds with a semialgebraic map $p : W(\mathbb{R}) \to X(\mathbb{R})$ instead of the real algebraic $p : W_{\mathbb{R}} \to X$. This slight generalisation will not be needed.

The height function we use here is denoted by H^{proj} by Pila, and is not the height function he uses in his statements. As mentioned in the introduction of [Pil09], it is possible to invoke his statements with H^{proj} instead.

Proof. We choose affine embeddings

$$W \subseteq \mathbb{A}^n \quad \text{and} \quad X \subseteq \mathbb{A}^m$$

defined over $\mathbb{Q}$ and $\mathbb{R}$. We can then write the morphism

$$p(w_1, \ldots, w_n) = (P_1(w_1, \ldots, w_n), \ldots, P_m(w_1, \ldots, w_n))$$

with polynomials $P_1, \ldots, P_m \in \mathbb{R}[T_1, \ldots, T_n]$. Let E be the finite-dimensional $\mathbb{Q}$-vector subspace of $\mathbb{R}$ generated by the coefficients of these polynomials.

We have

$$p(W(\mathbb{Q})) \subseteq E^m.$$

We choose an isomorphism $\iota : E \to \mathbb{Q}^d$ of $\mathbb{Q}$ vector spaces. For every P_i, the map

$$\iota \circ P_i : W(\mathbb{Q}) \to E \to \mathbb{Q}^d$$

is polynomial with coefficients in $\mathbb{Q}$. This can be checked for every monomial of P_i. The height on E^m considered in [Pil09, Theorem 1.7] can be written, with our notation,

$$H_E = H \circ (\iota, \ldots, \iota)$$

where H is the usual height on $\mathbb{Q}^{d \cdot m}$. It follows from the general 'functoriality' properties of heights of § 4.2 that

$$H_E \circ p \preccurlyeq H_W \quad \text{on } W(\mathbb{Q}).$$

Explicitly, for some $a, b \in \mathbb{R}_{>0}$ we have

$$p(\{W \in W(\mathbb{Q}) : H_W(w) \leq T\}) \subseteq \{e \in E^m : H_E(e) \leq a + T^b\}.$$

We apply [Pil09, Theorem 1.7] and obtain

$$\begin{aligned} &|(Z \smallsetminus Z^{\mathrm{alg}}) \cap p(\{w \in W(\mathbb{Q}) : H_W(w) \leq T\})| \\ &\quad \leq |(Z \smallsetminus Z^{\mathrm{alg}}) \cap \{e \in E^m : H_E(e) \leq a + T^b\}| = T^{o(1)}. \end{aligned}$$

□

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Appendix A. Exponentials of p-adic matrices

In this appendix we fix a prime p, an integer $d \in \mathbb{Z}_{\geq 1}$, and denote by $M_d(\mathbb{Q}_p)$ the space of square matrices of size d with entries in $\mathbb{Q}_p$. For $Z \in M_d(\mathbb{Q}_p)$ we denote by $\chi_Z(T) = \det(TZ - 1) \in \mathbb{Q}_p[T]$ its characteristic polynomial. Let $|\ |$ be the normalised absolute value on $\mathbb{Q}_p$, extended to $\overline{\mathbb{Q}_p}$: we have $|p| = 1/p$ and $|1/d| \leq d$ for $d \in \mathbb{Z}_{\geq 1}$. We denote the *norm* of Z, and the *local height* of Z by

$$\|Z\| = \max_{1\leq i,j\leq d} |Z_{i,j}| \quad \text{and} \quad H_p(Z) = \max\{1; \|Z\|\} = H_p(1+Z).$$

We define, whenever the corresponding series converges in $M_d(\mathbb{Q}_p)$,

$$\exp(Z) = \sum_{n\in\mathbb{Z}_{\geq 0}} \frac{1}{n!}\cdot Z^n \quad \text{and} \quad \log(1+Z) = -\sum_{n\in\mathbb{Z}_{\geq 1}} \frac{(-1)^n}{n}\cdot Z^n.$$

It is well known (see [Rob00, Ch. 5. § 4.1]) that, on $\mathbb{C}_p$, the series $\exp(T)$ has radius of convergence $|p|^{1/(p-1)}$ and the series $\log(1+T)$ has radius of convergence 1. It is also true that $\exp(Z)$, respectively, $\log(1+Z)$ converges if and only if the eigenvalues of Z are in the open disc of convergence of $\exp(T)$ respectively, $\log(1+T)$. (For the archimedean case, see [Hig08, § 1]. The relevant arguments carry over to ultrametric fields.)

PROPOSITION A.1. *Let $Y \in M_d(\mathbb{Q}_p)$ be such that $\log(1+Y)$ converges. Then*

$$\chi_Y(T) \in T^d + p\mathbb{Z}_p[T]. \tag{A.1}$$

Let $Y \in M_d(\mathbb{Q}_p)$ be such that

$$\chi_Y(T) \in T^d + p\mathbb{Z}_p[T]. \tag{A.2}$$

Then $\log(1+Y)$ converges and we have:

- *in general,*

$$\|\log(1+Y)\| \leq d\cdot H_p(Y)^{d-1}; \tag{A.3}$$

- *and for $p > d$, the sharper estimate*

$$\|\log(1+Y)\| \leq H_p(Y)^{d-1}. \tag{A.4}$$

We deal with the first conclusion (A.1).

Proof. Let $\lambda_1, \ldots, \lambda_d$ be the eigenvalues of Y, with repetitions. As can be seen on a Jordan form after passing to $\mathbb{C}_p$, the series $\log(1+Y)$ converges if and only if every $\log(\lambda_1), \ldots, \log(\lambda_d)$ converges. As the radius of convergence of $\log(1+T)$ is 1, this means

$$\forall\, i \in \{1; \ldots; d\}, \quad |\lambda_i| < 1. \tag{A.5}$$

Let $K = \mathbb{Q}_p(\lambda_1, \ldots, \lambda_d)$, let O_K be its ring of integers, and $\mathfrak{m}_K$ be the maximal ideal of O_K. Then (A.5) means

$$\{\lambda_1; \ldots; \lambda_d\} \subseteq \mathfrak{m}_K.$$

We deduce that the non-leading coefficients of

$$\chi_Y(T) = \prod_{i=1}^{d}(T - \lambda_i)$$

are in $\mathfrak{m}_K$. We recall that $\mathbb{Q}_p \cap \mathfrak{m}_K = p\mathbb{Z}_p$ and $\chi_Y(T) \in \mathbb{Q}_p[T]$. We conclude that

$$\chi_Y(T) \in \mathbb{Q}_p[T] \cap (T^d + \mathfrak{m}_K \cdot O_K[T]) = T^d + p\cdot\mathbb{Z}_p[T]. \qquad \square$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

We have proved (A.1) and before proving the rest of Proposition A.1, we prove an estimate on $\|Y^n\|$ for $n \in \mathbb{Z}_{\geq 0}$.

