Algebra & Number Theory

Volume 13

2019

No. 1

msp

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

The subscription price for 2019 is US $385/year for the electronic version, and $590/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

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

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

ALGEBRA AND NUMBER THEORY 13:1 (2019)
dx.doi.org/10.2140/ant.2019.13.1

Ordinary algebraic curves with many automorphisms in positive characteristic

Gábor Korchmáros and Maria Montanucci

Let $\mathscr{X}$ be an ordinary (projective, geometrically irreducible, nonsingular) algebraic curve of genus $\mathfrak{g}(\mathscr{X}) \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic p. Let $\mathrm{Aut}(\mathscr{X})$ be the group of all automorphisms of $\mathscr{X}$ which fix $\mathbb{K}$ elementwise. For any solvable subgroup G of $\mathrm{Aut}(\mathscr{X})$ we prove that $|G| \leq 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$. There are known curves attaining this bound up to the constant 34. For p odd, our result improves the classical Nakajima bound $|G| \leq 84(\mathfrak{g}(\mathscr{X})-1)\mathfrak{g}(\mathscr{X})$ and, for solvable groups G, the Gunby–Smith–Yuan bound $|G| \leq 6(\mathfrak{g}(\mathscr{X})^2 + 12\sqrt{21}\,\mathfrak{g}(\mathscr{X})^{3/2})$ where $\mathfrak{g}(\mathscr{X}) > cp^2$ for some positive constant c.

1. Introduction

In this paper, $\mathscr{X}$ stands for a (projective, geometrically irreducible, nonsingular) algebraic curve of genus $\mathfrak{g}(\mathscr{X}) \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic p. Let $\mathrm{Aut}(\mathscr{X})$ be the group of all automorphisms of $\mathscr{X}$ which fix $\mathbb{K}$ elementwise. The assumption $\mathfrak{g}(\mathscr{X}) \geq 2$ ensures that $\mathrm{Aut}(\mathscr{X})$ is finite. However, the classical Hurwitz bound $|\mathrm{Aut}(\mathscr{X})| \leq 84(\mathfrak{g}(\mathscr{X})-1)$ for complex curves fails in positive characteristic, and there exist four families of curves satisfying $|\mathrm{Aut}(\mathscr{X})| \geq 8\mathfrak{g}^3(\mathscr{X})$ [Stichtenoth 1973; Henn 1978; Hirschfeld et al. 2008, §11.12]. Each of them has p-rank $\gamma(\mathscr{X})$ (equivalently, its Hasse–Witt invariant) equal to zero; see for instance [Giulietti and Korchmáros 2014]. On the other hand, if $\mathscr{X}$ is ordinary, i.e., $\mathfrak{g}(\mathscr{X}) = \gamma(\mathscr{X})$, Guralnick and Zieve announced in 2004, as reported in [Gunby et al. 2015; Kontogeorgis and Rotger 2008], that for odd p there exists a sharper bound, namely $|\mathrm{Aut}(\mathscr{X})| \leq c_p\mathfrak{g}(\mathscr{X})^{8/5}$ with some constant c_p depending on p. It should be noticed that no proof of this sharper bound is available in the literature. In this paper, we concern ourselves with solvable automorphism groups G of an ordinary curve $\mathscr{X}$, and for odd p we prove the even sharper bound:

Theorem 1.1. *Let $\mathscr{X}$ be an algebraic curve of genus $\mathfrak{g}(\mathscr{X}) \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic p. If $\mathscr{X}$ is ordinary and G is a solvable subgroup of* $\mathrm{Aut}(\mathscr{X})$, *then*

$$|G| \leq 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}. \tag{1}$$

For odd p, our result provides an improvement on the classical Nakajima bound $|G| \leq 84(\mathfrak{g}(\mathscr{X})-1)\mathfrak{g}(\mathscr{X})$ [1987] and, for solvable groups, on the recent Gunby–Smith–Yuan bound $|G| \leq 6(\mathfrak{g}(\mathscr{X})^2 + 12\sqrt{21}\,\mathfrak{g}(\mathscr{X})^{3/2})$ proven in [Gunby et al. 2015] under the hypothesis that $\mathfrak{g}(\mathscr{X}) > cp^2$ for some positive constant c.

MSC2010: primary 14H37; secondary 14H05.
Keywords: algebraic curves, algebraic function fields, positive characteristic, automorphism groups.

The following example is due to Stichtenoth, and it shows that (1) is the best possible bound apart from the constant c [Korchmáros et al. 2018]. Let $\mathbb{F}_q$ be a finite field of order $q = p^h$, and let $\mathbb{K} = \overline{\mathbb{F}_q}$ denote its algebraic closure. For a positive integer m prime to p, let $\mathcal{Y}$ be the irreducible curve with affine equation

$$y^q + y = x^m + \frac{1}{x^m} \tag{2}$$

and $F = \mathbb{K}(\mathcal{Y})$ its function field. Let $t = x^{m(q-1)}$. The extension $F|\mathbb{K}(t)$ is a non-Galois extension as the Galois closure of F with respect to H is the function field $\mathbb{K}(x, y, z)$ where x, y, z are linked by (2) and $z^q + z = x^m$. Furthermore, $\mathfrak{g}(\mathcal{Y}) = (q-1)(qm-1)$, $\gamma(\mathcal{Y}) = (q-1)^2$, and $\mathrm{Aut}(\mathcal{Y})$ contains a subgroup $Q \rtimes U$ of index 2 where Q is an elementary abelian normal subgroup of order q^2 and the complement U is a cyclic group of order $m(q-1)$. If $m = 1$, then $\mathcal{Y}$ is an ordinary curve, and in this case $2\mathfrak{g}(\mathcal{Y})^{3/2} = 2(q-1)^3 < 2q^2(q-1) = |\mathrm{Aut}(\mathcal{X})|$, which shows indeed that (1) is sharp up to the constant c.

Lower bounds on the order of solvable automorphism groups of algebraic curves depending on their genera are due to Neftin and Zieve. Their [2015, Theorem 4.1] states that for every integer $\ell > 0$ there exists a curve $\mathcal{X}$ together with a solvable subgroup of $\mathrm{Aut}(\mathcal{X})$ of order d and derived length ℓ such that

$$\mathfrak{g}(\mathcal{X}) \le c_\ell d \log^{o\ell}(d),$$

where c_ℓ is a constant and $\log^{o\ell}$ denotes log iterated ℓ times. The curve $\mathcal{X}$ is constructed as a solvable cover of a curve with at least one rational point, in which a given set S of rational points splits completely.

2. Background and preliminary results

For a subgroup G of $\mathrm{Aut}(\mathcal{X})$, let $\overline{\mathcal{X}}$ denote a nonsingular model of $\mathbb{K}(\mathcal{X})^G$, that is, a (projective, nonsingular, geometrically irreducible) algebraic curve with function field $\mathbb{K}(\mathcal{X})^G$, where $\mathbb{K}(\mathcal{X})^G$ consists of all elements of $\mathbb{K}(\mathcal{X})$ fixed by every element in G. Usually, $\overline{\mathcal{X}}$ is called the quotient curve of $\mathcal{X}$ by G and denoted by $\mathcal{X}/G$. The field extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X})^G$ is Galois of degree $|G|$.

Since our approach is mostly group theoretical, we prefer to use notation and terminology from group theory rather than from function field theory.

Let Φ be the cover of $\mathcal{X}|\overline{\mathcal{X}}$ where $\overline{\mathcal{X}} = \mathcal{X}/G$. A point $P \in \mathcal{X}$ is a ramification point of G if the stabilizer G_P of P in G is nontrivial; the ramification index e_P is $|G_P|$; a point $\bar{Q} \in \overline{\mathcal{X}}$ is a branch point of G if there is a ramification point $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$; the ramification (branch) locus of G is the set of all ramification (branch) points. The G-orbit of $P \in \mathcal{X}$ is the subset $o = \{R \mid R = g(P),\ g \in G\}$ of $\mathcal{X}$, and it is *long* if $|o| = |G|$; otherwise o is *short*. For a point $\bar{Q}$, the G-orbit o lying over $\bar{Q}$ consists of all points $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$. If $P \in o$, then $|o| = |G|/|G_P|$ and hence $\bar{Q}$ is a branch point if and only if o is a short G-orbit. It may be that G has no short orbits. This is the case if and only if every nontrivial element in G is fixed-point-free on $\mathcal{X}$, that is, the cover Φ is unramified. On the other hand, G has a finite number of short orbits. For a nonnegative integer i, the i-th ramification group of $\mathcal{X}$ at P is denoted by $G_P^{(i)}$ (or $G_i(P)$ as in [Serre 1979, Chapter IV]) and defined to be

$$G_P^{(i)} = \{g \mid \mathrm{ord}_P(g(t) - t) \ge i + 1,\ g \in G_P\},$$

where t is a uniformizing element (local parameter) at P. Here $G_P^{(0)} = G_P$.

Let $\bar{\mathfrak{g}}$ be the genus of the quotient curve $\overline{\mathcal{X}} = \mathcal{X}/G$. The Riemann–Hurwitz genus formula gives

$$2\mathfrak{g} - 2 = |G|(2\bar{\mathfrak{g}} - 2) + \sum_{P \in \mathcal{X}} d_P, \tag{3}$$

where the different d_P at P is given by

$$d_P = \sum_{i \geq 0} (|G_P^{(i)}| - 1). \tag{4}$$

If $|G_P|$ is prime to p, then $d_P = |G_P| - 1$.

Let γ be the p-rank of $\mathcal{X}$, and let $\bar{\gamma}$ be the p-rank of the quotient curve $\overline{\mathcal{X}} = \mathcal{X}/G$. The Deuring–Shafarevich formula (see [Sullivan 1975] or [Hirschfeld et al. 2008, Theorem 11.62]) states that if G is a p-group then

$$\gamma - 1 = |G|(\bar{\gamma} - 1) + \sum_{i=1}^{k} (|G| - \ell_i) \tag{5}$$

where $\ell_1, \ldots, \ell_k$ are the sizes of the short orbits of G. If $\mathcal{X}$ is ordinary (and hence $G_P^{(2)}$ is trivial for every $P \in \mathcal{X}$; see Result 2.5(i)), then $d_P = |G_P^{(0)}| - 1 + |G_P^{(1)}| - 1 = 2(|G_P^{(0)}| - 1) = 2(|G_P| - 1)$ and hence (5) follows from (3) and vice versa.

The Nakajima bound (see [1987, Theorem 1] or [Hirschfeld et al. 2008, Theorem 11.84]) states that the existence of large p-groups of automorphisms implies that $\gamma = 0$.

Result 2.1. *If $\mathcal{X}$ has positive p-rank γ, then every p-subgroup of* $\mathrm{Aut}(\mathcal{X})$ *has order* $\leq p(\gamma - 1)/(p - 2)$.

A subgroup of $\mathrm{Aut}(\mathcal{X})$ is a prime to p group (or a p'-subgroup) if its order is prime to p. A subgroup G of $\mathrm{Aut}(\mathcal{X})$ is *tame* if the 1-point stabilizer of any point in G is p'-group. Otherwise, G is *nontame* (or *wild*). Obviously, every p'-subgroup of $\mathrm{Aut}(\mathcal{X})$ is tame, but the converse is not always true.

Result 2.2. *The following claims hold.*

(i) *If $|G| > 84(\mathfrak{g}(\mathcal{X}) - 1)$, then G is nontame.*

(ii) *If G is abelian, then $|G| \leq 4\mathfrak{g} + 4$.*

(iii) *If G has prime order other than p, then $|G| \leq 2\mathfrak{g} + 1$.*

The first two claims are due to Stichtenoth [1973]; see also [Hirschfeld et al. 2008, Theorems 11.56 and 11.79]. For a proof of claim (iii), see [Homma 1980] or [Hirschfeld et al. 2008, Theorem 11.108].

Henn's bound [1978] (see also [Hirschfeld et al. 2008, Theorem 11.127]) has the following corollary.

Result 2.3. *If $|G| > 8\mathfrak{g}^3$, then $\mathcal{X}$ has zero p-rank, and G is not solvable.*

An orbit o of G is *tame* if G_P is a p'-group for $P \in o$. The structure of G_P is well known; see for instance [Serre 1979, Chapter IV, Corollary 4] or [Hirschfeld et al. 2008, Theorem 11.49].

Result 2.4. *The stabilizer G_P of a point $P \in \mathcal{X}$ in G is a semidirect product $G_P = Q_P \rtimes U$ where the normal subgroup Q_P is a p-group while the complement U is a cyclic prime to p group.*

If $\mathscr{X}$ is ordinary, some more results are available; those used in this paper are collected below.

Result 2.5. *If $\mathscr{X}$ is an ordinary curve, then*

(i) $Q_P^{(2)}$ *is trivial*,

(ii) Q_P *is elementary abelian*,

(iii) *no nontrivial element of* U *commutes with a nontrivial element of* Q_P,

(iv) $|U|$ *divides* $|Q_P|-1$, *and*

(v) *the quotient curve* $\mathscr{X}/G$ *for a* p*-group* G *of automorphisms is also ordinary.*

Claim (i) is due to Nakajima [1987, Theorem 2.1]. Claim (ii) follows from claim (i) by Serre's result [1979, Corollary 3, p. 67] stating that the factor groups $Q_P^{(i)}/Q_P^{(i+1)}$ for $i \geq 1$ are elementary abelian; see also [Hirschfeld et al. 2008, Theorem 11.74]. Claim (iii) follows from claim (ii) by Serre's result [1979, Corollary 1, p. 69]; see also [Hirschfeld et al. 2008, Theorem 11.75(ii)]. Claim (iv) is a consequence of claim (iii) since the latter claim together with Result 2.4 imply that U induces an automorphism group of Q_P. Claim (v) follows from comparison of (3) to (5) taking into account claim (i).

For a nontrivial p-subgroup G of $\mathrm{Aut}(\mathscr{X})$, divide both sides in (3) by 2 and then subtract the result from (5). If $G_P^{(2)}$ is trivial for every $P \in \mathscr{X}$, then this computation gives

$$\mathfrak{g}(\mathscr{X}) - \gamma(\mathscr{X}) = |G|(\mathfrak{g}(\overline{\mathscr{X}}) - \gamma(\overline{\mathscr{X}})) \tag{6}$$

where $\overline{\mathscr{X}} = \mathscr{X}/Q$ [Nakajima 1987]. This shows the first two claims of the following result hold. The third one is due to Stichtenoth [1973]; see also [Hirschfeld et al. 2008, Theorem 11.79].

Result 2.6. *Let* Q *be nontrivial* p*-subgroup of* $\mathrm{Aut}(\mathscr{X})$. *Assume that* $Q_P^{(2)}$ *is trivial for every* $P \in \mathscr{X}$. *Then*

(i) (6) *holds*,

(ii) $\mathscr{X}$ *and its quotient curve* $\mathscr{X}/Q$ *are simultaneously ordinary or not*, *and*

(iii) $|Q_P| \leq p\mathfrak{g}(\mathscr{X})/(p-1)$.

The first two claims below on low-genus curves are well known; see for instance [Hirschfeld et al. 2008, Theorems 11.94 and 11.99]. The third one is a corollary of Henn's bound.

Result 2.7. *If* G *is an automorphism group of an elliptic curve* $\mathscr{E}$ *over* $\mathbb{K}$, *then for every point* $P \in \mathscr{E}$ *the order of the stabilizer* G_P *of* P *in* G *divides* 6 *when* $p > 3$ *and* 12 *when* $p = 3$. *The solvable automorphism groups of a genus*-2 *curve over* $\mathbb{K}$ *have order at most* 48. *For genus*-3 *curves the latter bound is* 216.

We also need a technical result.

Result 2.8. *Assume that* $\mathrm{Aut}(\mathscr{X})$ *has a solvable subgroup* G *of order larger than* $34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$. *If* N *is a normal subgroup of* G *and the quotient curve* $\overline{\mathscr{X}} = \mathscr{X}/N$ *is neither rational nor elliptic*, *then the automorphism group* $\overline{G} = G/N$ *of* $\overline{\mathscr{X}}$ *has order larger than* $34(\mathfrak{g}(\overline{\mathscr{X}})+1)^{3/2}$, *as well.*

Since $|N| = |G|/|\bar{G}|$, the claim is a straightforward consequence of (3) except for the cases where $\mathfrak{g}(\bar{\mathscr{X}}) = 2$, or $\mathfrak{g}(\bar{\mathscr{X}}) = 3$, $\mathfrak{g}(\mathscr{X}) = 5$, $|N| = 2$, and the cover $\mathscr{X}|\bar{\mathscr{X}}$ is unramified. Actually, the exceptional cases do not occur. In fact, $|\bar{G}| \geq |G|(\mathfrak{g}(\bar{\mathscr{X}})-1)/(\mathfrak{g}(\mathscr{X})-1) > 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}(\mathfrak{g}(\bar{\mathscr{X}})-1)/(\mathfrak{g}(\mathscr{X})-1)$ is bigger than 48 and $8 \cdot 27 = 216$ for $\mathfrak{g}(\bar{\mathscr{X}}) = 2$ and $\mathfrak{g}(\bar{\mathscr{X}}) = 3$, contradicting Results 2.7 and 2.3, respectively.

From group theory we use Dickson's classification of finite subgroups of the projective linear group $PGL(2, \mathbb{K})$; see [Valentini and Madan 1980] or [Hirschfeld et al. 2008, Theorem A.8].

Result 2.9. *The following is a complete list of finite solvable subgroups of* $PGL(2, \mathbb{K})$ *up to conjugacy*:

(i) *cyclic groups of order prime to* p,

(ii) *elementary abelian* p*-groups*,

(iii) *dihedral groups with an index-*2 *cyclic subgroup of order prime to* p,

(iv) *the alternating group* A_4,

(v) *the symmetric group* S_4,

(vi) *semidirect products of an elementary abelian* p*-group of order* p^h *by a cyclic group of order* n *with* $n \mid (p^h - 1)$.

If $PGL(2, \mathbb{K})$ is viewed as the automorphism group of the line over $\mathbb{K}$, any cyclic subgroup of order prime to p has exactly two points, while any p-subgroup has a unique fixed point [Valentini and Madan 1980].

We also use the Schur–Zassenhaus theorem; see for instance [Machì 2012, Corollary 7.5].

Result 2.10. *Let* G *be a finite group with a normal subgroup* N. *If* $|N|$ *is prime to the index* $[G : N]$ *of* N, *then* N *has a complement in* G, *that is*, $G = N \rtimes M$ *for a subgroup* M *of* G. *Such complements are pairwise conjugate in* G.

From representation theory, we need the Maschke theorem; see for instance [Machì 2012, Theorem 6.1].

Result 2.11. *Any representation of a finite group over a field whose characteristic is prime to the order of the group is completely reducible.*

The following two lemmas of independent interest play a role in our proof of Theorem 1.1.

Lemma 2.12. *Let* $\mathscr{X}$ *be an ordinary algebraic curve of genus* $\mathfrak{g}(\mathscr{X}) \geq 2$ *defined over an algebraically closed field* $\mathbb{K}$ *of odd characteristic* p. *Let* H *be a solvable automorphism group of* $\mathrm{Aut}(\mathscr{X})$ *containing a normal* p*-subgroup* Q *such that* $|Q|$ *and* $[H : Q]$ *are coprime. Suppose that a complement* U *of* Q *in* H *is abelian and that*

$$|H| > \begin{cases} 18(\mathfrak{g}-1) & \text{for } |U| = 3, \\ 12(\mathfrak{g}-1) & \text{otherwise}. \end{cases} \tag{7}$$

Then U *is cyclic, and the quotient curve* $\bar{\mathscr{X}} = \mathscr{X}/Q$ *is rational. Furthermore,* Q *has exactly two* (*nontame*) *short orbits, say* Ω_1, Ω_2. *They are also the only short orbits of* H, *and* $\mathfrak{g}(\mathscr{X}) = |Q| - (|\Omega_1| + |\Omega_2|) + 1$.

Proof. From Result 2.10, $H = Q \rtimes U$. Set $|Q| = p^k$ and $|U| = u$. Then $p \nmid u$. Furthermore, if $u = 2$, then $|H| = 2|Q| > 9\mathfrak{g}(\mathscr{X})$ whence $|Q| > 4.5\mathfrak{g}(\mathscr{X})$. From Result 2.1, $\mathscr{X}$ has zero p-rank, which is not possible as $\mathscr{X}$ is assumed to be ordinary of genus at least 2. Therefore, $u \geq 3$.

Three cases are treated separately according as the quotient curve $\overline{\mathscr{X}} = \mathscr{X}/Q$ has genus $\bar{\mathfrak{g}}$ at least 2, or $\overline{\mathscr{X}}$ is elliptic, or rational.

If $\mathfrak{g}(\overline{\mathscr{X}}) \geq 2$, then $\mathrm{Aut}(\overline{\mathscr{X}})$ has a subgroup isomorphic to U, and Result 2.2(ii) yields $4\mathfrak{g}(\overline{\mathscr{X}}) + 4 \geq |U|$. Furthermore, from (3) applied to Q, $\mathfrak{g} - 1 \geq |Q|(\mathfrak{g}(\overline{\mathscr{X}}) - 1)$. Let $c = 12$ or $c = 18$, according as $|U| > 3$ or $|U| = 3$, so that $|H| > c(\mathfrak{g} - 1)$ from (7). Then

$$(4\mathfrak{g}(\overline{\mathscr{X}}) + 4)|Q| \geq |U||Q| = |H| \geq c(\mathfrak{g} - 1) \geq c|Q|(\mathfrak{g}(\overline{\mathscr{X}}) - 1),$$

whence

$$c \leq 4\frac{\mathfrak{g}(\overline{\mathscr{X}}) + 1}{\mathfrak{g}(\overline{\mathscr{X}}) - 1}.$$

As the right-hand side is smaller than 12, a contradiction to the choice of the constant c is obtained.

If $\overline{\mathscr{X}}$ is elliptic, then the cover $\mathscr{X}|\overline{\mathscr{X}}$ ramifies; otherwise $\mathscr{X}$ itself would be elliptic. Thus, Q has some short orbits. The group H acts on the set of short orbits of Q. In this action, an orbit of a given short orbit o of Q with respect to H is a set of short orbits of Q having the same length of o. We will refer to these short orbits as images of o. Take a short orbit of Q together with its images $o_1, \ldots, o_{u_1}$ under the action of H. Since Q is a normal subgroup of H, $o = o_1 \cup \cdots \cup o_{u_1}$ is an H-orbit of size $u_1 p^v$ where $p^v = |o_1| = \cdots = |o_{u_1}|$. Equivalently, the stabilizer of a point $P \in o$ has order $p^{k-v}u/u_1$, and by Result 2.4, it is the semidirect product $Q_1 \rtimes U_1$ where $|Q_1| = p^{k-v}$ and $|U_1| = u/u_1$ for subgroups Q_1 of Q and U_1 of U, respectively. The point $\bar{P}$ lying under P in the cover $\mathscr{X}|\overline{\mathscr{X}}$ is fixed by the factor group $\bar{U}_1 = U_1Q/Q$. Since $\overline{\mathscr{X}}$ is elliptic, and p is prime to $|\bar{U}_1|$, Result 2.7 yields $|\bar{U}_1| \leq 4$ for $p = 3$ and $|\bar{U}_1| \leq 6$ for $p > 3$. As $\bar{U}_1 \cong U_1$, this yields the same bound for $|U_1|$, that is, $u \leq 4u_1$ for $p = 3$ and $u \leq 6u_1$ for $p > 3$. Furthermore, since the p-group Q_1 fixes P, and ${Q_1}^{(0)} = Q_1^{(1)} = Q_1$, we have $d_P = \sum_{i \geq 0}(|{Q_1}^{(i)}| - 1) \geq 2(|Q_1| - 1) = 2(p^{k-v} - 1) \geq \frac{4}{3}p^{k-v}$. From (3) applied to Q, since $P \in o$ and $|o| = p^v u_1$, if $p = 3$, then

$$2\mathfrak{g} - 2 \geq 3^v u_1 d_P \geq 3^v u_1\big(\tfrac{4}{3}3^{k-v}\big) = \tfrac{4}{3}3^k u_1 \geq \tfrac{1}{3}3^k u = \tfrac{1}{3}|Q||U| = \tfrac{1}{3}|H|,$$

while for $p > 3$,

$$2\mathfrak{g} - 2 \geq p^v u_1 d_P \geq p^v u_1\big(\tfrac{4}{3}p^{k-v}\big) = \tfrac{4}{3}p^k u_1 \geq \tfrac{2}{9}p^k u = \tfrac{2}{9}|Q||U| = \tfrac{2}{9}|H|,$$

but this contradicts (7).

If $\overline{\mathscr{X}}$ is rational, then Q has at least one short orbit. Furthermore, $\bar{U} = UQ/Q$ is isomorphic to a subgroup of $PGL(2, \mathbb{K}) \cong \mathrm{Aut}(\overline{\mathscr{X}})$. Since $U \cong \bar{U}$ and U is abelian, from Result 2.9, $\bar{U}$ is cyclic, $\bar{U}$ fixes two points $\bar{P}_0$ and $\bar{P}_\infty$, but no nontrivial element in $\bar{U}$ fixes a point other than $\bar{P}_0$ or $\bar{P}_\infty$. Let o_∞ and o_0 be the Q-orbits lying over $\bar{P}_0$ and $\bar{P}_\infty$, respectively. Obviously, o_∞ and o_0 are short orbits of H. We show that Q has at most two short orbits, the candidates being o_∞ and o_0. By absurd, there is a Q-orbit o

of size p^m with $m < k$ which lies over a point $\bar{P} \in \bar{\mathscr{X}}$ different from both $\bar{P}_0$ and $\bar{P}_\infty$. Since the orbit of $\bar{P}$ in $\bar{U}$ has length u, then the H-orbit of a point $P \in o$ has length up^m. If $u > 3$, (3) applied to Q gives

$$2\mathfrak{g}-2 \geq -2p^k + up^m(p^{k-m}-1) \geq -2p^k + up^m\tfrac{2}{3}p^{k-m} = -2p^k + \tfrac{2}{3}up^k = \tfrac{2}{3}(u-3)p^k > \tfrac{1}{6}up^k = \tfrac{1}{6}|H|,$$

a contradiction with $|H| > 12(\mathfrak{g}-1)$. If $u = 3$, then $p > 3$, and hence,

$$2\mathfrak{g}-2 \geq -2p^k + 3p^m(p^{k-m}-1) = p^k - 3p^m > \tfrac{1}{3}p^k,$$

whence $|H| = 3p^k < 18(\mathfrak{g}-1)$, a contradiction with (7). This proves that H has exactly two short orbits. Since, as we have showed, Q has either one or two short orbits, and they are contained in $o_\infty \cup o_0$, two cases arise correspondingly. Assume first that Q has two short orbits. They are o_∞ and o_0. If their lengths are p^a and p^b with $a, b < k$, then (5) (or (3)) applied to Q gives

$$\mathfrak{g}(\mathscr{X}) - 1 = \gamma(\mathscr{X}) - 1 = -p^k + (p^k - p^a) + (p^k - p^b)$$

whence $\mathfrak{g}(\mathscr{X}) = p^k - (p^a + p^b) + 1 > 0$. The same argument shows that if Q has just one short orbit, then $\gamma(\mathscr{X}) = 0$, a contradiction. □

Lemma 2.13. *Let N be an automorphism group of an algebraic curve of even genus such that $|N|$ is even. Then any 2-subgroup of N has a cyclic subgroup of index 2.*

Proof. Let U be a subgroup of N of order $d = 2^u \geq 2$, and $\bar{\mathscr{X}} = \mathscr{X}/U$ the arising quotient curve. From (3) applied to U,

$$2\mathfrak{g}(\mathscr{X}) - 2 = 2^u(2\mathfrak{g}(\bar{\mathscr{X}}) - 2) + \sum_{i=1}^{m}(2^u - \ell_i)$$

where $\ell_1, \ldots, \ell_m$ are the short orbits of U on $\mathscr{X}$. Since $\mathfrak{g}(\mathscr{X})$ is even, $2\mathfrak{g}(\mathscr{X}) - 2 \equiv 2 \pmod 4$. On the other hand, $2^u(2\mathfrak{g}(\bar{\mathscr{X}}) - 2) \equiv 0 \pmod 4$. Therefore, some ℓ_i $(1 \leq i \leq m)$ must be either 1 or 2. Therefore, U or a subgroup of U of index 2 fixes a point of $\mathscr{X}$ and hence is cyclic. □

3. The proof of Theorem 1.1

Our proof is by induction on the genus. Theorem 1.1 holds for $\mathfrak{g}(\mathscr{X}) = 2$, as $|G| \leq 48$ for any solvable automorphism group G of a genus-2 curve; see Result 2.7. For $\mathfrak{g}(\mathscr{X}) > 2$, $\mathscr{X}$ is taken by absurd for a minimal counterexample with respect the genera so that for any solvable subgroup of $\mathrm{Aut}(\bar{\mathscr{X}})$ of an ordinary curve $\bar{\mathscr{X}}$ of genus $\mathfrak{g}(\bar{\mathscr{X}}) \geq 2$ we have $|\bar{G}| \leq 34(\mathfrak{g}+1)^{3/2}$. Two cases are treated separately.

Case I. G contains a minimal normal p-subgroup.

Proposition 3.1. *Let $\mathscr{X}$ be an ordinary algebraic curve of genus $\mathfrak{g}$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic $p > 0$. If G is a solvable subgroup of* $\mathrm{Aut}(\mathscr{X})$ *containing a minimal normal p-subgroup N, then $|G| \leq 34(\mathfrak{g}+1)^{3/2}$.*

Proof. Before going through the proof we describe the main steps in it.

Take the largest normal p-subgroup Q of G. Let $\bar{\mathcal{X}}$ be the quotient curve of $\mathcal{X}$ with respect to Q, and let $\bar{G} = G/Q$. The first step is to show that $\bar{\mathcal{X}}$ is rational. Then we derive from the classification in Result 2.9 that G is a semidirect product of Q by cyclic group U of order prime to p. Therefore, Lemma 2.12 applies to G. This gives us enough information on the action of Q on $\mathcal{X}$: Q has exactly two (nontame) orbits, say Ω_1 and Ω_2, and they are also the only short orbits of G. Then a subgroup H of G of index ≤ 2 preserves both Ω_1 and Ω_2, inducing a permutation group on each of them. If both Ω_1 and Ω_2 are nontrivial, that is, $|\Omega_1| > 1$ and $|\Omega_2| > 1$, then two cases are possible, according as Q_P with $P \in \Omega_1$ is sharply transitive and faithful on Ω_2 or some nontrivial element in Q_P fixes Ω_2 pointwise. So the next step is to rule out both these possibilities using elementary permutation group theory together with Results 2.2 and 2.4. If $\Omega_1 = \{P\}$ and $|\Omega_2| > 1$, then G fixes P, and the structure of G is given by Result 2.4 where Q is an elementary abelian group, that is, a vector space over the prime field of $\mathbb{K}$ and G is a linear group so that some appropriate result from representation theory can be used. In fact, combining Result 2.11 with (5) allows us to rule out this possibility. If $\Omega_1 = \{P\}$ and $\Omega_2 = \{Q\}$, we are able to prove a much stronger bound, namely $|G| \le 2(\mathfrak{g}(\mathcal{X}) + 1)$. In this final step, our approach is function field theory rather than group theory as it uses some ideas from Nakajima's paper [1987] and the Riemann–Roch theorem together with some results on linearized polynomials over finite fields.

The quotient group $\bar{G}$ is a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$, and it has no normal p-subgroup; otherwise G would have a normal p-subgroup properly containing Q. For $\bar{\mathfrak{g}} = \mathfrak{g}(\bar{\mathcal{X}})$ three cases may occur, namely $\bar{\mathfrak{g}} \ge 2$, $\bar{\mathfrak{g}} = 1$, or $\bar{\mathfrak{g}} = 0$. If $\bar{\mathfrak{g}} \ge 2$, then Result 2.8 shows that $|\bar{G}| > 34(\bar{\mathfrak{g}} + 1)^{3/2}$. Since $\bar{\mathcal{X}}$ is still ordinary by Result 2.5(v), this contradicts our choice of $\mathcal{X}$ to be a minimal counterexample. If $\bar{\mathfrak{g}} = 1$, then the cover $\mathbb{K}(\mathcal{X})|\mathbb{K}(\bar{\mathcal{X}})$ ramifies. Take a short orbit Δ of Q. Let Γ be the nontame short orbit of G that contains Δ. Since Q is normal in G, the orbit Γ partitions into short orbits of Q whose components have the same length, which is equal to $|\Delta|$. Let k be the number of the Q-orbits contained in Γ. Then

$$|G_P| = \frac{|G|}{k|\Delta|}$$

holds for every $P \in \Gamma$. Moreover, the quotient group $G_P Q/Q$ fixes a place on $\bar{\mathcal{X}}$. Now, from Result 2.7,

$$\frac{|G_P Q|}{|Q|} = \frac{|G_P|}{|G_P \cap Q|} = \frac{|G_P|}{|Q_P|} \le 12.$$

From this together with (3) and Result 2.5(i),

$$2\mathfrak{g} - 2 \ge 2k|\Delta|(|Q_P| - 1) \ge 2k|\Delta|\frac{|Q_P|}{2} \ge \frac{k|\Delta||G_P|}{12} = \frac{|G|}{12},$$

which contradicts our hypothesis $|G| > 34(\mathfrak{g} + 1)^{3/2}$.

It turns out that $\bar{\mathcal{X}}$ is rational. Therefore, $\bar{G}$ is isomorphic to a subgroup of $PGL(2, \mathbb{K})$ which contains no normal p-subgroup. From Result 2.9, $\bar{G}$ is a prime to p subgroup which is either cyclic, or dihedral, or isomorphic to one of the groups Alt_4, Sym_4. In all cases, $\bar{G}$ has a cyclic subgroup U of index ≤ 6 and of order distinct from 3. We may dismiss all cases but the cyclic one up to replacing $\bar{G}$ with U, that is, up to assuming that $G = Q \rtimes U$ with $|G| \geq \frac{34}{6}(\mathfrak{g}(\mathscr{X})+1)^{3/2}$. Then $|G| > 12(\mathfrak{g}-1)$. Therefore, Lemma 2.12 applies to G. Thus, Q has exactly two (nontame) orbits, say Ω_1 and Ω_2, and they are also the only short orbits of G. More precisely,

$$\gamma - 1 = |Q| - (|\Omega_1| + |\Omega_2|). \tag{8}$$

We may also observe that G_P with $P \in \Omega_1$ contains a subgroup V isomorphic to U. In fact, $|Q||U| = |G| = |G_P||\Omega_1| = |Q_P \rtimes V||\Omega_1| = |V||Q_P||\Omega_1|$ with a prime to p subgroup V fixing P, whence $|U| = |V|$. Since V is cyclic the claim follows.

We proceed with the case where both Ω_1 and Ω_2 are nontrivial, that is, their lengths are at least 2.

Assume that Q is nonabelian, and look at the action of its center $Z(Q)$ on $\mathscr{X}$. Since $Z(Q)$ is a nontrivial normal subgroup of G, we can argue as before to show that quotient curve $\mathscr{X}/Z(Q)$ is rational, and hence that the Galois cover $\mathscr{X}|(\mathscr{X}/Z(Q))$ ramifies at some points. Indeed, observe that in the previous arguments normality of Q was only used to dismiss all cases but the rational one, and hence we may simply replace Q with $Z(Q)$. In other words, there is a point $P \in \Omega_1$ (or $R \in \Omega_2$) such that some nontrivial subgroup T of $Z(Q)$ fixes P (or R). Suppose that the former case occurs. Since Ω_1 is a Q-orbit, T fixes Ω_1 pointwise.

The group G has an index ≤ 2 subgroup H that induces a permutation group on Ω_1. Let M_1 be the kernel of this permutation representation. Obviously, T is a nontrivial p-subgroup of M_1. Therefore, M contains some but not all elements from Q. Since both M_1 and Q are normal subgroups of G, $N = M_1 \cap Q$ is a nontrivial normal p-subgroup of G. As we have proven before, the quotient curve $\tilde{\mathscr{X}} = \mathscr{X}/N$ is rational, and hence the factor group $\tilde{G} = G/N$ is isomorphic to a subgroup of $PGL(2, \mathbb{K})$. Since $1 \lneqq N \lneqq Q$, the order of $\tilde{G}$ is divisible by p. From Result 2.9, $\tilde{G} = \tilde{Q} \rtimes \tilde{U}$ where $\tilde{Q}$ is an elementary abelian p-group of order q and $\tilde{U} \cong UN/N \cong U$ with $|\tilde{U}| = |U|$ is a divisor of $q-1$.

This shows that Q acts on Ω_1 as an abelian transitive permutation group. Obviously this holds true when Q is abelian. Therefore, the action of Q on Ω_1 is sharply transitive. In terms of 1-point stabilizers of Q on Ω_1, we have $Q_P = Q_{P'}$ for any $P, P' \in \Omega_1$. Moreover, $Q_P = N$, and hence Q_P is a normal subgroup of G.

Furthermore, since $\mathscr{X}$ is an ordinary curve, Q_P is an elementary abelian group by Result 2.5(ii).

The quotient curve $\mathscr{X}/Q_P$ is rational, and its automorphism group contains the factor group Q/Q_P. Hence, exactly one of the Q_P-orbits is preserved by Q. Since Ω_1 is a Q-orbit consisting of fixed points of Q_P, Ω_2 must be a Q_P-orbit. Similarly, if $Z(Q) \neq Q_P$, the factor group $Z(Q)Q_P/Q_P$ is an automorphism group of $\mathscr{X}/Q_P$ and hence exactly one of the Q_P-orbits is preserved by $Z(Q)$. Either $Z(Q)$ fixes a point in Ω_1 but then $Z(Q) = Q_P$, or Ω_2 is a $Z(Q)$-orbit. This shows that either $Z(Q) = Q_P$, or $Z(G)$ acts transitively on Ω_2.

Two cases arise according as Q_P is sharply transitive and faithful on Ω_2 or some nontrivial element in Q_P fixes Ω_2 pointwise.

If some nontrivial element in Q_P fixes Ω_2 pointwise, then the kernel M_2 of the permutation representation of H on Ω_2 contains a nontrivial p-subgroup. Hence, the above results extend from Ω_1 to Ω_2, and Q_R is a normal subgroup of Q.

If Q_P is (sharply) transitive on Ω_2, then the abelian group $Z(Q)Q_P$ acts on Ω_2 as a sharply transitive permutation group, as well. Hence, either $Z(Q) = Q_P$, or as before M_2 contains a nontrivial p-subgroup, and Q_R is a normal subgroup of Q. In the former case, $Q = Q_P Q_R$ with $Q_R \cap Q_P = \{1\}$, and $Z(Q) = Q_P$ yields that

$$Q = Q_P \times Q_R. \tag{9}$$

This shows that Q is abelian, and hence $|Q| \leq 4\mathfrak{g}+4$ by Result 2.2(ii). Also, either $|Q_P|$ or $|Q_R|$ is at most $\sqrt{4\mathfrak{g}+4}$. From Result 2.5(i), $G_P^{(2)}$ at $P \in \Omega_1$ is trivial. Furthermore, for $G_P = Q_P \rtimes V$, Result 2.5(iv) gives $|U| = |V| \leq |Q_P| - 1$. Hence, $|U| < |Q_P| \leq \sqrt{|Q|} \leq \sqrt{4\mathfrak{g}+4}$ whence

$$|G| = |U||Q| \leq 8(\mathfrak{g}+1)^{3/2}. \tag{10}$$

If Q_R is a normal subgroup, take a point R from Ω_2, and look at the subgroup $Q_{P,R}$ of Q_P fixing R. Actually, we prove that either $Q_{P,R} = Q_P$ or $Q_{P,R}$ is trivial. Suppose that $Q_{P,R} \neq \{1\}$. Since $Q_{P,R} = Q_P \cap Q_R$ and both Q_P and Q_R are normal subgroups of G; the same holds for $Q_{P,R}$. By (ii), the quotient curve $\mathscr{X}/Q_{P,R}$ is rational and hence its automorphism group $Q/Q_{P,R}$ fixes exactly one point. Furthermore, each point in Ω_2 is totally ramified. Therefore, $Q_R = Q_{P,R}$; otherwise $Q_R/Q_{P,R}$ would fix any point lying under a point in Ω_1 in the cover $\mathscr{X}|(\mathscr{X}/Q_{P,R})$.

It turns out that either $Q_P = Q_R$ or $Q_P \cap Q_R = \{1\}$, whenever $P \in \Omega_1$ and $R \in \Omega_2$.

In the former case, from (5) applied to Q_P,

$$\gamma - 1 = -|Q_P| + |\Omega_1|(|Q_P| - 1) + |\Omega_2|(|Q_P| - 1) = -|Q_P| + |Q| - |\Omega_1| + |Q| - |\Omega_2|.$$

This together with (8) give $Q = Q_P$, a contradiction.

Therefore, the latter case must hold. Thus, $Q = Q_P \times Q_R$ and Q_P (and also Q_R) is an elementary abelian group since it is isomorphic to a p-subgroup of $PGL(2, \mathbb{K})$. Also, $|Q_P| = |Q_R| = \sqrt{|Q|}$. Since Q is abelian, this yields $|Q_P| \leq \sqrt{4\mathfrak{g}+4}$ by Result 2.2(ii). Now, the argument used after (9) can be employed to prove (10). This ends the proof in the case where both Ω_1 and Ω_2 are nontrivial.

Suppose next $\Omega_1 = \{P\}$ and $|\Omega_2| \geq 2$. Then G fixes P, and hence $G = Q \rtimes U$ with an elementary abelian p-group Q. Furthermore, G has a permutation representation on Ω_2 with kernel K. As Ω_2 is a short orbit of Q, the stabilizer Q_R of $R \in \Omega_2$ in Q is nontrivial. Since Q is abelian, this yields that K is nontrivial, and hence it is a nontrivial elementary abelian normal subgroup of G. In other words, Q is an r-dimensional vector space $V(r, p)$ over a finite field $\mathbb{F}_p$ with $|Q| = p^r$, the action of each nontrivial element of U by conjugacy is a nontrivial automorphism of $V(r, p)$, and K is a U-invariant subspace. By Result 2.11, K has a complementary U-invariant subspace. Therefore, Q has a subgroup M such that $Q = K \times M$, and M is a normal subgroup of G. Since $K \cap M = \{1\}$, and Ω_2 is an orbit of Q, this yields $|M| = |\Omega_2|$. The factor group G/M is an automorphism group of the quotient curve $\mathscr{X}/M$, and Q/M is a nontrivial p-subgroup of G/M whereas G/M fixes two points on $\mathscr{X}/M$. Therefore the quotient curve $\mathscr{X}/M$ is not rational since the 2-point stabilizer in the representation of $PGL(2, \mathbb{K})$ as an automorphism group of the rational function field is a prime to p (cyclic) group. We show that $\mathscr{X}/M$ is not elliptic either.

From (5), $\mathfrak{g}(\mathscr{X})-1=\gamma(\mathscr{X})-1=-|Q|+1+|\Omega_2|$, and so $\mathfrak{g}(\mathscr{X})$ is even. Since M is a normal subgroup of odd order, $\mathfrak{g}(\mathscr{X})\equiv 0 \pmod 2$ yields that $\mathfrak{g}(\mathscr{X}/M)\equiv 0 \pmod 2$. In particular, $\mathfrak{g}(\mathscr{X}/M)\neq 1$. Therefore, $\mathfrak{g}(\mathscr{X}/M)\geq 2$. At this point we may repeat our previous argument and prove $|G/M|>34(\mathfrak{g}(\mathscr{X}/M)+1)^{3/2}$. Again, we get a contradiction with our choice of $\mathscr{X}$ to be a minimal counterexample, which ends the proof in the case where just one of Ω_1 and Ω_2 is trivial.

We are left with the case where both short orbits of Q are trivial. Our goal is to prove a much stronger bound for this case, namely $|U|\leq 2$ whence

$$|G|\leq 2(\mathfrak{g}(\mathscr{X})+1). \tag{11}$$

We also show that if equality holds then $\mathscr{X}$ is a hyperelliptic curve with equation

$$f(U)=aT+b+cT^{-1}, \quad a,b,c\in\mathbb{K}^*, \tag{12}$$

where $f(U)\in\mathbb{K}[U]$ is an additive polynomial of degree $|Q|$.

Let $\Omega_1=\{P_1\}$ and $\Omega_2=\{P_2\}$. Then Q has two fixed points P_1 and P_2, but no nontrivial element in Q fixes a point of $\mathscr{X}$ other than P_1 and P_2. From (5),

$$\mathfrak{g}(\mathscr{X})+1=\gamma(\mathscr{X})+1=|Q|. \tag{13}$$

Therefore, $|U|\leq\mathfrak{g}(\mathscr{X})$. Actually, for our purpose, we need a stronger estimate, namely $|U|\leq 2$. To prove the latter bound, we use some ideas from Nakajima's paper [1987] regarding the Riemann–Roch spaces $\mathscr{L}(\boldsymbol{D})$ of certain divisors $\boldsymbol{D}$ of $\mathbb{K}(\mathscr{X})$. Our first step is to show

(i) $\dim_{\mathbb{K}}\mathscr{L}((|Q|-1)P_1)=1$ and

(ii) $\dim_{\mathbb{K}}\mathscr{L}((|Q|-1)P_1+P_2)\geq 2$.

Let $\ell\geq 1$ be the smallest integer such that $\dim_{\mathbb{K}}\mathscr{L}(\ell P_1)=2$, and take $x\in\mathscr{L}(\ell P_1)$ with $v_{P_1}(x)=-\ell$. As $Q=Q_{P_1}$, the Riemann–Roch space $\mathscr{L}(\ell P_1)$ contains all $c_\sigma=\sigma(x)-x$ with $\sigma\in Q$. This yields $c_\sigma\in\mathbb{K}$ by $v_{P_1}(c_\sigma)\geq -\ell+1$ and our choice of ℓ to be minimal. Also, $Q=Q_{P_2}$ together with $v_{P_2}(x)\geq 0$ show $v_{P_2}(c_\sigma)\geq 1$. Therefore, $c_\sigma=0$ for all $\sigma\in Q$, that is, x is fixed by Q. From $\ell=[\mathbb{K}(\mathscr{X}):\mathbb{K}(x)]=[\mathbb{K}:\mathbb{K}(\mathscr{X})^Q][\mathbb{K}(\mathscr{X})^Q:\mathbb{K}(x)]$ and $|Q|=[\mathbb{K}:\mathbb{K}(\mathscr{X})^Q]$, it turns out that ℓ is a multiple of $|Q|$. Thus $\ell>|Q|-1$ whence (i) follows. From the Riemann–Roch theorem, $\dim_{\mathbb{K}}\mathscr{L}((|Q|-1)P_1+P_2)\geq |Q|-g+1=2$, which proves (ii).

Let $d\geq 1$ be the smallest integer such that $\dim_{\mathbb{K}}\mathscr{L}(dP_1+P_2)=2$. From (ii)

$$d\leq |Q|-1. \tag{14}$$

Let α be a generator of the cyclic group U. Since α fixes both points P_1 and P_2, it acts on $\mathscr{L}(dP_1+P_2)$ as a $\mathbb{K}$-vector space automorphism $\bar{\alpha}$. If $\bar{\alpha}$ is trivial, then $\alpha(u)=u$ for all $u\in\mathscr{L}(dP_1+P_2)$. Suppose that $\bar{\alpha}$ is nontrivial. Since U is a prime to p cyclic group, $\bar{\alpha}$ has two distinct eigenspaces, so that $\mathscr{L}(dP_1+P_2)=\mathbb{K}\oplus\mathbb{K}u$ where $u\in\mathscr{L}(dP_1+P_2)$ is an eigenvector of $\bar{\alpha}$ with eigenvalue $\xi\in\mathbb{K}^*$ so that

$\bar{\alpha}(u) = \xi u$ with $\xi^{|U|} = 1$. Therefore, there is $u \in \mathscr{L}(dP_1 + P_2)$ with $u \neq 0$ such that $\alpha(u) = \xi u$ with $\xi^{|U|} = 1$. The pole divisor of u is

$$\mathrm{div}(u)_\infty = dP_1 + P_2. \tag{15}$$

Since $Q = Q_{P_1} = Q_{P_2}$, the Riemann–Roch space $\mathscr{L}(dP_1 + P_2)$ contains $\sigma(u)$ and hence contains all

$$\theta_\sigma = \sigma(u) - u, \quad \sigma \in Q.$$

By our choice of d to be minimal, this yields $\theta_\sigma \in \mathbb{K}$, and then defines the map θ from Q into $\mathbb{K}$ that takes σ to θ_σ. More precisely, θ is a homomorphism from Q into the additive group $(\mathbb{K}, +)$ of $\mathbb{K}$ as the following computation shows:

$$\theta_{\sigma_1 \circ \sigma_2} = (\sigma_1 \circ \sigma_2)(u) - u = \sigma_1(\sigma_2(u) - u + u) - u = \sigma_1(\theta_{\sigma_2}) + \sigma_1(u) - u = \theta_{\sigma_2} + \theta_{\sigma_1} = \theta_{\sigma_1} + \theta_{\sigma_2}.$$

Also, θ is injective. In fact, if $\theta_{\sigma_0} = 0$ for some $\sigma_0 \in Q \setminus \{1\}$, then u is in the fixed field of σ_0, which is impossible since $v_{P_2}(u) = -1$ whereas P_2 is totally ramified in the cover $\mathscr{X}|(\mathscr{X}/\langle\sigma_p\rangle)$. The image $\theta(Q)$ of θ is an additive subgroup of $\mathbb{K}$ of order $|Q|$. The smallest subfield of $\mathbb{K}$ containing $\theta(Q)$ is a finite field $\mathbb{F}_{p^m}$ and hence $\theta(Q)$ can be viewed as a linear subspace of $\mathbb{F}_{p^m}$ considered as a vector space over $\mathbb{F}_p$. Therefore, the polynomial

$$f(U) = \prod_{\sigma \in Q} (U - \theta_\sigma) \tag{16}$$

is a linearized polynomial over $\mathbb{F}_p$ [Lidl and Niederreiter 1983, §4, Theorem 3.52]. In particular, $f(U)$ is an additive polynomial of degree $|Q|$; see also [Serre 1962, Chapter V, §5]. Also, $f(U)$ is separable as θ is injective. From (16), the pole divisor of $f(u) \in \mathbb{K}(\mathscr{X})$ is

$$\mathrm{div}(f(u))_\infty = |Q|(dP_1 + P_2). \tag{17}$$

For every $\sigma_0 \in Q$,

$$\sigma_0(f(u)) = \prod_{\sigma \in Q} (\sigma_0(u) - \theta_\sigma) = \prod_{\sigma \in Q} (u + \theta_{\sigma_0} - \theta_\sigma) = \prod_{\sigma \in Q} (u - \theta_{\sigma\sigma_0^{-1}}) = \prod_{\sigma \in Q} (u - \theta_\sigma) = f(u).$$

Thus, $f(u) \in \mathbb{K}(\mathscr{X})^Q$. Furthermore, from $\alpha \in N_G(Q)$, for every $\sigma \in Q$ there is $\sigma' \in Q$ such that $\alpha\sigma = \sigma'\alpha$. Therefore,

$$\alpha(f(u)) = \prod_{\sigma \in Q} (\alpha(\sigma(u) - u)) = \prod_{\sigma \in Q} (\alpha(\sigma(u)) - \xi u) = \prod_{\sigma \in Q} (\sigma'(\alpha(u)) - \xi u) = \prod_{\sigma \in Q} (\sigma'(\xi u) - \xi u) = \xi f(u).$$

This shows that if $R \in \mathscr{X}$ is a zero of $f(u)$ then $\mathrm{Supp}(\mathrm{div}(f(u)_0))$ contains the U-orbit of R of length $|U|$. Actually, since $\sigma(f(u)) = f(u)$ for $\sigma \in Q$, $\mathrm{Supp}(\mathrm{div}(f(u)_0))$ contains the G-orbit of R of length $|G| = |Q||U|$. This together with (17) give

$$|U| \,|\, (d+1). \tag{18}$$

On the other hand, $\mathbb{K}(\mathscr{X})^Q$ is rational. Let $\bar{P}_1$ and $\bar{P}_2$ be the points lying under P_1 and P_2, respectively, and let $\bar{R}_1, \bar{R}_2, \ldots, \bar{R}_k$ with $k=(d+1)/|U|$ be the points lying under the zeros of $f(u)$ in the cover $\mathscr{X}|(\mathscr{X}/Q)$. We may represent $\mathbb{K}(\mathscr{X})^Q$ as the projective line $\mathbb{K}\cup\{\infty\}$ over $\mathbb{K}$ so that $\bar{P}_1=\infty$, $\bar{P}_1=0$, and $\bar{R}_i=t_i$ for $1\le i\le k$. Let $g(t)=t^d+t^{-1}+h(t)$ where $h(t)\in\mathbb{K}[t]$ is a polynomial of degree $k=(d+1)/|U|$ whose roots are $r_1,\ldots,r_k$. It turns out that $f(u), g(t)\in\mathbb{K}(\mathscr{X})$ have the same pole and zero divisors, and hence

$$cf(u)=t^d+t^{-1}+h(t), \quad c\in\mathbb{K}^*. \tag{19}$$

We prove that $\mathbb{K}(\mathscr{X})=\mathbb{K}(u,t)$. From [Sullivan 1975] (see also [Hirschfeld et al. 2008, Remark 12.12]), the polynomial $cTf(X)-T^{d+1}-1-h(T)T$ is irreducible, and the plane curve $\mathscr{C}$ has genus $\mathfrak{g}(\mathscr{C})=\frac{1}{2}(q-1)(d+1)$. Comparison with (13) shows $\mathbb{K}(\mathscr{X})=\mathscr{C}$ and $d=1$ whence $|U|\le 2$. If equality holds, then $\deg h(T)=1$ and $\mathscr{X}$ is a hyperelliptic curve with Equation (12). □

Case II. G contains no minimal normal p-subgroup.

Proposition 3.2. *Let $\mathscr{X}$ be an ordinary algebraic curve of genus $\mathfrak{g}$ defined over a field $\mathbb{K}$ of odd characteristic $p>0$. If G is a solvable subgroup of* $\mathrm{Aut}(\mathscr{X})$ *with a minimal normal subgroup N, then* $|G|\le 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$.

Proof. We begin with an outline of the proof.

Since $\mathscr{X}$ is chosen to be a (minimal) counterexample, Proposition 3.1 yields that G contains no nontrivial normal p-subgroup. The factor group $\bar{G}=G/N$ is a subgroup of $\mathrm{Aut}(\bar{\mathscr{X}})$ where $\bar{\mathscr{X}}=\mathscr{X}/N$. As in the proof of Proposition 3.1, we begin by showing that $\bar{\mathscr{X}}$ must be rational. This time Result 2.6(ii) does not apply and some more effort is needed to rule out the possibility of $\mathfrak{g}(\bar{\mathscr{X}})\ge 2$ while the elliptic case does not require a different approach. If $\bar{\mathscr{X}}$ is rational, the classification in Result 2.9 gives the possibility of the structure of $\bar{G}$ and its action on $\bar{\mathscr{X}}$. A careful analysis shows that $\bar{G}$ must be of type (vi) in Result 2.9. From this we obtain the possibilities for the action of G on $\mathscr{X}$. After that, (3) and (5) together with straightforward computation are sufficient to end the proof although the case where N is an elementary abelian 2-group requires some additional facts from group theory.

We prove that $\mathfrak{g}(\bar{\mathscr{X}})\ge 2$. By Result 2.2(ii), $|N|\le 4\mathfrak{g}(\mathscr{X})+4$ as N is abelian. If $\bar{\mathscr{X}}$ is also ordinary, then the choice of $\mathscr{X}$ to have minimal genus implies that $|\bar{G}|\le 34(\mathfrak{g}(\bar{\mathscr{X}})+1)^{3/2}$. Comparing this with Result 2.8 shows a contradiction. Therefore, the possibility for $\bar{\mathscr{X}}$ to be nonordinary is investigated.

From Result 2.5(i), any p-subgroup S of G has trivial second ramification group at any point $\mathscr{X}$. The latter property remains true when $\mathscr{X}$ and S are replaced by $\bar{\mathscr{X}}$ and the factor group $\bar{S}=SN/N$, respectively. To show this claim, take $\bar{P}\in\bar{\mathscr{X}}$ and let $\bar{S}_{\bar{P}}$ be the subgroup of $\bar{S}$ fixing $\bar{P}$. Since $p\nmid |N|$ there is a point $P\in\mathscr{X}$ lying over $\bar{P}$ which is fixed by S. Hence, the stabilizer S_P of P in S is a nontrivial normal subgroup of G_P. Since N is a normal subgroup in G, so is N_P in G_P. This yields that the product N_PS_P is actually a direct product. Therefore, N_P is trivial by Result 2.5(iii), that is, the cover $\mathscr{X}|\bar{\mathscr{X}}$ is unramified at $\bar{P}$. From this, the claim follows.

Actually, N may be taken to be the largest normal subgroup N_1 of G whose order is prime to p. Also, by our hypothesis, the quotient curve $\mathscr{X}_1=\mathscr{X}/N_1$ is neither rational, nor elliptic. From Result 2.8, its

$\mathbb{K}$-automorphism group $G_1 = G/N_1$ has order bigger than $34(\mathfrak{g}(\mathscr{X}_1)+1)^{3/2}$. Since G and hence G_1 are solvable, G_1 has a minimal normal d-subgroup where d must be equal to p by the choice of N_1 to be the largest normal, prime to p subgroup of G. Take the largest normal p-subgroup N_2 of G_1. Observe that $N_2 \neq G_1$. In fact, if $N_2 = G_1$, then G_1 is p-group of order bigger than $34(\mathfrak{g}(\mathscr{X}_1)+1)^{3/2} > p\mathfrak{g}(\mathscr{X}_1)/(p-2)$. From Result 2.1, $\mathscr{X}_1$ has zero p-rank, and hence G_1 fixes a point $P_1 \in \mathscr{X}_1$. On the other hand, since $G_1^{(2)}$ is trivial, Result 2.6(iii) shows $|G_1| \leq p\mathfrak{g}(\mathscr{X}_1)/(p-1)$, a contradiction. Now, define $\mathscr{X}_2$ to be the quotient curve $\mathscr{X}_1/N_2$. Since the second ramification group of N_1 at any point of $\mathscr{X}_1$ is trivial, Result 2.6(i) gives $\mathfrak{g}(\mathscr{X}_1) - \gamma(\mathscr{X}_1) = |N_2|(\mathfrak{g}(\mathscr{X}_2) - \gamma(\mathscr{X}_2))$. In particular, if $\mathscr{X}_2$ is ordinary or rational, then $\mathscr{X}_1$ is an ordinary curve. From the proof of Proposition 3.1, the case $\mathfrak{g}(\mathscr{X}_2) = 1$ cannot occur as $|G_1| > 34(\mathfrak{g}(\mathscr{X}_1)+1)^{3/2}$. Therefore, $\mathfrak{g}(\mathscr{X}_2) \geq 2$ with $\mathfrak{g}(\mathscr{X}_2) > \gamma(\mathscr{X}_2)$ may be assumed. The factor group $G_2 = G_1/N_2$ is a $\mathbb{K}$-automorphism group of the quotient curve $\mathscr{X}_2 = \mathscr{X}_1/N_2$, and it has a minimal normal d-subgroup with $d \neq p$, by the choice of N_2. Define N_3 to be the largest normal, prime to p subgroup of G_2. Observe that N_3 must be a proper subgroup of G_2; otherwise G_2 itself would be a prime to p subgroup of $\mathrm{Aut}(\mathscr{X}_2)$ of order bigger than $34(\mathfrak{g}(\mathscr{X}_2)+1)^{3/2}$, contradicting Result 2.2(i). Therefore, there exists a (maximal) nontrivial normal p-subgroup N_4 in the factor group $G_3 = G_2/N_3$. Now, the above argument remains valid whenever $G, N_1, G_1, N_2, \mathscr{X}_1, \mathscr{X}_2$ are replaced by $G_2, N_3, G_3, N_4, \mathscr{X}_3, \mathscr{X}_4$ where the quotient curves are $\mathscr{X}_3 = G_2/N_3$ and $\mathscr{X}_4 = G_3/N_4$. In particular, $\mathfrak{g}(\mathscr{X}_4) \neq 1$ and $\mathfrak{g}(\mathscr{X}_3) - \gamma(\mathscr{X}_3) = |N_4|(\mathfrak{g}(\mathscr{X}_4) - \gamma(\mathscr{X}_4))$. Repeating the above argument, a finite sharply decreasing sequence $\mathfrak{g}(\mathscr{X}_1) > \mathfrak{g}(\mathscr{X}_2) > \mathfrak{g}(\mathscr{X}_3) > \mathfrak{g}(\mathscr{X}_4) > \cdots$ arises. If this sequence has $n+1$ members, then $\mathfrak{g}(\mathscr{X}_n) - \gamma(\mathscr{X}_n) = |N_{n+1}|(\mathfrak{g}(\mathscr{X}_{n+1}) - \gamma(\mathscr{X}_{n+1}))$ with $\mathfrak{g}(\mathscr{X}_{n+1}) = \gamma(\mathscr{X}_{n+1}) = 0$. Therefore, for some (odd) index $m \leq n$, the curve $\mathscr{X}_m$ would not be ordinary, but the successive member $\mathscr{X}_{m+1}$ would be an ordinary curve. Since $\mathscr{X}_{m+1}$ is a quotient curve of $\mathscr{X}_m$ with respect to a p-subgroup, this is impossible by Result 2.6(ii).

We continue with the elliptic case. Since $\mathfrak{g}(\mathscr{X}) \geq 2$, (3) applied to $\bar{X}$ ensures that N has a short orbit. Let Γ be a short orbit of G containing a short orbit of N. Since N is a normal subgroup of G, Γ is partitioned into short orbits $\Sigma_1, \ldots, \Sigma_k$ of N each of length $|\Sigma_1|$. Take a point R_i from Σ_i for $i = 1, 2, \ldots, k$, and set $\Sigma = \Sigma_1$ and $S = S_1$. With this notation, $|G| = |G_S||\Gamma| = |G_S|k|\Sigma|$, and (3) gives

$$2\mathfrak{g}(\mathscr{X}) - 2 \geq \sum_{i=1}^{k} |\Sigma_i|(|N_{S_i}|-1) = k|\Sigma|(|N_S|-1) \geq +\tfrac{1}{2}k|\Sigma||N_S| = \tfrac{1}{2}|G|\frac{|N_S|}{|G_S|}. \tag{20}$$

Also, the factor group $G_S N/N$ is a subgroup of $\mathrm{Aut}(\bar{\mathscr{X}})$ fixing the point of $\bar{\mathscr{X}}$ lying under S in the cover $\mathscr{X}|\bar{\mathscr{X}}$. From Result 2.7,

$$\frac{|G_S N|}{|N|} = \frac{|G_S|}{|G_S \cap N|} = \frac{|G_S|}{|N_S|} \leq 12.$$

This and (20) yield $|G| \leq 48(\mathfrak{g}(\mathscr{X})-1)$, a contradiction with our hypothesis $34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$.

Therefore, $\bar{\mathscr{X}}$ is rational. Thus, $\bar{G}$ is isomorphic to a subgroup of $PGL(2,\mathbb{K})$. Since p divides $|G|$ but not $|N|$, $\bar{G}$ contains a nontrivial p-subgroup. From Result 2.9, either $p = 3$ and $\bar{G} \cong \mathrm{Alt}_4, \mathrm{Sym}_4$, or $\bar{G} = \bar{Q} \rtimes \bar{C}$ where $\bar{Q}$ is a normal p-subgroup and its complement $\bar{C}$ is a cyclic prime to p subgroup and $|\bar{C}|$ divides $|\bar{Q}|-1$.

If $\bar{G} \cong \mathrm{Alt}_4, \mathrm{Sym}_4$, then $|\bar{G}| \le 24$ whence $|G| \le 24|N| \le 96(\mathfrak{g}(\mathscr{X})+1)$ as N is abelian. Comparison with our hypothesis $|G| \ge 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$ shows that $\mathfrak{g}(\mathscr{X}) \le 6$. For small genera we need a little more. If $|N|$ is prime, then $|N| \le 2\mathfrak{g}(\mathscr{X})+1$ by Result 2.2(iii), and hence $|G| \le 48(\mathfrak{g}(\mathscr{X})+1)$, which is inconsistent with $|G| \ge 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$. Otherwise, since $p = 3$ and $|N|$ has order a power of prime distinct from p, the bound $|N| \le 4(\mathfrak{g}(\mathscr{X})+1)$ with $\mathfrak{g}(\mathscr{X}) \le 6$ is only possible for $(\mathfrak{g}(\mathscr{X}), |N|) \in \{(3,16), (4,16), (5,16), (6,16), (6,25)\}$. Comparison of $|G| \le 24|N|$ with $|G| \ge 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$ rule out the latter three cases. Furthermore, since N is an elementary abelian group of order 16, $\mathfrak{g}(\mathscr{X})$ must be odd by Lemma 2.13. Finally, $\mathfrak{g}(\mathscr{X}) = 3$, $|N| = 16$, and $G/N \cong \mathrm{Sym}_4$ is impossible as Result 2.3 would imply that $\mathscr{X}$ has zero p-rank.

Therefore, the case $\bar{G} = \bar{Q} \rtimes \bar{C}$ occurs. Also, $\bar{G}$ fixes a unique place $\bar{P} \in \bar{\mathscr{X}}$. Let Δ be the N-orbits in $\mathscr{X}$ that lie over $\bar{P}$ in the cover $\mathscr{X}|\bar{\mathscr{X}}$. We prove that Δ is a long orbit of N. By absurd, the permutation representation of G on Δ has a nontrivial 1-point stabilizer containing a nontrivial subgroup M of N. Since N is abelian, M is in the kernel. In particular, M is a normal subgroup of G contradicting our choice of N to be minimal.

Take a Sylow p-subgroup Q of G of order $|Q| = p^h$ with $h \ge 1$, and look at the action of Q on Δ. Since $|\Delta| = |N|$ is prime to p, Q fixes a point $P \in \Delta$, that is, $Q = Q_P$. Since $\mathscr{X}$ is an ordinary curve, Result 2.5(ii) shows that Q_P and hence Q are elementary abelian. Therefore, $G_P = Q \rtimes U$ where U is a prime to p cyclic group. Thus,

$$|\bar{Q}||\bar{C}||N| = |\bar{G}||N| = |G| = |G_P||\Delta| = |Q||U||\Delta| = |Q||U||N|, \tag{21}$$

whence $|Q| = |\bar{Q}|$ and $|U| = |\bar{C}|$. Consider the subgroup H of G generated by G_P and N. Since Δ is a long N-orbit, $G_P \cap N = \{1\}$. As N is normal in H this implies that $H = N \rtimes G_P = N \rtimes (Q \rtimes U)$ and hence $|H| = |N||Q||U|$, which proves $G = H = N \rtimes (Q \rtimes U)$.

Since $\bar{\mathscr{X}}$ is rational and $\bar{P}$ is the unique fixed point of nontrivial elements of $\bar{Q}$, each $\bar{Q}$-orbit other than $\{\bar{P}\}$ is long. Furthermore, $\bar{C}$ fixes a point $\bar{R}$ other than $\bar{P}$ and no nontrivial element of $\bar{C}$ fixes a point distinct from $\bar{P}$ and $\bar{R}$. This shows that the $\bar{G}$-orbit $\bar{\Omega}_1$ of $\bar{R}$ has length $|Q|$. In terms of the action of G on $\mathscr{X}$, there exist as many as $|Q|$ orbits of N, say $\Delta_1, \ldots, \Delta_{|Q|}$, whose union Λ is a short G-orbit lying over $\bar{\Omega}_1$ in the cover $\mathscr{X}|\bar{\mathscr{X}}$. Obviously, if at least one of Δ_i is a short N-orbit, then so are all.

We show that this actually occurs. Since the cover $\mathscr{X}|\bar{\mathscr{X}}$ ramifies, N has some short orbits, and by absurd there exists a short N-orbit Σ not contained in Λ. Then Σ and Λ are disjoint. Let Γ denote the (short) G-orbit containing Σ. Since N is a normal subgroup of G, Γ is partitioned into N-orbits, say $\Sigma = \Sigma_1, \ldots, \Sigma_k$, each of them of the same length $|\Sigma|$. Here $k = |Q||U|$ since the set of points of $\bar{\mathscr{X}}$ lying under these k short N-orbits is a long $\bar{G}$-orbit. Also, $|N| = |\Sigma_i||N_{R_i}|$ for $\le i \le k$ and $R_i \in \Sigma_i$. In particular, $|\Sigma_1| = |\Sigma_i|$ and $|N_{R_1}| = |B_{R_i}|$. From (3),

$$2\mathfrak{g}(\mathscr{X}) - 2 \ge -2|N| + \sum_{i=1}^{k} |\Sigma_i|(|N_{R_i}| - 1) = -2|N| + |Q||U||\Sigma_1|(|N_{R_1}| - 1).$$

Since N_{R_1} is nontrivial, $|N_{R_1}|-1 \geq \frac{1}{2}|N_{R_1}|$. Therefore,

$2\mathfrak{g}(\mathscr{X})-2 \geq -2|N|+\frac{1}{2}|Q||U||\Sigma_1||N_{R_1}| = -2|N|+\frac{1}{2}|Q||U||N| = |N|\big(\frac{1}{2}(|Q||U|-2)\big) = \frac{1}{2}|N|(|Q||U|-4)$.

As $|Q||U|-4 \geq \frac{1}{2}|Q||U|$ by $|Q||U| \geq 4$, this gives

$$2\mathfrak{g}(\mathscr{X})-2 \geq \frac{1}{4}|N||U||Q| = \frac{1}{4}|G|.$$

But this contradicts our hypothesis $|G| > 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$.

Therefore, the short orbits of N are exactly $\Delta_1, \ldots, \Delta_{|Q|}$. Take a point S_i from Δ_i for $i = 1, \ldots, |Q|$. Then N_{S_1} and N_{S_i} are conjugate in G, and hence $|N_{S_1}| = |N_{S_i}|$. From (3) applied to N,

$$2\mathfrak{g}(\mathscr{X})-2 = -2|N| + \sum_{i=1}^{|Q|}|\Delta_i|(|N_{S_i}|-1) = -2|N| + |Q||\Delta_1|(|N_{S_1}|-1) \geq -2|N| + \tfrac{1}{2}|Q||\Delta_1||N_{S_1}|.$$

Since $|N| = |\Delta_1||N_{S_1}|$, this gives $2\mathfrak{g}(\mathscr{X})-2 \geq \frac{1}{2}|N|(|Q|-4)$ whence $2\mathfrak{g}(\mathscr{X})-2 \geq \frac{1}{4}|N||Q|$ provided that $|Q| \geq 5$. The missing case, $|Q| = 3$, cannot actually occur since in this case $|\bar{C}| = |U| \leq |Q|-1 = 2$, whence $|G| = |Q||U||N| \leq 6|N| \leq 24(\mathfrak{g}(\mathscr{X})+1)$, a contradiction with $|G| > 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$. Thus,

$$|N||Q| \leq 8(\mathfrak{g}(\mathscr{X})-1). \tag{22}$$

Since $|N||U| < |N||Q|$, this also shows

$$|N||U| < 8(\mathfrak{g}(\mathscr{X})-1). \tag{23}$$

Therefore,

$$|G||N| = |N|^2|U||Q| < 64(\mathfrak{g}(\mathscr{X})-1)^2.$$

Equations (22) and (23) together with our hypothesis $|G| \geq 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$ yield

$$|N| < \tfrac{64}{34}\sqrt{\mathfrak{g}(\mathscr{X})-1}. \tag{24}$$

From (24) and $|G| = |N||Q||U| \geq 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$ we obtain

$$|Q||U| > \frac{34^2}{64}(\mathfrak{g}(\mathscr{X})-1) > 18(\mathfrak{g}(\mathscr{X})-1),$$

which shows that Lemma 2.12 applies to the subgroup $Q \rtimes U$ of $\mathrm{Aut}(\mathscr{X})$. With the notation in Lemma 2.12, this gives that $Q \rtimes U$ and Q have the same two short orbits, $\Omega_1 = \{P\}$ and Ω_2. In the cover $\mathscr{X}|\bar{\mathscr{X}}$, the point $\bar{P} \in \bar{\mathscr{X}}$ lying under P is fixed by Q. We prove that Ω_2 is a subset of the N-orbit Δ containing P. For this purpose, it suffices to show that for any point $R \in \Omega_2$, the point $\bar{R} \in \bar{\mathscr{X}}$ lying under R in the cover $\mathscr{X}|\bar{\mathscr{X}}$ coincides with $\bar{P}$. Since Ω_2 is a Q-short orbit, the stabilizer Q_R is nontrivial, and hence $\bar{Q}$ fixes $\bar{R}$. Since $\bar{\mathscr{X}}$ is rational, this yields $\bar{P} = \bar{R}$. Therefore, $\Omega_2 \cup \{P\}$ is contained in Δ, and either $\Delta = \Omega_2 \cup \{P\}$ or Δ contains a long Q-orbit. In the latter case, $|U| < |Q| < |N|$, and hence

$$|G|^2 = |N||Q||N||U||Q||U| < |N||Q||N||U||N|^2 \leq \frac{64^2}{34}(\mathfrak{g}(\mathscr{X})-1)^3$$

whence $|G| < 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$, a contradiction with our hypothesis. Otherwise $|N| = |\Delta| = 1+|\Omega_2|$. In particular, $|N|$ is even, and hence it is a power of 2. Also, by (5), $\mathfrak{g}(\mathscr{X})-1 = \gamma(\mathscr{X})-1 = -|Q|+1+|\Omega_2|$ where $|\Omega_2| \geq 1$ is a power of p. This implies that $\mathfrak{g}(\mathscr{X})$ is also even. Since N is an elementary abelian 2-group, Lemma 2.13 yields that either $|N| = 2$ or $|N| = 4$.

If $|N| = 2$, then Ω_2 consists of a unique point R and $Q \rtimes U$ fixes both points P and R. Since $\Delta = \{P, R\}$, and Δ is a G-orbit, the stabilizer $G_{P,R}$ is an index-2 (normal) subgroup of G. On the other hand, $G_{P,R} = Q \rtimes U$ and hence Q is the unique Sylow p-subgroup of $Q \rtimes U$. Thus, Q is a characteristic subgroup of the normal subgroup $G_{P,R}$ of G. But then Q is a normal subgroup of G, a contradiction with our hypothesis.

If $|N| = 4$, then $|\Delta| = 4$ and $p = 3$. The permutation representation of G of degree 4 on Δ contains a 4-cycle induced by N but also a 3-cycle induced by Q. Hence, if $K = \ker$, then $G/K \cong \mathrm{Sym}_4$. On the other hand, since both N and Ker are normal subgroups of G, their product NK is normal, as well. Hence, NK/K is a normal subgroup of G/K, but this contradicts $G/K \cong \mathrm{Sym}_4$. □

References

[Giulietti and Korchmáros 2014] M. Giulietti and G. Korchmáros, "Garden of curves with many automorphisms", pp. 93–120 in *Algebraic curves and finite fields*, edited by H. Niederreiter et al., Radon Ser. Comput. Appl. Math. **16**, de Gruyter, Berlin, 2014. MR Zbl

[Gunby et al. 2015] B. Gunby, A. Smith, and A. Yuan, "Irreducible canonical representations in positive characteristic", *Res. Number Theory* **1** (2015), art. id. 3. MR Zbl

[Henn 1978] H.-W. Henn, "Funktionenkörper mit großer Automorphismengruppe", *J. Reine Angew. Math.* **302** (1978), 96–115. MR Zbl

[Hirschfeld et al. 2008] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Univ., 2008. MR Zbl

[Homma 1980] M. Homma, "Automorphisms of prime order of curves", *Manuscripta Math.* **33**:1 (1980), 99–109. MR Zbl

[Kontogeorgis and Rotger 2008] A. Kontogeorgis and V. Rotger, "On abelian automorphism groups of Mumford curves", *Bull. Lond. Math. Soc.* **40**:3 (2008), 353–362. MR Zbl

[Korchmáros et al. 2018] G. Korchmáros, M. Montanucci, and P. Speziali, "Transcendence degree one function fields over a finite field with many automorphisms", *J. Pure Appl. Algebra* **222**:7 (2018), 1810–1826. MR Zbl

[Lidl and Niederreiter 1983] R. Lidl and H. Niederreiter, *Finite fields*, Encycl. Math. Appl. **20**, Addison-Wesley, Reading, MA, 1983. MR Zbl

[Machì 2012] A. Machì, *Groups: an introduction to ideas and methods of the theory of groups*, Unitext **58**, Springer, 2012. MR Zbl

[Nakajima 1987] S. Nakajima, "p-ranks and automorphism groups of algebraic curves", *Trans. Amer. Math. Soc.* **303**:2 (1987), 595–607. MR Zbl

[Neftin and Zieve 2015] D. Neftin and M. E. Zieve, "Solvable covers with many rational points", preprint, 2015, Available at https://neftin.net.technion.ac.il/files/2015/10/many-12-9-13.pdf.

[Serre 1962] J.-P. Serre, *Corps locaux*, Publ. Inst. Math. Univ. Nancago **8**, Hermann, Paris, 1962. MR Zbl

[Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Math. **67**, Springer, 1979. MR Zbl

[Stichtenoth 1973] H. Stichtenoth, "Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, II: Ein spezieller Typ von Funktionenkörpern", *Arch. Math.* (*Basel*) **24** (1973), 615–631. MR Zbl

[Sullivan 1975] F. J. Sullivan, "p-torsion in the class group of curves with too many automorphisms", *Arch. Math.* (*Basel*) **26** (1975), 253–261. MR Zbl

[Valentini and Madan 1980] R. C. Valentini and M. L. Madan, "A Hauptsatz of L. E. Dickson and Artin–Schreier extensions", *J. Reine Angew. Math.* **318** (1980), 156–177. MR Zbl

Communicated by Gavril Farkas
Received 2016-10-25 Revised 2018-10-18 Accepted 2018-11-20

gabor.korchmaros@unibas.it *Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, Potenza, Italy*

mariamontanucci@gmail.com *Dipartimento di Tecnica e Gestione dei Sistemi Industriali, Università degli Studi di Padova, Vicenza, Italy*

ALGEBRA AND NUMBER THEORY 13:1 (2019)
dx.doi.org/10.2140/ant.2019.13.19

Variance of arithmetic sums and L-functions in $\mathbb{F}_q[t]$

Chris Hall, Jonathan P. Keating and Edva Roditty-Gershon

We compute the variances of sums in arithmetic progressions of arithmetic functions associated with certain L-functions of degree 2 and higher in $\mathbb{F}_q[t]$, in the limit as $q \to \infty$. This is achieved by establishing appropriate equidistribution results for the associated Frobenius conjugacy classes. The variances are thus related to matrix integrals, which may be evaluated. Our results differ significantly from those that hold in the case of degree-1 L-functions (i.e., situations considered previously using this approach). They correspond to expressions found recently in the number field setting assuming a generalization of the pair correlation conjecture. Our calculations apply, for example, to elliptic curves defined over $\mathbb{F}_q[t]$.

1. Introduction

1.1. ***Analytic motivation.*** Let $\Lambda(n)$ denote the von Mangoldt function, defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

MSC2010: primary 11T55; secondary 11M38, 11M50.
Keywords: L-functions, Mellin transform.

The prime number theorem implies

$$\sum_{n \le x} \Lambda(n) = x + o(x)$$

as $x \to \infty$, determining the average of $\Lambda(n)$ over long intervals. In many problems one needs to understand sums over shorter intervals and in arithmetic progressions. This is significantly more difficult, because the fluctuations between different short intervals/arithmetic progressions can be large, and in many important cases we do not have rigorous results.

One may seek to characterize the fluctuations in these sums via their variances. These variances are the subject of several long-standing conjectures. For example, in the case of short intervals Goldston and Montgomery [1987] made the following conjecture:

Conjecture 1.1.1 (variance of primes in short intervals). *For any fixed* $\varepsilon > 0$,

$$\int_1^X \Big(\sum_{X \le n \le x+h} \Lambda(n) - h \Big)^2 dx \sim hX(\log X - \log h)$$

uniformly for $1 \le h \le X^{1-\varepsilon}$.