Proof. We consider

$$A := \mathbb{Z}_p + \mathbb{Z}_p \cdot Y + \cdots + \mathbb{Z}_p \cdot Y^{d-1}.$$

By hypothesis, we have $\chi_Y(T) = c_0 + \cdots + c_{d-1}T^{d-1} + T^d$ with $c_0, \ldots, c_{d-1} \in p\mathbb{Z}_p$. Let us first check that

$$YA \subseteq A \tag{A.6}$$

on a generating family: for $0 \leq i < d-1$ we have $Y \cdot Y^i \in A$ by construction; for $i = d-1$ the identity $\chi_Y(Y) = 0$ can be rearranged into

$$Y^d = -c_0 + \cdots - c_{d-1}Y^{d-1} \in pA. \tag{A.7}$$

Repeated use of (A.6) implies that, for $i \in \mathbb{Z}_{\geq 0}$, we have $Y^i A \subseteq A$. We deduce $Y^i pA \subseteq pA$. But $Y^d \in pA$ by (A.7), hence $Y^d \cdot Y^i = Y^i \cdot Y^d \in pA$. Applied to $i = 0, \ldots, d-1$ it implies $Y^d A \subseteq pA$ and by induction $(Y^d)^k A \subseteq p^k A$. We deduce again that $Y^i \cdot (Y^d)^k \in p^k A$. Writing $n = k \cdot d + i$ with $k = [n/d]$, we get the formula

$$Y^n \in p^{[n/d]} A$$

and the bound

$$\|Y^n\| \leq |p|^{[n/d]} \cdot \|A\| \quad \text{where } \|A\| := \max_{a \in A} \|a\|. \tag{A.8}$$

Using the ultrametric inequality $\|X + Z\| \leq \max\{\|X\|; \|Z\|\}$ and submultiplicativity $\|X \times Z\| \leq \|X\| \cdot \|Z\|$ of the norm, we get

$$\|A\| \leq \max\{\|Y^0\|; \ldots; \|Y^{d-1}\|\} \leq \max\{1; \ldots; \|Y\|^{d-1}\} = H_p(Y)^{d-1}. \tag{A.9}$$

□

We apply our estimate to the series $\log(1 + T)$ and finish the proof of Proposition A.1.

Proof. For the series $\log(1 + Y)$ the above (A.8) and (A.9) imply the bound

$$\left\| \frac{(-1)^n}{n} \cdot Y^n \right\| \leq \left| \frac{1}{n} \right| \cdot |p|^{[n/d]} \cdot H_p(|Y|)^{d-1}.$$

We note that $\lim_{n \to \infty} |1/n| \cdot |p|^{[n/d]} = 0$ which implies that $\log(1 + Y)$ converges, and that

$$\max_{n \in \mathbb{Z}_{\geq 1}} \left| \frac{1}{n} \right| \cdot |p|^{[n/d]} = \left| \frac{1}{d-1} \right| \cdot |p|^{[(d-1)/d]} = \left| \frac{1}{d-1} \right|.$$

By the ultrametric inequality and previous estimates,

$$\log(1 + Y) \leq \sup_{n \in \mathbb{Z}_{\geq 1}} \left\| \frac{(-1)^n}{n} \cdot Y^n \right\| \leq \left| \frac{1}{d-1} \right| \cdot H_p(Y)^{d-1}. \tag{A.10}$$

As we used the normalised p-adic norm, we have $|1/(d-1)| \leq d - 1 \leq d$ in general, and $|1/(d-1)| = 1$ if $p \geq d$. This gives (A.3) and (A.4), respectively. □

The main statement of this appendix will require the following observation.

Lemma A.2. *Let $Z \in M_d(\mathbb{Q}_p)$ be such that* $\exp(Z)$ *converges and let us write* $\exp(Z) = 1 + Y$. *Then* $\log(1 + Y)$ *converges and*

$$\log(1 + Y) = Z.$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Proof. For $d = 1$, it is [Rob00, § 5, Proposition 3].

For $d > 1$, it is [Rob00, § 6.1.1] applied to $(\partial/\partial Y)^i \log(1 + Y) \circ \exp$. □

The following statement is one of our main tools for proving lower bounds for Galois orbits.

Theorem A.3 (Lemma of the exponentials). *Let $X \in M_d(\mathbb{Q}_p)$ be such that $\exp(X)$ converges and denote by $\exp(X)^{\mathbb{Z}}$ the subgroup generated by $\exp(X)$ in $GL_d(\mathbb{Q}_p)$.*

Then:

- *in general, we have*
$$[\exp(X)^{\mathbb{Z}} : \exp(X)^{\mathbb{Z}} \cap GL_d(\mathbb{Z}_p)] \geq H_p(X)/d; \tag{A.11}$$
- *if $p > d$, we have more sharply*
$$[\exp(X)^{\mathbb{Z}} : \exp(X)^{\mathbb{Z}} \cap GL_d(\mathbb{Z}_p)] \geq H_p(X). \tag{A.12}$$

Proof. For every $i \in \mathbb{Z}$, we know that if $\exp(X)$ converge, then $\exp(iX)$ converges as well, and we have
$$\exp(iX) = \exp(X)^i.$$
By Lemma A.2, with $Y_i = \exp(i \cdot X) - 1$, we have convergence and identity
$$\log(1 + Y_i) = i \cdot X.$$
Proposition A.1 gives
$$\|i \cdot X\| = \|\log(1 + Y_i)\| \leq d \cdot H_p(1 + Y_i)^{d-1} \tag{A.13}$$
and, if $d \leq p$,
$$\|i \cdot X\| = \|\log(1 + Y_i)\| \leq H_p(1 + Y_i)^{d-1}. \tag{A.14}$$
Assume that
$$i = [\exp(X)^{\mathbb{Z}} : \exp(X)^{\mathbb{Z}} \cap GL_d(\mathbb{Z}_p)] < +\infty.$$
Then $H_p(1 + Y_i) = H_p(\exp(X)^i) = 1$, and (A.13), respectively, (A.14), specialises to
$$|i| \cdot \|X\| \leq d, \quad \text{respectively, } |i| \cdot \|X\| \leq 1.$$
Recall that $|i| \leq 1/i$ as we use the normalised p-adic absolute value. The conclusions (A.11), respectively, (A.12), follow. □

We finish with a sufficient criterion for $\exp(X)$ to converge.

Theorem A.4. *Let X be a matrix in $M_d(\mathbb{Q}_p)$ and $b \in \mathbb{Z}_{\geq 1}$ be such that*
$$\chi_X(T) \in T^d + p^k\mathbb{Z}_p[T] \quad \text{and} \quad d < k(p - 1).$$
Then $\exp(X)$ converges.

Proof. By the usual criterion, it is sufficient to prove that every eigenvalue λ of X is in the open disc of convergence for $\exp(T)$. This amounts to proving the inequality $|\lambda| < |p|^{1/(p-1)}$.

For any eigenvalue λ of X, we have $\chi_X(\lambda) = 0$, hence $\lambda^d \in p^k\mathbb{Z}_p[\lambda]$ by assumption. It follows $|\lambda|^d \leq |p|^k$, that is $|\lambda| \leq |p|^{k/d}$. Using the inequality $d < k(p - 1)$, it implies $|\lambda| < |p|^{1/(p-1)}$. □

Appendix B. Heights bounds for adelic orbits of linear groups

Our bound on p-adic exponentials is combined with structure theory of linear algebraic groups to obtain the following general lower bound. It is applied to Galois orbits in § 6.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Theorem B.1. *Let $M \leq GL(N)$ be a linear algebraic subgroup defined over $\mathbb{Q}$, denote by $\phi_0 : M \to GL(N)$ the identity morphism and W the $GL(N)$-conjugacy class of ϕ_0. We define*

$$M(\widehat{\mathbb{Z}}) = M(\mathbb{A}_f) \cap GL(N, \widehat{\mathbb{Z}}) \quad \text{and} \quad \mathfrak{m}_{\widehat{\mathbb{Z}}} = \mathfrak{m} \otimes \mathbb{A}_f \cap \mathfrak{gl}(N, \widehat{\mathbb{Z}}).$$

We consider the standard Weil $\mathbb{A}_f$-height function, see (17),

$$H_f : Hom(\mathfrak{m} \otimes \mathbb{A}_f, \mathfrak{gl}(N) \otimes \mathbb{A}_f) \to \mathbb{Z}_{\geq 1}$$

given by $H_f(\Phi) = \min\{n \in \mathbb{Z}_{\geq 1} : n\Phi(\mathfrak{m}_{\widehat{\mathbb{Z}}}) \subset \mathfrak{gl}(N, \widehat{\mathbb{Z}})\}$.