It is natural to try to compute the variance in Conjecture 1.1.1 using the Hardy–Littlewood conjecture

$$\sum_{n \le X} \Lambda(n)\Lambda(n+k) \sim \mathfrak{S}(k)X \tag{1.1.2}$$

as $X \to \infty$, where $\mathfrak{S}(k)$ is the singular series, defined in terms of products over primes p and q,

$$\mathfrak{S}(k) = \begin{cases} 2\prod_{p>2}\Big(1 - \frac{1}{(p-1)^2}\Big) \prod_{\substack{q>2 \\ q \mid k}} \frac{q-1}{q-2} & \text{if } k \text{ is even,} \\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

Montgomery and Soundararajan [2004] proved that (1.1.2), together with an assumption concerning the implicit error term, implies a more precise asymptotic for the variance in Conjecture 1.1.1 when $\log X \le h \le X^{1/2}$, namely that it is equal to

$$hX(\log X - \log h - \gamma_0 - \log 2\pi) + O_\varepsilon(h^{15/16}X(\log X)^{17/16} + h^2X^{1/2+\varepsilon}), \tag{1.1.3}$$

where γ_0 is the Euler–Mascheroni constant.

An alternative approach to computing this variance follows from

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

which links statistical properties of $\Lambda(n)$ to those of the zeros of the Riemann zeta-function $\zeta(s)$. Taking this line, Goldston and Montgomery [1987] proved that Conjecture 1.1.1 is equivalent to the following conjecture, due to Montgomery [1973], concerning the pair correlation of the nontrivial zeros of the zeta-function. Denoting the nontrivial zeros by $\frac{1}{2}+i\gamma$ and assuming the Riemann hypothesis (so $\gamma \in \mathbb{R}$), let

$$\mathcal{F}(X, T) = \sum_{0<\gamma,\gamma'\leq T} X^{i(\gamma-\gamma')} w(\gamma-\gamma'),$$

where $w(u) = 4/(4+u^2)$.

Conjecture 1.1.4 (Montgomery's pair correlation conjecture). *For any fixed* $A \geq 1$

$$\mathcal{F}(X, T) \sim \frac{T \log T}{2\pi}$$

uniformly for $T \leq X \leq T^A$.

See also [Chan 2003; Languasco et al. 2012], where lower-order terms are considered in the equivalence.

There is a similar theory in the case of sums in arithmetic progressions. The prime number theorem for arithmetic progression states that for a fixed modulus c, when A is coprime to c

$$\sum_{\substack{n\leq X\\ n=A \bmod c}} \Lambda(n) \sim \frac{X}{\phi(c)} \quad \text{as } X \to \infty, \tag{1.1.5}$$

where $\phi(c)$ is the Euler totient function, giving the number of reduced residues modulo c. The variance of sums over different arithmetic progressions is then defined by

$$G(X, c) = \sum_{\substack{A \bmod c\\ \gcd(A,c)=1}} \left| \sum_{\substack{n\leq X\\ n\equiv A \bmod c}} \Lambda(n) - \frac{X}{\phi(c)} \right|^2. \tag{1.1.6}$$

Asymptotic formulae are known when $G(X, c)$ is summed over a long range of values of c (see, e.g., [Montgomery 1970; Hooley 1975b; 1975c]), but much less is known concerning $G(X, c)$ itself. In the latter case, Hooley [1975a] made the following conjecture.

Conjecture 1.1.7 (variance of primes in arithmetic progressions).

$$G(X, c) \sim X \log c.$$

Hooley was not specific about the size of c relative to X for which this asymptotic should hold. Friedlander and Goldston [1996] showed that in the range $c > X^{1+o(1)}$,

$$G(X, c) \sim X \log X - X - \frac{X^2}{\phi(c)} + O\left(\frac{X}{(\log X)^A}\right) + O((\log c)^3). \tag{1.1.8}$$

This is a relatively straightforward range because it contains at most one prime. They conjectured that Hooley's asymptotic holds if $X^{1/2+\varepsilon} < c < X$ and further conjectured that if $X^{1/2+\varepsilon} < c < X^{1-\varepsilon}$ then

$$G(X, c) \sim X \log c - X \cdot \left(\gamma_0 + \log 2\pi + \sum_{p\,|\,c} \frac{\log p}{p-1}\right). \tag{1.1.9}$$

They showed that both Conjecture 1.1.7 and (1.1.9) hold assuming the Hardy–Littlewood conjecture with small remainders. For $c < X^{1/2}$ relatively little seems to be known.

Conjectures 1.1.1 and 1.1.7 remain open, but their analogues in the function-field setting have been proved in the limit of large field size [Keating and Rudnick 2014]. Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q[t]$ the ring of polynomials with coefficients in $\mathbb{F}_q$. Let $\mathcal{M} \subset \mathbb{F}_q[t]$ be the subset of monic polynomials and $\mathcal{M}_n \subset \mathcal{M}$ be the subset of polynomials of degree n. Let $\mathcal{I} \subset \mathcal{M}$ be the subset of irreducible polynomials and $\mathcal{I}_n = \mathcal{I} \cap \mathcal{M}_n$. The norm of a nonzero polynomial $f \in \mathbb{F}_q[t]$ is defined to be $|f| = q^{\deg f}$.

The von Mangoldt function is the function on $\mathcal{M}$ defined for $m \geq 1$ by

$$\Lambda(f) = \begin{cases} d & \text{if } f = \pi^m \text{ with } \pi \in \mathcal{I}_d, \\ 0 & \text{otherwise.} \end{cases}$$

The prime polynomial theorem in this context is the identity

$$\sum_{f \in \mathcal{M}_n} \Lambda(f) = q^n. \tag{1.1.10}$$

The analogue of Conjecture 1.1.1 is the following result, proved in [Keating and Rudnick 2014]: for $h \leq n-5$,

$$\frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \left| \sum_{|f-A| \leq q^h} \Lambda(f) - q^{h+1} \right|^2 \sim q^{h+1}(n-h-2) \tag{1.1.11}$$

as $q \to \infty$; note that $|\{f : |f-A| \leq q^h\}| = q^{h+1}$.

In the same vein, there is a function-field result, also established in [Keating and Rudnick 2014], that is similar to Conjecture 1.1.7: fix $n \geq 2$; then, given a sequence of finite fields $\mathbb{F}_q$ and square-free polynomials $c \in \mathbb{F}_q[t]$ with $2 \leq \deg(c) \leq n+1$, one has

$$\sum_{\substack{A \bmod c \\ \gcd(A,c)=1}} \left| \sum_{\substack{f \in \mathcal{M}_n \\ f \equiv A \bmod c}} \Lambda(f) - \frac{q^n}{\Phi(c)} \right|^2 \sim q^n(\deg(c) - 1) \tag{1.1.12}$$

as $q \to \infty$.

The asymptotic formulae (1.1.11) and (1.1.12) were established in [Keating and Rudnick 2014] by expressing the variances as sums over families of L-functions. These L-functions can be expressed as the characteristic polynomials of matrices representing Frobenius conjugacy classes. In the limit as $q \to \infty$, these matrices become equidistributed in one of the classical compact groups and the sums become matrix integrals of a kind familiar in random matrix theory. Evaluating these integrals leads to the expressions above.

This approach to computing variances has subsequently been applied to other arithmetic functions defined over function fields, including the Möbius function [Keating and Rudnick 2016], the square of the Möbius function (i.e., the characteristic function of square-free polynomials) [loc. cit.], square-full polynomials [Roditty-Gershon 2017], and the generalized divisor functions [Keating et al. 2018]. For overviews see [Rudnick 2014; Keating and Roditty-Gershon 2016; Rodgers 2018]. The arithmetic functions considered so far have all been associated with degree-1 L-functions (or simple functions of these). Our main aim in this paper is to extend the theory to arithmetic functions associated with

L-functions of degree 2 and higher. For example, our results apply to L-functions associated with elliptic curves defined over $\mathbb{F}_q[t]$, and one expects them to apply to all standard automorphic L-functions. This will require us to establish the appropriate equidistribution results for such L-functions. We achieve this using the machinery developed by Katz [2012].

The main reason for moving to higher-degree L-functions is the recent discovery in the number-field setting that one gets qualitatively new behavior when the degree exceeds 1 [Bui et al. 2016].

We summarize briefly now the results in [loc. cit.]. Let $\mathcal{S}$ denote the Selberg class L-functions. For $F \in \mathcal{S}$ primitive, write

$$F(s) = \sum_{n=1}^{\infty} \frac{a_F(n)}{n^s}.$$

Then $F(s)$ has an Euler product

$$F(s) = \prod_p \exp\biggl(\sum_{l=1}^{\infty} \frac{b_F(p^l)}{p^{ls}}\biggr) \tag{1.1.13}$$

and satisfies the functional equation

$$\Phi(s) = \varepsilon_F \overline{\Phi}(1-s),$$

where $\overline{\Phi}(s) = \overline{\Phi(\overline{s})}$ and

$$\Phi(s) = c^s \biggl(\prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j)\biggr) F(s)$$

for some $c > 0,\ \lambda_j > 0,\ \mathrm{Re}(\mu_j) \geq 0$ and $|\varepsilon_F| = 1$.

There are two important invariants of $F(s)$: the degree d_F and the conductor $\mathfrak{q}_F$, given by

$$d_F = 2\sum_{j=1}^{r} \lambda_j, \qquad \mathfrak{q}_F = (2\pi)^{d_F} c^2 \prod_{j=1}^{r} \lambda_j^{2\lambda_j},$$

respectively. Another is m_F, the order of the pole at $s = 1$, which equals 1 for the Riemann zeta function and is expected to be 0 otherwise.

Let Λ_F be the arithmetic function defined by

$$\frac{F'(s)}{F(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda_F(n)}{n^s},$$

and let ψ_F be the function defined by

$$\psi_F(x) := \sum_{n \leq x} \Lambda_F(n).$$

The former will be the main focus of our attention.

A generalized prime number theorem of the form

$$\sum_{n \leq x} \Lambda_F(n) = m_F x + o(x)$$

is expected to hold. In analogy with the case of the Riemann zeta function, it is natural to consider the variance

$$\widetilde{V}_F(X,h) := \int_1^X \left|\psi_F(x+h) - \psi_F(x) - m_F h\right|^2 dx,$$

where $h \neq 0$. For example, when F represents an L-function associated with an elliptic curve, $\widetilde{V}_F(X,h)$ is the variance of sums over short intervals involving the Fourier coefficients of the associated modular form evaluated at primes and prime powers; and in the case of Ramanujan's L-function, it represents the corresponding variance for sums involving the Ramanujan τ-function.

For most $F \in \mathcal{S}$ it is expected that

$$\sum_{n \le X} \Lambda_F(n)\Lambda_F(n+h) = o(X) \quad \text{when } h \neq 0.$$

This might lead one to expect that $\widetilde{V}_F(X,h)$ typically exhibits significantly different asymptotic behavior than in the case when F is the Riemann zeta-function because in that case (1.1.2) plays a central role in our understanding of the variance. However, all principal L-functions are believed to look essentially the same from the perspective of the statistical distribution of their zeros; that is, it is conjectured that the zeros of all primitive L-functions have a limiting distribution which coincides with that of random unitary matrices, as in Montgomery's conjecture (Conjecture 1.1.4). It was proved in [Bui et al. 2016], assuming the generalized Riemann hypothesis (GRH), that an extension of the pair correlation conjecture for the zeros that includes lower-order terms (and which itself follows from the ratio conjecture of [Conrey et al. 2008], along the lines of [Conrey and Snaith 2007]) is equivalent to the formulae (1.1.14) and (1.1.15) below for $\widetilde{V}_F(X,h)$, which generalize the Montgomery–Soundararajan formula (1.1.3).

If $0 < B_1 < B_2 \le B_3 < 1/d_F$, then

$$\widetilde{V}_F(X,h) = hX\Big(d_F \log\frac{X}{h} + \log \mathfrak{q}_F - (\gamma_0 + \log 2\pi)d_F\Big) + O_\varepsilon(hX^{1+\varepsilon}(h/X)^{c/3}) + O_\varepsilon(hX^{1+\varepsilon}(hX^{-(1-B_1)})^{1/3(1-B_1)}) \quad (1.1.14)$$

uniformly for $X^{1-B_3} \ll h \ll X^{1-B_2}$, for some $c > 0$.

Otherwise, if $1/d_F < B_1 < B_2 \le B_3 < 1$,

$$\widetilde{V}_F(X,h) = \tfrac{1}{6}hX(6\log X - (3 + 8\log 2)) + O_\varepsilon(hX^{1+\varepsilon}(h/X)^{c/3}) + O_\varepsilon(hX^{1+\varepsilon}(hX^{-(1-B_1)})^{1/3(1-B_1)}) \quad (1.1.15)$$

uniformly for $X^{1-B_3} \ll h \ll X^{1-B_2}$, for some $c > 0$.

If $d_F = 1$ there is only one regime of behavior, governed by (1.1.14). When $\mathfrak{q}_F = 1$, this coincides exactly with (1.1.3); and when $\mathfrak{q}_F \neq 1$, it generalizes (1.1.3) in a straightforward way.

If $d_F > 1$ there are two ranges depending on the size of h. In the first range, $\widetilde{V}_F(X,h)/h$ is proportional to $\log h$; in the second regime it is independent of h at leading order.

It is this kind of behavior that we seek to understand better in the context of function fields. We shall focus on variances defined over arithmetic progressions rather than short intervals. In that case we are able to establish unconditional theorems, Theorems 1.2.3 and 9.0.1 below, which again exhibit the qualitatively new form of the variance when the degree is 2 or higher.

Our function field results can be used to motivate predictions for the variance of sums over arithmetic progressions of Λ_F in the number-field context reviewed above. In order to illustrate these predictions, we focus now on two representative examples: elliptic curve L-functions and the Ramanujan L-function.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N defined over $\mathbb{Q}$. The associated L-function $F(s)$ will be denoted by $L(s, E)$ and is given by

$$L(s, E) = \prod_{p \mid N} (1 - a_p p^{-s-1/2})^{-1} \prod_{p \nmid N} (1 - a_p p^{-s-1/2} + p^{-2s})^{-1},$$

where a_p is the difference between $p+1$ and the number of points on the reduced curve mod p

$$a_p = p + 1 - \#\widetilde{E}(\mathbb{F}_p).$$

When $p \mid N$, then a_p is either 1, -1, or 0. In general, we have the Hasse bound on a_p, $|a_p| < 2\sqrt{p}$; hence we can write

$$\frac{a_p}{p^{1/2}} = 2\cos(\theta_p) = \alpha_p + \beta_p,$$

where, for $p \nmid N$, one has $\alpha_p = e^{i\theta_p}$ and $\beta_p = e^{-i\theta_p}$ with $\theta_p \in [0, \pi]$ and for $p \mid N$, one has $\alpha_p = a_p$, and $\beta_p = 0$. Let Λ_E be the arithmetic function defined by the logarithmic derivative of $L(s, E)$:

$$\frac{L(s, E)'}{L(s, E)} = -\sum_{n=1}^{\infty} \Lambda_E(n) n^{-s}.$$

It follows that for $e \geq 1$

$$\Lambda_E(n) = \begin{cases} \log p \cdot (\alpha_p^e + \beta_p^e) & \text{if } n = p^e \text{ with } p \text{ prime}, \\ 0 & \text{otherwise}. \end{cases}$$

Our results in the function-field setting are analogous to computing the variance of the sum of Λ_E in arithmetic progressions

$$S_{x,c,E}(A) := \sum_{\substack{n \leq x \\ n = A \bmod c}} \Lambda_E(n).$$

Our function-field result (see Theorem 9.0.1) leads us to predict that for $x^{\varepsilon} < c$, $\varepsilon > 0$, the following holds:

$$\mathrm{Var}(S_{x,c,E}) \sim \frac{x}{\phi(c)} \min\{\log x, 2\log c\}.$$

This demonstrates the two regimes of behavior. We can also detect the degree of the L-function in question as the coefficient of $\log c$.

Another example of a degree-2 L-function is the Ramanujan L-function

$$L(s, \tau) = \prod_p \left(1 - \frac{\tau(p)}{p^{s+11/2}} + \frac{1}{p^{2s}}\right)^{-1},$$

where τ is the Ramanujan tau function $\tau : \mathbb{N} \to \mathbb{Z}$ defined by the identity

$$\sum_{n\geq 1} \tau(n) q^n = q \prod_{n\geq 1} (1-q^n)^{24},$$

where $q = \exp(2\pi i z)$. Ramanujan conjectured (and his conjecture was proved by Deligne) that $|\tau(p)| \leq 2p^{11/2}$ for all primes p. Hence, as before, we can write

$$\frac{\tau(p)}{p^{11/2}} = 2\cos(\theta_p) = \alpha_p + \beta_p.$$

Let Λ_τ be the arithmetic function defined by the logarithmic derivative of $L(s,\tau)$:

$$\frac{L(s,\tau)'}{L(s,\tau)} = -\sum_{n=1}^{\infty} \Lambda_\tau(n) n^{-s}.$$

It follows that for $e \geq 1$

$$\Lambda_\tau(n) = \begin{cases} \log p \cdot (\alpha_p^e + \beta_p^e) & \text{if } n = p^e \text{ with } p \text{ prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Again we are led to speculate that for $x^\varepsilon < c$ and $\varepsilon > 0$, if

$$S_{x,c,\tau}(A) := \sum_{\substack{n\leq x \\ n=A \bmod c}} \Lambda_\tau(n)$$

then the following holds:

$$\mathrm{Var}(S_{x,c,\tau}) \sim \frac{x}{\phi(c)} \min\{\log x, 2\log c\}.$$

1.2. ***Function-field analogue.*** Our results are quite general and to state them requires a good deal of notation and terminology to be explained. For this reason we postpone presenting them until later sections, when the necessary theory has been developed. To illustrate them however we first present below a special case of one of them, and then we sketch a proof.

Remark 1.2.1. For reference, our main results are Theorems 9.0.1 and 12.3.1. The former provides the variance estimates we need in terms of a matrix integral and the latter provides an application of these estimates to L-functions of abelian varieties. Two key ingredients used to prove these theorems are Theorems 10.0.4 and 11.0.1, which provide requisite equidistribution and big-monodromy results respectively.

Suppose q is an odd prime power, and let $E_{\mathrm{Leg}}/\mathbb{F}_q(t)$ be the Legendre curve, that is, the elliptic curve with affine model

$$y^2 = x(x-1)(x-t).$$

Over the ring $\mathbb{F}_q[t]$, this curve has bad multiplicative reduction at $t = 0, 1$ and good reduction everywhere else, so it has conductor $s = t(t-1)$. It also has additive reduction at ∞, so the L-function is given by an Euler product

$$L(T, E_{\mathrm{Leg}}/\mathbb{F}_q(t)) = \prod_{\pi \in \mathcal{P}} L(T^{\deg(\pi)}, E_{\mathrm{Leg}}/\mathbb{F}_\pi)^{-1},$$

where $\mathcal{P} \subset \mathbb{F}_q[t]$ is the subset of monic irreducibles and $\mathbb{F}_\pi$ is the residue field $\mathbb{F}_q[t]/\pi\mathbb{F}_q[t]$.

Each Euler factor of $L(T, E_{\mathrm{Leg}}/\mathbb{F}_q(t))$ is the reciprocal of a polynomial in $\mathbb{Q}[T]$ and satisfies

$$T\frac{d}{dT}\log L(T, E_{\mathrm{Leg}}/\mathbb{F}_\pi)^{-1} = \sum_{m=1}^{\infty} a_{\pi,m}T^m \in \mathbb{Z}[\![T]\!].$$

Moreover, if we define Λ_{Leg} to be the function on the subset $\mathcal{M}$ of monic polynomials given by

$$\Lambda_{\mathrm{Leg}}(f) = \begin{cases} d \cdot a_{\pi,m} & \text{if } f = \pi^m \text{ with } \pi \in \mathcal{P} \text{ and } \deg(\pi) = d, \\ 0 & \text{otherwise,} \end{cases}$$

then the L-function satisfies

$$T\frac{d}{dT}\log(L(T, E_{\mathrm{Leg}}/\mathbb{F}_q(t))) = \sum_{n=1}^{\infty}\Bigg(\sum_{f\in\mathcal{M}_n}\Lambda_{\mathrm{Leg}}(f)\Bigg)T^n.$$

Let $c \in \mathbb{F}_q[t]$ be monic and square-free. For each $n \geq 1$ and each A in $\Gamma(c) = (\mathbb{F}_q[t]/c\mathbb{F}_q[t])^\times$, consider the sum

$$S_{n,c}(A) := \sum_{\substack{f\in\mathcal{M}_n \\ f\equiv A \bmod c}} \Lambda_{\mathrm{Leg}}(f). \tag{1.2.2}$$

Let A vary uniformly over $\Gamma(c)$, and consider the moments

$$\mathbb{E}[S_{n,c}(A)] = \frac{1}{|\Gamma(c)|}\sum_{A\in\Gamma(c)} S_{n,c}(A), \quad \mathrm{Var}[S_{n,c}(A)] = \frac{1}{|\Gamma(c)|}\sum_{A\in\Gamma(c)} |S_{n,c}(A) - \mathbb{E}[S_{n,c}(A)]|^2.$$

These moments (and the quantity $|\Gamma(c)|$) depend on q, so one can ask how they behave when we replace $\mathbb{F}_q$ by a finite extension, that is, let $q \to \infty$. Using the theory we develop in this paper one can prove the following theorem.

Theorem 1.2.3. *If* $\gcd(c, s) = t$ *and if* $\deg(c)$ *is sufficiently large, then*

$$|\Gamma(c)| \cdot \mathbb{E}[S_{n,c}(A)] = \sum_{\substack{f\in\mathcal{M}_n \\ \gcd(f,c)=1}} \Lambda_{\mathrm{Leg}}(f), \quad \lim_{q\to\infty}\frac{|\Gamma(c)|}{q^{2n}} \cdot \mathrm{Var}[S_{n,c}(A)] = \min\{n, 2\deg(c) - 1\}.$$

See Theorem 12.3.1. We sketch the proof below in Section 1.3.

Remark 1.2.4. This should be compared to (1.1.12). For definiteness, we could replace "sufficiently large" by $\deg(c) > 900$, but we do not believe this bound to be optimal. We also do not believe the hypothesis on $\gcd(c, s)$ is necessary (see Remark 11.0.2). We use it to deduce that certain monodromy groups are big. We do not have any examples of coprime c and s where we know the monodromy groups are *not* big.

Remark 1.2.5. The fact that the expression for the variance depends on $2\deg(c)$ is a direct consequence of the fact that the associated L-functions have degree 2. (For an L-function of degree r, one will get a leading term of $r\deg(c)$ instead.) This then leads to there being two ranges of behavior.

1.3. ***Sketch of proof of Theorem 1.2.3.*** The calculation of the first moment proceeds immediately from the definition (1.2.2). The first step in our proof of the rest of the theorem is to use Fourier analysis on the multiplicative group $\Gamma(c)$ and rewrite the first and second moments in terms of coefficients of twisted L-functions. Part of this step is to construct a 2-dimensional ℓ-adic Galois representation

$$\rho_{\mathrm{Leg}} : G_K \to \mathrm{GL}(V),$$

and for each character φ in the dual group $\Phi(c) = \mathrm{Hom}(\Gamma(c), \overline{\mathbb{Q}}_\ell^\times)$, to define a twisted L-function

$$L_{\mathcal{C}}(T, \rho_{\mathrm{Leg}} \otimes \varphi) = \prod_{\pi \nmid c} L(T^{d_\pi}, (\rho_{\mathrm{Leg}} \otimes \varphi)_\pi)^{-1} = \exp\left(\sum_{n=1}^{\infty} b_{\rho_{\mathrm{Leg}}\otimes\varphi,n} \frac{T^n}{n}\right),$$

where $\mathcal{C}$ is the set of finite places dividing c and the infinite place. The reason for doing this is that one can then rewrite the moments using orthogonality of characters, and we show that, for any field embedding $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$, one has

$$\mathbb{E}[S_{n,c}(A)] = \frac{1}{\phi(c)} \iota(b_{\rho_{\mathrm{Leg}}\otimes\mathbf{1},n}), \qquad \mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)^2} \sum_{\varphi\in\Phi(c)^*} |\iota(b_{\rho_{\mathrm{Leg}}\otimes\varphi,n})|^2,$$

where $S^* = S \smallsetminus \{\mathbf{1}\}$ for $S \subseteq \Phi(c)$.

The next step is to analyze the coefficients $b_{\rho_{\mathrm{Leg}}\otimes\varphi,n}$. It is relatively easy to show that they lie in $\overline{\mathbb{Q}}$. One can also interpret them cohomologically via a trace formula. Moreover, using Deligne's theorem one can show that, for some integer $R \geq 0$ and all φ in a subset $\Phi(c)_{\rho\,\mathrm{good}} \subseteq \Phi(c)$, the normalized L-function

$$L^*_{\mathcal{C}}(T, \rho_{\mathrm{Leg}} \otimes \varphi) = L_{\mathcal{C}}(T/q, \rho_{\mathrm{Leg}} \otimes \varphi) = \exp\left(\sum_{n=1}^{\infty} b^*_{\rho_{\mathrm{Leg}}\otimes\varphi,n} \frac{T^n}{n}\right)$$

is the reverse characteristic polynomial of a unitary matrix $\theta_{\rho,\varphi} \in U_R(\mathbb{C})$ which is unique up to conjugacy. Let

$$\Phi(c)_{\rho\,\mathrm{bad}} = \Phi(c) \smallsetminus \Phi(c)_{\rho\,\mathrm{good}}$$

so that we have

$$\frac{\phi(c)}{q^{2n}} \mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)} \sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{good}}} |\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2 + \frac{1}{\phi(c)} \sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{bad}}} |\iota(b^*_{\rho_{\mathrm{Leg}}\otimes\varphi,n})|^2.$$

The subset $\Phi(c)_{\rho\,\mathrm{bad}}$ has density zero as $q \to \infty$, and Deligne's theorem also implies that the terms in the sum over bad characters are uniformly bounded. In particular,

$$\frac{\phi(c)}{q^{2n}} \mathrm{Var}[S_{n,c}(A)] \sim \frac{1}{|\Phi(c)^*_{\rho\,\mathrm{good}}|} \sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{good}}} |\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2$$

as $q \to \infty$.

The final step in the proof is to show that

$$\frac{1}{|\Phi(c)^*_{\rho\,\text{good}}|}\sum_{\varphi\in\Phi(c)^*_{\rho\,\text{good}}}|\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2 \sim \int_{U_R(\mathbb{C})}|\mathrm{Tr}(\theta^n)|^2\,d\theta$$

with respect to Haar measure on $U_R(\mathbb{C})$. To do this, we must show that the $\theta_{\rho,\varphi}$ are equidistributed in $U_R(\mathbb{C})$. Roughly speaking, this is equivalent to showing that some accompanying monodromy group is big and is where the conditions on $\gcd(c, s)$ and $\deg(c)$ come into play. We say a bit more about this in the next section.

1.4. ***Underlying equidistribution theorem.*** The key ingredients we use to prove Theorem 1.2.3 and its generalizations are the Mellin transform and Katz's equidistribution theorem. More precisely, we start with a lisse sheaf $\mathcal{F}$ on a dense open $T \subseteq \mathbb{A}^1_t[1/s]$ and twist it by variable Dirichlet characters φ with square-free conductor c to obtain a family of lisse sheaves $\mathcal{F}_\varphi$ on $T[1/c]$; this family is a Mellin transform of $\mathcal{F}$. One can associate a monodromy group $\mathcal{G}_{\text{arith}}$ to this family generated by Frobenius conjugacy classes $\mathrm{Frob}_{E,\varphi}$ for variable Dirichlet characters φ over finite extensions $E/\mathbb{F}_q$. A priori $\mathcal{G}_{\text{arith}}$ is reductive and defined over $\overline{\mathbb{Q}}_\ell$, but Deligne's Riemann hypothesis allows us to associate the classes $\mathrm{Frob}_{E,\varphi}$ for "good" φ to well-defined conjugacy classes in a compact form of the "same" reductive group over $\mathbb{C}$. Katz's equidistribution theorem implies these classes are equidistributed.

For our applications, we need equidistribution in a unitary group $U_R(\mathbb{C})$, and thus we need $\mathcal{G}_{\text{arith}}$ to be as big as possible, namely $\mathrm{GL}_{R,\overline{\mathbb{Q}}_\ell}$. We were only able to prove this is the case under the hypotheses that $\deg(c) \gg 1$ and that $\mathcal{F}$ has a unipotent block of exact multiplicity 1 about $t = \gcd(c, s) = 0$. While we do expect that one may encounter exceptions when $\deg(c)$ is small, we do not believe our lower bound on $\deg(c)$ is sharp. On the other hand, the hypothesis on the monodromy about the unique prime dividing $\gcd(c, s)$ was made in order to ensure we could exhibit elements of $\mathcal{G}_{\text{arith}}$ whose existence helped ensure the group was big. We conjecture one still has big monodromy under the weaker hypothesis that $\gcd(c, s) = 1$.

1.5. ***Overview.*** The structure of this paper is as follows. We start in Section 2 by establishing notation and relatively basic facts that we need throughout the rest of the paper.

Throughout the first several sections of the paper we work over a global function field $K = \mathbb{F}_q(X)$, but starting in Section 5, we restrict to $K = \mathbb{F}_q(t)$. Throughout the entire paper we fix an ℓ-adic Galois representation

$$\rho : G_{K,\mathcal{S}} \to \mathrm{GL}(V),$$

where $G_{K,\mathcal{S}}$ is a quotient of the absolute Galois group G_K of K. We also fix a finite set of places $\mathcal{C}$ of K. Ultimately it consists of the place at infinity in $\mathbb{F}_q(t)$ and the finite places corresponding to primes dividing a square-free polynomial $c \in \mathbb{F}_q[t]$. The characters we twist by will be continuous homomorphisms

$$\varphi : G^{\mathrm{t}}_{K,\mathcal{C}} \to \overline{\mathbb{Q}}_\ell^\times,$$

where $G^{\mathrm{t}}_{K,\mathcal{C}}$ is another quotient of G_K.

In Section 3, we define two L-functions: a partial L-function $L_{\mathcal{C}}(T, \rho)$ and the complete L-function $L(T, \rho)$. It is the coefficients of the former which appear in our moment formulas, but the latter is what might be called "the" L-function of ρ. Both are defined via an Euler product: for the complete L-function, we use an Euler product over $\mathcal{P}$, the set of all places of K; for the other, we exclude the Euler factors over $\mathcal{C}$. They coincide if and only if the excluded (or missing) Euler factors are trivial. We recall the cohomological manifestation of each L-function and the trace formula. We also derive numerical invariants for ρ required for computing the degree of each L-function.

In Section 4, we consider twists of the representation ρ by tame ℓ-adic characters φ with conductor supported on $\mathcal{C}$. If one replaces ρ by $\rho \otimes \varphi$, then one can apply the material of Section 3 to define $L(T, \rho \otimes \varphi)$ and $L_{\mathcal{C}}(T, \rho \otimes \varphi)$. We provide an annotated version of those results in a manner which is convenient for us.

In Section 5, we revert to $K = \mathbb{F}_q(t)$ and define the von Mangoldt function Λ_ρ of our Galois representation. It is a multiplicative function $\mathcal{M} \to \overline{\mathbb{Q}}_\ell$ defined using the Euler factors $L(T, \rho_v)$ for the finite places in $\mathbb{F}_q(t)$, and for the trivial representation $\rho = \mathbf{1}$, one has, for $m \geq 1$,

$$\Lambda_{\mathbf{1}}(f) = \begin{cases} \deg(\pi) & \text{if } f = \pi^m \text{ and } \pi \text{ irreducible,} \\ 0 & \text{otherwise.} \end{cases}$$

For each $A \in \Gamma(c)$, we consider the sum

$$S_{n,c}(A) = \sum_{f \in \mathcal{M}_n(A)} \Lambda_\rho(f),$$

where $\mathcal{M}_n(A) = \{f \equiv A \bmod c\} \subseteq \mathcal{M}_n$. We regard the sum as random variable with values in $\overline{\mathbb{Q}}_\ell$ by varying A uniformly over $\Gamma(c)$ and express its moments as sums of coefficients of the partial L-functions $L_{\mathcal{C}}(T, \rho \otimes \varphi)$, where φ varies over characters of $\Gamma(c)$.

In Section 6, we define purity and weights. Purity boils down to saying that, in the complex plane, some set of numbers lies on a circle centered at zero, and weight corresponds to the radius. These are the properties usually used to state some sort of Riemann hypothesis. We impose purity on the (zeros of the) Euler factors of $L(T, \rho \otimes \varphi)$ and use Deligne's theorem to deduce purity of its cohomology factors $P_i(T, \rho \otimes \varphi)$. A priori, these factors are polynomials in $\overline{\mathbb{Q}}_\ell[T]$, but in fact, Deligne's theorem implies they have coefficients in $\overline{\mathbb{Q}}$. His theorem also tells us what the weight of each cohomological factor should be, so we can use a field embedding $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$ to regard the sums $S_{n,c}(A)$ as complex numbers.

In Section 7, we isolate conditions for a complete L-function $L(T, \rho \otimes \varphi)$ to be a pure polynomial, and they hold for most φ. These are the L-functions for which a suitable normalization $L^*(T, \rho \otimes \varphi)$ has coefficients in $\overline{\mathbb{Q}}$ and is unitary, that is, equals the characteristic polynomial of a complex unitary matrix. We also isolate conditions for $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ to be a pure polynomial since it is the coefficients of these L-functions which appear in our moment calculations. These conditions imply the partial and complete L-functions are polynomials and coincide.

In Section 8, we partition $\Phi(c)$ into subsets of good and bad characters, and then we further partition the bad characters into mixed and heavy characters. A character φ is good if it makes sense to say that a certain renormalization $L^*_C(T, \rho \otimes \varphi)$ of $L_C(T, \rho \otimes \varphi)$ is unitary, and otherwise it is bad, and $L^*_C(T, \rho \otimes \varphi)$ is no longer unitary. If $L_C(T, \rho \otimes \varphi)$ is an impure polynomial, then φ is mixed, and if $L_C(T, \rho \otimes \varphi)$ is not even a polynomial, then φ is heavy since $L_C(T, \rho \otimes \varphi)$ has poles of excess weight.

In Section 9, we return to our moment calculations. The main result of the section is that the second moment can be approximated using a matrix integral over some compact subgroup $\mathbb{K} \subseteq U_R(\mathbb{C})$, and one has control over the error term precisely when no nontrivial φ is heavy. At this stage, all we know about $\mathbb{K}$ is that each unitary $L^*_C(T, \rho \otimes \varphi)$ corresponds to a unique conjugacy class $\theta_{\rho,\varphi} \subset \mathbb{K}$ and that the classes become equidistributed in $\mathbb{K}$ as $q \to \infty$. In later sections we give conditions for it to be big, that is, equal to $U_R(\mathbb{C})$.

In Section 10, we partition $\Phi(c)$ into cosets of a “one-parameter” subgroup $\Phi(u)^\nu \subseteq \Phi(c)$, and then we attach a monodromy group to each coset $\varphi\Phi(u)^\nu$. We define what it means for one of these monodromy groups to be big, and then we define the big characters in $\Phi(c)$ to be those φ whose coset has big monodromy. We then show that if the density of big characters tends to 1 as $q \to \infty$, then the $\theta_{\rho,\varphi}$ are equidistributed in $\mathbb{K} = U_R(\mathbb{C})$. In this case we say the Mellin transform of ρ has big monodromy.

In Section 11, we prove a theorem which asserts that the Mellin transform of ρ has big monodromy provided ρ satisfies certain hypotheses. The material in this section rests heavily on the monumental works of Katz, most notably the monograph [Katz 2012]. In order to prove our result, we were forced to impose the condition that the (square-free) conductor s of ρ and the twisting conductor c satisfy $\deg(\gcd(c, s)) = 1$. We also imposed conditions on the local monodromy of ρ at the zero of $\deg(c, s)$. We used both of these hypotheses to deduce that the relevant monodromy groups contained an element so special that the group was forced to be big (e.g., for the specific example considered in Theorem 1.2.3 one obtains pseudoreflections). While the specific result we proved is new, it borrows heavily from the rich set of tools developed by Katz, and one familiar with his work will easily recognize the intellectual debt we owe him.

In Section 12, we bring everything together and show how Galois representations arising from (Tate modules of) certain abelian varieties satisfy the requisite properties to apply the theorems of the earlier sections. More precisely, we consider Jacobians of (elliptic and) hyperelliptic curves of arbitrary genus, the Legendre curve being one such example. Because we chose to work with hyperelliptic curves we were forced to assume q is odd. Nonetheless, we expect one can find other suitable examples in characteristic 2.

There are four appendices to the paper containing material we needed for the results in Section 11. In Appendix A we recall the definition of and some basic facts about middle-extension sheaves. In Appendix B we recall well-known formulas for Euler–Poincaré characteristic. In Appendix C we prove the group-theoretic result which asserts that a reductive subgroup of GL_R with the sort of special element alluded to above is big. In Appendix D we recall much of the abstract formalism required to define the monodromy groups which we want to show are big. While none of this material is new, it elaborates on some of the facts which we felt were not always easy to give a direct reference for in [Katz 2012]. In particular, our work should not be regarded as a substitute for Katz's original monograph, but we hope some readers will find it an acceptable and enriching complement to his masterful presentation.

2. Notation

Let $q = q_0^n$ be powers of a prime p and $\mathbb{F}_q$ be a finite field with q elements. We write $q \to \infty$ to mean $n \to \infty$.

Let X be a proper smooth geometrically connected curve over $\mathbb{F}_{q_0}$ and K be the function field $\mathbb{F}_q(X)$ (e.g., $X = \mathbb{P}_t^1$ and $K = \mathbb{F}_q(t)$). Let $\mathcal{P}$ be the set of places of K, and for each $v \in \mathcal{P}$, let $\mathbb{F}_v$ be its residue field and $d_v = [\mathbb{F}_v : \mathbb{F}_q]$ be its degree. We identify the elements of $\mathcal{P}$ with the closed points of X in the usual way.

Let K^{sep} be a separable closure of K and $\overline{\mathbb{F}}_q \subset K^{\text{sep}}$ be the algebraic closure of $\mathbb{F}_q \subset K$. Let $G_K = \text{Gal}(K^{\text{sep}}/K)$ and $G_{\mathbb{F}_q} = \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, and let $\overline{G}_K \subseteq G_K$ be the stabilizer of $\overline{\mathbb{F}}_q$ so that there is an exact sequence

$$1 \to \overline{G}_K \to G_K \to G_{\mathbb{F}_q} \to 1$$

of profinite groups. Given a quotient $G_K \twoheadrightarrow Q$ of profinite groups, we write $\overline{Q} \subseteq Q$ for the image of $\overline{G}_K$ and call it the *geometric subgroup*.

For each subset $\mathcal{S} \subset \mathcal{P}$, let $K_{\mathcal{S}} \subseteq K^{\text{sep}}$ be the maximal subextension unramified *away* from $\mathcal{S}$ and $K_{\mathcal{S}}^{\text{t}} \subseteq K_{\mathcal{S}}$ be the maximal subextension *tamely* ramified over $\mathcal{S}$. Both extensions are Galois over K, so we write $G_{K,\mathcal{S}}$ and $G_{K,\mathcal{S}}^t$ for their respective Galois groups. There is a commutative diagram

$$\begin{array}{ccc} G_K & \longrightarrow & G_{K,\mathcal{S}} \\ & \searrow \quad \swarrow & \\ & G_{K,\mathcal{S}}^{\text{t}} & \end{array} \tag{2.0.1}$$

of quotients.

For each $v \in \mathcal{P}$, we fix a place of K^{sep} over v and write $D(v) \subseteq G_K$ for its decomposition group; the latter is well-defined up to conjugacy. Let $I(v) \subseteq D(v)$ be the inertia subgroup and $P(v) \subseteq I(v)$ be the wild inertia subgroup (i.e., the p-Sylow subgroup). The quotient $G_v = D(v)/I(v)$ is the absolute Galois group of $\mathbb{F}_v$, and we write $\text{Frob}_v \in G_v$ for the Frobenius element $\text{Frob}_q^{d_v}$ and $\text{Frob}_v I(v)$ for its preimage in $D(v)$.

If $v \notin S$, then the inertia subgroup $I(v)$ is contained in the kernel of the horizontal map in (2.0.1). In particular, every element of the coset $\text{Frob}_v I(v)$ maps to the same element of $G_{K,\mathcal{S}}$, which we denote by $\text{Frob}_v \in G_{K,\mathcal{S}}$.

Given a smooth geometrically connected curve U over $\mathbb{F}_q$, we write $\overline{U}$ for the base change curve $U \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. We fix a geometric generic point $\bar{\eta}$ of U and write $\pi_1(U)$ and $\pi_1(\overline{U})$ for the arithmetic and geometric étale fundamental groups of U respectively. Moreover, if T is a second smooth geometrically connected curve over $\mathbb{F}_q$ and if $T \to U$ is a finite étale cover, then we implicitly suppose the geometric generic point of T maps to that of U and write $\pi_1(T) \to \pi_1(U)$ for the induced inclusion of fundamental groups.

Let $\ell \in \mathbb{Z}$ be a prime distinct from p and $\overline{\mathbb{Q}}_\ell$ be an algebraic closure of $\mathbb{Q}_\ell$. All sheaves on U we consider are constructible étale $\overline{\mathbb{Q}}_\ell$-sheaves, unless stated otherwise, and we write $H^i(\overline{U}, \mathcal{F})$ and $H_c^i(\overline{U}, \mathcal{F})$ for the étale cohomology groups of $\mathcal{F}$. For each integer n, we also write $\mathcal{F}(n)$ for the Tate twisted sheaf $\mathcal{F} \otimes_{\overline{\mathbb{Q}}_\ell} \overline{\mathbb{Q}}_\ell(n)$ and recall that

$$\det(1 - T\,\mathrm{Frob}_q \mid H^i(\bar{U}, \mathcal{F}(n))) = \det(1 - q^n T\,\mathrm{Frob}_q \mid H^i(\bar{U}, \mathcal{F})).$$

A similar identity holds for cohomology with compact supports (see [SGA 4½ 1977, Sommes trig., Theorem 1.13]). In particular, we have identities

$$\dim(H^i(\bar{U}, \mathcal{F}(n))) = \dim(H^i(\bar{U}, \mathcal{F})), \quad \dim(H^i_c(\bar{U}, \mathcal{F}(n))) = \dim(H^i_c(\bar{U}, \mathcal{F}))$$

for every i and n.

The sheaf $\mathcal{F}$ is lisse (or locally constant) on U if and only it corresponds to a continuous representation $\pi_1(U) \to \mathrm{GL}(V)$ from the étale fundamental group to a finite-dimensional $\overline{\mathbb{Q}}_\ell$ vector space V (cf. [Milne 1980, II.3.16.d]). In that case one has identifications

$$H^0(\bar{U}, \mathcal{F}) = V^{\pi_1(\bar{U})} \quad \text{and} \quad H^2_c(\bar{U}, \mathcal{F}(2)) = V_{\pi_1(\bar{U})} \tag{2.0.2}$$

with the subspace of $\pi_1(\bar{U})$-invariants and quotient space of $\pi_1(\bar{U})$-coinvariants (see [SGA 4½ 1977, Sommes trig., Remarques 1.18(d)]).

3. *L*-functions

In this section, we recall the construction of two L-functions attached to a Galois representation of the absolute Galois group of a global function field K. A priori, both L-functions are given via Euler products, the essential difference being that one Euler product is over all places of K while the other excludes the Euler factors at a finite set of places of K. We call them the complete and partial L-functions respectively. Each will play a role in later sections, and in particular, when they differ, that is, when at least one omitted Euler factor is nontrivial, their roles will also differ. We do not elucidate the difference in this section, but we do give necessary and sufficient criteria for the L-functions to coincide.

As we recall, both L-functions have a cohomological genesis via the Grothendieck–Lefschetz trace formula. Therefore they can be expressed as rational functions, that is, quotients of polynomials in a single variable, and the polynomials are products of (reverse) characteristic polynomials of an operator acting on certain ℓ-adic cohomology groups. Given basic information about ρ, we show how to calculate the degrees of its L-functions, e.g., in terms of numerical invariants such as Swan and absolute conductors.

3.1. ***Euler products.*** Let $\mathcal{S} \subset \mathcal{P}$ be a finite subset of places. Let V be a finite-dimensional $\overline{\mathbb{Q}}_\ell$-vector space and ρ be a homomorphism

$$\rho : G_{K,\mathcal{S}} \to \mathrm{GL}(V)$$

which is continuous with respect to the profinite topologies.

The decomposition group $D(v)$ stabilizes the subspace $V_v = V^{I(v)}$, and the inertia subgroup $I(v)$ acts trivially on it, so there is a representation

$$\rho_v : G_v \to \mathrm{GL}(V_v).$$

The *Euler factor* of ρ at v is given by

$$L(T, \rho_v) := \det(1 - T\rho_v(\mathrm{Frob}_v) \mid V_v) \in \overline{\mathbb{Q}}_\ell[T],$$

and its degree equals the dimension of V_v.

Let $\mathcal{C} \subset \mathcal{P}$ be a finite subset. The *partial* and *complete L-functions* of ρ are the formal power series in $\overline{\mathbb{Q}}_\ell[T]$ with respective Euler products

$$L_{\mathcal{C}}(T, \rho) := \prod_{v \notin \mathcal{C}} L(T^{d_v}, \rho_v)^{-1} \quad \text{and} \quad L(T, \rho) := \prod_{v \in \mathcal{P}} L(T^{d_v}, \rho_v)^{-1}. \tag{3.1.1}$$

The ratio

$$M_{\mathcal{C}}(T, \rho) := L(T, \rho)/L_{\mathcal{C}}(T, \rho) = \prod_{v \in \mathcal{C}} L(T^{d_v}, \rho_v)^{-1}$$

is the reciprocal of a polynomial, and $M_{\mathcal{C}}(T, \rho) = 1$ if and only if $L(T, \rho) = L_{\mathcal{C}}(T, \rho)$.

3.2. ***Galois modules versus sheaves.*** While most of this paper uses the language of global fields, it is useful to adopt a geometric language. Certain readers will find the latter language more to their taste, and we acknowledge that many of our results may have a more appealing formulation in the language of geometry (and sheaves). However, we felt the language of Galois representations over global (function) fields was accessible to a broader audience, so we tried to do “as much as possible” in that language.

3.3. ***Middle extensions.*** Recall X is a proper smooth geometrically connected curve over $\mathbb{F}_q$. Let $U \subseteq X$ be a dense Zariski open subset over $\mathbb{F}_q$. Let $\mathcal{F}$ be a sheaf on X and $\mathcal{F}_{\bar{\eta}}$ be its geometric generic stalk. The latter is a G_K-module, and up to replacing U by a dense open subset, it is even a module over the étale fundamental group $\pi_1(U)$; that is, $\mathcal{F}$ is *lisse* on U. Conversely, for every finite-dimensional $\overline{\mathbb{Q}}_\ell$-vector space V and continuous homomorphism $\pi_1(U) \to \mathrm{GL}(V)$, there is a lisse $\overline{\mathbb{Q}}_\ell$-sheaf on U whose stalk over $\bar{\eta}$ is the $\pi_1(U)$-module V.

There are two sheaves and morphisms one can associate to the inclusion $j : U \to X$: those in the diagram

$$j_! j^* \mathcal{F} \to \mathcal{F} \to j_* j^* \mathcal{F} \tag{3.3.1}$$

and constructed in Appendix A.

Definition 3.3.2. We say $\mathcal{F}$ is *supported on* U if and only if the first map of (3.3.1) is an isomorphism, and $\mathcal{F}$ is a *middle extension* if and only if the second map is an isomorphism for *every* j.

The following proposition shows that there is a canonical middle-extension sheaf on X we can associate to ρ. We denote it by $\mathrm{ME}(\rho)$.

Proposition 3.3.3. *There is a middle extension* $\mathcal{F}$ *with* $\mathcal{F}_{\bar{\eta}} = V$ *as* G_K*-modules, and it is unique up to isomorphism.*

Proof. One can identify V_v with the stalk $\mathrm{ME}(\rho)_v$ and ρ_v with the restriction of $\pi_1(U) \to \mathrm{GL}(V)$ to the decomposition group $D(v) \subset \pi_1(U)$ See Proposition A.0.4 and compare [Milne 1980, 3.1.16]. □

Corollary 3.3.4. *Let $\mathcal{S}' \subset \mathcal{P}$ be a finite subset containing $\mathcal{S}$ and $\rho' : G_{K,\mathcal{S}'} \to \mathrm{GL}(V)$ be the composition of ρ with the natural quotient $G_{K,\mathcal{S}'} \twoheadrightarrow G_{K,\mathcal{S}}$. Then $\mathrm{ME}(\rho)$ and $\mathrm{ME}(\rho')$ are isomorphic.*

Proof. The quotient $G_K \to G_{K,\mathcal{S}}$ factors as $G_K \twoheadrightarrow G_{K,\mathcal{S}'} \twoheadrightarrow G_{K,\mathcal{S}}$, and $\mathrm{ME}(\rho')_{\bar{\eta}} = V = \mathrm{ME}(\rho)$ as G_K-modules. Since $\mathrm{ME}(\rho), \mathrm{ME}(\rho')$ are both middle extensions, Proposition 3.3.3 implies they are isomorphic. □

3.4. *Cohomological manifestation.* Suppose $Z = X \smallsetminus U$ equals $\mathcal{C}$. Then $L(T, \rho)$ and $L_{\mathcal{C}}(T, \rho)$ equal the L-functions of the sheaves $\mathrm{ME}(\rho)$ and $j_! j^* \mathrm{ME}(\rho)$ respectively. More precisely, the Euler products of the latter coincide with (3.1.1). Moreover, they all have the same Euler factors over U; hence $M_{\mathcal{C}}(T, \rho)$ has an Euler product over Z which coincides with that of the L-function of $\mathrm{ME}(\rho)$ over Z.

The étale cohomology groups of these sheaves are finite-dimensional $\overline{\mathbb{Q}}_\ell$-vector spaces, and Frob_q acts $\overline{\mathbb{Q}}_\ell$-linearly on them. In particular, we have characteristic polynomials

$$P_{\mathcal{C},i}(T, \rho) := \det(1 - T\,\mathrm{Frob}_q \mid H^i_c(\bar{U}, \mathrm{ME}(\rho))), \tag{3.4.1}$$

which are trivial for $i \neq 0, 1, 2$ since U is a curve. Moreover, $P_{\mathcal{C},i}(T) = 1$ if U is an affine curve, that is, if $\mathcal{C}$ is nonempty, and then

$$L_{\mathcal{C}}(T, \rho) = P_{\mathcal{C},1}(T, \rho)/P_{\mathcal{C},2}(T, \rho). \tag{3.4.2}$$

Similarly, the characteristic polynomials

$$P_i(T, \rho) := \det(1 - T\,\mathrm{Frob}_q \mid H^i(\bar{X}, \mathrm{ME}(\rho))) \tag{3.4.3}$$

are trivial for $i \neq 0, 1, 2$ since X is a curve, and they satisfy

$$L(T, \rho) = \frac{P_1(T, \rho)}{P_0(T, \rho) P_2(T, \rho)}. \tag{3.4.4}$$

Finally, if $\mathcal{C} = \varnothing$ and thus $U = X$, then

$$P_{\varnothing,i}(T, \rho) = P_i(T, \rho) \quad \text{for all } i,$$

and thus $L(T, \rho) = L_{\varnothing}(T, \rho)$.

3.5. *Numerical invariants of ρ.* Let

$$\mathrm{rank}_v(\rho) := \deg(L(T, \rho_v)), \qquad \mathrm{drop}_v(\rho) := \dim(V) - \mathrm{rank}_v(\rho),$$

and $\mathrm{Swan}_v(\rho)$ be the Swan conductor of V as an $\overline{\mathbb{Q}}_\ell[I(v)]$-module (see [Katz 1988, 1.6]). We call these and

$$\mathrm{drop}_{\mathcal{C}}(\rho) := \sum_{v \in \mathcal{C}} d_v \cdot \mathrm{drop}_v(\rho)$$

the *local invariants* of ρ. On the other hand, we call

$$\mathrm{rank}(\rho) := \dim(V), \quad \mathrm{drop}(\rho) := \sum_{v \in \mathcal{P}} d_v \cdot \mathrm{drop}_v(\rho), \quad \mathrm{Swan}(\rho) := \sum_{v \in \mathcal{P}} d_v \cdot \mathrm{Swan}_v(\rho)$$

and

$$r_\varnothing(\rho) := \deg(L(T,\rho)), \quad r_{\mathcal{C}}(\rho) := \deg(L_{\mathcal{C}}(T,\rho))$$

the *global invariants*.

Proposition 3.5.1. *Let g be the genus of $\overline{X}$. Then the Euler characteristics $\chi(\overline{X}, \mathrm{ME}(\rho))$ and $\chi_c(\overline{U}, \mathrm{ME}(\rho))$ (see (B.0.5)) satisfy*

$$r_\varnothing(\rho) = -\chi(\overline{X}, \mathrm{ME}(\rho)) = (\mathrm{drop}(\rho) + \mathrm{Swan}(\rho)) - (2-2g)\cdot \mathrm{rank}(\rho), \tag{3.5.2}$$

$$r_{\mathcal{C}}(\rho) = -\chi_c(\overline{U}, \mathrm{ME}(\rho)) = (\mathrm{drop}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho) + \mathrm{Swan}(\rho)) - (2-2g-\deg(\mathcal{C}))\cdot \mathrm{rank}(\rho). \tag{3.5.3}$$

Moreover, if $\mathrm{ME}(\rho)$ *is supported on U (see Definition 3.3.2), then* $\chi_c(\overline{U}, \mathrm{ME}(\rho)) = \chi(\overline{X}, \mathrm{ME}(\rho))$.

Proof. See Proposition B.1.1 and Corollary B.1.2. □

One deduces immediately that

$$r_{\mathcal{C}}(\rho) = r_\varnothing(\rho) + \deg(\mathcal{C})\cdot \mathrm{rank}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho). \tag{3.5.4}$$

3.6. *Trace formula.* The *local traces* of ρ are given by

$$a_{\rho,v,m} := \mathrm{Tr}(\rho_v(\mathrm{Frob}_v)^m \mid V_v) \quad \text{for } v \in \mathcal{P} \text{ and } m \geq 1, \tag{3.6.1}$$

and they satisfy

$$T\frac{d}{dT}\log L(T,\rho_v)^{-1} = \sum_{m=1}^{\infty} a_{\rho,v,m}T^m \quad \text{for } v \in \mathcal{P}. \tag{3.6.2}$$

Combining this with (3.1.1) yields the identity

$$T\frac{d}{dT}\log L_{\mathcal{C}}(T,\rho) = \sum_{n=1}^{\infty}\Bigg(\sum_{md=n}\ \sum_{v\in\mathcal{P}_d\smallsetminus\mathcal{C}} d\cdot a_{\rho,v,m}\Bigg)T^n, \tag{3.6.3}$$

where $\mathcal{P}_d \subset \mathcal{P}$ is the finite subset of places of degree d.

Let $\overline{U} \subseteq \overline{X}$ be the open complement of $\mathcal{C}$. The *cohomological traces* of ρ are given by

$$b_{\rho,n} := \sum_{i=0}^{2}(-1)^i\cdot \mathrm{Tr}(\mathrm{Frob}_q \mid H^i_c(\overline{U}, \mathrm{ME}(\rho))) \quad \text{for } n \geq 1$$

and they satisfy

$$T\frac{d}{dT}\log L_{\mathcal{C}}(T,\rho) = \sum_{n=1}^{\infty} b_{\rho,n}T^n. \tag{3.6.4}$$

Combining this with (3.6.3) yields the Grothendieck–Lefschetz trace formula

$$\sum_{md=n}\ \sum_{v\in\mathcal{P}_d\smallsetminus\mathcal{C}} d\cdot a_{\rho,v,m} = b_{\rho,n}. \tag{3.6.5}$$

See [SGA 4½ 1977, Rapport, §3] for details.

4. Twisted L-functions

In this section, we apply the theory of the previous section to the twist of a Galois representation by a Dirichlet character. We start by defining the twist and its L-functions, and then we apply the theory from the previous section, e.g., to calculate the respective degrees.

4.1. ***Twists by characters.*** Let $\mathcal{S} \subset \mathcal{P}$ be a finite subset and V be a finite-dimensional $\overline{\mathbb{Q}}_\ell$-vector space. Let

$$\rho : G_{K,\mathcal{S}} \to \mathrm{GL}(V)$$

be a *Galois representation*, that is, a continuous homomorphism.

Let $\mathcal{C} \subset \mathcal{P}$ be a finite subset. An *ℓ-adic character with conductor supported on* $\mathcal{C}$ is a continuous homomorphism

$$\varphi : G_{K,\mathcal{C}} \to \overline{\mathbb{Q}}_\ell^\times,$$

and we write $\Phi(\mathcal{C})$ for the set of all such characters which also have finite image. By definition, φ factors as a composite homomorphism

$$G_{K,\mathcal{C}} \twoheadrightarrow G_{K,\mathcal{C}}^{\mathrm{ab}} \to \overline{\mathbb{Q}}_\ell^\times$$

through the maximal abelian quotient. We say it is *tame* if and only if it factors as a composite homomorphism

$$G_{K,\mathcal{C}}^{\mathrm{ab}} \twoheadrightarrow G_{K,\mathcal{C}}^{\mathrm{t,ab}} \to \overline{\mathbb{Q}}_\ell^\times$$

through the maximal tame (abelian) quotient.

Let $\mathcal{R} = \mathcal{C} \cup \mathcal{S}$ so that there are natural quotients

$$G_{K,\mathcal{R}} \twoheadrightarrow G_{K,\mathcal{S}} \quad \text{and} \quad G_{K,\mathcal{R}} \twoheadrightarrow G_{K,\mathcal{C}}.$$

Let ρ_R and φ_R be the respective compositions

$$\rho_R : G_{K,\mathcal{R}} \twoheadrightarrow G_{K,\mathcal{S}} \to \mathrm{GL}(V), \quad \varphi_R : G_{K,\mathcal{R}} \twoheadrightarrow G_{K,\mathcal{C}} \to \overline{\mathbb{Q}}_\ell^\times.$$

The *tensor product* of ρ and φ is the representation

$$\rho \otimes \varphi = (g \mapsto \rho_R(g)\varphi_R(g)) : G_{K,\mathcal{R}} \to \mathrm{GL}(V_\varphi),$$

where $V_\varphi = V$ as $\overline{\mathbb{Q}}_\ell$-vector spaces.

4.2. ***L-functions.*** The Euler factors of the L-functions of $\rho \otimes \varphi$ are given by

$$L(T, (\rho \otimes \varphi)_v) := \det(1 - T\,(\rho \otimes \varphi)_v(\mathrm{Frob}_v) \mid V_\varphi^{I(v)}),$$

and in particular,

$$L(T, (\rho \otimes \varphi)_v) = L(\varphi_{\mathcal{C}}(\mathrm{Frob}_v)T, \rho_v) \quad \text{for } v \notin \mathcal{C}. \tag{4.2.1}$$

Moreover, the partial and complete L-functions of $\rho \otimes \varphi$ satisfy

$$L_{\mathcal{C}}(T, \rho \otimes \varphi) := \prod_{v \notin \mathcal{C}} L(T^{d_v}, (\rho \otimes \varphi)_v)^{-1} = \prod_i P_{\mathcal{C},i}(T, \rho \otimes \varphi)^{(-1)^{i+1}}$$

and

$$L(T,\rho\otimes\varphi) := \prod_{v\in\mathcal{P}} L(T^{d_v},(\rho\otimes\varphi)_v)^{-1} = \prod_i P_i(T,\rho\otimes\varphi)^{(-1)^{i+1}}$$

respectively, where

$$P_{\mathcal{C},i}(T,\rho\otimes\varphi) := \det(1-T\,\mathrm{Frob}_q \mid H^i_c(\bar{U},\mathrm{ME}(\rho\otimes\varphi))),$$
$$P_i(T,\rho\otimes\varphi) := \det(1-T\,\mathrm{Frob}_q \mid H^i(\bar{X},\mathrm{ME}(\rho\otimes\varphi))).$$

Recall $\bar{U}\subset\bar{X}$ is the open complement of $\mathcal{C}$. Compare (3.1.1), (3.4.1), and (3.4.2).

4.3. *Numerical invariants.* Recall the numerical invariants defined in Section 3.5. We say a character φ is *tame* if and only if it factors through the maximal tame quotient $G_{K,\mathcal{C}} \twoheadrightarrow G^{\mathrm{t}}_{K,\mathcal{C}}$, or equivalently, $\mathrm{Swan}(\rho)$ vanishes. Let

$$r_{\mathcal{C}}(\rho\otimes\varphi) := \deg(L_{\mathcal{C}}(T,\rho\otimes\varphi))$$

as in Section 3.5.

Proposition 4.3.1. *If φ is tame, then*

$$r_{\mathcal{C}}(\rho\otimes\varphi) = r_{\mathcal{C}}(\rho) = \deg(L(T,\rho)) + (\deg(c)+1)\dim(V) - \mathrm{drop}_{\mathcal{C}}(\rho). \tag{4.3.2}$$

Proof. If φ is tame and g is the genus of $\bar{X}$, then Proposition 3.5.1 and Lemma B.1.3 imply

$$\begin{aligned} r_{\mathcal{C}}(\rho\otimes\varphi) &\overset{(3.5.3)}{=} (\mathrm{drop}(\rho\otimes\varphi) - \mathrm{drop}_{\mathcal{C}}(\rho\otimes\varphi) + \mathrm{Swan}(\rho\otimes\varphi)) - (2-2g-\deg(\mathcal{C}))\cdot\mathrm{rank}(\rho\otimes\varphi).\\ &\overset{B.1.3}{=} (\mathrm{drop}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho) + \mathrm{Swan}(\rho)) - (2-2g-\deg(\mathcal{C}))\cdot\mathrm{rank}(\rho)\\ &\overset{(3.5.3)}{=} r_{\mathcal{C}}(\rho)\\ &\overset{(3.5.4)}{=} r_{\varnothing}(\rho) + \deg(\mathcal{C})\cdot\mathrm{rank}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho). \end{aligned}$$

The proposition follows by observing that

$$r_{\varnothing}(\rho) = \deg(L(T,\rho)), \quad \deg(\mathcal{C}) = \deg(c)+1, \quad \mathrm{rank}(\rho) = \dim(V).$$ □

Remark 4.3.3. Observe $\deg(L_{\mathcal{C}}(T,\rho\otimes\varphi))$ is independent of φ.

4.4. *Trace formula.* By (4.2.1), we have

$$T\frac{d}{dT}\log L(T,(\rho\otimes\varphi)_v)^{-1} = \sum_{m=1}^{\infty} \varphi(\mathrm{Frob}_v)^m a_{\rho,v,m} T^m \quad \text{for } v\in\mathcal{P}\smallsetminus\mathcal{C}. \tag{4.4.1}$$

We also have

$$T\frac{d}{dT}\log L_{\mathcal{C}}(T,\rho\otimes\varphi) = \sum_{n=1}^{\infty} b_{\rho\otimes\varphi,n} T^n, \tag{4.4.2}$$

where

$$b_{\rho\otimes\varphi,n} := \sum_{i=1}^{2} (-1)^i\cdot\mathrm{Tr}(\mathrm{Frob}_q \mid H^i_c(\bar{U},\mathrm{ME}(\rho\otimes\varphi))) \quad \text{for } n\geq 1.$$

Thus, we have the twisted Grothendieck–Lefschetz trace formula

$$\sum_{md=n} \sum_{v \in \mathcal{P}_d \smallsetminus \mathcal{C}} d \cdot \varphi(\mathrm{Frob}_v)^m a_{\rho,v,m} = b_{\rho\otimes\varphi,n}. \tag{4.4.3}$$

Compare (3.6.5).

5. Sums in arithmetic progressions

Throughout this section (and many of the remaining sections) we suppose that X is the projective t-line $\mathbb{P}^1_t$ and thus that $K = \mathbb{F}_q(t)$.

5.1. ***Dirichlet characters.*** Let $c \in \mathbb{F}_q[t]$ be monic and square-free of degree $d \geq 1$, and let

$$\Gamma(c) := (\mathbb{F}_q[t]/c\,\mathbb{F}_q[t])^\times \quad \text{and} \quad \Phi(c) := \mathrm{Hom}(\Gamma(c), \overline{\mathbb{Q}}^\times).$$

The latter are finite abelian groups and are noncanonically isomorphic of order equal to the Euler totient $\phi(c)$. Let $\mathcal{U}_\mathcal{C} \subset \mathcal{P}$ be the complement of the finite set

$$\mathcal{C} := \mathrm{supp}(c) = \{v \in \mathcal{P} : \mathrm{ord}_v(c) \neq 0\}.$$

Then $\infty \in \mathcal{C}$ and $\sum_{v\in\mathcal{C}} \deg(v) = d + 1$.

The elements of u of $\mathcal{U}_\mathcal{C}$ are in natural bijection with the maximal ideals $\mathfrak{p}_u \subset \mathbb{F}_q[t]$ which do not contain c, and such an ideal is generated by a unique monic $\pi_u \in \mathfrak{p}_u$. In particular, abelian class field theory supplies both a well-defined element $\mathrm{Frob}_u \in G^{\mathrm{ab}}_{K,\mathcal{C}}$ and a homomorphism

$$\alpha_\mathcal{C} : G^{\mathrm{ab}}_{K,\mathcal{C}} \to \Gamma(c), \quad \text{with } \alpha_\mathcal{C}(\mathrm{Frob}_u) = \pi_u \bmod c \text{ for } u \in \mathcal{U}_\mathcal{C}.$$

This allows us to regard any character $\varphi \in \Phi(c)$ as a (continuous) composite homomorphism

$$\varphi : G_{K,\mathcal{C}} \twoheadrightarrow G^{\mathrm{t,ab}}_{K,\mathcal{C}} \twoheadrightarrow \Gamma(c) \to \overline{\mathbb{Q}}^\times.$$

We call the composite homomorphism a *tame Dirichlet character* and say it has *conductor supported in* $\mathcal{C}$.

5.2. ***Von Mangoldt function.*** Let $\mathcal{M} \subset \mathbb{F}_q[t]$ be the subset of monic polynomials, $\mathcal{I} \subset \mathcal{M}$ be the subset of irreducibles, and $\mathcal{I}_d \subset \mathcal{I}$ be the monics of degree d. There is a natural bijection between the finite places $v \in \mathcal{P} \smallsetminus \{\infty\}$ and the elements $\pi \in \mathcal{I}$ since $X = \mathbb{P}^1_t$. We write $v : \mathcal{I} \to \mathcal{P} \smallsetminus \{\infty\}$ for the map sending an irreducible to its corresponding place.

We define the *von Mangoldt function* of ρ to be the map $\Lambda_\rho : \mathcal{M} \to \overline{\mathbb{Q}}_\ell$ given by

$$\Lambda_\rho(f) = \begin{cases} d \cdot a_{\rho,v(\pi),m} & \text{if } f = \pi^m, \text{ where } m \geq 1 \text{ and } \pi \in \mathcal{I}_d, \\ 0 & \text{otherwise.} \end{cases} \tag{5.2.1}$$

Recall $a_{\rho,v(\pi),m}$ is the local trace defined in (3.6.1), and in (3.6.2), it is completely determined by the Euler factor $L(T, \rho_v)$. We also define the *extension by zero* of $\varphi \in \Phi(c)$ to be the map $\varphi_! : \mathcal{M} \to \overline{\mathbb{Q}}_\ell$ given by

$$\varphi_!(f) = \begin{cases} \varphi(f + c\,\mathbb{F}_q[t]) & \text{if } \gcd(f, c) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

It is multiplicative and satisfies

$$\varphi_!(\pi) = \begin{cases} \varphi(\mathrm{Frob}_{v(\pi)}) & \text{if } \pi \nmid c, \\ 0 & \text{otherwise} \end{cases} \quad \text{for } \pi \in \mathcal{I}.$$

There may be other multiplicative maps extending φ, but for our extension we have the identity

$$b_{\rho\otimes\varphi,n} = \sum_{f\in\mathcal{M}_n} \varphi_!(f)\Lambda_\rho(f) \quad \text{for } n \geq 1 \tag{5.2.2}$$

by (4.4.3). We observe that in the special case $\varphi = \mathbf{1}$ this simplifies to

$$b_{\rho,n} = \sum_{A\in\Gamma(c)} \sum_{f\in\mathcal{M}_n(A)} \Lambda_\rho(f), \tag{5.2.3}$$

where $\mathcal{M}_n(A) \subseteq \mathcal{M}_n$ is the subset of f satisfying $f \equiv A \bmod c$.

5.3. ***Sums in random arithmetic progressions.*** Consider the sum

$$S_{n,c}(A) := \sum_{f\in\mathcal{M}_n(A)} \Lambda_\rho(f) \quad \text{for } A \in \Gamma(c) \text{ and } n \geq 1, \tag{5.3.1}$$

where $\Lambda_\rho : \mathcal{M} \to \overline{\mathbb{Q}}_\ell$ is the von Mangoldt function of ρ.

For each n, we would like to regard the sum as a random variable on $\Gamma(c)$, e.g., so that we can speak of the mean and variance. If we were loathe to impose hypotheses on the range of Λ_ρ, we might consider the drastic measure of choosing a field isomorphism $\overline{\mathbb{Q}}_\ell \to \mathbb{C}$. Instead, we fix field embeddings $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$ and $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_\ell$ and suppose the range of Λ_ρ is a subset of $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_\ell$. This allows us to define the elements

$$\mathbb{E}[S_{n,c}(A)] := \frac{1}{\phi(c)} \sum_{A\in\Gamma(c)} S_{n,c}(A), \tag{5.3.2}$$

$$\mathrm{Var}[S_{n,c}(A)] := \frac{1}{\phi(c)} \sum_{A\in\Gamma(c)} \left|\iota(S_{n,c}(A) - \mathbb{E}[S_{n,c}(A)])\right|^2 \tag{5.3.3}$$

in $\overline{\mathbb{Q}}$ and $\mathbb{C}$ respectively.

5.4. ***Coefficients of L-functions.*** Observe that, for each $A_1, A_2 \in \Gamma(c)$, one has

$$\frac{1}{\phi(c)} \sum_{\varphi\in\Phi(c)} \varphi(A_1)\bar{\varphi}(A_2) = \begin{cases} 1 & \text{if } A_1 = A_2, \\ 0 & \text{if } A_1 \neq A_2, \end{cases}$$

and thus by (5.2.2), one has

$$S_{n,c}(A) = \frac{1}{\phi(c)} \sum_{f\in\mathcal{M}_n} \Lambda_\rho(f) \sum_{\varphi\in\Phi(c)} \varphi_!(f)\bar{\varphi}_!(A) = \frac{1}{\phi(c)} \sum_{\varphi\in\Phi(c)} b_{\rho\otimes\varphi,n} \cdot \bar{\varphi}_!(A).$$

Therefore, if we write $\mathbf{1} \in \Phi(c)$ for the trivial character, then (5.3.2) becomes

$$\mathbb{E}[S_{n,c}(A)] = \frac{1}{\phi(c)^2} \sum_{\varphi\in\Phi(c)} b_{\rho\otimes\varphi,n} \sum_{A\in\Gamma(c)} \bar{\varphi}_!(A) = \frac{1}{\phi(c)} b_{\rho,\mathbf{1},n}$$

since, for every $\varphi_1, \varphi_2 \in \Phi(c)$, one has

$$\frac{1}{\phi(c)} \sum_{A \in \Gamma(c)} \varphi_1(A)\bar{\varphi}_2(A) = \begin{cases} 1 & \text{if } \varphi_1 = \varphi_2, \\ 0 & \text{if } \varphi_1 \neq \varphi_2. \end{cases} \tag{5.4.1}$$

In particular, we have the identity

$$S_{n,c}(A) - \mathbb{E}[S_{n,c}(A)] = \frac{1}{\phi(c)} \sum_{\varphi \in \Phi(c)^*} b_{\rho\otimes\varphi,n} \cdot \bar{\varphi}(A), \quad \text{where } \Phi(c)^* = \Phi(c) \setminus \{\mathbf{1}\},$$

and (5.3.3) becomes

$$\mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)^3} \sum_{A \in \Gamma(c)} \sum_{\varphi_1, \varphi_2 \in \Phi(c)^*} b_{\rho\otimes\varphi_1,n} \bar{b}_{\rho\otimes\varphi_2,n} \cdot \bar{\varphi}_{1!}(A)\varphi_{2!}(A) = \frac{1}{\phi(c)^2} \sum_{\varphi \in \Phi(c)^*} |b_{\rho\otimes\varphi,n}|^2$$

by (5.4.1).

In summary, the function $S_{n,c}(A)$ of the random variable A satisfies

$$\mathbb{E}[S_{n,c}(A)] = \frac{1}{\phi(c)} b_{\rho\otimes\mathbf{1},n}, \quad \mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)^2} \sum_{\substack{\varphi \in \Phi(c) \\ \varphi \neq \mathbf{1}}} |\iota(b_{\rho\otimes\varphi,n})|^2. \tag{5.4.2}$$

In order to say anything meaningful about these numbers individually or as q grows, we need to impose additional hypotheses on ρ, e.g., that the Euler factors of $L(T, \rho)$ satisfy a suitable Riemann hypothesis. Doing so will enable us to apply Deligne's theorem and to rewrite the variance in terms of a matrix integral.

6. Purity and weights

Let $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_\ell$ and $\iota : \bar{\mathbb{Q}} \to \mathbb{C}$ be field embeddings. Using these embeddings we can define what it means for a representation such as ρ to be pointwise ι-pure of some weight $w \in \mathbb{R}$. We do so by imposing a Riemann hypothesis on the zeros of each of the Euler factors, i.e., that they embed in $\mathbb{C}$ via ι and lie on a suitable circle centered at the origin. The property is local in that it places constraints on each of the Euler factors, and it does not immediately say anything global. To show that the partial and complete L-functions also satisfy a suitable Riemann hypothesis, one needs Deligne's theorem.

6.1. ***Purity.*** We say a polynomial in $\bar{\mathbb{Q}}_\ell[T]$ is *ι-pure of q-weight w* if and only if it is nonzero and each of its zeros $\alpha \in \bar{\mathbb{Q}}_\ell$ lies in $\bar{\mathbb{Q}}$ and satisfies

$$|\iota(\alpha)|^2 = (1/q)^w.$$

We also say it is *pure of q-weight w* if and only if it is ι-pure of q-weight w for every ι. More generally, we say it is *mixed of q-weights $\leq w$* if and only if it is a product of polynomials, each pure of q-weight $\leq w$.

Remark 6.1.1. Our terminology is unconventional in that we incorporate q; however, we need to make q explicit since we have not said where the polynomial comes from.

Remark 6.1.2. In many applications w is usually rational and often an integer.

6.2. *Riemann hypothesis.* We say the representation $\rho \otimes \varphi$ is *pointwise* (ι-)*pure of weight* w if and only if the Euler factor $L(T^{d_v}, (\rho \otimes \varphi)_v)$ is (ι-)pure of q-weight w for every $v \notin \mathcal{S}$.

Theorem 6.2.1. (Deligne) *If $\rho \otimes \varphi$ is pointwise (ι-)pure of weight w, then the cohomological factors $P_{i,\mathcal{C}}(T, \rho \otimes \varphi)$ are (ι-)mixed of q-weights $\le w + n$ and the factors $P_i(T, \rho \otimes \varphi)$ both lie in $\overline{\mathbb{Q}}[T]$ and are (ι-)pure of q-weight $w + n$.*

Proof. See Theorems 1 and 2 of [Deligne 1980] for the respective assertions about $P_{i,\mathcal{C}}(T, \rho \otimes \varphi)$ and $P_i(T, \rho \otimes \varphi)$ in terms of the middle extension $\mathrm{ME}(\rho \otimes \varphi)$. The theorems are stated in terms of ι, but one can easily deduce the statement for pointwise pure $\rho \otimes \varphi$ by considering all ι simultaneously. □

The following lemma implies every twist $\rho \otimes \varphi$ is pointwise pure if and only if ρ is.

Lemma 6.2.2. *If $\rho = \rho \otimes \mathbf{1}$ is pointwise ι-pure of weight w, then so is $\rho \otimes \varphi$.*

Proof. Observe that $\zeta = \varphi_{\mathcal{C}}(\mathrm{Frob}_v)$ is a root of unity since $\Gamma(c)$ has finite order; hence $\zeta \in \overline{\mathbb{Q}}$ and $|\iota(\zeta)|^2 = 1$. If $v \notin \mathcal{C}$ and if $\alpha \in \overline{\mathbb{Q}}$ is a zero of $L(T, (\rho \otimes \varphi)_v)$, then (4.2.1) implies that α/ζ is a zero of $L(T, \rho_v)$. In particular, $|\alpha|^2 = |\alpha/\zeta|^2 = (1/q^{d_v})^w$; hence $L(T^{d_v}, (\rho \otimes \varphi)_v)$ is ι-pure of q-weight w for almost all v. □

6.3. *Weight bound for missing Euler factors.* Let $\mathcal{F}$ be a middle-extension sheaf on X (e.g., $\mathrm{ME}(\rho \otimes \varphi)$). We say that $\mathcal{F}$ is *pointwise* (ι-)*pure of weight* w if and only if for some dense Zariski open subset $U \subseteq X$ on which $\mathcal{F}$ is lisse, the corresponding representation of $\pi_1(U)$ is pointwise (ι-)pure of weight w. In general, even for U maximal among such U, the complement $Z = X \smallsetminus U$ may be nonempty, and there may be mild degeneration among the zeros of the corresponding Euler factors.

Lemma 6.3.1. *Let $j : U \to X$ be the inclusion of a dense Zariski open subset and $Z = X \smallsetminus U$. If $\mathcal{F}$ is lisse on U and pointwise ι-pure of weight w, then*

$$\det(1 - T\mathrm{Frob}_q \mid H^0(\bar{Z}, j_*\mathcal{F})) = \prod_{z \in Z} L(T^{d_z}, \mathcal{F}_z)$$

is ι-mixed of q-weights $\le w$.

Proof. See [Deligne 1980, 1.8.1]. □

7. Polynomial L-functions

A priori, the partial and complete L-functions are different and rational, that is, a quotient of two polynomials. We suppose that ρ is pointwise ι-pure of known weight so that we can speak of the weights of the zeros and poles of the L-functions. Under suitable additional conditions on φ, the L-functions of $\rho \otimes \varphi$ coincide, are polynomials, *and* are ι-pure of known q-weight. As we explain in the next section, these properties will allow us to associate a conjugacy class of unitary matrices to $\rho \otimes \varphi$.

7.1. ***Semisimplicity.*** Consider an exact sequence of $G_{K,\mathcal{S}}$-modules

$$0 \to V_1 \to V \to V_2 \to 0, \tag{7.1.1}$$

and let $\rho : G_{K,\mathcal{S}} \to \mathrm{GL}(V)$ and $\rho_i : G_{K,\mathcal{S}} \to \mathrm{GL}(V_i)$ for $i = 1, 2$ be the corresponding structure homomorphisms.

A priori, (7.1.1) does not split, but we say ρ is *arithmetically semisimple* if and only if the sequence splits for *every* $G_{K,\mathcal{S}}$-invariant subspace $V_1 \subseteq V$. By Clifford's theorem, the condition implies that ρ is *geometrically semisimple* since $\bar{G}_{K,\mathcal{S}}$ is normal in $G_{K,\mathcal{S}}$ (cf. [Curtis and Reiner 1962, 49.2]): every $\bar{G}_{K,\mathcal{S}}$-invariant subspace of V has a $\bar{G}_{K,\mathcal{S}}$-invariant complement. We also say that ρ is *geometrically simple* if and only if ρ is irreducible and geometrically semisimple.

Lemma 7.1.2. *If ρ is geometrically simple, then so is $\rho \otimes \varphi$.*

Proof. If $W_\varphi \subseteq V_\varphi$ is a $\bar{G}_{K,\mathcal{R}}$-invariant subspace, then $W = W_\varphi \otimes \bar{\varphi}$ is a $\bar{G}_{K,\mathcal{R}}$-invariant subspace. Moreover, if ρ is geometrically simple, then W equals 0 or V; hence W_φ equals 0 or V_φ. □

7.2. ***Invariants and coinvariants.*** We say ρ has *trivial geometric invariants* if and only if the subspace in V of $\bar{G}_{K,\mathcal{S}}$-invariants is zero, and it has *trivial geometric coinvariants* if and only if the quotient space of $\bar{G}_{K,\mathcal{S}}$-coinvariants of V is zero. These properties are equivalent when ρ is geometrically semisimple.