There exists $c = c(\phi_0) \in \mathbb{R}_{>0}$ such that, as ϕ ranges through $W(\mathbb{A}_f)$, we have

$$[\phi(M(\widehat{\mathbb{Z}})) : \phi(M(\widehat{\mathbb{Z}})) \cap GL(N, \widehat{\mathbb{Z}})] \geq \frac{1}{c^{\omega(H_f(d\phi))}} \cdot H_f(d\phi), \tag{B.1}$$

where $\omega(n)$ counts the number of prime factors of n.

The proof of Theorem B.1 will start in Appendix B.1. We deduce from Theorem B.1 the following.

Corollary B.2. *We have*

$$[\phi(M(\widehat{\mathbb{Z}})) : \phi(M(\widehat{\mathbb{Z}})) \cap GL(N, \widehat{\mathbb{Z}})] \geq H_f(d\phi)^{1-o(1)}, \tag{B.2}$$

and, if M is reductive and connected and $\iota : W \to \mathbb{A}^d$ is an affine embedding, then, as ϕ ranges through $W(\mathbb{A}_f)$,

$$H_{\iota,f}(\phi) \approx H_f(d\phi) \preccurlyeq [\phi(M(\widehat{\mathbb{Z}})) : \phi(M(\widehat{\mathbb{Z}})) \cap GL(N, \widehat{\mathbb{Z}})]. \tag{B.3}$$

Furthermore, for every $\Phi \in Hom(\mathfrak{m} \otimes \mathbb{A}_f, \mathfrak{gl}(N) \otimes \mathbb{A}_f)$, we have

$$\forall\, m \in M(\widehat{\mathbb{Z}}),\ \ g \in G(\widehat{\mathbb{Z}}), H_f(g \circ \Phi \circ m) = H_f(\Phi). \tag{B.4}$$

Proof of Corollary B.2. One passes from (B.1) to (B.2) by recalling the known estimate (see [HW79, 22.10])

$$c^{\omega(n)} \leq n^{|\log(c_2)| \cdot ((1+o(1))/(\log \log n))} = n^{o(1)}.$$

As for (B.3), we know that W is affine as M is reductive, and $\phi \mapsto d\phi$ is an affine embedding because M is connected. Lastly, two heights functions on W are polynomially equivalent, so we may replace $H_{W,f}(\phi)$ by $H_f(d\phi)$ and this follows from (B.2).

The identity in (B.4) follows from the observations

$$m \cdot \mathfrak{m}_{\widehat{\mathbb{Z}}} = \mathfrak{m}_{\widehat{\mathbb{Z}}}, \quad \text{and} \quad g^{-1} \cdot \mathfrak{gl}(N, \widehat{\mathbb{Z}}) = \mathfrak{gl}(N, \widehat{\mathbb{Z}})$$

and the defining property we provided: we have $n \cdot g \cdot \Phi(m\mathfrak{m}_{\widehat{\mathbb{Z}}}) \subset \mathfrak{gl}(N, \widehat{\mathbb{Z}})$ if and only if

$$n\Phi(\mathfrak{m}_{\widehat{\mathbb{Z}}}) = n\Phi(m\mathfrak{m}_{\widehat{\mathbb{Z}}}) \subset g^{-1}\mathfrak{gl}(N, \widehat{\mathbb{Z}}) = \mathfrak{gl}(N, \widehat{\mathbb{Z}}).$$ □

The combination of Theorem C.1 (C.1) with (B.3) gives the following.

Theorem B.3. *Let $M \leq GL(N)$ be a connected reductive linear algebraic subgroup defined over $\mathbb{Q}$, denote $\phi_0 : M \to GL(N)$ the identity morphism and W the $GL(N)$-conjugacy class of ϕ_0, and let $\iota : W \to \mathbb{A}^d$ be an affine embedding. Then, as ϕ ranges through $W(\mathbb{A}_f)$,*

$$H_{\iota,f}(\phi) \approx H_f(d\phi) \approx [\phi(M(\widehat{\mathbb{Z}})) : \phi(M(\widehat{\mathbb{Z}})) \cap GL(N, \widehat{\mathbb{Z}})]. \tag{B.5}$$

B.1 Proof of Theorem B.1

The global theorem B.1 will follow directly from (B.6) in the analogous local theorem below.

THEOREM B.4. *We keep M, ϕ_0, W, and H_f as in Theorem B.1.*

For every prime p, let $H_p : Hom(\mathfrak{m}\otimes\mathbb{A}_f, \mathfrak{gl}(N)\otimes\mathbb{A}_f) \to \mathbb{Z}_{\geq 1}$ be given by $H_p(\Phi) = \min\{p^k \in p^{\mathbb{Z}_{\geq 1}} : p^k\Phi(\mathfrak{m}_{\mathbb{Z}_p}) \subset \mathfrak{gl}(N,\mathbb{Z}_p)\}$.

There exists $c = c(\phi_0) \in \mathbb{R}_{>0}$ such that, for every prime p, and every $\phi \in W(\mathbb{Q}_p)$,

$$[\phi(M(\mathbb{Z}_p)) : \phi(M(\mathbb{Z}_p)) \cap \mathrm{GL}(N,\mathbb{Z}_p)] \geq \frac{H_p(d\phi)}{c} \tag{B.6}$$

and if $\mathfrak{m}_{\mathbb{Z}_p}$ is generated over $\mathbb{Z}_p$ by nilpotent elements and $p > N$,

$$[\phi(M(\mathbb{Z}_p)) : \phi(M(\mathbb{Z}_p)) \cap \mathrm{GL}(N,\mathbb{Z}_p)] \geq H_p(d\phi). \tag{B.7}$$

Here is how to deduce Theorem B.1 from Theorem B.4.

Proof. Let us multiply the inequalities (B.6) for the $\omega(H_f(d\phi))$ primes dividing $H_f(d\phi)$ with the trivial inequalities

$$[\phi(M(\mathbb{Z}_p)) : \phi(M(\mathbb{Z}_p)) \cap \mathrm{GL}(N,\mathbb{Z}_p)] \geq 1$$

for all the other primes. Then one can identify the product on both sides with the corresponding sides of (B.1). □

Theorem B.4 will follow from different cases gathered in Theorem B.5.

THEOREM B.5. *We keep the notation from Theorem B.4. For every prime p, let $K_p := GL(N,\mathbb{Z}_p)$ and, for any $U \leq G(\mathbb{Q}_p)$, let $[U]_p := [U : U \cap K_p]$. We write $N^* = \mathrm{lcm}(1,\ldots,N)$ so that $|1/N^*|_p = p^{[\log_p(N)]}$ and $|N^*|_p = 1$ if $p > N$.*

(i) *For every prime p we have $\exp(2p\mathfrak{m}_{\mathbb{Z}_p}) \leq M(\mathbb{Z}_p)$ and*

$$[\phi(\exp(2p\mathfrak{m}_{\mathbb{Z}_p}))]_p \geq |2pN^*|_p \cdot H_p(d\phi) \geq \frac{1}{2Np}\cdot H_p(d\phi). \tag{B.8}$$

(ii) *Assume that M is unipotent or more generally that $\mathfrak{m}_{\mathbb{Z}_p}$ is generated over $\mathbb{Z}_p$ by nilpotent elements, then*

$$[\phi(M(\mathbb{Z}_p))]_p \geq |N^*|_p \cdot H_p(d\phi). \tag{B.9}$$

(iii) *Assume that M is an algebraic torus. There is $c_2 = c_2(\phi_0) \in \mathbb{R}_{>0}$ such that for every prime p, and every $\phi \in W(\mathbb{Q}_p)$,*

$$\text{if } H_p(d\phi) \neq 1 \text{ then } \left|\frac{\phi(M(\mathbb{Z}_p))}{\phi(\exp(2p\mathfrak{m}_{\mathbb{Z}_p}))\cdot\phi(M(\mathbb{Z}_p))\cap K_p}\right| \geq \frac{p}{c_2}. \tag{B.10}$$

We deduce Theorem B.4 from Theorem B.5.

Proof. The bound (B.7) follows from (B.9), and the observation that $|N^*|_p = p^{[\log_p(N)]} = p^0 = 1$ for $p > N$.

Let U be the unipotent radical of M^0 and L be a reductive Levi subgroup of M^0 so that we have the Levi decomposition $\mathfrak{m} = \mathfrak{u} + \mathfrak{l}$. By the principle of Appendix B.1.1 we may assume $M = U$ or $M = L$.

In the first case $M = U$, one deduces (B.6), with $c = N^* \geq |1/N^*|_p$, from (B.9).

In the second case, $M = L$ is reductive, and thus generated by algebraic tori. By the principle of Appendix B.1.1 we may assume that M is a torus.

Let us mention a simpler argument giving the following weaker conclusion, which is sufficient for the purpose of this article:

$$[\phi(M(\mathbb{Z}_p)) : \phi(M(\mathbb{Z}_p)) \cap GL(N,\mathbb{Z}_p)] \geq \frac{H_p(d\phi)^{1/2}}{c_2}. \tag{B.11}$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Proof. We know that $H_p(d\phi)$ is a power p^k of p. For $k=0$, we may take $c=1$. For $k=1$ we deduce from conclusion (iii) of Theorem B.5 that[18]

$$[\phi(M(\mathbb{Z}_p))]_p \geq p/c_2 = H_p(d\phi)/c_2. \tag{B.12}$$

For $k \geq 2$, we have $H_p(d\phi)/p \geq \sqrt{H_p(d\phi)}$ and we take $c_2 = 2N$ and use (B.8). □

We now explain how to improve upon the exponent $1/2$.

We suppose that p is large enough, that $p \neq 2$, and that the reduction $T_{\mathbb{F}_p}$ of the torus $T = M$ is a torus over $\mathbb{F}_p$. Then $T_{\mathbb{F}_p}(\mathbb{F}_p)$ is diagonalisable over $\overline{\mathbb{F}_p}$ and its elements have order prime to p and, thus, the order $|T_{\mathbb{F}_p}(\mathbb{F}_p)|$ is prime to p.

From the exact sequence

$$0 \to p \cdot \mathfrak{t}_{\mathbb{Z}_p} \xrightarrow{\exp} T(\mathbb{Z}_p) \to T_{\mathbb{F}_p}(\mathbb{F}_p)$$

we deduce that $U_p := \exp(p\mathfrak{t}_{\mathbb{Z}_p}) \leq T(\mathbb{Z}_p)$ is a topological p-group and $T(\mathbb{Z}_p)/U_p \hookrightarrow T(\mathbb{F}_p)$ has order prime to p.

For any open subgroup $H \leq T(\mathbb{Z}_p)$, we have

$$[T(\mathbb{Z}_p) : H] = [T(\mathbb{Z}_p) : U_p \cdot H] \cdot [U_pH : U_p \cap H]. \tag{B.13}$$

We now choose H defined by $\phi(H) = K_p \cap \phi(T(\mathbb{Z}_p))$. We have

$$[T(\mathbb{Z}_p) : H] = [T(\mathbb{Z}_p)]_p, \quad [U_p : U_p \cap H] = [U_p]_p \tag{B.14}$$

and

$$[T(\mathbb{Z}_p) : U_p \cdot H] = \left| \frac{\phi(T(\mathbb{Z}_p))}{\phi(\exp(2p\mathfrak{t}_{\mathbb{Z}_p})) \cdot \phi(M(\mathbb{Z}_p)) \cap K_p} \right|. \tag{B.15}$$

Substituting (B.14) and (B.15) in (B.13) yields

$$[T(\mathbb{Z}_p)]_p = [U_p]_p \cdot \left| \frac{\phi(T(\mathbb{Z}_p))}{\phi(\exp(2p\mathfrak{t}_{\mathbb{Z}_p})) \cdot \phi(M(\mathbb{Z}_p)) \cap K_p} \right|. \tag{B.16}$$

We now use (B.13) and (B.8) and (B.10) from Theorem B.5 and conclude

$$[T(\mathbb{Z}_p)]_p \geq \frac{1}{2Np} \cdot H_p(d\phi) \cdot \frac{p}{c} = \frac{1}{2cN} H_p(d\phi).$$ □

We now prove Theorem B.5.

Proof of conclusion (i). Assume for now the claim that exp converges on $2p\mathfrak{m}_{\mathbb{Z}_p}$ and $U := \exp(2p\mathfrak{m}_{\mathbb{Z}_p}) \leq M(\mathbb{Z}_p)$. Let $X_1, \ldots, X_k$ be generators of $\mathfrak{m}_{\mathbb{Z}_p}$, then

$$H_p(d\phi) = \max\{H_p(d\phi X_1); \ldots; H_p(d\phi X_k)\}. \tag{B.17}$$

As $U_i := \exp(2pX_i)^{\mathbb{Z}} \leq U$ for every $i \in \{1; \ldots; k\}$ we have

$$[\phi(U)]_p = |\phi(U) \cdot K_p/K_p| \geq |\phi(U_i) \cdot K_p/K_p| = [\phi(U_i)]_p,$$

and, thus,

$$[\phi(U)]_p \geq \max_{i=1,\ldots,k} [\exp(2p \cdot d\phi(X_i))^{\mathbb{Z}}]_p. \tag{B.18}$$

According to Theorem A.3 for $X = 2p \cdot d\phi(X_i)$ we have

$$[\exp(2pd\phi(X_i))^{\mathbb{Z}}]_p \geq |N^*|_p \cdot H_p(2p \cdot d\phi(X_i)). \tag{B.19}$$

[18] The bound (B.12) is from [EY03, Proposition 4.3.9].

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

We remark

$$\begin{aligned} H_p(2p\cdot d\phi(X_i)) &= \max\{1; \|2p\cdot d\phi(X_i)\|\}\\ &\geq |2p|_p\cdot \max\{1; \|d\phi(X_i)\|\} = |2p|_p\cdot \|d\phi(X_i)\|. \end{aligned} \tag{B.20}$$

Substituting (B.20) into (B.19) and (B.19) into (B.18), we get

$$[\phi(U_p)]_p \geq |2pN^*|_p\cdot \max_{i=1,\dots,k} H_p(d\phi(X_i)) = |2pN^*|_p\cdot H_p(d\phi).$$

We now recall why, for $2pX\in 2p\mathfrak{m}_{\mathbb{Z}_p}$, the series $\exp(2pX)$ converges and $\exp(2pX)\in M(\mathbb{Z}_p)$ for $2pX\in 2p\mathfrak{m}_{\mathbb{Z}_p}$.