Proposition 7.2.1. *If ρ is pointwise ι-pure, then it is geometrically semisimple, and in particular it has trivial geometric invariants if and only if it has trivial geometric coinvariants.*

Proof. One can rephrase semisimplicity for ρ in terms of semisimplicity for $\mathrm{ME}(\rho)$ (cf. [Beĭlinson et al. 1982, 5.1.7]). It follows that both are geometrically semisimple if ρ is ι-pure (see [Beĭlinson et al. 1982, 5.3.8]), and then the spaces of invariants and coinvariants are isomorphic, so both vanish or neither does. □

Corollary 7.2.2. *If ρ is pointwise ι-pure and has trivial geometric invariants, then $H^i(\bar{X}, \mathrm{ME}(\rho))$ and $H^i_c(\bar{U}, \mathrm{ME}(\rho))$ vanish for $i \neq 1$, and there is an exact sequence*

$$0 \to H^0(\bar{Z}, \mathrm{ME}(\rho)) \to H^1_c(\bar{U}, \mathrm{ME}(\rho)) \to H^1(\bar{X}, \mathrm{ME}(\rho)) \to 0. \tag{7.2.3}$$

Therefore $L(T, \rho) = P_1(T, \rho)$ and $L_{\mathcal{C}}(T, \rho) = P_{1,\mathcal{C}}(T, \rho)$.

Proof. Suppose ρ is pointwise ι-pure and has trivial geometric invariants so that Proposition 7.2.1 implies ρ has trivial geometric coinvariants. We claim $H^i(\bar{X}, \mathrm{ME}(\rho))$ vanishes for $i \neq 1$. The corollary then follows by observing that (B.0.3) simplifies to (7.2.3) and that $H^2_c(\bar{U}, \mathrm{ME}(\rho))$ vanishes by (B.0.4).

The claim is independent of U, so up to shrinking U, we suppose $j^*\mathrm{ME}(\rho)$ is lisse. Then

$$H^0(\bar{X}, \mathrm{ME}(\rho)) = H^0(\bar{U}, \mathrm{ME}(\rho)) \quad \text{and} \quad H^2(\bar{X}, \mathrm{ME}(\rho)) = H^2_c(\bar{U}, \mathrm{ME}(\rho))$$

are the subspace of $\pi_1(\bar{U})$-invariants and (a Tate twist of the) quotient space of $\pi_1(\bar{U})$-coinvariants, respectively, of V by (2.0.2). The claim is also independent of $\mathcal{S}$, so up to replacing $\mathcal{S}$ by a finite superset in $\mathcal{P}$, we suppose ρ factors through a natural quotient $\bar{G}_{K,\mathcal{S}} \twoheadrightarrow \pi_1(\bar{U})$. Then the cohomology spaces in question are the $\overline{G}_{K,\mathcal{S}}$-invariants and $\overline{G}_{K,\mathcal{S}}$-coinvariants of V, which are trivial by hypothesis, so $H^i(\overline{X}, \mathrm{ME}(\rho))$ vanishes for $i \neq 1$ as claimed. □

7.3. *Pure polynomial L-functions.* In this section we present two theorems. They address the partial and complete L-functions of $\rho \otimes \varphi$ respectively. In both cases we focus on necessary and sufficient conditions for the L-function in question to be a polynomial.

Let $\mathbb{A}^1_t[1/c] \subseteq \mathbb{A}^1_t$ be the open complement of the locus $c = 0$. To say that a sheaf $\mathcal{F}$ on $\mathbb{P}^1_t$ is *supported on* $U \subseteq \mathbb{P}^1_t$ means that the stalks of $\mathcal{F}$ vanish over the points of the complement $Z = \mathbb{P}^1_t \setminus U$.

Theorem 7.3.1. *The following are equivalent*:

(i) $M_{\mathcal{C}}(T, \rho) = 1$; *that is*, $\mathrm{ME}(\rho)$ *is supported on* $\mathbb{A}^1_t[1/c]$.

(ii) $L_{\mathcal{C}}(T, \rho)$ *is a polynomial which is ι-pure of q-weight $w + 1$.*

Note, $M_{\mathcal{C}}(T, \rho)$ is the L-function of the restriction of $\mathrm{ME}(\rho)$ to Z, so the former is trivial if and only if the latter is.

Proof. If (i) holds, then the subspace of $I(\infty)$-invariants of V is trivial, so a fortiori, the subspace of $\overline{G}_{K,\mathcal{S}}$-invariants is trivial. Therefore Corollary 7.2.2 implies $L_{\mathcal{C}}(T, \rho)$ equals $L(T, \rho) = P_1(T, \rho)$ and hence Theorem 6.2.1 implies (ii) holds.

If (ii) holds, then $P_{2,\mathcal{C}}(T, \rho)$ divides $P_{1,\mathcal{C}}(T, \rho)$ by (3.4.2). Theorem 6.2.1 implies $P_{2,\mathcal{C}}(T, \rho) = P_2(T, \rho)$ is ι-pure of q-weight $w + 2$, so it is coprime to $P_{1,\mathcal{C}}(T, \rho)$ and hence trivial. Therefore $H^2(\overline{X}, \mathrm{ME}(\rho))$ vanishes, and hence $H^0(\overline{X}, \mathrm{ME}(\rho))$ also vanishes since ρ is geometrically semisimple. That is, ρ has trivial geometric invariants. Moreover, $1/M_{\mathcal{C}}(T, \rho)$ is a polynomial which is ι-mixed of q-weights $\leq w$ by Lemma 6.3.1, while $L(T, \rho)$ is a polynomial which is ι-pure of q-weight w, so Corollary 7.2.2 implies (i) holds. □

Now we turn to the complete L-function.

Theorem 7.3.2. *Suppose $\rho \otimes \varphi$ is pointwise ι-pure of weight w. Then the following assertions are equivalent*:

(i) *The complete L-function $L(T, \rho \otimes \varphi)$ is in $\overline{\mathbb{Q}}(T)$ but not $\overline{\mathbb{Q}}[T]$.*

(ii) *The cohomological factors $P_0(T, \rho \otimes \varphi)$ and $P_2(T, \rho \otimes \varphi)$ are nontrivial polynomials in $\overline{\mathbb{Q}}[T]$.*

(iii) *The cohomological factor $P_2(T, \rho \otimes \varphi)$ is a nontrivial polynomial in $\overline{\mathbb{Q}}[T]$.*

(iv) *The twist $\rho \otimes \varphi$ has nontrivial geometric coinvariants.*

(v) *The twist $\rho \otimes \varphi$ has nontrivial geometric invariants and coinvariants.*

If these assertions are not true, *then*:

(vi) $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ *equals* $P_{1,\mathcal{C}}(T, \rho \otimes \varphi)$ *and is ι-mixed of q-weights $\leq w + 1$.*

(vii) $L(T, \rho \otimes \varphi)$ *is the largest ι-pure factor of q-weight $w + 1$ of* $L_{\mathcal{C}}(T, \rho \otimes \varphi)$.

Proof. First we prove the assertions are equivalent. On one hand, Theorem 6.2.1 implies that the cohomological factors $P_i(T,\rho)$ are relatively prime, so (i) and (ii) are equivalent. Moreover, (ii) and (v) (resp. (iii) and (iv)) are equivalent by (2.0.2) and (3.4.1). On the other hand, Proposition 7.2.1 implies that $P_0(T,\rho\otimes\varphi)$ is trivial if and only if $P_2(T,\rho\otimes\varphi)$ is trivial, so (ii) and (iii) are equivalent.

Now suppose the assertions are not true. On one hand, Corollary 7.2.2 implies

$$L(T,\rho\otimes\varphi)=P_1(T,\rho\otimes\varphi),\quad L_{\mathcal{C}}(T,\rho\otimes\varphi)=P_{1,\mathcal{C}}(T,\rho\otimes\varphi),$$

so both are polynomials as claimed. On the other hand, Theorem 6.2.1 implies $L(T,\rho\otimes\varphi)$ is ι-pure of q-weight $w+1$ and $L_{\mathcal{C}}(T,\rho\otimes\varphi)$ is ι-mixed of q-weights $\le w+1$ since $\rho\otimes\varphi$ is pointwise ι-pure of weight w. Moreover, Lemma 6.3.1 implies that $L_{\mathcal{C}}(T,\rho\otimes\varphi)/L(T,\rho\otimes\varphi)=1/M_{\mathcal{C}}(T,\rho\otimes\varphi)$ is a polynomial which is ι-mixed of q-weights $\le w$, so $L(T,\rho\otimes\varphi)$ is the largest ι-pure factor of $L_{\mathcal{C}}(T,\rho\otimes\varphi)$ of q-weight $w+1$ as claimed. ☐

Remark 7.3.3. Observe that $L_{\mathcal{C}}(T,\rho\otimes\varphi)$ is “usually” a pure polynomial of degree $r_{\varnothing}(\rho)$ (compare Remark 4.3.3).

8. Trichotomy of characters

Fix field embeddings $\overline{\mathbb{Q}}\to\overline{\mathbb{Q}}_\ell$ and $\iota:\overline{\mathbb{Q}}\to\mathbb{C}$. We suppose throughout this section that ρ is pointwise ι-pure of weight w so that we can apply Deligne’s theorem and talk about the weights of the zeros and poles of $L_{\mathcal{C}}(T,\rho\otimes\varphi)$ as φ varies. Having done so, we partition $\Phi(c)$ into three classes of characters based the possible size of the summands of

$$\mathrm{Var}[S_{n,c}(A)]=\frac{1}{\phi(c)^2}\sum_{\varphi\in\Phi(c)\smallsetminus\{\mathbf{1}\}}|\iota(b_{\rho\otimes\varphi,n})|^2. \tag{8.0.1}$$

In our classification, each $\varphi\in\Phi(c)$ is either good or bad (for ρ), and each bad character is either mixed or heavy. On one hand, one can show that most characters are good and that they’re the ones for which we will regard

$$b^*_{\rho\otimes\varphi,n}:=\frac{\iota(b_{\rho\otimes\varphi,n})}{q^{n(1+w)/2}}$$

as the trace of a unitary matrix. This will allow us to approximate the sum in (8.0.1) using a matrix integral. On the other hand, the heavy characters are those for which $|b^*_{\rho\otimes\varphi,n}|^2$ is unbounded as $q\to\infty$, and their number is bounded as $q\to\infty$.

8.1. ***Good versus bad.*** We say that a character $\varphi\in\Phi(c)$ is *good for* ρ if and only if it belongs to the subset

$$\Phi(c)_{\rho\text{ good}}:=\{\varphi\in\Phi(c):L_{\mathcal{C}}(T,\rho\otimes\varphi)=L(T,\rho\otimes\varphi)\in\overline{\mathbb{Q}}[T]\}, \tag{8.1.1}$$

and otherwise we say it is *bad for* ρ and define

$$\Phi(c)_{\rho\text{ bad}}:=\Phi(c)\smallsetminus\Phi(c)_{\rho\text{ good}}.$$

As we will see, this coincides with Katz’s classification of characters in [Katz 2012] (cf. Lemma 10.3.1).

By Theorem 7.3.2, the good characters are precisely those for which the partial L-function $L_{\mathcal{C}}(T, \rho\otimes\varphi)$ has three properties: it is identical to the polynomial

$$P_{1,\mathcal{C}}(T,\rho) = \det\bigl(1 - T\,\mathrm{Frob}_q \mid H^1_c(\bar{\mathbb{A}}^1_t[1/c], \mathrm{ME}(\rho\otimes\varphi))\bigr),$$

it has degree $R = r_{\mathcal{C}}(\rho)$, and it is ι-pure of q-weight $w+1$. Equivalently, they are the characters for which the normalized L-function

$$L^*_{\mathcal{C}}(T,\rho\otimes\varphi) = L_{\mathcal{C}}(T/(\sqrt{q})^{1+w}, \rho\otimes\varphi) \tag{8.1.2}$$

is a polynomial and ι-pure of q-weight zero.

In particular, if $\mathrm{std}: U_R(\mathbb{C}) \to \mathrm{GL}_R(\mathbb{C})$ is the inclusion $U_R(\mathbb{C}) \subseteq \mathrm{GL}_R(\mathbb{C})$, then for each good φ, there is a unique conjugacy class

$$\theta_{\rho,\varphi} \subset U_R(\mathbb{C}) \subseteq \mathrm{GL}_R(\mathbb{C})$$

such that $\iota(L^*_{\mathcal{C}}(T,\rho\otimes\varphi))$ equals the characteristic polynomial of $\mathrm{std}(\theta_{\rho,\varphi})$. Therefore, from the identity

$$T\frac{d}{dT}\iota(L^*_{\mathcal{C}}(T,\rho\otimes\varphi)) = \sum_{n=1}^{\infty} b^*_{\rho\otimes\varphi,n}T^n \tag{8.1.3}$$

one deduces that

$$b^*_{\rho\otimes\varphi,n} = -\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi})) \quad \text{for } \varphi\in\Phi(c)_{\rho\,\mathrm{good}} \tag{8.1.4}$$

and $n \geq 1$.

8.2. ***Equidistributed matrices.*** If we combine (8.0.1) with (8.1.4), then

$$\frac{\phi(c)}{q^{n(1+w)}}\mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)}\sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{good}}} |\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2 + \frac{1}{\phi(c)}\sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{bad}}} |\iota(b^*_{\rho\otimes\varphi,n})|^2. \tag{8.2.1}$$

Definition 8.2.2. Let $\mathbb{K} \subseteq U_R(\mathbb{C})$ be a compact reductive subgroup, say a maximal compact subgroup of a reductive subgroup $G(\mathbb{C}) \subseteq \mathrm{GL}_R(\mathbb{C})$. The multiset

$$\Theta_{\rho,q} := \{\theta_{\rho,\varphi} : \varphi\in\Phi(c)_{\rho\,\mathrm{good}}\} \subseteq U_R(\mathbb{C})$$

becomes equidistributed in $\mathbb{K}$ *as* $q\to\infty$ if and only if it satisfies:

(i) $\mathbb{K}\cap\theta$ is nonempty, for any $\theta\in\Theta_{\rho,q}$ and any q.

(ii) For *any* continuous central function $f:\mathbb{K}\to\mathbb{C}$, one has

$$\lim_{q\to\infty}\frac{1}{|\Phi(c)^*_{\rho\,\mathrm{good}}|}\sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{good}}} f(\theta_{\rho,\varphi}) = \int_{\mathbb{K}} f(\theta)\,d\theta, \tag{8.2.3}$$

where $d\theta$ is probability Haar measure on $\mathbb{K}$.

The general theory of Katz tells us that, in favorable situations, some such $\mathbb{K}$ exists and is unique up to conjugation.

Remark 8.2.4. The Peter–Weyl theorem implies that proving 8.2.2(ii) holds is equivalent to proving that (8.2.3) holds for every f of the form $f = \mathrm{Tr} \circ \Lambda$, where

$$\Lambda : \mathbb{K} \to \mathrm{GL}_{\dim(\Lambda)}(\mathbb{C})$$

is a finite-dimensional representation. One may even restrict to irreducible representations.

8.3. *Refining bad: mixed versus heavy.* There are two ways a character can be bad:

(i) either $L(T, \rho \otimes \varphi)$ is not a polynomial in $\overline{\mathbb{Q}}(T)$;

(ii) or $L(T, \rho \otimes \varphi)$ and $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ are polynomials but not equal to each other in $\overline{\mathbb{Q}}[T]$.

What distinguishes the first case from the second is that $\iota(L(T, \rho \otimes \varphi))$ has poles some of which have excessive weight. More precisely, if the factor $P_2(T, \rho \otimes \varphi)$ of the denominator of $L(T, \rho \otimes \varphi)$ is nontrivial, then it ι-mixed of q-weights $\leq w + 1$ but not ι-mixed of q-weights $\leq w$ (cf. Theorem 7.3.2).

Definition 8.3.1. We say that φ is *heavy for* ρ (or ρ*-heavy*) if and only if it lies in the subset

$$\Phi(c)_{\rho\,\text{heavy}} := \{\varphi \in \Phi(c)_{\rho\,\text{bad}} : L(T, \rho \otimes \varphi) \notin \overline{\mathbb{Q}}[T]\}.$$

Otherwise, we say that φ is *mixed for* ρ (or ρ*-mixed*) to mean it lies in the subset

$$\Phi(c)_{\rho\,\text{mixed}} := \Phi(c)_{\rho\,\text{bad}} \smallsetminus \Phi(c)_{\rho\,\text{heavy}}.$$

Equivalently, φ is mixed for ρ if and only if $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ is a polynomial which is ι-mixed of q-weights $\leq w + 1$ but not ι-pure of q-weight $w + 1$.

Lemma 8.3.2. *Suppose ρ is geometrically simple and pointwise ι-pure and $\varphi \in \Phi(c)$. Then φ is heavy for ρ if and only if $\rho \otimes \varphi$ is geometrically isomorphic to the trivial representation.*

Proof. The essential point is that since $\rho \otimes \varphi$ is geometrically simple, the quotient space of geometric coinvariants $(V_\varphi)_{\overline{G}_{K,\mathcal{R}}}$ either vanishes or equals V_φ. The former occurs if and only if $\rho \otimes \varphi$ is geometrically isomorphic to the trivial representation, so the lemma follows from Theorem 7.3.2. □

Corollary 8.3.3. *Suppose ρ is geometrically simple and pointwise ι-pure, and let $r = \dim(V)$. Then $\Phi(c)_{\rho\,\text{heavy}} \subseteq \{\mathbf{1}\}$ if and only if one of the following hold:*

(i) $r > 1$.

(ii) $r = 1$ *and ρ is geometrically isomorphic to the trivial representation.*

(iii) $r = 1$ *and ρ is not geometrically isomorphic to a Dirichlet character in $\Phi(c)$.*

Moreover, $\Phi(c)_{\rho\,\text{heavy}} = \{\mathbf{1}\}$ if and only if (ii) holds.

Proof. Let $\varphi \in \Phi(c)$. Lemma 8.3.2 implies that φ is heavy for ρ if and only if $\rho \otimes \varphi$ is geometrically isomorphic to the trivial representation (and hence $r = 1$). By the contrapositive, φ is not heavy for ρ if and only if $r > 1$ or ρ is not geometrically isomorphic to $1/\varphi$. Therefore (i) or (iii) holds if and only if $\Phi(c)_{\rho\,\text{heavy}}$ is empty, and (ii) holds if and only if $\Phi(c)_{\rho\,\text{heavy}} = \{\mathbf{1}\}$. □

9. Variance revisited

We have yet to make precise what we mean when we say that most characters are good or that most bad characters are mixed. Nonetheless, the following theorem shows how we can express the $\mathrm{Var}[S_{n,c}(A)]$ using our trichotomy of characters.

Theorem 9.0.1. *Let $\mathbb{K} \subseteq U_R(\mathbb{C})$ be a compact reductive subgroup and $d\theta$ be its Haar measure. Suppose that ρ is pointwise ι-pure of weight w, that $\Theta_{\rho,q}$ is equidistributed in $\mathbb{K}$ as $q \to \infty$, and that $\Phi(c)_{\rho\,\mathrm{heavy}} \subseteq \{\mathbf{1}\}$. Then*

$$\frac{\phi(c)}{q^{n(1+w)}} \cdot \mathrm{Var}[S_{n,c}(A)] = \frac{|\Phi(c)_{\rho\,\mathrm{good}}|}{|\Phi(c)|} \int_{\mathbb{K}} |\mathrm{Tr}(\theta^n)|^2\, d\theta + O\left(\frac{|\Phi(c)_{\rho\,\mathrm{mixed}} \setminus \{\mathbf{1}\}|}{|\Phi(c)|}\right)$$

as $q \to \infty$.

The proof is in Section 9.2.

Remark 9.0.2. Later we will prove

$$|\Phi(c)_{\rho\,\mathrm{good}}| \sim |\Phi(c)|, \quad |\Phi(c)_{\rho\,\mathrm{mixed}} \setminus \{\mathbf{1}\}| = O(|\Phi(c)|/q).$$

See Corollaries 10.3.2 and 10.3.3.

Remark 9.0.3. One can also show that

$$\int_{U_R(\mathbb{C})} |\mathrm{Tr\,std}(\theta^n)|^2\, d\theta = \min\{n, R\}. \tag{9.0.4}$$

See[1] [Diaconis and Evans 2001, Theorem 1].

9.1. *Archimedean bounds.*

Lemma 9.1.1. *If M is an invertible $d \times d$ matrix with coefficients in $\overline{\mathbb{Q}}_\ell$ and if $\det(1 - M\,T)$ is mixed of q-weights $\leq w$, then $\mathrm{Tr}(M) \in \overline{\mathbb{Q}}$ and $|\iota(\mathrm{Tr}(M))|^2 \leq dq^w$ for every field embedding $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$.*

Proof. If M is invertible and $\psi(T) = \det(1 - M\,T)$ is mixed, there exist $\beta_1, \ldots, \beta_d \in \overline{\mathbb{Q}}^\times$ such that

$$\psi(T) = \prod_{i=1}^{d} (1 - \beta_i T) = 1 - \mathrm{Tr}(M) \cdot T + \cdots + (-1)^d \cdot \det(M) \cdot T^d$$

and such that $\mathrm{Tr}(M) = \beta_1 + \cdots + \beta_m$ also lies in $\overline{\mathbb{Q}}$. Therefore, if $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$ is a field embedding, then

$$|\mathrm{Tr}(M)|^2 = \left|\sum_{i=1}^{d} \iota(\beta_i)\right|^2 \leq \sum_{i=1}^{d} |\iota(\beta_i)|^2 = dq^w$$

as claimed. □

[1] The reference [Diaconis and Shahshahani 1994, Theorem 2] is sometimes used, but as explained in [Diaconis and Evans 2001], the theorem is incorrectly stated.

Lemma 9.1.2. *Suppose ρ is pointwise ι-pure of weight w and $\varphi \in \Phi(c)$. If φ is heavy for ρ, then $|b^*_{\rho\otimes\varphi,n}|^2 = O(q^n)$, and otherwise $|b^*_{\rho\otimes\varphi,n}|^2 = O(1)$. Moreover, the bounds assume n tends to infinity and the implied constants depend only on ρ.*

Proof. Consider the Tate twist

$$\mathcal{F} := \mathrm{ME}(\rho\otimes\varphi)\otimes\overline{\mathbb{Q}}_\ell((1+w)/2).$$

It is pointwise ι-pure of weight -1 since $\mathcal{F}$ is pointwise ι-pure of weight w, and its partial L-function is $L^*_C(T,\rho\otimes\varphi)$. Therefore

$$b^*_{\rho\otimes\varphi,n} = -\mathrm{Tr}(\mathrm{Frob}^n_q \mid H^1_c(\bar{\mathbb{A}}^1_t[1/c],\mathcal{F})) + \mathrm{Tr}(\mathrm{Frob}^n_q \mid H^2_c(\bar{\mathbb{A}}^1_t[1/c],\mathcal{F}))$$

by (8.1.3). Moreover, the second term on the right vanishes unless φ is heavy, and

$$\left|\iota\big(\mathrm{Tr}(\mathrm{Frob}^n_q \mid H^i_c(\bar{\mathbb{A}}^1_t[1/c],\mathcal{F}))\big)\right|^2 = O(q^{n(i-1)})$$

by Theorem 6.2.1 and Lemma 9.1.1. □

9.2. *Proof of Theorem 9.0.1.* By (8.2.1) we have

$$\frac{\phi(c)}{q^{n(1+w)}}\mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)}\sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{good}}}|\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2 + \frac{1}{\phi(c)}\sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{bad}}}|\iota(b^*_{\rho\otimes\varphi,n})|^2$$

for any $S\subseteq\Phi(c)$.

On one hand, by (8.2.3) we have

$$\lim_{q\to\infty}\frac{1}{\phi(c)}\sum_{\substack{\varphi\in\Phi(c)_{\rho\,\mathrm{good}}\\ \varphi\neq\mathbf{1}}}|\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2 = \frac{|\Phi(c)_{\rho\,\mathrm{good}}|}{|\Phi(c)|}\int_{U_R(\mathbb{C})}|\mathrm{Tr}(\theta^n)|^2\,d\theta.$$

On the other hand, by Lemma 9.1.2 we have

$$\begin{aligned}\frac{1}{\phi(c)}\sum_{\substack{\varphi\in\Phi(c)_{\rho\,\mathrm{bad}}\\ \varphi\neq\mathbf{1}}}|\iota(b^*_{\rho\otimes\varphi,n})|^2 &= \frac{1}{|\Phi(c)|}\sum_{\substack{\varphi\in\Phi(c)_{\rho\,\mathrm{mixed}}\\ \varphi\neq\mathbf{1}}}O(1) + \frac{1}{|\Phi(c)|}\sum_{\substack{\varphi\in\Phi(c)_{\rho\,\mathrm{heavy}}\\ \varphi\neq\mathbf{1}}}O(q^n)\\ &= \frac{|\Phi(c)_{\rho\,\mathrm{mixed}}\smallsetminus\{\mathbf{1}\}|}{|\Phi(c)|}\cdot O(1) + \frac{|\Phi(c)_{\rho\,\mathrm{heavy}}\smallsetminus\{\mathbf{1}\}|}{|\Phi(c)|}\cdot O(q^n),\end{aligned}$$

where the implied constants are independent of φ, and the last term vanishes if $\Phi(c)_{\rho\,\mathrm{heavy}}\subseteq\{\mathbf{1}\}$.

Remark 9.2.1. While we do not need the result, we point out that (5.4.2) and Lemma 9.1.2 imply

$$\frac{\phi(c)}{q^{n(1+w)}}\cdot|\iota(\mathbb{E}[S_{n,c}(A)])|^2 = |b^*_{\rho,n}|^2 = O(1)\quad\text{for } q\to\infty,$$

when ρ is pointwise ι-pure of weight w and φ is not heavy for ρ.

10. Big monodromy implies equidistribution

In principle, one could try to exhibit equidistribution for all of $\Theta_{\rho,q}$ at once. Instead we follow Katz and (try to) prove simultaneous and uniform equidistribution for certain one-parameter families of characters. More precisely, we partition $\Phi(c)$ into cosets $\varphi\Phi(u)^{\nu}$ of a subgroup $\Phi(u)^{\nu}$ (defined in Section 10.2) and (try to) prove equidistribution for characters in

$$\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}} = \varphi\Phi(u)^{\nu} \cap \Phi(c)_{\rho\,\mathrm{good}}. \tag{10.0.1}$$

Doing so for a single coset is equivalent to showing that an associated monodromy group we denote by $\mathcal{G}_{\mathrm{geom}}(\rho, \varphi\Phi(u)^{\nu})$ equals $\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$. See Sections 10.2, 10.3, and 10.4.

The monodromy group is an algebraic subgroup of $\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$. We say the former is *big* if and only if it equals the latter, and we write

$$\Phi(c)_{\rho\,\mathrm{big}} = \{\varphi \in \Phi(c) : \mathcal{G}_{\mathrm{geom}}(\rho, \varphi\Phi(u)^{\nu}) \text{ is big}\} \tag{10.0.2}$$

for the subset of big characters. We say that the *Mellin transform* of ρ has *big monodromy* in $\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$ if and only if

$$|\Phi(c)_{\rho\,\mathrm{big}}| \sim |\Phi(c)| \quad \text{as } n \to \infty, \tag{10.0.3}$$

where $q = q_0^n$ for prime power q_0. We show that it implies $\Theta_{\rho,q}$ becomes equidistributed in $U_R(\mathbb{C})$. By Remark 8.2.4, it suffices to prove the following theorem.

Theorem 10.0.4. *Suppose ρ is pointwise ι-pure and φ is in $\Phi(c)_{\rho\,\mathrm{big}}$. Let $\Lambda : U_R(\mathbb{C}) \to \mathrm{GL}_{\dim(\Lambda)}(\mathbb{C})$ be a finite-dimensional representation. If $q = q_0^n$ is sufficiently large, then*

$$\frac{1}{|\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}|} \sum_{\varphi' \in \varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}} \mathrm{Tr}\,\Lambda(\theta_{\rho,\varphi'}) = \int_{U_R(\mathbb{C})} \mathrm{Tr}\,\Lambda(\theta)\,d\theta + o(1) \quad \text{as } n \to \infty, \tag{10.0.5}$$

and the implicit constant depends only on $r = \dim(V)$ and $\dim(\Lambda)$. In particular, if the Mellin transform of ρ has big monodromy, then $\Theta_{\rho,q}$ becomes equidistributed in $U_R(\mathbb{C})$ as $n \to \infty$.

The proof is in Section 10.5.

Remark 10.0.6. Observe that the q-weight w of ρ plays no role in the statement of the theorem. This is because we factored out the weight in the normalization (8.1.2). Another way to achieve the same renormalization is to replace ρ by an appropriate Tate twist so that $w = -1$ and $L^*_{\mathcal{C}}(T, \rho \otimes \varphi) = L_{\mathcal{C}}(T, \rho \otimes \varphi)$.

10.1. ***Reduction to*** $\mathbb{G}_m$**.** Recall $X = \mathbb{P}^1_t$ and $c \in \mathbb{F}_q[t] \subset K$ is monic and square-free. Let $\mathbb{P}^1_u$ denote the projective u-line and $U_c = X \smallsetminus \mathcal{C}$. Moreover, let L equal $\mathbb{F}_q(u) \to K$, the $\mathbb{F}_q$-linear field embedding generated by $u \mapsto c$ and corresponding to the finite cover $c : X \to \mathbb{P}^1_u$. The morphism has generic degree $n = \deg(c)$ and is generically étale since it has n distinct points over $u = 0$. It also fits in a commutative diagram

$$\begin{array}{ccccc} U_c & \longrightarrow & X & \longleftarrow & \mathcal{C} \\ \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle c} \\ \mathbb{G}_m & \longrightarrow & \mathbb{P}^1_u & \longleftarrow & \mathcal{C}' = \{0, \infty\} \end{array}$$

where the outer vertical maps are finite morphisms.

Let $\mathcal{R}$ be a finite set of places in L including those lying under $\mathcal{C} \cup \mathcal{S}$ and those which ramify in K/L, and let $U' \subset \mathbb{P}^1_u$ be the corresponding open complement. Then for each $\varphi \in \Phi(c)$, we have an induced representation

$$\mathrm{Ind}(\rho \otimes \varphi) : G_{L,\mathcal{R}} \to \mathrm{GL}(\mathrm{Ind}(V_\varphi)),$$

where $\mathrm{Ind}(V_\varphi)$ is a vector space of dimension $n \cdot \dim(V_\varphi)$. The representation is the geometric generic fiber of $\mathcal{F} = \mathbb{Q}_* \mathrm{ME}(\rho \otimes \varphi)$, and the hypotheses on $\mathcal{R}$ imply $\mathcal{F}$ is lisse on $U' \subset \mathbb{P}^1_u$. (In fact, Proposition A.0.4 implies $\mathcal{F}$ and $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi))$ are isomorphic on U'.). In particular, if $\bar{u}$ is a geometric closed point of $\mathbb{P}^1_u$, that is, the image of a closed point of $\overline{X}$, and if

$$c^{-1}(\bar{u}) = \{\bar{t}_1, \ldots, \bar{t}_m\} \subset \overline{X},$$

then the various geometric stalks satisfy

$$(\mathbb{Q}_*\mathcal{F})_{\bar{u}} = H^0(\bar{u}, \mathbb{Q}_*\mathcal{F}) = \bigoplus_{i=1}^{m} H^0(\bar{t}_i, \mathcal{F}) = \bigoplus_{i=1}^{m} \mathcal{F}_{\bar{t}_i} \tag{10.1.1}$$

as $\overline{\mathbb{Q}}_\ell$-vector spaces (cf. [Milne 1980, II.3.1(e) and II.3.5(c)]). Thus if $\mathcal{F}$ is supported on U_c, then $\mathbb{Q}_*\mathcal{F}$ is supported on $\mathbb{G}_m$.

Lemma 10.1.2. *If ρ is pointwise ι-pure of weight w, then so is* $\mathrm{Ind}(\rho \otimes \varphi)$.

Proof. Let $\bar{v}$ be a place in L not lying in $\mathcal{R}$, and let $v \mid \bar{v}$ denote any place in K lying over $\bar{v}$. Then

$$L(T^{\deg(\bar{v})}, \mathrm{Ind}(\rho \otimes \varphi)_{\bar{v}}) = \prod_{v \mid \bar{v}} L(T^{\deg(v)}, (\rho \otimes \varphi)_v)$$

by (10.1.1). In particular, Lemma 6.2.2 implies the factors on the right are ι-pure of q-weight w, so the left side is also ι-pure of q-weight w. □

The functorial properties of $\mathbb{Q}_*$ yield canonical isomorphisms

$$H^i(\overline{X}, \mathcal{F}) = H^i(\overline{X}, \mathbb{Q}_*\mathcal{F}) \quad \text{and} \quad H^i_c(\overline{U}_c, \mathcal{F}) = H^i_c(\overline{\mathbb{G}}_m, \mathbb{Q}_*\mathcal{F}) \tag{10.1.3}$$

for each i. For example, $\mathbb{Q}_*$ is exact since c is a finite map, so the first identity in (10.1.3) is a consequence of the (trivial) Leray spectral sequence (cf. [Milne 1980, II.3.6 and III.1.18]). In particular, the identities (3.4.2), (3.4.4), and (10.1.3) jointly imply that

$$L(T, \mathrm{ME}(\rho \otimes \varphi)) = L(T, \mathbb{Q}_*\mathrm{ME}(\rho \otimes \varphi)) \quad \text{and} \quad L_{\mathcal{C}}(T, \mathrm{ME}(\rho \otimes \varphi)) = L_{\mathcal{C}'}(T, \mathbb{Q}_*\mathrm{ME}(\rho \otimes \varphi)) \tag{10.1.4}$$

for $\varphi \in \Phi(c)$.

10.2. ***One-parameter families.*** Recall $c \in \mathbb{F}_q[t] \subset K$ is monic and square-free and $\mathbb{F}_q(u) \to K$ is the function-field embedding which sends u to c. The norm map $K \to \mathbb{F}_q(u)$ is multiplicative and sends $t-a$ to $(-1)^n u$ for $n = \deg(c)$ and $a \in \mathbb{F}_q$ a zero of c. It also induces homomorphisms

$$\nu : \Gamma(c) \to \Gamma(u) \quad \text{and} \quad \nu^* : \Phi(u) \to \Phi(c),$$

where

$$\Gamma(u) := (\mathbb{F}_q[u]/u\mathbb{F}_q[u])^\times \quad \text{and} \quad \Phi(u) := \mathrm{Hom}(\Gamma(u), \overline{\mathbb{Q}}_\ell^\times)$$

(see [Katz 2013, §2]). In particular, ν is surjective, so its dual ν^* is injective, and we can identify $\Phi(u)$ with its image $\Phi(u)^\nu$. Moreover, as the following lemma shows, twisting by elements of the coset $\varphi\Phi(u)^\nu$ is the "same" as twisting by elements of $\Phi(u)$.

Lemma 10.2.1. *Let $\varphi \in \Phi(c)$ and $\alpha \in \Phi(u)$:*

(i) $\mathbb{Q}_*\mathrm{ME}(\rho \otimes \varphi)$ *is isomorphic to* $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi))$.

(ii) $\mathbb{Q}_*\mathrm{ME}(\rho \otimes \varphi\alpha^\nu)$ *is isomorphic to* $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi) \otimes \alpha)$.

Proof. By [Katz 2002, 3.3.1], $\mathbb{Q}_*\mathrm{ME}(\rho \otimes \varphi)$ is a middle extension, and since it is generically equal to the middle-extension sheaf $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi))$, Proposition 3.3.3 implies part (i) holds.

Up to replacing ρ by $\rho \otimes \varphi$, we suppose without loss of generality that $\varphi = \mathbf{1}$. Let $T \subseteq \mathbb{P}^1_t$ be a dense Zariski open subset and $U = c(T)$. Suppose that $U \subseteq \mathbb{G}_m$ so that $c^*\mathrm{ME}(\alpha)$ is lisse on T, that the restriction $c : T \to U$ is étale, and that $\mathrm{ME}(\rho)$ is lisse on T. Let $i : T \to \mathbb{P}^1_t$ and $j : U \to \mathbb{P}^1_u$ be the inclusions. We have

$$\mathrm{ME}(\rho \otimes \alpha^\nu) \simeq i_*i^*(\mathrm{ME}(\rho \otimes \alpha^\nu)) \simeq i_*i^*(\mathrm{ME}(\rho) \otimes \mathrm{ME}(\alpha^\nu)) \simeq i_*i^*(\mathrm{ME}(\rho) \otimes c^*\mathrm{ME}(\alpha))$$

since each of the sheaves is a middle extension and lisse on T. Therefore the projection formula implies

$$\mathbb{Q}_*\mathrm{ME}(\rho \otimes \alpha^\nu) \simeq \mathbb{Q}_*(i_*i^*(\mathrm{ME}(\rho) \otimes c^*\mathrm{ME}(\alpha))) \simeq j_*j^*(\mathbb{Q}_*\mathrm{ME}(\rho) \otimes \mathrm{ME}(\alpha))$$

since each of the sheaves is lisse on U and a middle extension on $\mathbb{P}^1_u$ (by part (i)) and since $c : T \to U$ is étale. Finally,

$$j_*j^*(\mathbb{Q}_*\mathrm{ME}(\rho) \otimes \mathrm{ME}(\alpha)) \simeq j_*j^*(\mathrm{ME}(\mathrm{Ind}(\rho)) \otimes \mathrm{ME}(\alpha)) \simeq \mathrm{ME}(\mathrm{Ind}(\rho) \otimes \alpha)$$

and thus part (ii) holds. □

10.3. ***Counting good characters.*** We say a character $\varphi \in \Phi(c)$ is *good for* ρ or simply *good* if and only if it lies in the subset $\Phi(c)_{\rho\,\mathrm{good}}$ defined in (8.1.1). When $c = t$ and thus $\mathbb{A}^1_t[1/c] = \mathbb{G}_m$, our notion of good coincides with that of [Katz 2012, Chapter 3]. For general c, the following lemma shows how our notion relates to his via $\mathbb{Q}_*$:

Lemma 10.3.1. *If $\varphi \in \Phi(c)$ and $\alpha \in \Phi(u)$, then the following are equivalent*:

(i) $\varphi\alpha^\nu$ *is good for* ρ.

(ii) $\mathrm{ME}(\rho \otimes \varphi\alpha^\nu)$ *is supported on* $\mathbb{A}^1_t[1/c]$.

(iii) $\mathrm{ME}(\mathrm{Ind}(\rho\otimes\varphi)\otimes\alpha)$ *is supported on* $\mathbb{G}_m$.

(iv) $\alpha\in\Phi(u)$ *is good for* $\mathbb{Q}_*\mathrm{ME}(\rho\otimes\varphi)$.

Proof. Theorem 7.3.1 implies the first conditions (i) and (ii) are equivalent. Conditions (ii) and (iii) are equivalent by the identity in (10.1.1) for $\bar{u}\in\mathcal{C}'$. Finally, taking $c=t$ and applying the equivalence of (i) and (ii) yields the equivalence of (iii) and (iv). □

Let $\Phi(c)_{\rho\,\mathrm{bad}}$ be the complement $\Phi(c)\smallsetminus\Phi(c)_{\rho\,\mathrm{good}}$ and $\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{bad}}=\Phi(c)_{\rho\,\mathrm{bad}}\cap\varphi\Phi(u)^{\nu}$.

Corollary 10.3.2. $$|\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{bad}}|\le(1+\deg(c))\cdot\mathrm{rank}(\rho).$$

Proof. If $\varphi\in\Phi(c)_{\rho\,\mathrm{bad}}$, then φ it coincides with some tame character of ρ at some $v\in\mathcal{C}$, and there are at most $(1+\deg(c))\cdot\mathrm{rank}(\rho)$ such characters. Compare [Katz 2012, pp. 12–13]. □

Corollary 10.3.3. $$|\Phi(c)_{\rho\,\mathrm{good}}|\sim|\Phi(c)|\quad \textit{as } q\to\infty.$$

Proof. Observe that Corollary 10.3.2 implies

$$|\Phi(c)|-|\Phi(c)_{\rho\,\mathrm{good}}|=|\Phi(c)_{\rho\,\mathrm{bad}}|=\sum_{\varphi\Phi(u)^{\nu}}|\Phi(u)^{\nu}_{\rho\,\mathrm{bad}}|\le O(|\Phi(c)|/|\Phi(u)^{\nu}|)=o(|\Phi(c)|)$$

as $q\to\infty$. □

One can also show that

$$|\Phi(c_0)_{\rho\,\mathrm{good}}|\sim|\Phi(c_0)|\quad\text{as } q\to\infty \tag{10.3.4}$$

for any monic divisor $c_0\mid c$.

10.4. *Tannakian monodromy groups.* Suppose $c=t$ and thus $\mathcal{C}'=\mathcal{C}=\{0,\infty\}$ and $\Phi(u)=\Phi(c)$. Suppose moreover that ρ is geometrically simple and $\dim(V)>1$ so that no geometric subquotient of $\mathrm{ME}(\rho)$ is a Kummer sheaf.

Let $j:\mathbb{G}_m\to\mathbb{P}^1_u$ be the inclusion, let $j_0:\mathbb{G}_m\to\mathbb{A}^1_u$ be the inclusion map, and for each $\alpha\in\Phi(u)$, let

$$\omega_\alpha(\mathrm{ME}(\rho))=H^1_c(\bar{\mathbb{A}}^1_u,\,j_{0*}j^*\mathrm{ME}(\rho\otimes\alpha)).$$

It is a $G_{\mathbb{F}_q}$-module; that is, Frob_q acts functorially, and it corresponds to a well-defined conjugacy class of elements $\mathrm{Frob}_{\mathbb{F}_q,\alpha}\subset\mathrm{GL}(\omega(\mathrm{ME}(\rho)))$, where $\omega(\mathrm{ME}(\rho))=\omega_{\mathbf{1}}(\mathrm{ME}(\rho))$ and $\mathbf{1}\in\Phi(u)$ is the trivial character. Moreover, if α is good, then

$$\omega_\alpha(\mathrm{ME}(\rho))=H^1_c(\bar{\mathbb{G}}_m,\mathrm{ME}(\rho\otimes\alpha)),$$

and in particular

$$L_{\mathcal{C}}(T,\rho\otimes\alpha)=\det(1-\mathrm{Frob}_\alpha T\mid\omega(\mathrm{ME}(\rho))).$$

In a way we will not make precise here, the Frob_α "generate" ℓ-adic reductive subgroups

$$\mathcal{G}_{\mathrm{geom}}(\rho,\Phi(u)^{\nu})\subseteq\mathcal{G}_{\mathrm{arith}}(\rho,\Phi(u)^{\nu})\subseteq\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$$

which are well-defined up to conjugacy. They are fundamental groups of certain Tannakian categories, and we call them the *Tannakian monodromy groups of* ρ. See Appendix D for details. We say the Mellin transform of ρ has *big Tannakian monodromy* if and only if $\mathcal{G}_{\mathrm{geom}}(\rho,\Phi(u)^{\nu}) = \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$.

For general c and $\varphi \in \Phi(c)$, we write

$$\mathcal{G}_{\mathrm{geom}}(\rho,\varphi\Phi(u)^{\nu}) \subseteq \mathcal{G}_{\mathrm{arith}}(\rho,\varphi\Phi(u)^{\nu}) \subseteq \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$$

for the Tannakian monodromy groups of $\mathrm{Ind}(\rho\otimes\varphi)$, and we say that the Mellin transform of $\rho\otimes\varphi$ has *big Tannakian monodromy* if and only if $\mathcal{G}_{\mathrm{geom}}(\rho,\varphi\Phi(u)^{\nu}) = \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$. Now the action of Frob_q on $\omega_\alpha(\mathrm{ME}(\rho\otimes\varphi))$ corresponds to a well-defined conjugacy class $\mathrm{Frob}_{\mathbb{F}_q,\alpha} \subset \mathcal{G}_{\mathrm{arith}}(\rho,\varphi\Phi(u)^{\nu})$.

10.5. ***Proof of Theorem 10.0.4.*** We may suppose without loss of generality that Λ is irreducible since it is semisimple and $\mathrm{Tr}(\Lambda_1\oplus\Lambda_2) = \mathrm{Tr}(\Lambda_1)+\mathrm{Tr}(\Lambda_2)$ for any representations Λ_1, Λ_2. Moreover, we have the Schur orthogonality relations

$$\int_{U_R(\mathbb{C})} \mathrm{Tr}\,\Lambda(\theta)\,d\theta = \begin{cases} 1 & \text{if } \Lambda \text{ is the trivial representation,}\\ 0 & \text{otherwise,}\end{cases}$$

so to prove (10.0.5) we must show that

$$\frac{1}{|\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}|}\sum_{\varphi'\in\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}} \mathrm{Tr}\,\Lambda(\theta_{\rho,\varphi'}) = \begin{cases} 1 & \text{if } \Lambda \text{ is the trivial representation,}\\ o(1) & \text{otherwise,}\end{cases} \tag{10.5.1}$$

when q is large.

If q is sufficiently large, then Corollary 10.3.2 implies

$$|\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{bad}}| \le (1+\deg(c))\cdot\mathrm{rank}(\rho) < |\varphi\Phi(u)^{\nu}|$$

and thus $\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}$ is nonempty. In particular, the left side of (10.5.1) is defined for large q, and it is identically 1 when Λ is the trivial representation. On the other hand, if Λ is nontrivial and if q is bigger than $(|\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{bad}}|+1)^2$, then [Katz 2012, 7.5] implies

$$\frac{1}{|\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}|}\left|\sum_{\varphi'\in\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}} \mathrm{Tr}\,\Lambda(\theta_{\rho,\varphi'})\right| \le (\dim(V)+\dim(\Lambda))\left(\frac{1}{\sqrt{q}}+\frac{1}{\sqrt{q}^3}\right). \tag{10.5.2}$$

Thus (10.5.1) holds, as claimed, and the implicit constant depends only on r and $\dim(\Lambda)$.

To complete the proof of the theorem we must show that $\Theta_{\rho,q}$ becomes equidistributed in $U_R(\mathbb{C})$. We observe that

$$|\mathrm{Tr}\,\Lambda(\theta_{\rho,\varphi'})| \le \dim(\Lambda) \quad \text{for } \varphi'\in\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}. \tag{10.5.3}$$

Therefore

$$\sum_{\varphi\in\Phi(c)_{\rho\,\mathrm{good}}} \mathrm{Tr}\,\Lambda(\theta_{\rho,\varphi}) = \sum_{\varphi\in\Phi(c)_{\rho\,\mathrm{good}\,\cap\,\rho\,\mathrm{big}}} \mathrm{Tr}\,\Lambda(\theta_{\rho,\varphi}) + o(1)\cdot|\Phi(c)_{\rho\,\mathrm{good}} \smallsetminus \Phi(c)_{\rho\,\mathrm{good}\,\cap\,\rho\,\mathrm{big}}|,$$

where

$$\Phi(c)_{\rho\,\text{good}\cap\rho\,\text{big}} = \Phi(c)_{\rho\,\text{good}} \cap \Phi(c)_{\rho\,\text{big}}.$$

In particular, if the Mellin transform of ρ has big monodromy, that is, if (10.0.3) holds, then

$$\frac{|\Phi(c)_{\rho\,\text{good}} \smallsetminus \Phi(c)_{\rho\,\text{good}\cap\rho\,\text{big}}|}{|\Phi(c)_{\rho\,\text{good}}|} = o(1) \quad \text{for } q \to \infty$$

and thus

$$\frac{1}{|\Phi(c)_{\rho\,\text{good}}|} \sum_{\varphi\in\Phi(c)_{\rho\,\text{good}}} \operatorname{Tr}\Lambda(\theta_{\rho,\varphi}) \overset{(10.5.3)}{=} \frac{1}{|\Phi(c)_{\rho\,\text{good}}|} \sum_{\varphi\in\Phi(c)_{\rho\,\text{good}\cap\rho\,\text{big}}} \operatorname{Tr}\Lambda(\theta_{\rho,\varphi}) + o(1)\cdot O(\dim(\Lambda))$$
$$\overset{(10.0.5)}{=} \int_{U_R(\mathbb{C})} \operatorname{Tr}\Lambda(\theta)\,d\theta + o(1)$$

as $q \to \infty$. Therefore $\Theta_{\rho,q}$ becomes equidistributed in $U_R(\mathbb{C})$ as claimed.

11. Exhibiting big monodromy

In this section we present sufficient criteria for the Mellin transform of ρ to have big monodromy and refer the interested reader to Section 12 for explicit examples of representations meeting these criteria. Before stating the main theorem, we make some hypotheses and introduce pertinent terminology.

Throughout this section, we suppose that $\gcd(s, c) = t - a$ for some $a \in \mathbb{F}_q$. One could easily argue that this is less general than supposing that s, c are relatively prime; however, we do not presently have a way to avoid our hypothesis. For ease of exposition, we also suppose that $a = 0$ and observe that, up to performing an additive translation $t \mapsto t + a$, this represents no additional loss of generality.

For $t = 0, \infty$, we regard V_φ as an $I(t)$-module and then denote it by $V_\varphi(t)$. We write $V_\varphi(t)^{\text{unip}}$ for the maximal subspace of $V_\varphi(t)$ on which $I(t)$ acts unipotently. It is a direct summand of $V_\varphi(t)$, and each simple e-dimensional submodule of it is isomorphic to a common module $\operatorname{Unip}(e)$. We say $V_\varphi(t)$ has a *unique unipotent block of exact multiplicity* 1 if and only if, for a unique integer $e \geq 1$, some $I(t)$-submodule is isomorphic $\operatorname{Unip}(e)$ but no submodule is isomorphic to $\operatorname{Unip}(e) \oplus \operatorname{Unip}(e)$.

Theorem 11.0.1. *Suppose that* $\gcd(s, c) = t$ *and that* $\deg(c) \geq 3$. *Suppose moreover that* $V(0)$ *has a unique unipotent block of exact multiplicity* 1 *and that* ρ *is geometrically simple and pointwise pure. If* $r := \dim(V)$ *and* $\deg(c)$ *satisfy*

$$\deg(c) > \frac{1}{r}\big(72(r^2+1)^2 - r - \deg(L(T,\rho)) + \operatorname{drop}_C(\rho)\big),$$

then the Mellin transform of ρ *has big monodromy.*

We prove the theorem in Section 11.11.

Remark 11.0.2. As the reader will notice, the proof of our theorem has a lot in common with the proof of [Katz 2012, Theorem 17.1]. We need both the hypothesis on $\gcd(c, s)$ and the structure of $V(0)^{\text{unip}}$ in order to exhibit special elements of the relevant arithmetic monodromy groups. More precisely, the hypothesis that $\gcd(c, s) = t$ helps ensure that, for sufficiently many φ, some induced representation $\mathrm{Ind}(V_\varphi)$ has the property that $\mathrm{Ind}(V_\varphi)(0)^{\mathrm{unip}} = V(0)^{\mathrm{unip}}$ (cf. Lemma 11.10.1). The hypothesis on the structure of these coincident modules then leads to the desired element (cf. Lemma 11.7.4). We expect one can remove this hypothesis but do not know how to do so.

Remark 11.0.3. The hypothesis $\gcd(c, s) = t$ also plays a minor role in Proposition 11.9.1. However, one could easily make other hypotheses (e.g., $\gcd(c, s) = 1$) and still be able to proceed (cf. [Katz 2013, Theorem 5.1]).

11.1. ***Two norm maps.*** This subsection recalls material from [Katz 2012, §2] and borrows heavily from that paper.

Let B be the finite $\mathbb{F}_q$-algebra $\mathbb{F}_q[t]/c\,\mathbb{F}_q[t]$. It is a direct product of finite extensions of $\mathbb{F}_q$ and hence étale since c is square-free. More generally, for each finite extension $E/\mathbb{F}_q$, the $\mathbb{F}_q$-algebra

$$B_E = B \otimes_{\mathbb{F}_q} E$$

is étale and has the structure of a free B-module of rank $d = [E : \mathbb{F}_q]$.

Let $\mathbb{B}$ be the functor from the category of $\mathbb{F}_q$-algebras to itself defined for an $\mathbb{F}_q$-algebra R by

$$\mathbb{B}(R) = R[t]/cR[t].$$

It is the functor $R \mapsto B_R = B \otimes_{\mathbb{F}_q} R$. In fact, $\mathbb{B}(R)$ even has the structure of an étale R-algebra which is free of rank $\deg(c)$. In particular, for each $\mathbb{F}_q$-algebra R, there is a norm map $\mathbb{B}(R) \to R$ which is part of a transformation

$$\mathrm{Norm}_{B/\mathbb{F}_q} : \mathbb{B} \to \mathrm{id}_{\mathbb{F}_q-\text{algebras}}$$

between $\mathbb{B}$ and the identity functor on the category of $\mathbb{F}_q$-algebras.

Let $\mathbb{B}^\times$ be the functor from the category of $\mathbb{F}_q$-algebras to the category of groups defined by

$$\mathbb{B}^\times(R) = (R[t]/cR[t])^\times.$$

It is the composition of $\mathbb{B}$ with the functor $A \mapsto A^\times$ of $\mathbb{F}_q$-algebras. Moreover, the restriction of the norm map $\mathbb{B}(R) \to R$ to the group of units yields a homomorphism

$$\nu_R : \mathbb{B}^\times(R) \to R^\times,$$

and in particular, $\nu_{\mathbb{F}_q}$ is the map ν of Section 10.2.

For each finite extension $E/\mathbb{F}_q$, let $\mathbb{B}_E$, $\mathbb{B}_E^\times$ be the functors on variable $\mathbb{F}_q$-algebras R defined by

$$\mathbb{B}_E(R) = B_E \otimes_{\mathbb{F}_q} R, \quad \mathbb{B}_E^\times(R) = (B_E \otimes_{\mathbb{F}_q} R)^\times$$

respectively.

On one hand, $\mathbb{B}_E$ takes values in the category of $\mathbb{F}_q$-algebras. However, $\mathbb{B}_E(R)$ also has the structure of an étale B_R-algebra which is free of rank d as a B_R-module since

$$B_E \otimes_{\mathbb{F}_q} R = B \otimes_{\mathbb{F}_q} E \otimes_{\mathbb{F}_q} R = B_R \otimes_{\mathbb{F}_q} E$$

and since B_E is an étale B-algebra which is free of rank d as a B-module. In particular, there is a transformation

$$\mathrm{Norm}_{E/\mathbb{F}_q} : \mathbb{B}_E \to \mathbb{B}$$

between the functors $\mathbb{B}_E$ and $\mathbb{B}$.

On the other hand, $\mathbb{B}_E^\times$ takes values in the category of groups and is even a smooth commutative group scheme. More precisely, $\mathbb{B}^\times$ is a group scheme over $\mathbb{F}_q$ of multiplicative type (i.e., a torus), and $\mathbb{B}_E^\times$ is the torus $\mathrm{Res}_{E/\mathbb{F}_q}(\mathbb{B}^\times)$ over $\mathbb{F}_q$ given by extending scalars to E and then taking the Weil restriction of scalars of $\mathbb{B}^\times$ back down to $\mathbb{F}_q$ (cf. [Bosch et al. 1990, §7.6]). Moreover, the transformation $\mathrm{Norm}_{E/\mathbb{F}_q}$ induces a transformation

$$\mathrm{Norm}_{E/\mathbb{F}_q} : \mathbb{B}_E^\times \to \mathbb{B}^\times$$

which is even an étale surjective homomorphism of tori. In particular, since

$$\mathbb{B}_E^\times(\mathbb{F}_q) = \mathbb{B}^\times(E) = (E[t]/cE[t])^\times,$$

one obtains a second norm map

$$\nu_E' : (E[t]/cE[t])^\times \to (\mathbb{F}_q[t]/c\mathbb{F}_q[t])^\times$$

which is a surjective homomorphism by Lang's theorem.

11.2. ***Characters of a twisted torus.*** Let $E/\mathbb{F}_q$ be a finite extension and $\Phi_E(c)$ be the dual group $\mathrm{Hom}(\mathbb{B}^\times(E), \overline{\mathbb{Q}}_\ell^\times)$ so that $\Phi_{\mathbb{F}_q}(c) = \Phi(c)$. Suppose that c splits completely over E, and let $a_1, \ldots, a_n \in E$ be the zeros of c so that $c = \prod_{i=1}^n (t - a_i)$ in $E[t]$.

For each E-algebra R, the Chinese remainder theorem implies that there is a unique algebra isomorphism

$$R[t]/cR[t] \to \prod_{i=1}^{n} R[t]/(t-a_i)R[t] \tag{11.2.1}$$

which sends the residue class of t to the tuple $(a_1, \ldots, a_n)$ of residue class representatives. Writing it as an isomorphism $\mathbb{B}(R) \to R^n$ and restricting to units yields a group isomorphism $\mathbb{B}^\times(R) \to (R^\times)^n$. As R varies over E-algebras, the latter isomorphisms in turn yield an isomorphism of tori $\sigma : \mathbb{B}^\times \to \mathbb{G}_m^n$ over E. In particular, applying Weil restriction of scalars from E to $\mathbb{F}_q$ yields an isomorphism

$$\mathrm{Res}_{E/\mathbb{F}_q}(\sigma) : \mathbb{B}_E^\times \to \mathbb{G}_{m,E}^n$$

of tori over $\mathbb{F}_q$, where $\mathbb{G}_{m,E} = \mathrm{Res}_{E/\mathbb{F}_q}(\mathbb{G}_m)$.

There is a unique permutation $\phi \in \mathrm{Sym}([n])$, where $[n] = \{1, 2, \ldots, n\}$, satisfying $a_{\phi^{-1}(i)} = a_i^q$ since c is square-free and has coefficients in $\mathbb{F}_q$. While σ does not descend to a morphism $\mathbb{B}^\times \to \mathbb{G}_m^n$ in general, we can use ϕ to construct a twisted form $\mathbb{T}$ of $\mathbb{G}_m^n$ over $\mathbb{F}_q$ such that σ is the pullback of a morphism $\mathbb{B}^\times \to \mathbb{T}$ over $\mathbb{F}_q$. More precisely, we define the twisted Frobenius τ on $\mathbb{T} = \mathbb{G}_m^n$ as the composition

$$(b_1, \ldots, b_n) \mapsto (b_1^q, \ldots, b_n^q) \mapsto (b_{\phi(1)}^q, \ldots, b_{\phi(n)}^q)$$

of the usual Frobenius automorphism and a permutation of the coordinates of $\mathbb{G}_m^n$. One can easily verify that τ^d is the d-th power of the usual Frobenius and thus $\mathbb{T}$ is indeed a twist of $\mathbb{G}_m^n$ (cf. [Carter 1985, Section 1.17 and Chapter 3] or [Platonov and Rapinchuk 1994, §2.1.7]). Moreover, one can also show that $(a_1, \dots, a_n)$ is fixed by τ and even that

$$\mathbb{T}(\mathbb{F}_q) = \mathbb{T}^{\tau=1} = \mathbb{B}^\times(\mathbb{F}_q).$$

In particular, by precomposing with τ we obtain the automorphism $\tau_E^\vee$ on

$$\operatorname{Hom}(\mathbb{T}(E), \overline{\mathbb{Q}}_\ell^\times) = \operatorname{Hom}(\mathbb{G}_m^n(E), \overline{\mathbb{Q}}_\ell^\times) = \operatorname{Hom}(E^\times, \overline{\mathbb{Q}}_\ell^\times)^n$$

given by

$$\tau_E^\vee : (\varphi_1, \dots, \varphi_n) \mapsto (\varphi_{\phi^{-1}(1)}^q, \dots, \varphi_{\phi^{-1}(n)}^q). \tag{11.2.2}$$

Composition of $\operatorname{Res}_{E/\mathbb{F}_q}(\sigma)$ with the projection $\mathbb{G}_{m,E}^n \to \mathbb{G}_{m,E}$ onto the i-th factor yields a surjective homomorphism

$$\pi_i : \mathbb{B}_E^\times \to \mathbb{G}_{m,E}$$

of tori over $\mathbb{F}_q$. In particular, taking duals of the respective groups of E-rational points and using the bijections $\mathbb{G}_{m,E}(\mathbb{F}_q) = \mathbb{G}_m(E) = E^\times$ yields an isomorphism

$$\sigma_E^\vee : \prod_{i=1}^n \operatorname{Hom}(E^\times, \overline{\mathbb{Q}}_\ell^\times) \ni (\varphi_1, \dots, \varphi_n) \mapsto \prod_{i=1}^n \varphi_i \pi_i \in \Phi_E(c).$$

We observe that since ν_E' is surjective its dual $\nu_E'^\vee$ is a monomorphism $\Phi(c) \to \Phi_E(c)$ and thus we can identify $\Phi(c)$ with a subset of $\operatorname{Hom}(E^\times, \overline{\mathbb{Q}}_\ell^\times)^n$. More precisely, it is the subgroup of characters fixed by $\tau_E^\vee$ and thus

$$(\sigma_E^\vee)^{-1}(\nu_E'^\vee(\Phi(c))) = \{(\varphi_1, \dots, \varphi_n) \in \operatorname{Hom}(E^\times, \overline{\mathbb{Q}}_\ell^\times)^n : \varphi_{\phi(i)} = \varphi_i^q \text{ for } i \in [n]\}. \tag{11.2.3}$$

11.3. *Characters with distinct components.* We say that a character $\varphi \in \Phi_E(c)$ *has distinct components* if and only if it lies in the subset

$$\Phi_E(c)_{\text{distinct}} = \{\sigma_E^\vee(\varphi_1, \dots, \varphi_n) \in \Phi_E(c) : \varphi_i \neq \varphi_j \text{ for } 1 \leq i < j \leq n\},$$

and we define the corresponding subset of $\Phi(c)$ as the intersection

$$\Phi(c)_{\text{distinct}} = \Phi_E(c)_{\text{distinct}} \cap \nu_E'^\vee(\Phi(c)),$$

where $\nu_E'^\vee : \Phi(c) \to \Phi_E(c)$ is the dual of ν_E'.

Lemma 11.3.1. $\Phi(c)_{\text{distinct}}$ *is well-defined*; *that is*, *it does not depend upon our choice of* E.

Proof. Let E'/E be a finite extension and observe that the norm map $E'^\times \to E^\times$ is surjective so it induces a monomorphism

$$\operatorname{Hom}(E^\times, \overline{\mathbb{Q}}_\ell^\times) \to \operatorname{Hom}(E'^\times, \overline{\mathbb{Q}}_\ell^\times),$$

and thus

$$\Phi_E(c)_{\text{distinct}} = \Phi_{E'}(c)_{\text{distinct}} \cap \Phi_E(c).$$

In particular, if $E''/\mathbb{F}_q$ is a second finite extension over which c splits completely and if E' contains the compositum EE'', then

$$\Phi_E(c)_{\text{distinct}} \cap \nu_E'^{\vee}(\Phi(c)) = \Phi_{E'}(c)_{\text{distinct}} \cap \nu_{E'}'^{\vee}(\Phi(c)) = \Phi_{E''}(c)_{\text{distinct}} \cap \nu_{E''}'^{\vee}(\Phi(c))$$

and $\Phi(c)_{\text{distinct}}$ is indeed well-defined. □

Let $c = \prod_{j=1}^r \pi_i \in \mathbb{F}_q[t]$ be a factorization into monic irreducibles. The quotient $E_j = \mathbb{F}_q[t]/\pi_j\mathbb{F}_q[t]$ is a finite extension of $\mathbb{F}_q$ of degree $n_j = \deg(\pi_j)$. It is also the splitting field of π_j and thus may be embedded in E. Moreover, there are bijections

$$\Phi(c) = \prod_{j=1}^r \Phi(\pi_j) = \prod_{j=1}^r \mathrm{Hom}(E_j^\times, \overline{\mathbb{Q}}_\ell^\times), \quad \Phi_E(c) = \prod_{j=1}^r \Phi_E(\pi_j) = \prod_{j=1}^r \mathrm{Hom}(E^\times, \overline{\mathbb{Q}}_\ell^\times)^{n_j} \tag{11.3.2}$$

given by applying the Chinese remainder theorem.

For each monic factor c_0 of c in $\mathbb{F}_q[t]$, let $\Phi(c_0)_{\text{distinct}}$ be the subset of $\Phi(c_0)$ defined much as above but with c_0 in lieu of c. One can easily verify that it does not depend upon the polynomial c of which c_0 is a factor.

Lemma 11.3.3. $|\Phi(\pi_j)_{\text{distinct}}| \sim |\Phi(\pi_j)|$ *for each $j \in [r]$, as $q \to \infty$.*

Proof. Let $j \in [r]$, and suppose without loss of generality that $a_1, \dots, a_{n_j}$ are the zeros of π_j and $\phi(i) \equiv i + 1 \bmod n_j$ for $i \in [n_j]$. Then by (11.2.3) and (11.3.2) there is an identification

$$\Phi(\pi_j) = \{(\varphi_1, \dots, \varphi_{n_j}) \in \mathrm{Hom}(E_j^\times, \overline{\mathbb{Q}}_\ell^\times)^{n_j} : \varphi_{i+1} = \varphi_i^q \text{ for } i \in [n_j - 1]\},$$

since any $\varphi \in \mathrm{Hom}(E^\times, \overline{\mathbb{Q}}_\ell^\times)$ factors through an inclusion $E_j^\times \to E^\times$ if $\varphi^{q^{n_j}} = \varphi$.

The groups $E_j^\times$ and $\mathrm{Hom}(E_j^\times, \overline{\mathbb{Q}}_\ell^\times)$ are cyclic and noncanonically isomorphic, so let g and χ be respective generators. Then we have a further identifications

$$\begin{aligned}\Phi(\pi_j) &= \{(\chi^{e_1}, \dots, \chi^{e_{n_j}}) \in \mathrm{Hom}(E_j^\times, \overline{\mathbb{Q}}_\ell^\times)^{n_j} : e_{i+1} \equiv qe_i \bmod q^{n_j} - 1 \text{ for } i \in [n_j - 1]\} \\ &= \{(g^{e_1}, \dots, g^{e_{n_j}}) \in (E_j^\times)^{n_j} : e_{i+1} \equiv qe_i \bmod q^{n_j} - 1 \text{ for } i \in [n_j - 1]\}.\end{aligned}$$

From this last identification one easily deduces an identification between $\Phi(\pi_j)_{\text{distinct}}$ and the set

$$\{(g^{e_1}, \dots, g^{e_{n_j}}) \in (E_j^\times)^{n_j} : e_{i+1} \equiv qe_i \bmod q^{n_j} - 1 \text{ for } i \in [n_j - 1] \text{ and } \mathbb{F}_q(g^{e_1}) = E_j\},$$

and thus

$$|\Phi(\pi_j)_{\text{distinct}}| = |\{g^e \in E_j^\times : e \in [q^{n_j} - 1] \text{ and } E_j = \mathbb{F}_q(g^e)\}|.$$

Finally, it is well known that the cardinality of the right-hand set is asymptotic to $q^{n_j} - 1$ as $q \to \infty$ (cf. [Rosen 2002, 2.2]), and thus

$$|\Phi(\pi_j)| = |\mathrm{Hom}(E_j^\times, \overline{\mathbb{Q}}_\ell^\times)| = |E_j^\times| = q^{n_j} - 1 \sim |\Phi(\pi_j)_{\text{distinct}}| \quad \text{for } q \to \infty$$

as claimed. □

Corollary 11.3.4. *If c_0 is a monic factor of c in $\mathbb{F}_q[t]$, then $|\Phi(c_0)_{\text{distinct}}| \sim |\Phi(c_0)|$ as $q \to \infty$.*

Proof. Suppose without loss of generality that $c = \pi_1 \cdots \pi_s$ with $s \in [r]$ so that there is a bijection

$$\Phi(c_0) = \prod_{j=1}^{s} \Phi(\pi_j).$$

This bijection in turn induces an inclusion

$$\Phi(c_0)_{\text{distinct}} \to \prod_{j=1}^{s} \Phi(\pi_j)_{\text{distinct}}$$

whose coimage is bounded above by $\prod_{j=1}^{s}(\deg(c_0) - n_j)$ since an element of the codomain lies in the image if (and only if) the components are pairwise distinct. In particular,

$$|\Phi(c_0)_{\text{distinct}}| \sim \prod_{j=1}^{s} |\Phi(\pi_j)_{\text{distinct}}| \overset{\text{Lem.11.3.3}}{\sim} \prod_{j=1}^{s} |\Phi(\pi_j)| \quad \text{for } q \to \infty$$

as claimed. □

11.4. *Properties of H_c^2.* Let X be a smooth geometrically connected curve over $\mathbb{F}_q$, let $T \subseteq X$ be a dense Zariski open subset, and let $\mathcal{F}$ be a sheaf on X.

Lemma 11.4.1. *There is an isomorphism $H_c^2(\overline{T}, \mathcal{F}) \to H_c^2(\overline{X}, \mathcal{F})$.*

Proof. See [SGA 4½ 1977, Sommes trig., Remarques 1.18(d)] and also [Deligne 1980, §1.4, (1.4.1b)]. □

Let $\mathcal{G}$ be a sheaf on X and $\mathcal{G}^\vee$ be its dual. Suppose $\mathcal{F}$ and $\mathcal{G}$ are lisse on T, and thus so is $\mathcal{G}^\vee$. Let $\rho : \pi_1(T) \to \mathrm{GL}(V)$, $\omega : \pi_1(T) \to \mathrm{GL}(W)$, and $\omega^\vee : \pi_1(T) \to \mathrm{GL}(W^\vee)$ be the respective corresponding representations.

Lemma 11.4.2. *Suppose $\mathcal{F}$ and $\mathcal{G}$ are lisse and geometrically simple on T:*

(i) $\dim(H_c^2(\overline{T}, \mathcal{F} \otimes \mathcal{G}^\vee)) = \dim(\mathrm{Hom}_{\pi_1(\overline{T})}(W, V)) \leq 1$.

(ii) $\dim(H_c^2(\overline{T}, \mathcal{F} \otimes \mathcal{G}^\vee)) = 1$ *if and only if $\mathcal{F}$ and $\mathcal{G}$ are geometrically isomorphic on T.*

Proof. Use [SGA 4½ 1977, Sommes trig., Remarques 1.18(d)] and Schur's lemma [Curtis and Reiner 1962, 27.3]. Compare [Katz 1996, §7.0]. □

11.5. *Invariant scalars.* Let $\lambda \in \overline{\mathbb{F}}_q^\times$. If we identify $\mathbb{G}_m$ with $\mathbb{P}_u^1 \smallsetminus \{0, \infty\}$ and regard λ as an element of $\mathbb{G}_m(\overline{\mathbb{F}}_q)$, then multiplication by it (i.e., translation) induces an automorphism of $\mathbb{P}_u^1$ over $\overline{\mathbb{F}}_q$, which we also denote by $\lambda : \mathbb{P}_u^1 \to \mathbb{P}_u^1$. We say λ is an *invariant scalar* of $\mathcal{G}$ if and only if the direct image $\lambda_* \mathcal{G}$ is geometrically isomorphic to $\mathcal{G}$. For example, 1 is an invariant scalar for every $\mathcal{G}$, and every λ is an invariant scalar of the constant sheaf $\overline{\mathbb{Q}}_\ell$.

Let $\alpha : \pi_1(\mathbb{G}_m) \to \overline{\mathbb{Q}}_\ell^\times$ be a tame character. The corresponding sheaf $\mathcal{L}_\alpha = \mathrm{ME}(\alpha)$ is a so-called Kummer sheaf.

Lemma 11.5.1. *Every $\lambda \in \overline{\mathbb{F}}_q^\times$ is an invariant scalar of $\mathcal{L}_\alpha$.*

Proof. The tame fundamental group of $\mathbb{G}_m$ is a quotient and completely generated by the images of the inertia groups $I(0)$ and $I(\infty)$. The character α is completely determined by these images, and translation by λ does not change how $I(0)$ and $I(\infty)$ act since it fixes both 0 and ∞. Therefore $\lambda_*\mathcal{L}_\alpha$ and $\mathcal{L}_\alpha$ are lisse and geometrically isomorphic on $\mathbb{G}_m$, and λ is an invariant scalar of $\mathcal{L}_\alpha$. □

Corollary 11.5.2. *λ is an invariant scalar of $\mathcal{G}$ if and only if it is an invariant scalar of $\mathcal{G} \otimes \mathcal{L}_\alpha$.*

In particular, the answer to the question of whether or not λ is an invariant scalar of $\mathbb{Q}_*\mathrm{ME}(\rho \otimes \varphi)$ depends only on the coset $\varphi\Phi(u)^\nu$.

Proof. The sheaves $\lambda_*\mathcal{L}_\alpha$ and $\mathcal{L}_\alpha$ are lisse and geometrically isomorphic on $\mathbb{G}_m$ by Lemma 11.5.1. Moreover,

$$\lambda_*(\mathcal{G} \otimes \mathcal{L}_\alpha) \otimes (\mathcal{G} \otimes \mathcal{L}_\alpha)^\vee = \lambda_*\mathcal{G} \otimes (\lambda_*\mathcal{L}_\alpha \otimes \mathcal{L}_\alpha^\vee) \otimes \mathcal{G}^\vee,$$

so $\lambda_*\mathcal{G} \otimes \mathcal{G}^\vee$ and $\lambda_*(\mathcal{G} \otimes \mathcal{L}_\alpha) \otimes (\mathcal{G} \otimes \mathcal{L}_\alpha)^\vee$ are lisse and geometrically isomorphic on $\mathbb{P}^1_u \smallsetminus \{0, \infty\}$. Thus λ is an invariant scalar of $\mathcal{G}$ if and only if it is an invariant scalar of $\mathcal{G} \otimes \mathcal{L}_\alpha$. □

The following lemma gives a cohomological criterion for detecting invariant scalars.

Lemma 11.5.3. *Let $\lambda \in \bar{\mathbb{F}}_q^\times$. Suppose $\lambda_*\mathcal{G}$ and $\mathcal{G}$ are lisse and geometrically simple on U. Then the following are equivalent*:

(i) *λ is an invariant scalar of $\mathcal{G}$.*

(ii) $H^2_c(\bar{U}, \lambda_*\mathcal{G} \otimes \mathcal{G}^\vee) \neq 0$.

(iii) $H^2(\bar{\mathbb{P}}^1_u, \lambda_*\mathcal{G} \otimes \mathcal{G}^\vee) \neq 0$.

Proof. Lemma 11.4.2 implies the equivalence of (1) and (2), and Lemma 11.4.1 implies the equivalence of (2) and (3). □

11.6. ***Avoiding invariant scalars.*** Consider the affine plane curve

$$X_\lambda : \lambda c(x_1) = c(x_2),$$

and let $\pi_i : X_\lambda \to \mathbb{A}^1_t$ be the map $(x_1, x_2) \mapsto x_i$. They are part of a commutative diagram

$$\begin{array}{ccc} X_\lambda & \xrightarrow{\pi_2} & \mathbb{A}^1_t \\ {\scriptstyle \pi_1}\downarrow & \overset{\pi}{\searrow} & \downarrow{\scriptstyle c} \\ \mathbb{A}^1_t & \xrightarrow[\lambda c]{} & \mathbb{A}^1_u \end{array}$$

where $\pi = c\pi_2 = \lambda c\pi_1$. Moreover, the maps c and λc are generically étale of degree $n = \deg(c)$; thus their fiber product π is generically étale of degree n^2. Let $g : X_\lambda \to \mathbb{A}^1_t \times \mathbb{A}^1_t$ be the product map (π_1, π_2).

Let $E/\mathbb{F}_q$ be a finite extension over which c splits and $Z = \{a_1, \ldots, a_n\} \subseteq E$ be the zeros of c.

Lemma 11.6.1. *X_λ is smooth over the n^2 points of $Z \times_{\mathbb{A}^1_u} Z = Z \times Z$.*

Proof. The subset $Z \subset \mathbb{A}^1_t$ is the vanishing locus of c and λc; hence $Z \times_{\mathbb{A}^1_u} Z = Z \times Z$. Moreover,

$$\frac{\partial}{\partial x_2}(\lambda c(x_1) - c(x_2)) = c'(x_2) = \sum_{i=1}^{n} \prod_{j \neq i} (x - a_j)$$

does not vanish at any $a_i \in Z$ since c is square-free, so X_λ is smooth at every $(a_i, a_j) \in Z \times Z$. □

Consider the external tensor product sheaf

$$\mathcal{E}_{\rho\otimes\varphi,\lambda} := \mathrm{ME}(\rho \otimes \varphi) \boxtimes \mathrm{ME}(\rho \otimes \varphi)^\vee = \pi_1^* \mathrm{ME}(\rho \otimes \varphi) \otimes \pi_2^* \mathrm{ME}(\rho \otimes \varphi)^\vee$$

on $\mathbb{A}^1_t \times \mathbb{A}^1_t$ and the tensor product sheaf

$$\mathcal{T}_{\rho\otimes\varphi,\lambda} := \lambda \mathbb{Q}_* \mathrm{ME}(\rho \otimes \varphi) \otimes \mathbb{Q}_* \mathrm{ME}(\rho \otimes \varphi)^\vee$$

on $\mathbb{P}^1_u$. They have respective generic ranks r^2 and $(nr)^2$ since both $\mathrm{ME}(\rho \otimes \varphi)$ and its dual have generic rank r and since c has degree n.

Let $T_\lambda \subseteq X_\lambda$ be a smooth dense Zariski open subset and $U_\lambda = \pi(T_\lambda)$. Up to shrinking T_λ, we suppose that $\mathcal{E}_{\rho\otimes\varphi,\lambda}$ is lisse on T_λ and that π is étale over U_λ.

Lemma 11.6.2. *The sheaves $\pi_* g^*(\mathcal{E}_{\rho\otimes\varphi,\lambda})$ and $\mathcal{T}_{\rho\otimes\varphi,\lambda}$ are lisse and isomorphic on U_λ.*

Proof. Consider the commutative diagram

$$\begin{array}{ccccc}
T_\lambda & \xrightarrow{\;g\;} & \pi_1(T_\lambda) \times \pi_2(T_\lambda) & \xrightarrow{\;i\;} & \mathbb{A}^1_t \times \mathbb{A}^1_t \\
\downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle (\lambda c, c)} \\
U_\lambda & \xrightarrow[\Delta]{} & U_\lambda \times U_\lambda & \xrightarrow[j]{} & \mathbb{A}^1_u \times \mathbb{A}^1_u
\end{array}$$

where i and j are the canonical inclusions, h is induced by $(\lambda c, c)$, and Δ is the diagonal map. On one hand, h is étale, so $h_* i^*(\mathcal{E}_{\rho\otimes\varphi,\lambda})$ is lisse on $U_\lambda \times U_\lambda$ and therefore $\Delta^* h_* i^*(\mathcal{E}_{\rho\otimes\varphi,\lambda})$ is lisse on U_λ. On the other hand, there are canonical isomorphisms

$$\pi_* g^*(\mathcal{E}_{\rho\otimes\varphi,\lambda}) \simeq \pi_*(\pi_1, \pi_2)^* i^*(\mathcal{E}_{\rho\otimes\varphi,\lambda}) \simeq \Delta^* h_* i^*(\mathcal{E}_{\rho\otimes\varphi,\lambda}) \simeq \Delta^* j^*(\lambda c, c)_*(\mathcal{E}_{\rho\otimes\varphi,\lambda}) \simeq \Delta^* j^* \mathcal{T}_{\rho\otimes\varphi,\lambda}$$

on U_λ. □

The contrapositive of the following corollary gives us a way to show some λ is *not* an invariant scalar.

Corollary 11.6.3. *Suppose ρ is geometrically simple and $\varphi \in \Phi(c)$. Then the following are equivalent*:

(i) *λ is an invariant scalar of* $\mathbb{Q}_* \mathrm{ME}(\rho \otimes \varphi)$.

(ii) $H^2_c(\overline{U}_\lambda, \mathcal{T}_{\rho\otimes\varphi,\lambda}) \neq 0$.

They imply

(iii) $H^2_c(\overline{T}_\lambda, \mathcal{E}_{\rho\otimes\varphi,\lambda}) \neq 0$.

Proof. Lemmas 11.5.3 and 11.6.2 imply the equivalence of (1) and (2). If $\pi_1(U_\lambda) \to \mathrm{GL}(V)$ is the representation corresponding to $\mathcal{T}_\lambda$, then $V^{\pi_1(U_\lambda)} \subseteq V^{\pi_1(T_\lambda)}$ so (2.0.2) and (2) imply (3). □

The following proposition was inspired by [Katz 2002, Proof of Theorem 5.1.3].

Proposition 11.6.4. *Suppose* $\deg(c) \geq 2 + \deg(\gcd(c, s))$ *and* $\varphi \in \Phi(c)_{\mathrm{distinct}}$:

(i) *If* ρ *is geometrically irreducible, then so is* $\mathrm{ME}(\rho \otimes \varphi)$.