Proof. We remark that $\exp(2pT)\in\mathbb{Z}_{(p)}[[T]]$ and recall that the p-adic radius of convergence of $\exp(2pT)$ is $2\cdot p/p^{1/(p-1)}>1$. For $2pX\in 2p\mathfrak{m}_{\mathbb{Z}_p}$, we have $\|X\|\leq 1$ and so $\exp(2pX)$ converges. We have $\exp(2pX)\in M(d,\mathbb{Z}_p)$ because $\exp(2pT)\in\mathbb{Z}_p[[X]]$ has $\mathbb{Z}_p$ entries. Likewise, and $\exp(2pX)^{-1}=\exp(-2pX)\in M(d,\mathbb{Z}_p)$ and we conclude $\exp(2pX)\in GL(N,\mathbb{Z}_p)$. □

Conclusion (i) has been proved. □

Proof of conclusion (ii). Let $X_1,\dots,X_k$ be a nilpotent basis of $\mathfrak{m}_{\mathbb{Z}_p}$. Then the $d\phi(X_1),\dots,d\phi(X_k)$ generate $d\phi(\mathfrak{m}_{\mathbb{Z}_p})$ and there exists an $i\in\{1;\dots;k\}$ such that $H_p(d\phi)=H_p(d\phi(X_i))$. Because X_i is nilpotent, we have

$$\exp(N^*\cdot X_i) = 1 + N^*\cdot X_i + \cdots + \frac{1}{(N-1)!}(N^*\cdot X_i)^{N-1}$$

and, thus, $\exp(N^*\cdot X_i)\in M(\mathbb{Z}_p)$.

Thus,

$$[\phi(M(\mathbb{Z}_p))]_p \geq [\phi(\exp(N^*\cdot X_i))^{\mathbb{Z}}]_p.$$

Finally, by (A.11), we have

$$[\phi(\exp(N^*\cdot X_i\cdot\mathbb{Z}_p))]_p \geq H_p(d\phi(N^*\cdot X_i))/N.$$

Because $H_p(d\phi(N^*\cdot X_i))$ and $[\phi(\exp(N^*\cdot X_i\cdot\mathbb{Z}_p))]_p$ are powers of p, we actually have

$$[\phi(\exp(N^*\cdot X_i\cdot\mathbb{Z}_p))]_p \geq |N|_p\cdot H_p(d\phi(d^*\cdot X_i)) \geq |N^*|_p\cdot H_p(d\phi).$$ □

Conclusion (iii) is due to [EY03] and we detail how their formulation [EY03, Proposition 4.3.9] relates to ours.

Proof of conclusion (iii). We can discard finitely many primes and assume p is big enough so that [EY03, Proposition 4.3.9] and its proof applies.

We first note that, in the matrix algebra $M(N,\mathbb{Q})$, the subalgebra $\mathbb{Q}[T(\mathbb{Q})]$ contains $\mathfrak{t}$.

Proof. The inclusion of vector spaces can be checked after passing to $\mathbb{R}/\mathbb{Q}$. We know that

$$\mathbb{R}[T(\mathbb{Q})] = \mathbb{R}[T(\mathbb{R})]$$

because, by weak approximation, $T(\mathbb{Q})$ is dense in $T(\mathbb{R})$. Let t be a sufficiently small element in $\mathfrak{t}\otimes\mathbb{R}$, so that $\log(\exp(t))$ converges and $\log(\exp(t))=t$. Then $t\in\mathbb{R}[\exp(t)]$, as is seen using Jordan forms, and $\exp(t)\in T(\mathbb{R})$. Because $\mathfrak{t}\otimes\mathbb{R}$ admits a basis of such elements, we can conclude. □

We can choose $t_1, \ldots, t_k$ in $\mathbb{Q}[T(\mathbb{Q})]$ so that

$$\mathfrak{t} \subset t_1 \cdot \mathbb{Q} + \cdots + t_k \cdot \mathbb{Q}$$

and, thus, $t_1 \cdot \mathbb{Z} + \cdots + t_k \cdot \mathbb{Z}$ contains a lattice of $\mathfrak{t}$. It will hence contain $n \cdot (\mathfrak{t} \cap \mathfrak{gl}(N, \mathbb{Z}))$ for some commensurability index $n \in \mathbb{Z}_{\geq 1}$.

As we discard finitely many primes p, we may assume that p do not divide the denominators of the t_i and do not divide n. We will then have

$$t_1, \ldots, t_k \in T(\mathbb{Z}_{(p)})$$

and

$$\mathfrak{t}_{\mathbb{Z}_p} = \mathfrak{t} \cap \mathfrak{gl}(N, \mathbb{Z}_{(p)}) \subset t_1 \cdot \mathbb{Z}_{(p)} + \cdots + t_k \cdot \mathbb{Z}_{(p)}, \tag{B.21}$$

and, applying $\otimes_{\mathbb{Z}_{(p)}} \mathbb{Z}_p$, we may replace $\mathbb{Z}_{(p)}$ by $\mathbb{Z}_p$.

Let $\phi \in W(\mathbb{Q}_p)$. Using Theorem 2.11, we can write

$$\phi = g \phi_0 g^{-1}$$

for some $g \in GL(N, \mathbb{Q}_p)$. We assume $H_p(d\phi) \neq 1$, that is

$$g \mathfrak{t}_{\mathbb{Z}_p} g^{-1} \not\subset \mathfrak{gl}(N, \mathbb{Z}_p),$$

and, by (B.21), there is at least one $i \in \{1; \ldots; k\}$ such that

$$g t_i g^{-1} \notin \mathfrak{gl}(N, \mathbb{Z}_p).$$

Equivalently, $g t_i g^{-1} \notin GL(N, \mathbb{Z}_p)$, which also means

$$t_i \cdot g\mathbb{Z}_p^d \neq g\mathbb{Z}_p^d.$$

As $t_i \in T(\mathbb{Z}_p)$, this implies, in the sense of [EY03, Proposition 4.3.9] (for $W_{\mathbb{Z}_p} = g\mathbb{Z}_p^d$),

‘$T_{\mathbb{Z}_p}$ does not fix $\{W_{\mathbb{Z}_p}\}$’.

Looking into the proof of [EY03, Proposition 4.3.9] we note that their lower bound is given by a lower bound of some orbit of $T(\mathbb{F}_p)$, thus, in (B.12), there exists $n \in \mathbb{Z}_{\geq 1}$ such that n divides $|T(\mathbb{F}_p)|$ and

$$[\phi(T(\mathbb{Z}_p))]_p \geq n \geq p/c.$$

In the factorisation (B.16) the first factor in the right-hand side is a power of p and prime to n. Thus the inequality $[\phi(T(\mathbb{Z}_p))]_p \geq n$ comes from the second factor, i.e. we have inequality of conclusion (iii). □

B.1.1 *Subgroup principle.* The following elementary lemmas were useful in passing to subgroups in the proofs of Theorems B.1, B.4 and B.5. Proofs are left to the reader.

Lemma B.6 (Global subgroup principle). *Let $M_1, \ldots, M_k \leq M \leq GL(N)$ be algebraic groups over $\mathbb{Q}$ such that $\mathfrak{m}_1 + \cdots + \mathfrak{m}_k = \mathfrak{m}$.*

(i) *Then*

$$\Lambda := \mathfrak{m}_1 \cap \mathfrak{gl}(N, \mathbb{Z}) + \cdots + \mathfrak{m}_k \cap \mathfrak{gl}(N, \mathbb{Z}) \leq \mathfrak{m} \cap \mathfrak{gl}(N, \mathbb{Z}) \tag{B.22a}$$

and the index

$$c = [\mathfrak{m} \cap \mathfrak{gl}(N, \mathbb{Z}) : \Lambda] \tag{B.22b}$$

is finite. For every prime p, we have

$$\Lambda \otimes \mathbb{Z}_p = \mathfrak{m}_1 \otimes \mathbb{Q}_p \cap \mathfrak{gl}(N, \mathbb{Z}_p) + \cdots + \mathfrak{m}_k \otimes \mathbb{Q}_p \cap \mathfrak{gl}(N, \mathbb{Z}_p) \leq \mathfrak{m} \otimes \mathbb{Q}_p \cap \mathfrak{gl}(N, \mathbb{Z}_p) \tag{B.22c}$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

and

$$[\mathfrak{m}\otimes\mathbb{Q}_p\cap\mathfrak{gl}(N,\mathbb{Z}_p):\Lambda\otimes\mathbb{Z}_p]=|1/c|_p \tag{B.22d}$$

with $|1/c|_p\leq c$ *and* $|1/c|_p=1$ *if* $gcd(c,p)=1$.

(ii) *Assume, moreover, that for some morphism* $\phi:M\to GL(d)$ *defined over* $\mathbb{Q}$, *we have*

$$[\phi(M_i(\widehat{\mathbb{Z}})):\phi(M_i(\widehat{\mathbb{Z}}))\cap GL(d,\widehat{\mathbb{Z}})]\geq\frac{H_f(d\phi)}{c_i}. \tag{B.22e}$$

Then we have, with $c=n\cdot\max\{c_1;\ldots;c_k\}$,

$$[\phi(M(\widehat{\mathbb{Z}})):\phi(M(\widehat{\mathbb{Z}}))\cap GL(d,\widehat{\mathbb{Z}})]\geq\frac{H_f(d\phi)}{c}. \tag{B.22f}$$

Lemma B.7 (Local subgroup principle). *Let* p *be a prime and* $M_1,\ldots,M_k\leq M\leq GL(N)$ *be algebraic groups over* $\mathbb{Q}_p$.

(i) *Then*

$$[M(\mathbb{Z}_p)]_p\geq\max_{i\in\{1;\ldots;k\}}[M_i(\mathbb{Z}_p)]_p. \tag{B.23a}$$

(ii) *Assume that* $\mathfrak{m}_1+\cdots+\mathfrak{m}_k=\mathfrak{m}$, *then the index*

$$[\mathfrak{m}_{\mathbb{Z}_p}:\Lambda]=n \tag{B.23b}$$

is a finite power of p.

(iii) *With* n *as above, for any* $\mathbb{Q}_p$ *linear map* $\Phi:\mathfrak{m}\to\mathfrak{gl}(d,\mathbb{Q}_p)$, *we have*

$$\frac{1}{n}H_p(\Phi)\leq\max_{i\in\{1;\ldots;k\}}H_p(\Phi|_{\mathfrak{m}_i})\leq H_p(\Phi). \tag{B.23c}$$

(iv) *Assume, moreover, for some morphism* $\phi:M\to GL(N)$ *defined over* $\mathbb{Q}_p$ *that we have* (B.23*c*) *for* $\Phi=d\phi$ *and that*

$$\forall\, i\in\{1;\ldots;k\},\ [M_i(\mathbb{Z}_p)]_p\geq\frac{1}{c_i}\cdot H_p(d\phi). \tag{B.23d}$$

Then we have, with $c=n\cdot\max\{c_1;\ldots;c_k\}$,

$$[M(\mathbb{Z}_p)_p]\geq\frac{1}{c}\cdot H_p(d\phi). \tag{B.23e}$$

Appendix C. Upper bound on Adelic orbits

In this appendix, we prove upper bounds on adelic orbits. Combined with Proposition 3.6 this implies corresponding upper bounds on Galois orbits. This is not used in the proof of our main result but we believe can be useful in other contexts.

Theorem C.1. *Let* $M\leq G$ *be reductive groups over* $\mathbb{Q}$, $K\leq G(\mathbb{A}_f)$ *be a compact open subgroup, and* $K_M\leq K\cap M(\mathbb{A}_f)$ *be a compact subgroup.*

Let $\phi_0:M\to G$ *be the inclusion monomorphism, and* $W=G\cdot\phi_0$ *be the conjugacy class of* ϕ_0, *as an algebraic variety.*

Let $\iota:W\hookrightarrow\mathbb{A}^N$ *be an affine embedding, and let* H_f *be as defined in* (17). *Then we have, as* ϕ *describes* $W(\mathbb{A}_f)$,

$$[\phi(K_M):\phi(K_M)\cap K]\preccurlyeq H_{\iota,f}(\phi). \tag{C.1}$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

We prove a more precise version. Let $\rho : G \hookrightarrow GL(d)$ be a faithful representation and let us identify G with $\rho(G)$. In the associative algebra $\operatorname{End}(\mathbb{Q}^d)$, we denote the subalgebras linearly generated by $M(\mathbb{Q})$ and $G(\mathbb{Q})$ by

$$B_M := \sum_{m \in M(\mathbb{Q})} \mathbb{Q} \cdot m \quad \text{and} \quad B_G := \sum_{g \in G(\mathbb{Q})} \mathbb{Q} \cdot g.$$

Let $\Phi_0 : B_M \to B_G$ denote the inclusion. We have $M(\mathbb{Q}) \subseteq B_M$, $G(\mathbb{Q}) \subseteq B_G$, and $\phi_0 : M(\mathbb{Q}) \to G(\mathbb{Q})$ is the restriction of Φ_0.

For every field extension $L/\mathbb{Q}$, and $\phi = g \cdot \phi_0 \cdot g^{-1} \in W(L)$, with $g \in G(\overline{L})$, the map

$$B_\phi = g \cdot \Phi_0 \cdot g^{-1} : B_M \otimes L \to B_G \otimes L$$

is a L-linear extension of ϕ to $B_M \otimes L$, and is the unique L-linear extension.

We choose linear bases of B_M and B_G generating $B_M \cap \operatorname{End}(\mathbb{Z}^d)$ and $B_G \cap \operatorname{End}(\mathbb{Z}^d)$, respectively, and we consider the corresponding isomorphism $\operatorname{Hom}(B_M, B_G) \simeq \mathbb{Q}^{\dim(B_M)\cdot\dim(B_G)}$. Then $\phi \mapsto B_\phi$ induces an affine embedding $\iota_\rho : W \hookrightarrow \operatorname{Hom}(B_M, B_G) \simeq \mathbb{Q}^{\dim(B_M)\cdot\dim(B_G)}$.

Theorem C.2. *Define $G(\widehat{\mathbb{Z}}) := G(\mathbb{A}_f) \cap GL(d, \widehat{\mathbb{Z}})$ and $M(\widehat{\mathbb{Z}}) := M(\mathbb{A}_f) \cap GL(d, \widehat{\mathbb{Z}})$. Then, for every $\phi \in W(\mathbb{A}_f)$, we have*

$$[\phi(M(\widehat{\mathbb{Z}})) : \phi(M(\widehat{\mathbb{Z}})) \cap G(\widehat{\mathbb{Z}})] \leq H_{\iota_\rho, f}(\phi)^{2+d^2}.$$

We note that if G is of adjoint type, we can use the adjoint representation and pick $d = \dim(G)$.

Let us prove Theorem C.2.