(ii) $\lambda = 1$ *is the only invariant scalar of* $\mathbb{Q}_* \mathrm{ME}(\rho \otimes \varphi)$.

Proof. Let $E/\mathbb{F}_q$ be a splitting field of c and $a_1, a_2 \in E$ be zeros of c which are distinct from each other and the zeros of s. Let $\varphi_1, \varphi_2 \in \mathrm{Hom}(E^\times, \overline{\mathbb{Q}}_\ell^\times)$ be the corresponding components of $(\sigma_E^\vee)^{-1}(\nu_E'^\vee(\varphi))$ as an element of $(\sigma_E^\vee)^{-1}(\Phi_E(c))$ (compare (11.2.3) and (11.3.2)). Then φ_1, φ_2 are distinct characters, so $\alpha = \varphi_1/\varphi_2$ is a nontrivial character.

Let $\lambda \in \overline{\mathbb{F}}_q^\times$ be an arbitrary scalar. If $\lambda \neq 1$, then for each component $T'_\lambda \subseteq T_\lambda$ over $\overline{\mathbb{F}}_q$, there is a smooth point $t' = (t'_1, t'_2) \in T'_\lambda(\overline{\mathbb{F}}_q)$ satisfying $\{t'_1, t'_2\} = \{a_1, a_2\}$. The map π is étale over 0 since c is square-free; hence we can use π to identify $I(t')$ with $I(0)$. We can also identify $I(t'_1)$ and $I(t'_2)$ with $I(0)$.

On one hand, the stalk of $\mathrm{ME}(\rho \otimes \varphi)$ at $t = t'_i$ and the stalk at $t = 0$ of $\overline{\mathbb{Q}}_\ell^r \otimes \mathcal{L}_{\varphi_i}$ are isomorphic as $I(0)$-modules since $s(a_i) \neq 0$. Moreover, the stalk of $\mathcal{E}_{\rho\otimes\varphi,\lambda}$ at t' and the stalk at $u = 0$ of $\overline{\mathbb{Q}}_\ell^{r^2} \otimes \mathcal{L}_\varphi$ are isomorphic as $I(0)$-modules. On the other hand, the latter stalks have no $I(0)$-invariants since φ is nontrivial, so a fortiori, the geometric generic stalk of $\mathcal{E}_{\rho\otimes\varphi,\lambda}$ has no $\pi_1(\overline{T}_\lambda)$-invariants. Therefore (2.0.2) implies $H_c^2(\overline{T}_\lambda, \mathcal{E}_{\rho\otimes\varphi,\lambda})$ vanishes for $\lambda \neq 1$, and hence the contrapositive of Corollary 11.6.3 implies $\lambda = 1$ is the only invariant scalar of $\mathbb{Q}_* \mathrm{ME}(\rho \otimes \varphi)$. □

11.7. *Baby theorem.* In this subsection we prove a simplified version of Theorem 11.0.1.

Let U be a dense Zariski open subset of $\mathbb{G}_m = \mathbb{P}_u^1 \smallsetminus \{0, \infty\}$ and $\theta : \pi_1(U) \to \mathrm{GL}(W)$ be a continuous representation to a finite-dimensional $\overline{\mathbb{Q}}_\ell$-vector space W. Let $\Phi(u)$ be the dual of $\Gamma(u) = (\mathbb{F}_q[u]/u\mathbb{F}_q[u])^\times$ (cf. Section 10.2). For $u = 0, \infty$, let $W(u)$ denote W regarded as an $I(u)$-module and $W(u)^{\mathrm{unip}}$ be its maximal submodule where $I(u)$ acts unipotently. If θ is geometrically simple and pointwise pure of weight w and if $\dim(W) > 1$, then we can associate to θ a pair of Tannakian monodromy groups

$$\mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u)) \subseteq \mathcal{G}_{\mathrm{arith}}(\theta, \Phi(u)) \subseteq \mathrm{GL}_{R, \overline{\mathbb{Q}}_\ell}$$

for $R = \chi(\overline{\mathbb{G}}_m, \mathrm{ME}(\theta))$ (see Section D.14 and Theorem D.7.1).

Theorem 11.7.1. *Suppose that* θ *is geometrically simple and pointwise pure of weight* w, *that* $\dim(W) > 1$ *or that* θ *does not factor through the composed quotient* $\pi_1(U) \twoheadrightarrow \pi_1(\mathbb{G}_m) \twoheadrightarrow \pi_1^t(\mathbb{G}_m)$, *and that* $\lambda = 1$ *is the only invariant scalar of* $\mathrm{ME}(\theta)$. *Suppose moreover that* $W(0)^{\mathrm{unip}}$ *has dimension at most* r *and a unique unipotent block of exact multiplicity* 1 *and that* $R > 72(r^2+1)^2$. *Finally, suppose* $W(\infty)^{\mathrm{unip}} = 0$. *Then* $\mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u))$ *equals* $\mathrm{GL}_{R, \overline{\mathbb{Q}}_\ell}$.

The proof consists of a few steps and will occupy the remainder of this section.

Let $G = \mathcal{G}_{\mathrm{arith}}(\theta, \Phi(u))$ and $H = \mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u))$.

Lemma 11.7.2. *G and H are reductive and there is an exact sequence*

$$1 \to H \to G \to T \to 1$$

for some torus T over $\overline{\mathbb{Q}}_\ell$.

Proof. Observe that $\mathrm{ME}(\theta)$ is geometrically simple yet is not a Kummer sheaf since otherwise one would have $\dim(W) = 1$ and θ would factor through $\pi_1(U) \twoheadrightarrow \pi_1^{\mathrm{t}}(\mathbb{G}_m)$. Moreover, θ is geometrically simple and pointwise pure of weight w by hypothesis. Therefore the lemma follows from Proposition D.14.1(i). □

A priori G or H could be disconnected, so let G^0 and H^0 be the respective identity components.

Lemma 11.7.3. *G^0 and H^0 are (Lie-)irreducible subgroups of $\mathrm{GL}_{R,\overline{\mathbb{Q}}_\ell}$.*

Proof. This follows from [Katz 2012, Theorem 8.2 and Corollary 8.3] since $\lambda = 1$ is the only invariant scalar of $\mathrm{ME}(\theta)$. □

Let $\mu_m : (\overline{\mathbb{Q}}^\times)^m \to \mathbb{Z}^m$ be the m-th weight multiplicity map for $m = R$ given in Definition C.1.2.

Lemma 11.7.4. *There exist an element $g \in G^0$ and an eigenvalue tuple $\gamma \in (\overline{\mathbb{Q}}_\ell^\times)^R$ of g satisfying the following*:

(i) *$\gamma = (\gamma_1, \ldots, \gamma_R)$ lies in $(\overline{\mathbb{Q}}^\times)^R$ and thus $\det(g) = \gamma_1 \cdots \gamma_R$ lies in $\overline{\mathbb{Q}}^\times$.*

(ii) *$|\iota(\det(g))|^2 = (1/q)^w$ for some $w \neq 0$ and every field embedding $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$.*

(iii) *$c = \mu_R(\gamma)$ satisfies $\mathrm{len}(c) \le r + 1$ and $1 = c_{\mathrm{len}(c)} < c_{\mathrm{len}(c)-1}$ and $c_2 \le r$.*

Proof. This follows from Proposition D.14.1(ii) with $g = f^c$ for any element $f \in \mathrm{Frob}_{\mathbb{F}_q,\mathbf{1}}$ and for $c = [G : G^0]$. More precisely, if $\alpha = (\alpha_1, \ldots, \alpha_R)$ is an eigenvalue tuple of f, then all the α_i lie in $\overline{\mathbb{Q}}$, all the nonzero weights $w_1, \ldots, w_n$ of the α_i are negative since $W(\infty)^{\mathrm{unip}}$ vanishes, one has $1 \le n \le r$ since $1 \le \dim(W(0)^{\mathrm{unip}}) \le r$, there is a unique nonzero weight of multiplicity 1 since $W(0)^{\mathrm{unip}}$ has a unique unipotent block of exact multiplicity 1, and the weight zero has multiplicity $R - n \ge R - r > 1$. Hence it suffices to take $\gamma \in (\overline{\mathbb{Q}}^\times)^R$ to be the eigenvalue tuple with $\gamma_i = \alpha_i^c$ for $1 \le i \le R$ and w to be $(w_1 + \cdots + w_n)c$. □

Corollary 11.7.5. $$\det(H) = \overline{\mathbb{Q}}_\ell^\times.$$

Proof. This follows from Lemma 11.7.4(ii) and the argument in [Katz 2012, Proof of Theorem 17.1] using the element g in Lemma 11.7.4. □

Let $[G^0, G^0]$ be the derived subgroup of G^0.

Lemma 11.7.6. $$[G^0, G^0] = \mathrm{SL}_{R,\overline{\mathbb{Q}}_\ell}.$$

Proof. Combine Lemmas 11.7.3 and 11.7.4 to deduce that the hypotheses of Theorem C.4.1 hold, and thus G^0 equals one of $\mathrm{SL}_R(\overline{\mathbb{Q}}_\ell)$ or $\mathrm{GL}_R(\overline{\mathbb{Q}}_\ell)$. The derived subgroup of both of these groups equals $\mathrm{SL}_R(\overline{\mathbb{Q}}_\ell)$. □

We may now complete the proof of the theorem. First, we have inclusions

$$[G^0, G^0] \subseteq [G, G] \subseteq [\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}, \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}] = \mathrm{SL}_{R,\bar{\mathbb{Q}}_\ell},$$

and Lemma 11.7.6 implies the outer terms are equal, so the inclusions are equalities. Moreover, Lemma 11.7.2 implies H is normal in G and G/H is abelian, so H contains $[G, G] = \mathrm{SL}_{R,\bar{\mathbb{Q}}_\ell}$, and hence, by Corollary 11.7.5, $H = \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$ as claimed.

11.8. ***Frobenius reciprocity.*** Let $c : T \to U$ be a finite étale map of smooth geometrically connected curves over $\mathbb{F}_q$. Let $\mathcal{F}$ be a lisse sheaf on T and $\pi_1(T) \to \mathrm{GL}(V)$ be the corresponding representation. Similarly, let $\mathcal{G}$ be a lisse sheaf U and $\pi_1(U) \to \mathrm{GL}(W)$ be the corresponding representation. Let $\mathcal{F}^\vee$ be the dual of $\mathcal{F}$ and $\pi_1(T) \to \mathrm{GL}(V^\vee)$ be the corresponding representation.

Lemma 11.8.1. *$\mathbb{Q}_*(\mathcal{F}^\vee)$ is isomorphic to the dual of $\mathbb{Q}_*\mathcal{F}$.*

Proof. See [Katz 2002, Lemmma 3.1.3]. □

Therefore we may unambiguously write $\mathbb{Q}_*\mathcal{F}^\vee$.

Proposition 11.8.2. $\dim(H^2_c(\bar{T}, c^*\mathcal{G} \otimes \mathcal{F}^\vee)) = \dim(H^2_c(\bar{U}, \mathcal{G} \otimes \mathbb{Q}_*\mathcal{F}^\vee))$.

Proof. Let $H = \pi_1(\bar{T})$ and $G = \pi_1(\bar{U})$. We suppose that V is a left H-module and W is a left G-module, and define $\mathrm{Ind}_H^G(V)$ to be the (Mackey) induced module $\mathrm{Hom}_G(\bar{\mathbb{Q}}_\ell[H], V)$ and $\mathrm{Res}_H^G(W)$ to be the restricted module W regarded as a left H-module. Then Frobenius reciprocity implies that there is a bijection of vector spaces

$$\mathrm{Hom}_H(\mathrm{Res}_H^G(W), V) \to \mathrm{Hom}_G(W, \mathrm{Ind}_H^G(V))$$

given by $\psi \mapsto (w \mapsto (r \mapsto \psi(rv)))$ (cf. [Katz 2002, §3.0]). Moreover, Lemma 11.4.2 implies

$$\dim(H^2_c(\bar{T}, c^*\mathcal{G} \otimes \mathcal{F}^\vee)) = \dim(\mathrm{Hom}_H(\mathrm{Res}_H^G(W), V)),$$
$$\dim(H^2_c(\bar{U}, \mathcal{G} \otimes \mathbb{Q}_*\mathcal{F}^\vee)) = \dim(\mathrm{Hom}_G(W, \mathrm{Ind}_H^G(V))),$$

so the proposition follows immediately. □

11.9. ***Begetting simplicity.*** In this section we give a criterion for $\mathrm{Ind}(\rho \otimes \varphi)$ to be geometrically simple. Our argument was inspired by [Katz 2013, Proof of Theorem 5.1.1].

Proposition 11.9.1. *Let $\varphi \in \Phi(c)_{\mathrm{distinct}}$. Suppose that $\gcd(c, s) = t$, that $\deg(c) \geq 2$, and that $\varphi(\Gamma(t)) = 1$. If ρ is geometrically simple, then so are $\rho \otimes \varphi$ and $\mathrm{Ind}(\rho \otimes \varphi)$.*

Proof. Let $T \subseteq \mathbb{P}^1_t$ be a dense Zariski open subset and $U = c(T)$. Up to shrinking T, we suppose that $\mathcal{F} = \mathrm{ME}(\rho \otimes \varphi)$ is lisse over T and that c is étale over U.

Suppose that ρ is geometrically simple and thus so is $\rho \otimes \varphi$. Let $\mathcal{G} = \mathbb{Q}_*\mathcal{F}^\vee$ (cf. Lemma 11.8.1), and observe that Lemma 10.2.1(i) implies that $\mathcal{G}$ and $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi))^\vee$ are isomorphic over U. We wish to show that $\dim(H^2(\bar{U}, \mathcal{G} \otimes \mathcal{G}^\vee)) = 1$ so that Lemma 11.4.2 implies that $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi))$ is geometrically simple over U, that is, that $\mathrm{Ind}(\rho\otimes\varphi)$ is geometrically simple. In fact, Lemma 11.4.1 and Proposition 11.8.2 imply

$$\dim(H_c^2(\bar{\mathbb{P}}_u^1,\mathcal{G}\otimes\mathcal{G}^\vee))=\dim(H_c^2(\bar{U},\mathbb{Q}_*\mathcal{F}\otimes\mathbb{Q}_*\mathcal{F}^\vee))=\dim(H_c^2(\bar{T},c^*\mathbb{Q}_*\mathcal{F}\otimes\mathcal{F}^\vee)),$$

so it suffices to show the last term equals 1.

The functor c^* is left adjoint to the functor $\mathbb{Q}_*$ since c is finite (cf. [Milne 1980, II.3.14]), so the identify map $\mathbb{Q}_*\mathcal{F}\to\mathbb{Q}_*\mathcal{F}$ induces an adjoint $c^*\mathbb{Q}_*\mathcal{F}\to c$. Generically it is the trace map $\mathrm{Ind}(V_\varphi)\to V_\varphi$ and thus is surjective (cf. [Milne 1980, V.1.12]). Let $\mathcal{K}$ be the kernel so that we have an exact sequence of sheaves

$$0\to\mathcal{K}\to c^*\mathbb{Q}_*\mathcal{F}\to\mathcal{F}\to 0. \tag{11.9.2}$$

These sheaves and $\mathcal{F}^\vee$ are all lisse over T, so the sequence

$$0\to\mathcal{K}\otimes\mathcal{F}^\vee\to c^*\mathbb{Q}_*\mathcal{F}\otimes\mathcal{F}^\vee\to\mathcal{F}\otimes\mathcal{F}^\vee\to 0 \tag{11.9.3}$$

is exact on T. In particular, we have a corresponding exact sequence of cohomology

$$H_c^2(\bar{U},\mathcal{K}\otimes\mathcal{F}^\vee)\to H_c^2(\bar{T},c^*\mathbb{Q}_*\mathcal{F}\otimes\mathcal{F}^\vee)\to H_c^2(\bar{T},\mathcal{F}\otimes\mathcal{F}^\vee)\to H_c^3(\bar{T},\mathcal{K}\otimes\mathcal{F}^\vee),$$

the last term of which vanishes. The hypothesis that $\mathcal{F}$ is geometrically simple implies the penultimate term has dimension 1 by Lemma 11.4.2, so it suffices to show that the first term vanishes.

Let $E/\mathbb{F}_q$ be a splitting field of c, let $a_1,\dots,a_n\in E$ be the zeros of c, and let

$$(\varphi_1,\dots,\varphi_n)=(\sigma_E^\vee)^{-1}(\nu_E'^\vee(\varphi))\in\mathrm{Hom}(E^\times,\bar{\mathbb{Q}}_\ell^\times)^n$$

as in (11.2.3). We suppose without loss of generality that $a_1=0$ and thus $s(a_2)\cdots s(a_n)\neq 0$ since $\gcd(c,s)=t$.

Let $H=\pi_1(\bar{T})$ and $G=\pi_1(\bar{U})$, and let $H\to\mathrm{GL}(V_\varphi)$ and $G\to\mathrm{GL}(\mathrm{Ind}_H^G(V_\varphi))$ be the representations corresponding to $\mathcal{F}$ and $\mathbb{Q}_*\mathcal{F}$ respectively. The exact sequences (11.9.2) and (11.9.3) correspond to exact sequences of H-modules

$$0\to K\to R\to V_\varphi\to 0 \tag{11.9.4}$$

and

$$0\to K\otimes V_\varphi^\vee\to R\otimes V_\varphi^\vee\to V_\varphi\otimes V_\varphi^\vee\to 0,$$

where $R=\mathrm{Res}_H^G(\mathrm{Ind}_H^G(V_\varphi))$. We claim the first term of the latter sequence has no $I(0)$-coinvariants so a fortiori has no $\pi_1(\bar{T})$-coinvariants, and hence $H^2(\bar{T},\mathcal{K}\otimes\mathcal{F}^\vee)$ vanishes as claimed.

The translation map $t\mapsto t+a_i$ induces an isomorphism $I(0)\simeq I(a_i)$ for each $i\in[n]$, so we can regard $V_\varphi(a_i)$ as an $I(0)$-module. In fact, we have isomorphisms of $I(0)$-modules

$$R(0)\simeq\bigoplus_{i=1}^n V_\varphi(a_i),\qquad K(0)\simeq\bigoplus_{i=2}^n V_\varphi(a_i),\qquad (K\otimes V_\varphi^\vee)(0)\simeq\bigoplus_{i=2}^n(\bar{\mathbb{Q}}_\ell^{r-1}\otimes\varphi_i^{-1}).$$

More precisely, the first isomorphism corresponds to the fact that the geometric stalks of $c^*\mathbb{Q}_*\mathcal{F}$ and $\mathcal{F}$ satisfy $(c^*\mathbb{Q}_*\mathcal{F})_0=\bigoplus_{c(a)=0}\mathcal{F}_a$ since c is étale over $u=0$ (cf. (10.1.1)); the second isomorphism uses

(11.9.4) and the assumption that $a_1 = 0$ to identify $K(0)$ with $R(0)/V_\varphi(0)$; and the last isomorphism uses that $s(a_2)\cdots s(a_n) \neq 0$, that is, $\mathcal{C} \smallsetminus \{a_1\}$ lies in the locus of lisse reduction of $\mathrm{ME}(\rho \otimes \varphi)^\vee$.

The hypothesis that $\Gamma(t)$ is in the kernel of φ implies that $V_\varphi(0) \simeq V(0)$ as $I(0)$-modules. Moreover, $\varphi_2, \ldots, \varphi_n$ are all nontrivial since they are distinct from the trivial character φ_1 by hypothesis, so each of the summands $(\overline{\mathbb{Q}}_\ell^{r-1} \otimes \varphi_i^{-1})$ has *trivial* $I(0)$-coinvariants. Therefore $K \otimes V_\varphi^\vee$ has trivial $\pi_1(\overline{T})$-coinvariants as claimed. □

11.10. *Preserving unipotent blocks.* For each monic divisor c_0 of c in $\mathbb{F}_q[t]$, consider the subset

$$\Phi(c_0)_{\rho\,\mathrm{good}} = \{\varphi \in \Phi(c_0) : \mathrm{ME}(\rho \otimes \varphi) \text{ is supported on } \mathbb{A}^1_t[1/c_0]\}.$$

If ρ is the trivial representation, then it consists of the odd primitive characters of conductor c_0.

For $t = 0, \infty$, let $V_\varphi(t)$ denote V_φ regarded as an $I(t)$-module. Similarly, for $u = 0, \infty$, let $\mathrm{Ind}(V_\varphi)(u)$ denote $\mathrm{Ind}(V_\varphi)$ regarded as an $I(u)$-module, and let $\mathrm{Ind}(V_\varphi)(u)^{\mathrm{unip}}$ be the maximal submodule of $\mathrm{Ind}(V_\varphi)(u)$, where $I(u)$ acts unipotently. We say that $\mathrm{Ind}(V_\varphi)(0)$ (resp. $V_\varphi(0)$) has a *unipotent block of dimension e and exact multiplicity m* if and only if it has an $I(0)$-submodule isomorphic to $U(e)^{\oplus m}$ but no $I(0)$-submodule isomorphic to $U(e)^{\oplus m+1}$.

Lemma 11.10.1. *Suppose* $\gcd(c, s) = t$, *and let* $c_0 = c/t$ *and* $\varphi \in \Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}$. *Then*:

(i) $\mathrm{Ind}(V_\varphi)(0)$ *has a unipotent block of dimension e and exact multiplicity m if and only if* $V(0)$ *does.*

(ii) $\mathrm{Ind}(V_\varphi)(\infty)^{\mathrm{unip}} = 0$.

Proof. On one hand, $V_\varphi(z)^{\mathrm{unip}} = 0$ for every $z \in \mathcal{C} \smallsetminus \{0\}$ since φ is in $\Phi(c_0)_{\rho\,\mathrm{good}}$ and $\gcd(c_0, s) = 1$. Moreover, $V_\varphi(0)$ and $V(0)$ are isomorphic as $I(0)$-modules since $\varphi(\Gamma(t)) = 1$. Therefore the only unipotent blocks of $\mathrm{Ind}(V_\varphi)(0)$ are those coming from $V_\varphi(0)$, and all such blocks contribute identical blocks to $V_\varphi(0)$ (cf. [Milne 1980, II.3.1(e) and II.3.5(c)]), so (i) holds. On the other hand, every unipotent block of $\mathrm{Ind}(V_\varphi)(\infty)$ contributes to $V_\varphi(\infty)^{\mathrm{unip}}$, and the latter vanishes since φ is good for ρ, so (ii) holds. □

11.11. *Proof of Theorem 11.0.1.* Recall that R is given by

$$R := r_{\mathcal{C}}(\rho) = (\deg(c) + 1)r + \deg(L(T, \rho)) - \mathrm{drop}_{\mathcal{C}}(\rho) \tag{11.11.1}$$

and it equals $\deg(L_{\mathcal{C}}(T, \rho \otimes \varphi))$ for all $\varphi \in \Phi(c)$ (see Proposition 4.3.1).

Lemma 11.11.2. $$R > 72(r^2 + 1)^2.$$

Proof. This follows from (11.11.1) and the hypothesis on $\deg(c)$ in the statement of the theorem. □

Let $c_0 = c/t$.

Lemma 11.11.3. *Suppose* $\varphi \in \Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}$. *Then the following hold*:

(i) $\mathrm{Ind}(\rho \otimes \varphi)$ *is geometrically simple.*

(ii) $\dim(\mathrm{Ind}(V_\varphi)(0)^{\mathrm{unip}}) = \dim(V_\varphi(0)^{\mathrm{unip}})$ *and* $\mathrm{Ind}(V_\varphi)(0)$ *has a unique unipotent block of exact multiplicity* 1.

(iii) $\mathrm{Ind}(V_\varphi)(\infty)^{\mathrm{unip}} = 0$.

Proof. Part (i) follows from Proposition 11.9.1 since φ is in $\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)$, since ρ is geometrically simple, and since $\deg(c) \geq 2$. Parts (ii) and (iii) follow from Lemma 11.10.1 since φ is also in $\Phi(c_0)_{\rho\,\mathrm{good}}$ and since $V(0)$ has a unique unipotent block of exact multiplicity 1. □

Corollary 11.11.4. $$(\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}) \subseteq \Phi(c)_{\rho\,\mathrm{big}}.$$

Proof. Let $\varphi \in \Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}$, and let $\theta = \mathrm{Ind}(\rho \otimes \varphi)$ and $W = \mathrm{Ind}(V_\varphi)$. Then Lemmas 11.11.3 and 10.1.2 imply that $\theta = \mathrm{Ind}(\rho \otimes \varphi)$ is geometrically simple and pointwise pure of weight w since $\varphi \in \Phi(c)_{\mathrm{distinct}}$. Moreover, $\dim(W) = \deg(c) \cdot \dim(V) > 2$ since $\deg(c) \geq 2$, and Proposition 11.6.4 implies that $\lambda = 1$ is the only invariant scalar of $\mathrm{ME}(\theta) \simeq \mathbb{Q}_*\mathrm{ME}(\rho \otimes \varphi)$ since $\deg(c) \geq 3$ and $\varphi \in \Phi(c)_{\mathrm{distinct}}$. Lemma 11.11.3 also implies that $W(0)$ has a unique unipotent block of exact multiplicity 1, that $\dim(W(0)^{\mathrm{unip}}) = \dim(V(0)^{\mathrm{unip}}) \leq \dim(V) = r$, and that $W(\infty)^{\mathrm{unip}} = 0$. Finally, Lemma 11.11.2 implies $R > 72(r^2+1)^2$. Therefore the hypotheses of Theorem 11.7.1 hold, and hence $\varphi \in \Phi(c)_{\rho\,\mathrm{big}}$. □

Corollary 11.11.5. $$(\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}})\Phi(u)^\nu \subseteq \Phi(c)_{\rho\,\mathrm{big}}.$$

Proof. This follows from Corollary 11.11.4 since $\Phi(c)_{\rho\,\mathrm{big}}$ is a union of cosets $\varphi\Phi(u)^\nu$. □

Let $\varphi \in \Phi(c)$ and $\varphi\Phi(u)^\nu$ be the corresponding coset.

Lemma 11.11.6. $$|\varphi\Phi(u)^\nu \cap \Phi(c_0)| = 1.$$

Proof. We must show that there is a unique element $\alpha \in \Phi(u)$ satisfying $\varphi\alpha^\nu(\Gamma(t)) = 1$. Since $\gcd(s, c) = t$, we can speak of the component of φ at $t = 0$: it is the character given by restricting χ to the subgroup $\Gamma(t) \subseteq \Gamma(c)$. There is a unique element of $\Phi(u)^\nu$ with the same component at $t = 0$; call it β^ν. Then $\alpha = 1/\beta$ is the desired character. □

We need one more estimate to complete the proof of the theorem.

Lemma 11.11.7. $|\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}| \sim |\Phi(c_0)_{\mathrm{distinct}}| \sim |\Phi(c_0)|$ *as* $q \to \infty$.

Proof. We observe that there are natural inclusions

$$\left(\Phi(c_0)_{\mathrm{distinct}} \smallsetminus \bigcup_{\pi \mid c_0} \Phi(c_0/\pi)\right) \subseteq (\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)) \subseteq \Phi(c_0)_{\mathrm{distinct}}$$

since an element of $\Phi(c_0)_{\mathrm{distinct}}$ will fail to lie in $\Phi(c)_{\mathrm{distinct}}$ only if one of its $\deg(c_0)$ components is trivial, that is, if it lies in $\Phi(c_0/\pi)$ for some prime factor $\pi \mid c_0$. Intersecting with $\Phi(c_0)_{\rho\,\mathrm{good}}$ gives further inclusions

$$\left((\Phi(c_0)_{\rho\,\mathrm{good}} \cap \Phi(c_0)_{\mathrm{distinct}}) \smallsetminus \bigcup_{\pi \mid c_0} \Phi(c_0/\pi)\right) \subseteq (\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}) \subseteq \Phi(c_0)_{\mathrm{distinct}}.$$

Finally, we know that

$$|\Phi(c_0)_{\rho\,\mathrm{good}}| \overset{(10.3.4)}{\sim} |\Phi(c_0)| \overset{11.3.4}{\sim} |\Phi(c_0)_{\mathrm{distinct}}|, \qquad \left|\bigcup_{\pi\,|\,c_0} \Phi(c_0/\pi)\right| / |\Phi(c)| \ll 1/q = o(1)$$

and hence

$$\left|(\Phi(c_0)_{\rho\,\mathrm{good}} \cap \Phi(c_0)_{\mathrm{distinct}}) \smallsetminus \bigcup_{\pi\,|\,c_0} \Phi(c_0/\pi)\right| \sim |\Phi(c_0)|$$

as $q \to \infty$. □

Corollary 11.11.8. $|(\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}})\Phi(u)^{\nu}| \sim |\Phi(c)|$ *for* $q \to \infty$.

Proof. Combine Lemma 11.11.6 and Lemma 11.11.7. □

The theorem now follows by observing that

$$|\Phi(c)| \overset{\mathrm{Cor.}11.11.8}{\sim} |(\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}})\Phi(u)^{\nu}| \overset{\mathrm{Cor.}11.11.5}{\leq} |\Phi(c)_{\rho\,\mathrm{big}}| \leq |\Phi(c)|$$

and thus

$$|\Phi(c)_{\rho\,\mathrm{big}}| \sim |\Phi(c)|$$

for $q \to \infty$.

Therefore, the Mellin transform of ρ has big monodromy as claimed and Theorem 11.0.1 holds.

12. Application to explicit abelian varieties

In this section we apply the theory developed in the previous sections to representations coming from (the Tate modules of) a general class of abelian varieties. More precisely, we give an explicit family of abelian varieties for which we can show the corresponding representations satisfy the hypotheses of Theorem 11.0.1. Our principal application, of which Theorem 1.2.3 is a special case, is Theorem 12.3.1.

Throughout this section we suppose that q is an odd prime power so that we can speak of hyperelliptic curves. One who is interested in even characteristic or in L-functions whose Euler factors have odd degree is encouraged to consider Kloosterman sheaves (e.g., see [Katz 1988, 7.3.2]).

12.1. ***Some hyperelliptic curves and their Jacobians.*** Let g be a positive integer. In this section we construct an explicit family of abelian varieties which give rise to Galois representations we can easily show satisfy the hypotheses of Theorem 10.0.4. One member of this family is an elliptic curve, the Legendre curve, and it has affine model

$$X_{\mathrm{Leg}} : y^2 = x(x-1)(x-t).$$

It is isomorphic to its own Jacobian, and the general abelian varieties in our family will be Jacobians of curves. More precisely, we fix a monic square-free $f \in \mathbb{F}_q[x]$ of degree $2g$ and consider the projective plane curve X/K with affine model

$$X : y^2 = f(x)(x-t). \tag{12.1.1}$$

For technical reasons we will eventually suppose that f has a zero a in $\mathbb{F}_q$, and up to the change of variables $x \mapsto x + a$, we will suppose that $a = 0$. We do not need this hypothesis yet since the discussion in this section does not use it.

The curve X has genus g. If $g > 1$, it is a so-called hyperelliptic curve, and otherwise it is an elliptic curve. Either way its Jacobian J is a g-dimensional principally polarized abelian variety over K. See [Cohen et al. 2006] for more information about hyperelliptic curves and their Jacobians.

For each finite place $v = \pi$, one can define a reduction $X/\mathbb{F}_\pi$ starting with the reduction of (12.1.1) modulo π.

Lemma 12.1.2. *The monic polynomial $s = f(t) \in \mathbb{F}_q[t]$ satisfies the following*:

(i) *If $\pi \nmid s$, then $X/\mathbb{F}_\pi$ is a smooth projective curve of genus g.*

(ii) *If $\pi \mid s$, then $X/\mathbb{F}_\pi$ is smooth away from a single node and has genus $g - 1$.*

Proof. The essential point is that, for any monic polynomial $h(x)$ with coefficients in a field F of characteristic not 2, the affine curve $y^2 = h(x)$ is smooth if and only if h is a square-free polynomial. More generally, if $h = h_1 h_2^2$, where $h_1, h_2 \in F[x]$ are square-free and relatively prime, then the following hold:

(i) The map $(x, y) \mapsto (x, y/h_2(x))$ induces a birational map from $y^2 = h_1(x)$ to $y^2 = h(x)$.

(ii) The $\deg(h_2)$ points (x, y) satisfying $h_2(x) = y = 0$ are so-called nodes of $y^2 = h(x)$.

(iii) The map in (1) corresponds to blowing up the nodes in (2).

(iv) The curve $y^2 = h_1(x)$ is smooth of genus $\lfloor (\deg(h_1) - 1)/2 \rfloor$ since h_1 is square-free.

(v) Both curves have one point at infinity if $\deg(h)$ is odd and two points at infinity if $\deg(h)$ is even.

(Compare [Hartshorne 1977, Chapter I, Exercises 5.6.1–3].) The proof of the lemma will consist of showing that we are in this general situation.

Let $t_0 \in \mathbb{F}_\pi$ satisfy $t \equiv t_0 \bmod \pi$, and let $h_0(x) := f(x)(x - t_0) \in \mathbb{F}_\pi[x]$. The polynomial $f(x)$ is square-free by hypothesis, so $h_0(x)$ is square-free if and only if $f(t_0) = 0$, or equivalently, $\pi \mid s$. In particular, if $\pi \nmid s$, then h_0 is square-free and $y^2 = h_0(x)$ is smooth of genus g. Otherwise, $h_0 = h_1 h_2^2$, where $h_1 = f/(x - t_0)$ and $h_2 = x - t_0$ are coprime (since f is square-free), and thus $y^2 = h_0(x)$ is smooth away from the node $(t_0, 0)$ and birational to the curve $y^2 = h_1(x)$, which is smooth of genus $g - 1$. □

Remark 12.1.3. One can also define a reduction $X/\mathbb{F}_\infty$ by writing $t = 1/u$ and clearing denominators, and one eventually finds that $X/\mathbb{F}_\infty$ has genus zero. However, the arguments are subtler and beyond the scope of this article, so we omit them.

For example, X_{Leg} has smooth reduction away from $t = 0, 1, \infty$, over $t = 0, 1$ its reduction is a so-called node, and over $t = \infty$ it is a so-called cusp. Since it is isomorphic to its Jacobian, these are sometimes referred to as good, multiplicative, and additive reduction respectively. However, in general, one needs to construct separately reductions $J/\mathbb{F}_\pi$, for every π, and also a reduction $J/\mathbb{F}_\infty$.

Lemma 12.1.4. (i) *If $\pi \nmid s$, then $J/\mathbb{F}_\pi$ is the Jacobian of $X/\mathbb{F}_\pi$ so it is a g-dimensional abelian variety.*

(ii) *If $\pi \mid s$, then $J/\mathbb{F}_\pi$ is an extension of an abelian variety by a 1-dimensional torus.*

Proof. Both statements are easy consequences of Lemma 12.1.2. More precisely, if $X/\mathbb{F}_\pi$ is projective and smooth away from n nodes, then $J/\mathbb{F}_\pi$ is an extension of a $(g-n)$-dimensional abelian variety by an n-dimensional torus. See [Bosch et al. 1990, 9.2.8] and keep in mind Lemma 12.1.2. □

Remark 12.1.5. One can also show that $J/\mathbb{F}_\infty$ is a g-dimensional additive linear algebraic group, but demonstrating it directly is harder and requires a finer statement than the claim in Remark 12.1.3.

One can regard the various reductions of J as the special fibers of the (identity component of the) Néron model of J/K over $\mathbb{P}^1_t$. However, for our purposes, Lemma 12.1.4 contains all the information we need about the model. More precisely, we only need to know the respective dimensions g_π, m_π, and a_π of the good, multiplicative, and additive parts of $J/\mathbb{F}_\pi$. Thus

$$(g_\pi, m_\pi, a_\pi) = \begin{cases} (g, 0, 0) & \text{if } \pi \nmid s, \\ (g-1, 1, 0) & \text{if } \pi \mid s \end{cases} \tag{12.1.6}$$

by Lemma 12.1.4. In Section 12.2 we will show that

$$(g_\infty, m_\infty, a_\infty) = (0, 0, g)$$

as claimed in Remark 12.1.5.

12.2. *Tate modules.* Let ℓ be a prime distinct from the characteristic p of $\mathbb{F}_q$. For each $m \geq 0$, let $J[\ell^m] \subseteq J(\bar{K})$ be the subgroup of ℓ^m-torsion; it is isomorphic to $(\mathbb{Z}/\ell^m)^{2g}$ and hence is a finite Galois module. Multiplication by ℓ induces an epimorphism $J[\ell^{m+1}] \twoheadrightarrow J[\ell^m]$ for each m, and the $\mathbb{Z}_\ell$-Tate module of J is the projective limit

$$T_\ell(J) := \varprojlim J[\ell^m].$$

Concretely one can regard $T_\ell(J)$ as the set

$$\{(P_0, P_1, \ldots) : P_m \in J[\ell^m] \text{ and } \ell P_{m+1} = P_m \text{ for } m \geq 0\}.$$

It is even a Galois $\mathbb{Z}_\ell$-module (since the action of G_K and multiplication by ℓ commute), and it is isomorphic to ${\mathbb{Z}_\ell}^{2g}$ as a $\mathbb{Z}_\ell$-module (cf. [Serre and Tate 1968, §1]).

Let V be the vector space $T_\ell(J) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell$ and $G_K \to \mathrm{GL}(V)$ be the corresponding Galois representation. For each $v \in \mathcal{P}$, let $V(v)$ denote V as an $I(v)$-module and let $V(v)^{\mathrm{unip}}$ be the maximal submodule where $I(v)$ acts unipotently.

Proposition 12.2.1. *Let $v \in \mathcal{P}$, and let g_z and m_z be the respective dimensions of the abelian and multiplicative part of $J/\mathbb{F}_v$ Then*

$$V(v)^{\mathrm{unip}} \simeq U(1)^{\oplus 2g_v} \oplus U(2)^{\oplus m_v}.$$

Proof. This is a general fact about Tate modules of abelian varieties. See [SGA 7_{I} 1972, Exposé IX, §2.1]. □

Let $\mathcal{S} = \{\pi \in \mathcal{P} : \pi \mid s\} \cup \{\infty\}$, where $s = f(t)$ as in Lemma 12.1.2. Then by Proposition 12.2.1, the action of G_K on V induces a representation

$$\rho : G_{K,\mathcal{S}} \to \mathrm{GL}(V)$$

since

$$\dim(V^{I(v)}) = \dim(V) = 2g \quad \text{for } v \in \mathcal{P} \smallsetminus \mathcal{S}$$

by (12.1.6).

Lemma 12.2.2. *The representation ρ is geometrically simple and pointwise pure of weight 1, and it satisfies*

$$\mathrm{drop}_v(\rho) = \begin{cases} 0, & v \in \mathcal{P} \smallsetminus \mathcal{S}, \\ 1, & v \in \mathcal{S} \smallsetminus \{\infty\}, \\ 2g, & v = \infty, \end{cases} \qquad \mathrm{Swan}(\rho) = 0.$$

Proof. The values $\mathrm{drop}_v(\rho)$ for $v \neq \infty$ follow directly from (12.1.6) since

$$\mathrm{drop}_v(\rho) = \dim(V) - \dim(V^{I(v)}) = 2g - 2g_v - m_v$$

by Proposition 12.2.1. For the assertions about geometric simplicity and weight and about $\mathrm{drop}_\infty(\rho)$ and $\mathrm{Swan}(\rho)$ we refer to [Katz and Sarnak 1999, 10.1.9 and 10.1.17] (cf. [Hall 2008, §5] for a related discussion about $J[\ell]$). □

Corollary 12.2.3. $L(T, J/K) = 1$; *that is, it is a polynomial and* $\deg(L(T, J/K)) = 0$.

Proof. The representation ρ is geometrically simple and $\dim(V) = 2g > 0$, so ρ has trivial geometric invariants. Moreover, it is pointwise pure of weight $w = 1$, so Theorem 7.3.2 implies $L(T, \rho)$ is a polynomial of degree

$$r_\varnothing(\rho) \overset{(3.5.2)}{=} \mathrm{drop}(\rho) + \mathrm{Swan}(\rho) - 2 \cdot \dim(V) \overset{12.2.2}{=} (\deg(f) \cdot 1 + 1 \cdot 2g) + 0 - 2 \cdot 2g = 0$$

as claimed. □

Let $c \in \mathbb{F}_q[t]$ be monic and square-free and $\mathcal{C} \subset \mathcal{P}$ be the finite subset consisting of ∞ and $v(\pi)$ for every prime factor π of c (cf. Section 4).