Proof. We endow $\operatorname{Hom}(B_M \otimes \mathbb{Q}_p, B_G \otimes \mathbb{Q}_p)$ with the norm

$$\|\Phi\| = \min\{p^k \in p^{\mathbb{Z}} : \ \forall m \in B_M \otimes \mathbb{Q}_p \cap \operatorname{End}(\mathbb{Z}_p^d), p^k \cdot \Phi(m) \in B_G \otimes \mathbb{Q}_p \cap \operatorname{End}(\mathbb{Z}_p^d)\}. \tag{C.2}$$

We note that $H_{\iota_\rho, p}(\phi) = \max\{1; \|B_\phi\|\}$.

It suffices to prove that, for every prime p, and $\phi \in W(\mathbb{Q}_p)$, we have

$$[\phi(M(\mathbb{Z}_p)) : \phi(M(\mathbb{Z}_p)) \cap G(\mathbb{Z}_p)] \leq \|B_\phi\|_p^{2+d^2}. \tag{C.3}$$

Let us write $\|B_\phi\|_p = p^k$. Then, in the notation of Lemma C.3, we have

$$\phi(M(\mathbb{Z}_p)) \subseteq S(d, p, p^k).$$

Thus, (C.3) follows from (C.4). □

We deduce Theorem C.1 from Theorem C.2.

Proof. The assumptions imply the finiteness of

$$C_M := [K_M : K_M \cap M(\widehat{\mathbb{Z}})] = [\phi(K_M) : \phi(K_M) \cap \phi(M(\widehat{\mathbb{Z}}))]$$

and

$$C_G := [G(\widehat{\mathbb{Z}}) : K \cap G(\widehat{\mathbb{Z}})].$$

We have

$$[\phi(K_M) : \phi(K_M) \cap K] \leq C_M \cdot C_G \cdot [\phi(M(\widehat{\mathbb{Z}})) : \phi(M(\widehat{\mathbb{Z}})) \cap G(\widehat{\mathbb{Z}})].$$

By Proposition 4.1, we have $H_f \approx H_{\iota_\rho, f}$. Using (C.2), we conclude

$$[\phi(K_M) : \phi(K_M) \cap K] \leq C_M \cdot C_G \cdot H_{\iota_\rho, f}(\phi)^{2+d^2} \approx H_f(\phi). \qquad \square$$

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Lemma C.3. *Let p be a prime, d be in $\mathbb{Z}_{\geq 0}$, and k be in $\mathbb{Z}_{\geq 0}$.*

Define $S(d,p,p^k) = \{b \in \mathrm{End}(\mathbb{Q}_p^d) : \|b\| \leq p^k, \det(b) \in \mathbb{Z}_p^\times\}$.

Then $S(d,p,p^k) = S(d,p,p^k) \cdot GL(d,\mathbb{Z}_p)$ and

$$\#S(d,p,p^k)/GL(d,\mathbb{Z}_p) \leq (p^k)^{2+d^2}. \tag{C.4}$$

Proof. We endow $\mathrm{End}(\mathbb{Q}_p^d)$ with the additive Haar measure μ normalised by $\mu(B(1)) = 1$, where $B(p^k)$, for $k \in \mathbb{Z}_{\geq 1}$ is the ball of radius p^k. One knows that the Haar measure satisfies $\mu(g \cdot A) = |\det(g)| \cdot \mu(A)$.

For $A = B(1)$ and $g = p^k \cdot \mathrm{Id}$ this yields

$$\mu(S(d,p,p^k)) \leq \mu(B(p^k)) = (p^k)^{d^2}.$$

For $b \in GL(N,\mathbb{Q}_p)$ such that $\det(b) \in \mathbb{Z}_p^\times$ this yields

$$\mu(b \cdot GL(d,\mathbb{Z}_p)) = \mu(GL(d,\mathbb{Z}_p)). \tag{C.5}$$

One can also check

$$\begin{aligned}\mu(GL(d,\mathbb{Z}_p)) = \frac{\#GL(d,\mathbb{F}_p)}{\#\mathrm{End}(\mathbb{F}_p^d)} &= \prod_{i=1}^{d} 1 - \frac{1}{p^i} \\ &\geq \prod_{i=1}^{\infty} 1 - \frac{1}{2^i} \geq 0.25 \geq 1/p^2. \end{aligned} \tag{C.6}$$

The norm multiplicativity $\|b \cdot g\| = \|b\| \cdot \|g\|$ implies the right invariance

$$S(d,p,p^k) = S(d,p,p^k) \cdot GL(d,\mathbb{Z}_p). \tag{C.7}$$

Equivalently, we can write

$$S(d,p,p^k) = b_1 \cdot GL(d,\mathbb{Z}_p) \sqcup \cdots \sqcup b_c \cdot GL(d,\mathbb{Z}_p),$$

with $c = \#S(d,p,p^k)/GL(d,\mathbb{Z}_p)$.

Using (C.5), we deduce

$$\#S(d,p,p^k)/GL(d,\mathbb{Z}_p) = \mu(S(d,p,p^k))/\mu(GL(d,\mathbb{Z}_p)).$$

Assume $k = 0$. Then (C.4) follows from

$$S(d,p,p^k) = GL(d,\mathbb{Z}_p) \text{ and } \#S(d,p,p^k)/GL(d,\mathbb{Z}_p) = 1 \leq 1^{2+d^2}.$$

We may now assume $k \geq 1$. Then (C.4) follows from

$$\#S(d,p,p^k)/GL(d,\mathbb{Z}_p) \leq p^2 \cdot (p^k)^{(d^2)} \leq (p^k)^{2+d^2}.$$

□

Acknowledgements

The second named author has been contemplating the André–Pink–Zannier problem and how to use the Mumford–Tate conjecture to approach it for 20 years. He had a number of discussions on the subject with Bas Edixhoven, Richard Pink, Yves André, Emmanuel Ullmo, Bruno Klingler, Martin Orr, Christopher Daw, and more. Both authors would like to thank them all.

Conflicts of interest

None.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Financial support

Both authors were supported by Leverhulme Trust Grant RPG-2019-180. The first author is also supported by the EPSRC grant EP/Y020758/1. The support of the Leverhulme Trust is gratefully acknowledged.

Journal information

Compositio Mathematica is owned by the Foundation Compositio Mathematica and published by the London Mathematical Society in partnership with Cambridge University Press. All surplus income from the publication of *Compositio Mathematica* is returned to mathematics and higher education through the charitable activities of the Foundation, the London Mathematical Society and Cambridge University Press.

References

And89 Y. André, G-*functions and geometry* (Max-Planck-Institut für Mathematik, Bonn, 1989).

Bal20 G. Baldi, *On the geometric Mumford-Tate conjecture for subvarieties of Shimura varieties*, Proc. Amer. Math. Soc. **148** (2020).

BCR98 J. Bochnak, M. Coste and M.-F. Roy, *Real algebraic geometry*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 36 (Springer, 1998).

BG06 E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4 (Cambridge University Press, 2006).

BJ06 A. Borel and L. Ji, *Compactifications of symmetric and locally symmetric spaces*, Mathematics: Theory & Applications (Birkhäuser, Boston, MA, 2006).

BT65 A. Borel and J. Tits, *Groupes réductifs*, Inst. Hautes Études Sci. Publ. Math. **27** (1965).

CK16 A. Cadoret and A. Kret, *Galois-generic points on Shimura varieties*, Algebra Number Theory **10** (2016), 1893–1934.

CM20 A. Cadoret and B. Moonen, *Integral and adelic aspects of the Mumford-Tate conjecture*, J. Inst. Math. Jussieu **19** (2020).

COU01 L. Clozel, H. Ooh and E. Ullmo, *Hecke operators and equidistribution of Hecke points*, Invent. Math. **144** (2001), 327–351.

Del71 P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389.

Del79 P. Deligne, *Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques*, in *Automorphic forms, representations and L-functions*, Proceedings of Symposia in Pure Mathematics, vol. XXXIII, Part 2 (American Mathematical Society, 1979), 247–289.

DSMS99 J. D. Dixon, M. P. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups*, second edition, Cambridge Studies in Advanced Mathematics, vol. 61 (Cambridge University Press, 1999).

EY03 B. Edixhoven and A. Yafaev, *Subvarieties of Shimura varieties*, Ann. of Math. (2) **157** (2003), 621–645.

EMS96 A. Eskin, S. Mozes and N. Shah, *Unipotent flows and counting lattice points on homogeneous varieties*, Ann. of Math. (2) **143** (1996), 253–299.

EO06 A. Eskin and H. Oh, *Ergodic theoretic proof of equidistribution of Hecke points*, Ergodic Theory Dynam. Systems **26** (2006), 163–167.

Hal03 B. C. Hall, *Lie groups, Lie algebras, and representations (An elementary introduction)*, Graduate Texts in Mathematics, vol. 222 (Springer, 2003).

HW79 G. H. Hardy and E. M. Wright, *Introduction to the theory of numbers*, fifth edition (The Clarendon Press, Oxford University Press, New York, 1979).

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Hig08 N. J. Higham, *Functions of matrices, theory and computation* (Society for Industrial and Applied Mathematics (SIAM), 2008).

HR16 M. Hindry and N. Ratazzi, *Torsion pour les variétés abéliennes de type I et II*, Algebra Number Theory (2016).

Hum75 J. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics, vol. 21 (Springer, New York–Heidelberg, 1975).

KUY16 B. Klingler, E. Ullmo and A. Yafaev, *The hyperbolic Ax-Lindemann-Weierstrass conjecture*, Publ. Math. Inst. Hautes Etudes Sci. **123** (2016), 333–360.

KY14 B. Klingler and A. Yafaev, *The André-Oort conjecture*, Ann. of Math. (2) **180** (2014).

Kne69 M. Kneser, *Lectures on Galois cohomology of classical groups*, Tata Institute of Fundamental Research Lectures on Mathematics, vol. 47 (Tata Institute of Fundamental Research, Bombay, 1969).

Lom16 D. Lombardo, *On the ℓ-adic Galois representations attached to nonsimple abelian varieties*, Ann. Inst. Fourier **66** (2016), 1217–1245.

MT11 G. Malle and D. Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge Studies in Advanced Mathematics, vol. 133 (Cambridge University Press, 2011).

MVW84 C. R. Matthews, L. N. Vaserstein and B. Weisfeiler, *Congruence properties of Zariski-dense subgroups. I*, Proc. Lond. Math. Soc. (3) **48** (1984).

Moo98 B. Moonen, *Linearity properties of Shimura varieties. I*, J. Algebraic Geom. **7** (1998), 539–567.

Nor87 M. Nori, *On subgroups of $GL_n(\boldsymbol{F}_p)$*, Invent. Math. **88** (1987).

Orr15 M. Orr, *Families of abelian varieties with many isogenous fibres*, J. Reine Angew. Math. **705** (2015), 211–231.

Orr18 M. Orr, *Height bounds and the Siegel property*, Algebra Number Theory **12** (2018), 455–478.

Pil09 J. Pila, *On the algebraic points of a definable set*, Selecta Math. (N.S.) **15** (2009).

Pin05 R. Pink, *A combination of the conjectures of Mordell-Lang and André-Oort*, in *Geometric methods in algebra and number theory*, Progress in Mathematics, vol. 235 (de Gruyter, 2005), 251–282.

Pin98 R. Pink, *l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture*, J. Reine Angew. Math. **495** (1998), 187–237.

PR94 V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, 139 (Academic Press, Boston, MA, 1994).

Ric09 R. Richard, *Sur quelques questions d'équidistribution en géométrie arithmétique*, Partie I, chapitre 3, *Équidistribution et Variétés de Shimura* (2009), https://tel.archives-ouvertes.fr/tel-00438515/.

RU24 R. Richard and E. Ullmo, *Equidistribution de sous-variétés spéciales et o-minimalité: André-Oort géométrique* (with an appendix with J. Chen), Ann. Inst. Fourier (Grenoble) **74** (2024), 2667–2721.

RY19 R. Richard and A. Yafaev, *Topological and equidistribution refinement of the André–Pink–Zannier conjecture at finitely many places*, C. R. Math. **357** (2019), 231–235.

Ric67 R. Richardson, *Conjugacy classes in Lie algebras and algebraic groups*, Ann. of Math. (2) **86** (1967).

Ric88 R. Richardson, *Conjugacy classes of n-tuples in Lie algebras and algebraic groups*, Duke Math. J. **57** (1988).

Rob00 A. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, 198 (Springer, 2000).

Ser64 J.-P. Serre, *Sur les groupes de congruence des variétés abéliennes (1964)*, in *Œuvres II: 1960–1971*, Springer Collected Works in Mathematics (Springer, 2013), Article 162.

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press

Ser94a J.-P. Serre, *Lettre à K. Ribet (1994)*, in *Œuvres IV: 1985–1998*, Springer Collected Works in Mathematics (Springer, 2013), Article 133.

Ser94b J.-P. Serre, *Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques (1994)*, in *Œuvres IV: 1985–1998*, Springer Collected Works in Mathematics (Springer, 2013), Article 161.

Ser97 J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics (Friedrich Vieweg & Sohn, Braunschweig, 1997).

Ser98 J.-P. Serre, *Œuvres IV: 1985–1998*, Springer Collected Works in Mathematics (Springer, 2013).

Tit79 J. Tits, *Reductive groups over local fields*, in *Automorphic forms, representations and L-functions*, Proceedings of Symposia in Pure Mathematics, vol. XXXIII (American Mathematical Society, 1979), 29–69.

Ull14 E. Ullmo, *Applications du theorème d'Ax–Lindemann hyperbolique*, Compos. Math. **150** (2014), 175–190.

UY11 E. Ullmo and A. Yafaev, *A characterization of special subvarieties*, Mathematika **57** (2011), 263–273.

UY13 E. Ullmo and A. Yafaev, *Mumford-Tate and generalised Shafarevich conjectures*, Ann. Math. Qué. **37** (2013), 255–284.

UY14 E. Ullmo and A. Yafaev, *Galois orbits and equidistribution of special subvarieties: towards the André-Oort conjecture*, Ann. of Math. (2) **180** (2014).

vdDri98 L. van den Dries, *Tame topology and o-minimal structure*, London Mathematical Society Lecture Notes Series, vol. 248 (Cambridge University Press, 1998).

Yaf00 A. Yafaev, *Sous-variétés des variétés de Shimura*, Thèse de doctorat, Université de Rennes 1 (2000), https://theses.hal.science/tel-04391600.

Zan12 U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry* (with appendices by David Masser), Annals of Mathematics Studies, vol. 181 (Princeton University Press, Princeton, NJ, 2012).

Rodolphe Richard rodolphe.richard@normalesup.org
UCL Department of Mathematics, University College London, Gower Street,
London WC1E 6BT, UK

and

Institut des Hautes Études Scientifiques, 35 Rte de Chartres, 91440 Bures-sur-Yvette, France

Current address: Department of Mathematics, The University of Manchester,
Alan Turing Building, Oxford Road, Manchester M13 9PL, UK

Andrei Yafaev yafaev@ucl.ac.uk
UCL Department of Mathematics, University College London, Gower Street,
London WC1E 6BT, UK

https://doi.org/10.1112/S0010437X2400722X Published online by Cambridge University Press