Lemma 12.2.4. *For every $\varphi \in \Phi(c)$, the representation $\rho \otimes \varphi$ is geometrically simple and pointwise pure of weight* 1, *and φ is not heavy.*

Proof. Lemma 7.1.2 implies that $\rho \otimes \varphi$ is geometrically simple since ρ is. Moreover, it has trivial geometric invariants since $\dim(V) = 2g > 1$, so φ is not heavy. Finally, Lemma 6.2.2 implies that it is pointwise pure of weight $w = 1$ since ρ is. □

Corollary 12.2.5. *If $\varphi \in \Phi(c)$, then $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ is a polynomial and*

$$\deg(L_{\mathcal{C}}(T, \rho \otimes \varphi)) = 2g \cdot \deg(c) - \deg(\gcd(c, s)).$$

Proof. By Lemma 12.2.4 the hypotheses of Theorem 7.3.2 hold, and hence $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ is a polynomial of degree

$$r_{\mathcal{C}}(\rho) \overset{(4.3.2)}{=} \deg(L(T, \rho)) + (\deg(c) + 1)\dim(V) - \mathrm{drop}_{\mathcal{C}}(\rho) = 2g \cdot (\deg(c) + 1) - \mathrm{drop}_{\mathcal{C}\cap\mathcal{S}}(\rho).$$

The corollary follows by observing that

$$\mathrm{drop}_{\mathcal{C}\cap\mathcal{S}}(\rho) = \sum_{v\in\mathcal{C}\cap\mathcal{S}} d_v \cdot \mathrm{drop}_v(\rho) = \deg(\gcd(c, s)) \cdot 1 + \mathrm{drop}_\infty(\rho)$$

and that $\mathrm{drop}_\infty(\rho) = 2g$. □

12.3. ***Arithmetic application.*** In this section we show how to apply our main theorem to the example given above. Let $\mathcal{M} \subset \mathbb{F}_q[t]$ be the subset of monic polynomials, $\mathcal{I} \subset \mathcal{M}$ and $\mathcal{M}_n \subset \mathcal{M}$ be the subsets of irreducibles and polynomials of degree n respectively, and $\mathcal{I}_d = \mathcal{M}_d \cap \mathcal{I}$. Recall that $K = \mathbb{F}_q(t)$ and that $\pi \mapsto v(\pi)$ induces a bijection $\mathcal{I} \to \mathcal{P} \smallsetminus \{\infty\}$.

The Euler factor at $v = \infty$ of the L-function of J is trivial since $\mathrm{drop}_\infty(\rho) = \dim(V)$, and thus the complete L-function satisfies

$$L(T, J/K) = \prod_{\pi\in\mathcal{I}} L(T^{\deg(\pi)}, J/\mathbb{F}_\pi)^{-1} = \prod_{v\in\mathcal{P}} L(T^{d_v}, \rho_v)^{-1} = L_f(T, \rho).$$

Similarly, for the partial L-function of ρ, we have

$$L_{\mathcal{C}}(T, \rho) = \prod_{v\in\mathcal{P}\smallsetminus\mathcal{C}} L(T^{d_v}, \rho_v)^{-1} = \prod_{\substack{\pi\in\mathcal{I} \\ \pi\nmid c}} L(T^{\deg(\pi)}, J/\mathbb{F}_\pi)^{-1}.$$

For each $\pi \in \mathcal{I}$, the Euler factor $L(T, J/\mathbb{F}_\pi)^{-1}$ is the reciprocal of a polynomial with coefficients in $\mathbb{Z}$ so it satisfies

$$T\frac{d}{dT}\log(L(T, J/\mathbb{F}_\pi)) = \sum_{n=1}^{\infty} a_{\pi,n} T^n$$

for integers $a_{\pi,n} \in \mathbb{Z}$.

The complete L-function is also a polynomial with coefficients in $\mathbb{Z}$, and it satisfies

$$T\frac{d}{dT}\log(L(T, J/K)) = T\frac{d}{dT}\log(L_f(T, \rho)) = \sum_{n=1}^{\infty}\Bigg(\sum_{f\in\mathcal{M}_n} \Lambda_\rho(f)\Bigg)T^n,$$

where $\Lambda_\rho(f) : \mathcal{M} \to \mathbb{Z}$ is the von Mangoldt function of ρ defined in (5.2.1) by

$$\Lambda_\rho(f) = \begin{cases} d \cdot a_{\pi,n} & \text{if } f = \pi^m \text{ and } \pi \in \mathcal{I}_d, \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, the partial L-function of ρ is a polynomial with coefficients in $\mathbb{Z}$ and satisfies

$$T\frac{d}{dT}L_{\mathcal{C}}(T, \rho) = \sum_{n=1}^{\infty}\Bigg(\sum_{\substack{f\in\mathcal{M}_n \\ \gcd(f,c)=1}} \Lambda_\rho(f)\Bigg)T^n.$$

For A in $\Gamma(c) = (\mathbb{F}_q[t]/c\mathbb{F}_q[t])^\times$ and positive integer n, we defined the sum $S_{n,c}(A)$ in (5.3.1) by

$$S_{n,c}(A) = \sum_{\substack{f \in \mathcal{M}_n \\ f \equiv A \bmod c}} \Lambda_\rho(f).$$

We then defined the expected value and variance of this sum as A varies uniformly over $\Gamma(c)$ by

$$\mathbb{E}[S_{n,c}(A)] = \frac{1}{\phi(c)} \sum_{A \in \Gamma(c)} S_{n,c}(A), \quad \mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)} \sum_{A \in \Gamma(c)} \left| S_{n,c}(A) - \mathbb{E}[S_{n,c}(A)] \right|^2$$

respectively, where $\phi(c) = |\Gamma(c)|$ (see (5.4.2)).

Theorem 12.3.1. *Suppose that* $\gcd(c, s) = t$ *and that* $\deg(c) > \frac{1}{2g}(72(4g^2+1)^2+1)$. *Then*

$$\phi(c) \cdot \mathbb{E}[S_{n,c}(A)] = \sum_{\substack{f \in \mathcal{M}_n \\ \gcd(f,c)=1}} \Lambda_\rho(f) \quad \textit{and} \quad \lim_{q \to \infty} \frac{\phi(c)}{q^{2n}} \cdot \mathrm{Var}[S_{n,c}(A)] = \min\{n, 2g \cdot \deg(c) - 1\}.$$

Proof. This will follow from applying Theorems 11.0.1, 10.0.4, and 9.0.1 successively, the last with Remarks 9.0.2 and 9.0.3 in mind. To complete the proof we show that all the hypotheses of the first theorem are met.

Lemma 12.2.4 implies that ρ is pointwise pure of weight $w = 1$ and that $\Phi(c)_{\rho\,\mathrm{heavy}}$ is empty.[2] Moreover, Proposition 12.2.1 implies that $V(0)$ has a unique unipotent block of dimension 2 and no other unipotent block of multiplicity 1 (since $2g - 2 \neq 1$); hence Theorem 11.0.1 implies that the Mellin transform of ρ has big monodromy since $\gcd(c, s) = t$ and since

$$\deg(c) > \frac{1}{2g}(72((2g)^2+1)^2 - 2g - 0 + (1+2g)) = \frac{1}{2g}(72(4g^2+1)^2+1).$$

Therefore the hypotheses of Theorem 11.0.1 hold as claimed. □

Taking $g = 1$ and $f = x(x-1)$ yields Theorem 1.2.3 from Section 1.

Appendix A: Middle extension sheaves

Recall the following notation:

- X is a proper smooth geometrically connected curve over $\mathbb{F}_q$.
- U is a dense Zariski open subset of X defined over $\mathbb{F}_q$.
- K is the function field $\mathbb{F}_q(X)$.
- $\mathcal{P}$ is the set of places of K.
- $\mathcal{C}$ is a finite subset of $\mathcal{P}$.
- G_K is the absolute Galois group $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$.

[2] There *are* mixed characters, but as shown the proof of Theorem 9.0.1, they do not contribute to the main term of the variance estimate.

- $I(v)$ is the inertia subgroup in G_K of $v \in \mathcal{P}$.
- $G_{K,\mathcal{C}}$ is the quotient of G_K by normal closure of $\langle I(v) \mid v \in \mathcal{P} \smallsetminus \mathcal{C} \rangle$.
- ℓ is a prime in $\mathbb{N}$ coprime to q.
- $\mathcal{F}$ is a sheaf on X.
- $\mathcal{G}$ is a sheaf on U.

All sheaves in this section are constructible and étale with coefficients in $\overline{\mathbb{Q}}_\ell$.

Let $j : U \to X$ be the inclusion of a dense Zariski open subset. Given $\mathcal{G}$ (e.g., the pullback sheaf $\mathcal{F}|_U = j^*\mathcal{F}$), there are two[3] functorial extensions of $\mathcal{G}$ to a sheaf on all of X we wish to consider: the extension by zero $j_!\mathcal{G}$ and the direct image $j_*\mathcal{G}$. As $\mathcal{F}$ and $\mathcal{G}$ vary we have

$$\mathrm{Hom}_X(j_!\mathcal{G}, \mathcal{F}) = \mathrm{Hom}_U(\mathcal{G}, j^*\mathcal{F}) \quad \text{and} \quad \mathrm{Hom}_X(\mathcal{F}, j_*\mathcal{G}) = \mathrm{Hom}_U(j^*\mathcal{F}, \mathcal{G});$$

that is, the functors $j_!$, j_* are adjoints of j^* (cf. [Milne 1980, II.3.14.a]). In particular, the adjoints of the identity $j^*\mathcal{F} \to j^*\mathcal{F}$ are maps of the form $j_!j^*\mathcal{F} \to \mathcal{F}$ and $\mathcal{F} \to j_*j^*\mathcal{F}$ called *adjunction maps*. We say that $\mathcal{F}$ is *supported on* U if and only if the first map is an isomorphism, and $\mathcal{F}$ is a *middle extension* if and only if the second map is an isomorphism for *every* j.

Lemma A.0.1. (i) *If $j^*\mathcal{F}$ is lisse and $\mathcal{F} \to j_*j^*\mathcal{F}$ is an isomorphism, then $\mathcal{F}$ is a middle extension.*

(ii) *If $\mathcal{G}$ is lisse, then $j_*\mathcal{G}$ is a middle extension.*

Proof. Let $U' \subseteq X$ be a dense Zariski open and $U'' = U \cap U'$. Consider the commutative diagram

$$\begin{array}{ccc} U'' & \xrightarrow{i'} & U' \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j'} \\ U & \xrightarrow[j]{} & X \end{array}$$

of inclusions and the corresponding commutative diagram

$$\begin{array}{ccc} \mathcal{F} & \longrightarrow & j_*j^*\mathcal{F} \\ \downarrow & & \downarrow \\ j'_*j'^*\mathcal{F} & \longrightarrow & (ij)_*(ij)^*\mathcal{F} = (i'j')_*(i'j')^*\mathcal{F} \end{array} \tag{A.0.2}$$

of adjunction maps.

Suppose $\mathcal{G}$ is lisse. On one hand, this implies the map $\mathcal{G} \to i_*i^*\mathcal{G}$ is an isomorphism, so the right map of (A.0.2) is an isomorphism when $\mathcal{G} = j^*\mathcal{F}$. In particular, if the top map of (A.0.2) is also an isomorphism, then the left map must also be an isomorphism for *every* j'; hence (i) holds. On the other hand, the direct image map $j_*\mathcal{G} \to j_*i_*i^*\mathcal{G}$ is also an isomorphism. It even coincides with the adjunction map $j_*\mathcal{G} \to j'_*j'^*j_*\mathcal{G}$ via the functorial identities $j_*i_*i^*\mathcal{G} = j'_*i'_*i^*\mathcal{G} = j'_*j'^*j_*\mathcal{G}$, so (ii) holds. □

[3]One can also consider hybrid versions such as $j''_!j'_*\mathcal{G}$ for inclusions $j' : U \to U'$ and $j'' : U'' \to X$, but we do not need such versions.

Lemma A.0.3. *Suppose $\mathcal{F}$ is a middle extension. If $j^*\mathcal{F} \simeq \mathcal{G}$ on U, then $\mathcal{F} \simeq j_*\mathcal{G}$ on X.*

Proof. Let $j_*j^*\mathcal{F} \to \mathcal{F}$ be the inverse of the adjunction map $\mathcal{F} \to j_*j^*\mathcal{F}$, and let $j^*\mathcal{F} \to \mathcal{G}$ and $\mathcal{G} \to j^*\mathcal{F}$ be mutually inverse morphisms. Then the composed maps

$$\mathcal{F} \to j_*j^*\mathcal{F} \to j_*\mathcal{G} \quad \text{and} \quad j_*\mathcal{G} \to j_*j^*\mathcal{F} \to \mathcal{F}$$

are mutually inverse. □

Let $\bar{\eta}$ be a geometric generic point of X and V be a finite-dimensional $\overline{\mathbb{Q}}_\ell[G_{K,\mathcal{C}}]$-module. The following proposition shows that there is a canonical middle-extension sheaf on X we can associate to V (cf. [Milne 1980, 3.1.16]).

Proposition A.0.4. *There is a middle extension $\mathcal{F}$ with $\mathcal{F}_{\bar{\eta}} = V$ as $G_{K,\mathcal{C}}$-modules, and it is unique up to isomorphism.*

Proof. Suppose $U \subseteq X$ is the open complement corresponding to $\mathcal{C}$ so that the structure map $G_K \to \mathrm{GL}(V)$ factors through the quotient $G_K \twoheadrightarrow G_{K,\mathcal{C}}$ and so that we can identify $G_{K,\mathcal{C}}$ with the étale fundamental group $\pi_1(U, \bar{\eta})$. Then there is a lisse sheaf $\mathcal{G}$ on U corresponding to the representation $\pi_1(U, \bar{\eta}) \to \mathrm{GL}(V)$ through which $G_K \to \mathrm{GL}(V)$ factors, and it is unique up to isomorphism. In particular, $\mathcal{G}$ and $\mathcal{F} = j_*\mathcal{G}$ are middle-extension sheaves by Lemma A.0.1(ii) and $\mathcal{F}_{\bar{\eta}} = \mathcal{G}_{\bar{\eta}} = V$ as $G_{K,\mathcal{C}}$-modules. Every isomorphism $\mathcal{F}_{\bar{\eta}} \simeq V$ of $G_{K,\mathcal{C}}$-modules extends to an isomorphism $j^*\mathcal{F} \to \mathcal{G}$ of lisse sheaves, and Lemma A.0.3 implies the latter extends to an isomorphism $\mathcal{F} \simeq j_*\mathcal{G}$. □

Appendix B: Euler characteristics

We continue the notation of the previous section. Let $j : U \to X$ be the inclusion of a dense Zariski open subset and $\mathcal{F}$ be a sheaf on U. Then there is an exact sequence

$$0 \to j_!\mathcal{F} \to j_*\mathcal{F} \to \mathcal{S}_\mathcal{F} \to 0,$$

where $\mathcal{S}_\mathcal{F}$ is a skyscraper sheaf supported on $Z = X \smallsetminus U$, and the corresponding long exact sequence of (étale) cohomology (over $\overline{\mathbb{F}}_q$) can be written

$$\cdots \to H^i(\bar{Z}, \mathcal{S}_\mathcal{F}) \to H_c^{i+1}(\bar{U}, \mathcal{F}) \to H^{i+1}(\bar{X}, j_*\mathcal{F}) \to \cdots, \tag{B.0.1}$$

where $n \in \mathbb{Z}$.

Lemma B.0.2. *There exist exact sequences*

$$0 \to H_c^0(\bar{U}, \mathcal{F}) \to H^0(\bar{X}, j_*\mathcal{F}) \to H^0(\bar{Z}, \mathcal{S}_\mathcal{F}) \to H_c^1(\bar{U}, \mathcal{F}) \to H^1(\bar{X}, j_*\mathcal{F}) \to 0 \tag{B.0.3}$$

and

$$0 \to H_c^2(\bar{U}, \mathcal{F}) \to H^2(\bar{X}, j_*\mathcal{F}) \to 0 \tag{B.0.4}$$

and all other cohomology groups in (B.0.1) vanish.

Proof. The first term of (B.0.1) vanishes unless $n = 0$ since $\dim(Z) = 0$, and the other two terms vanish for $n+1 \neq 0, 1, 2$ since U and X are curves. Therefore (B.0.1) breaks into the pieces (B.0.3) and (B.0.4), and all other terms vanish. □

If $U = X$, then the middle term of (B.0.3) vanishes, and otherwise the first term vanishes since any curve $U \subsetneq X$ is affine. Either way, the Euler characteristics

$$\chi(\bar{X}, j_*\mathcal{F}) := \sum_{n=0}^{2}(-1)^n \dim(H^i(\bar{X}, j_*\mathcal{F})), \quad \chi_c(\bar{U}, j_*\mathcal{F}) := \sum_{n=0}^{2}(-1)^n \dim(H_c^i(\bar{U}, j_*\mathcal{F})), \tag{B.0.5}$$

and $\chi(\bar{Z}, \mathcal{S}_{\mathcal{F}}) = \dim(H^0(\bar{Z}, \mathcal{S}_{\mathcal{F}}))$ satisfy

$$\chi(\bar{X}, j_*\mathcal{F}) - \chi_c(\bar{U}, \mathcal{F}) = \chi(\bar{Z}, \mathcal{S}_{\mathcal{F}}) = \sum_{z \in Z} \deg(z) \cdot \dim(\mathcal{F}_{\bar{\eta}}^{I(z)}). \tag{B.0.6}$$

B.1. *Middle extensions.* Let ρ be a Galois representation and $\mathrm{ME}(\rho)$ be the corresponding middle-extension sheaf.

Proposition B.1.1. *Let g be the genus of $\bar{X}$. Then*

$$\chi(\bar{X}, \mathrm{ME}(\rho)) = (2-2g) \cdot \mathrm{rank}(\rho) - (\mathrm{drop}(\rho) + \mathrm{Swan}(\rho)).$$

Proof. Suppose $\mathrm{ME}(\rho)$ is lisse on U; we may since $\mathrm{ME}(\rho)$ is a middle extension. On one hand, the Euler–Poincaré formula, as proved by Raynaud [1966, Théorème 1], asserts

$$\chi_c(\bar{U}, \mathrm{ME}(\rho)) = \chi_c(\bar{U}) \cdot \mathrm{rank}(\rho) - \mathrm{Swan}(\rho), \quad \chi_c(\bar{U}) = 2 - 2g - \deg(Z).$$

On the other hand, a short calculation shows

$$\chi(\bar{Z}, \mathrm{ME}(\rho)) = \deg(Z) \cdot \mathrm{rank}(\rho) - \mathrm{drop}(\rho)$$

since U is open and dense in X and hence Z is finite, and thus

$$\chi(\bar{X}, \mathrm{ME}(\rho)) = \chi_c(\bar{U}, \mathrm{ME}(\rho)) + \chi(\bar{Z}, \mathrm{ME}(\rho)) = (2-2g) \cdot \mathrm{rank}(\rho) - \mathrm{drop}(\rho) - \mathrm{Swan}(\rho)$$

as claimed. □

Let $\mathcal{C} \subset \mathcal{P}$ be the subset of places corresponding to the finite complement $Z = X \setminus U$.

Corollary B.1.2. *If* $\mathrm{ME}(\rho)$ *is supported on* U*, then* $\chi_c(\bar{U}, \mathrm{ME}(\rho)) = \chi(\bar{X}, \mathrm{ME}(\rho))$*, and*

$$\chi_c(\bar{U}, \mathrm{ME}(\rho)) = (2 - \deg(\mathcal{C})) \cdot \mathrm{rank}(\rho) - (\mathrm{drop}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho) + \mathrm{Swan}(\rho))$$

in general.

Proof. If $\mathrm{ME}(\rho)$ is supported on U, then $\mathrm{drop}_{\mathcal{C}}(\rho) = \deg(\mathcal{C}) \cdot \mathrm{rank}(\rho)$, so it suffices to show (3.5.3) holds in general. Recall that $Z = \mathcal{C}$, so the desired identity follows easily from the identities

$$\chi_c(\bar{U}, \mathrm{ME}(\rho)) = \chi(\bar{X}, \mathrm{ME}(\rho)) - \chi(\bar{Z}, \mathrm{ME}(\rho)),$$
$$\chi(\bar{Z}, \mathrm{ME}(\rho)) = \deg(\mathcal{C}) \cdot \mathrm{rank}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho)$$

and (3.5.2). □

Let φ be a character of conductor supported by $\mathcal{C}$.

Lemma B.1.3. (i) *If φ is tame, then* $\mathrm{Swan}(\rho \otimes \varphi) = \mathrm{Swan}(\rho)$.

(ii) $\mathrm{drop}(\rho \otimes \varphi) - \mathrm{drop}(\rho) = \mathrm{drop}_{\mathcal{C}}(\rho \otimes \varphi) - \mathrm{drop}_{\mathcal{C}}(\rho)$.

Proof. If $v \in \mathcal{P}$, then $\mathrm{Swan}_v(\rho \otimes \varphi) = \mathrm{Swan}_v(\rho)$ since tensoring with tamely ramified character (e.g., φ) does not change the local Swan conductor. Moreover, if $v \notin \mathcal{C}$, then V and V_φ are isomorphic as $I(v)$-modules (since φ has conductor supported on $\mathcal{C}$). Hence $L(T, \rho_v)$ and $L(T, (\rho \otimes \varphi)_v)$ have the same degree, and in particular,

$$\mathrm{drop}_v(\rho \otimes \varphi) - \mathrm{drop}_v(\rho) = \deg(L(T, \rho_v)) - \deg(L(T, (\rho \otimes \varphi)_v)) = 0$$

when $v \notin \mathcal{C}$. □

Appendix C: Detecting a big subgroup of $\mathbf{GL}_R$

Let R be a positive integer and G be a connected reductive subgroup of $\mathrm{GL}_R(\overline{\mathbb{Q}}_\ell)$, and suppose G acts irreducibly on $\overline{\mathbb{Q}}_\ell^R$. The main goal of this section is to state and prove a theorem of the following form:

Claim C.0.1. *If G contains a suitable element g, then $G = \mathrm{SL}_R(\overline{\mathbb{Q}}_\ell)$ or $G = \mathrm{GL}_R(\overline{\mathbb{Q}}_\ell)$.*

We give explicit conditions on g after introducing some terminology and preliminary results.

C.1. *Weight multiplicity map.* Let m be a positive integer and $[m] = \{1, \dots, m\}$.

Definition C.1.1. A *weight partition map* of an element $\alpha = (\alpha_1, \dots, \alpha_m)$ in $(\overline{\mathbb{Q}}^\times)^m$ is a map $w_\alpha : [m] \to [m]$ satisfying the following for every $i, j \in [m]$:

$$w_\alpha(i) = w_\alpha(j) \quad \text{if and only if} \quad |\iota(\alpha_i)| = |\iota(\alpha_j)|,$$
$$|w_\alpha^{-1}(i)| \geq |w_\alpha^{-1}(j)| \quad \text{if } i \leq j.$$

The fibers of w_α partition the indices $i \in [m]$ according to the corresponding weights $-\log_q |\iota(\alpha_i)|^2$ and are ordered according to size.

In general, α may have multiple weight partition maps, but all will induce the same partition of $[m]$, have the same range, and yield the same map $[m] \to \mathbb{Z}$ given by $i \mapsto |w_\alpha^{-1}(i)|$. In particular, if w_α is a weight partition map of α and if $\sigma \in \mathrm{Sym}(m)$, then the composed map $w_\alpha \sigma$ is also a weight partition map of α.

Definition C.1.2. The *m-th weight multiplicity map* is the map

$$\mu_m : (\overline{\mathbb{Q}}^\times)^m \to \mathbb{Z}^m$$

which sends an element α to the tuple $\lambda = (\lambda_1, \dots, \lambda_m)$ satisfying $\lambda_i = |w_\alpha^{-1}(i)|$ for some weight partition map w_α and every $i \in [m]$.

Definition C.1.3. For any $\lambda = \mu_m(\alpha)$, let $\mathrm{len}(\lambda) = \max\{1 \leq i \leq m : \lambda_i \neq 0\}$.

Observe that $[\mathrm{len}(\lambda)]$ is the range of any weight partition map w_α of α and $(\lambda_1, \ldots, \lambda_{\mathrm{len}(\lambda)})$ is a partition of m.

Example C.1.4. Let $\lambda = \mu_5(1, -1, q, -q, q^2)$. Then $\lambda = \mu_5(q^2, -q, q, -1, 1) = (2, 2, 1, 0, 0)$, and thus $\mathrm{len}(\lambda) = 3$ and $(2, 2, 1)$ is a partition of 5.

Lemma C.1.5. *Let $\alpha, \beta \in (\overline{\mathbb{Q}}^\times)^m$, and let $s \in \overline{\mathbb{Q}}^\times$ and $\sigma \in \mathrm{Sym}(m)$. Suppose $\beta_i = s\alpha_{\sigma(i)}$ for every $i \in [m]$. Then $\mu_m(\alpha) = \mu_m(\beta)$.*

Proof. Let w_α, w_β be respective weight partition maps of α, β. Then for every $i, j \in [m]$, one has

$$w_\beta(i) = w_\beta(j) \iff |\iota(\beta_i)| = |\iota(\beta_j)| \iff |\iota(\alpha_{\sigma(i)})| = |\iota(\alpha_{\sigma(j)})| \iff w_\alpha\sigma(i) = w_\alpha\sigma(j).$$

In particular, the weight partition maps $\sigma w_\alpha, w_\beta$ of α, β respectively coincide, so $\mu_m(\alpha) = \mu_m(\beta)$ as claimed. □

C.2. *Tensor indecomposability.* Let $m, n \geq 2$ be integers, let $\alpha \in (\overline{\mathbb{Q}}^\times)^m$, $\beta \in (\overline{\mathbb{Q}}^\times)^n$, and $\gamma \in (\overline{\mathbb{Q}}^\times)^{mn}$ be elements, and let $a = \mu_m(\alpha)$, $b = \mu_n(\beta)$, $c = \mu_{mn}(\gamma)$. We regard α and β as respective tuples of eigenvalues of matrices $A \in \mathrm{GL}_m(\overline{\mathbb{Q}})$ and $B \in \mathrm{GL}_n(\overline{\mathbb{Q}})$. We also suppose that γ is an eigenvalue tuple of the tensor product $A \otimes B$, and thus there exists a bijection $\tau : [m] \times [n] \to [mn]$ satisfying

$$\gamma_{\tau(i,j)} = \alpha_i \beta_j \quad \text{for } (i, j) \in [m] \times [n].$$

Let $w_\alpha, w_\beta, w_\gamma$ be weight partition maps of α, β, γ respectively.

Lemma C.2.1. *There exists a unique map $\kappa : [\mathrm{len}(a)] \times [\mathrm{len}(b)] \to [\mathrm{len}(c)]$ which makes the following diagram commute*:

$$\begin{array}{ccc} [m] \times [n] & \xrightarrow{\ \tau\ } & [mn] \\ {\scriptstyle w_\alpha \times w_\beta}\big\downarrow & & \big\downarrow{\scriptstyle w_\gamma} \\ [\mathrm{len}(a)] \times [\mathrm{len}(b)] & \xrightarrow[\kappa]{} & [\mathrm{len}(c)]. \end{array}$$

In particular,

$$c_k = \sum_{\kappa(i,j)=k} a_i b_j. \tag{C.2.2}$$

Proof. To see that such a map exists observe that $w_\gamma\tau$ factors through $w_\alpha \times w_\beta$ since

$$\begin{aligned} (w_\alpha \times w_\beta)(i_1, j_1) = (w_\alpha \times w_\beta)(i_2, j_2) &\iff |\alpha_{i_1}| = |\alpha_{i_2}| \text{ and } |\beta_{j_1}| = |\beta_{j_2}| \\ &\implies |\alpha_{i_1}\beta_{j_1}| = |\alpha_{i_2}\beta_{j_2}| \\ &\iff |\gamma_{\tau(i_1,j_1)}| = |\gamma_{\tau(i_2,j_2)}| \\ &\iff w_\gamma\tau(i_1, j_1) = w_\gamma\tau(i_2, j_2) \end{aligned}$$

for every $i_1, i_2 \in [m]$ and $j_1, j_2 \in [n]$. To see that the map is unique, observe that the left vertical map of the diagram is surjective and that the map must satisfy $l \mapsto w_\gamma\tau(i, j)$ for any (i, j) in $(w_\alpha \times w_\beta)^{-1}(l)$.

Finally, (C.2.2) follows from the identities

$$\begin{aligned} c_k &= |w_\gamma^{-1}(k)| = |(\tau \circ w_\gamma)^{-1}(k)| = |(w_\alpha \times w_\beta \circ \kappa)^{-1}(k)| \\ &= \sum_{\kappa(i,j)=k} |(w_\alpha \times w_\beta)^{-1}(i, j)| = \sum_{\kappa(i,j)=k} a_i b_j. \end{aligned}$$

□

Example C.2.3. Let $\alpha = (1, 1, q)$, $\beta = (1, q, q)$, and $\gamma = (1, 1, q, q, q, q, q, q^2, q^2)$. The maps w_α and w_β are canonical and given by

$$w_\alpha(i) = \begin{cases} 1, & i = 1, 2, \\ 2, & i = 3, \end{cases} \qquad w_\beta(j) = \begin{cases} 2, & j = 1, \\ 1, & j = 2, 3. \end{cases}$$

The maps τ and w_γ are not canonical, so we choose

$$\tau(i, j) = 3(j-1) + i, \qquad w_\gamma(j) = \begin{cases} 2, & i = 1, 2, \\ 1, & j = 3, \dots, 7, \\ 3, & i = 8, 9. \end{cases}$$

Then one has $a = b = (2, 1, 0)$ and $c = (4, 2, 2, 0, 0, 0, 0, 0, 0)$, and also

$$w_\gamma \tau(i, j) = \begin{cases} 1, & (i, j) = (1, 1), (2, 1), \\ 3, & (i, j) = (3, 2), (3, 2), \\ 2, & \text{otherwise} \end{cases}$$

for $(i, j) \in [3] \times [3]$. Therefore, the domain and codomain of κ are $[2] \times [2]$ and $[3]$ respectively, and

$$\kappa(i, j) = \begin{cases} 1, & (i, j) = (1, 1), (2, 2), \\ 2, & (i, j) = (1, 2), \\ 3, & (i, j) = (2, 1) \end{cases}$$

for $(i, j) \in [2] \times [2]$.

Lemma C.2.4. *For each $l \in [\mathrm{len}(a)]$, the restriction of κ to $\{l\} \times [\mathrm{len}(b)]$ is injective, and in particular,* $\mathrm{len}(b) \le \mathrm{len}(c)$.

Proof. Recall that $[\mathrm{len}(a)]$ and $[\mathrm{len}(b)]$ are the respective ranges of w_α and w_β, so suppose $i \in [m]$ and $j_1, j_2 \in [n]$. Moreover, one has

$$\begin{aligned} \kappa(w_\alpha(i), w_\beta(j_1)) = \kappa(w_\alpha(i), w_\beta(j_2)) &\iff w_\gamma \tau(i, j_1) = w_\gamma \tau(i, j_2) \\ &\iff |\gamma_{\tau(i,j_1)}| = |\gamma_{\tau(i,j_2)}| \\ &\iff |\alpha_i \beta_{j_1}| = |\alpha_i \beta_{j_2}| \\ &\iff w_\beta(j_1) = w_\beta(j_2), \end{aligned}$$

and thus the restriction of κ to $\{w_\alpha(i)\} \times [\mathrm{len}(b)]$ is injective as claimed. □

Let r be a positive integer.

Lemma C.2.5. (i) *If $c_{\mathrm{len}(c)} \le r$, then $a_{\mathrm{len}(a)} \le r$ and $b_{\mathrm{len}(b)} \le r$.*

(ii) *If $a_1 > r$ then $c_{\mathrm{len}(b)} > r$ and if $b_1 > r$ then $c_{\mathrm{len}(a)} > r$.*

Proof. For part (i), we prove the contrapositive. More precisely, if $k \in [\mathrm{len}(c)]$, then one has

$$c_k \overset{(C.2.2)}{=} \sum_{\kappa(i,j)=k} a_i b_j \geq a_{\mathrm{len}(a)} b_{\mathrm{len}(b)} \geq \max\{a_{\mathrm{len}(a)}, b_{\mathrm{len}(b)}\},$$

and thus $c_{\mathrm{len}(c)} > r$ if $a_{\mathrm{len}(a)} > r$ or $b_{\mathrm{len}(b)} > r$. Thus (i) holds.

For part (ii), we suppose, without loss of generality, that $a_1 > r$ and show that $c_{\mathrm{len}(b)} > r$. We first observe that Lemma C.2.4 implies the integers $\kappa(1,1), \ldots, \kappa(1, \mathrm{len}(b))$ are distinct. Moreover, for each $l \in [\mathrm{len}(b)]$, one has

$$c_{\kappa(1,l)} \geq a_1 b_l > r \cdot 1 = r.$$

Therefore at least $\mathrm{len}(b)$ integers in the monotone decreasing sequence $c_1, \ldots, c_{\mathrm{len}(b)}$ exceed r, and thus (ii) holds. □

The following proposition is the main result of this subsection. We will use it to deduce that a certain representation is tensor indecomposable whenever $mn \gg r$.

Proposition C.2.6. *Suppose* $c_{\mathrm{len}(c)} = 1 < \mathrm{len}(c)$ *and* $c_2 \leq r$. *If* $\mathrm{len}(c) \leq r+1$, *then* $m, n \leq r^2+1$ *and thus* $mn \leq (r^2+1)^2$.

Proof. Lemma C.2.5(i) implies that $a_{\mathrm{len}(a)} = b_{\mathrm{len}(b)} = 1$ since $c_{\mathrm{len}(c)} = 1$. Therefore $\mathrm{len}(a) \geq 2$ and $\mathrm{len}(b) \geq 2$ since $m \geq 2$ and $n \geq 2$ respectively, and moreover, $c_2 \geq c_{\mathrm{len}(a)}$ or $c_2 \geq c_{\mathrm{len}(b)}$. Hence the contrapositive of Lemma C.2.5(ii) implies $a_1 \leq r$ and $b_1 \leq r$ since $c_2 \leq r$. In particular, if $\mathrm{len}(c) \leq r+1$, then Lemma C.2.4 implies $\mathrm{len}(a), \mathrm{len}(b) \leq r+1$, and thus

$$m = \sum_{i=1}^{\mathrm{len}(a)} a_i \leq r a_1 + a_{\mathrm{len}(a)} \leq r^2+1, \quad n = \sum_{j=1}^{\mathrm{len}(b)} b_j \leq r b_1 + b_{\mathrm{len}(b)} \leq r^2+1$$

as claimed. □

C.3. ***Pairing avoidance.*** Let n be a positive integer and I be the $n \times n$ identity matrix. We define the orthogonal and symplectic groups of matrices by

$$\mathrm{O}_n(\overline{\mathbb{Q}}) = \{M \in \mathrm{GL}_n(\overline{\mathbb{Q}}) : MM^t = I\},$$
$$\mathrm{Sp}_{2n}(\overline{\mathbb{Q}}) = \left\{M \in \mathrm{GL}_{2n}(\overline{\mathbb{Q}}) : MPM^t = P \text{ for } P = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\right\}$$

respectively.

Lemma C.3.1. *Suppose* $h \in \mathrm{GL}_m(\overline{\mathbb{Q}})$, *where* $m = n$ (*resp.* $m = 2n$) *and* $hgh^{-1} \in \mathrm{O}_n(\overline{\mathbb{Q}})$ (*resp.* $hgh^{-1} \in \mathrm{Sp}_{2n}(\overline{\mathbb{Q}})$). *Let* $\alpha \in (\overline{\mathbb{Q}}^\times)^m$ *be a tuple of the eigenvalues of* g *and* $a = \mu_m(\alpha)$. *Then some involution* $\pi \in \mathrm{Sym}(\mathrm{len}(a))$ *satisfies the following*:

(i) $a_i = a_{\pi(i)}$ *for every* $i \in [\mathrm{len}(a)]$.

(ii) π *has at most one fixed point.*

Proof. Since g and hgh^{-1} have the same eigenvalues, we suppose without loss of generality that $h = 1$. The involution $s \mapsto 1/s$ of $\overline{\mathbb{Q}}^\times$ induces a permutation of the eigenvalues of elements of $\mathrm{O}_n(\overline{\mathbb{Q}})$ and $\mathrm{Sp}_{2n}(\overline{\mathbb{Q}})$. The latter is an involution $\sigma \in \mathrm{Sym}(m)$ with the property that, for any weight partition map w_α of α and every $i \in [m]$, one has

$$w_\alpha(i) = w_\alpha\sigma(i) \iff |\alpha_i| = |\alpha_{\sigma(i)}| \iff |\alpha_i| = |1/\alpha_i| \iff |\alpha_i| = 1.$$

The involution in question is given by $w_\alpha(i) \mapsto w_\alpha\sigma(i)$ for every $i \in [m]$; recall w_α maps onto $[\mathrm{len}(a)]$. □

The following is the main result of this subsection. We will use it to show that some subgroup of $\mathrm{GL}_m(\overline{\mathbb{Q}})$ fails to preserve nondegenerate pairings which are either symmetric or alternating.

Proposition C.3.2. *Let g be an element of $\mathrm{GL}_m(\overline{\mathbb{Q}})$, $\alpha \in (\overline{\mathbb{Q}}^\times)^m$ be a tuple of its eigenvalues, and $a = \mu_m(\alpha)$. If there exist i, j such that a_i, a_j are distinct from each other and from all a_k for $k \neq i, j$, then g is not conjugate to an element of $\mathrm{O}_m(\overline{\mathbb{Q}})$. If moreover $m = 2n$, then g is not conjugate to an element of $\mathrm{Sp}_{2n}(\overline{\mathbb{Q}})$.*

Proof. We prove the contrapositive. More precisely, if $hgh^{-1} \in \mathrm{O}_m(\overline{\mathbb{Q}})$ or $hgh^{-1} \in \mathrm{Sp}_{2n}(\overline{\mathbb{Q}})$ for some $h \in \mathrm{GL}_m(\overline{\mathbb{Q}})$ and if $\pi \in \mathrm{Sym}(\mathrm{len}(a))$ is an involution satisfying the properties of Lemma C.3.1, then $\pi(i) = i$ for at most one i. Therefore, for all but at most one i and for $j = \pi(i)$, one has $i \neq j$ and $a_i = a_j$. In particular, there is at most one i such that $a_i \neq a_j$ for $j \neq i$. □

C.4. *Main theorem.* In this section we state and prove the main result of this appendix.

Theorem C.4.1. *Let r, R be positive integers and G be a connected reductive subgroup of $\mathrm{GL}_R(\overline{\mathbb{Q}}_\ell)$. Let $g \in G$ be an element and $\gamma \in (\overline{\mathbb{Q}}_\ell^\times)^R$ be an eigenvector tuple of g. Suppose that G is irreducible, that γ lies in $(\overline{\mathbb{Q}}^\times)^R$, and that $c = \mu_R(\gamma)$ satisfies $1 < \mathrm{len}(c) \leq r + 1$ and $1 = c_{\mathrm{len}(c)} < c_{\mathrm{len}(c)-1}$ and $c_2 \leq r$. If $R > 72(r^2 + 1)^2$, then either $G = \mathrm{SL}_R(\overline{\mathbb{Q}}_\ell)$ or $G = \mathrm{GL}_R(\overline{\mathbb{Q}}_\ell)$.*

The proof will occupy the remainder of this subsection.

Since G is algebraic, it contains the semisimplification of g, an element for which γ is also an eigenvector. Hence we replace g by its semisimplification and suppose without loss of generality that g is semisimple. We also replace G and g by the conjugates $h^{-1}Gh$ and $h^{-1}gh$ by a suitable element $h \in \mathrm{GL}_R(\overline{\mathbb{Q}}_\ell)$ so that we may suppose without loss of generality that g is the diagonal matrix $\mathrm{diag}(\gamma_1, \ldots, \gamma_R)$.

Let $V = \overline{\mathbb{Q}}_\ell^R$ and f be the diagonal matrix

$$f = \mathrm{diag}(|\iota(\gamma_1)|, \ldots, |\iota(\gamma_R)|).$$

We claim we may regard f as an element of $\mathrm{GL}_R(\overline{\mathbb{Q}}_\ell)$. More precisely, it is an element of $\mathrm{GL}_R(\iota(\overline{\mathbb{Q}})) \subset \mathrm{GL}_R(\mathbb{C})$ since $|\iota(\gamma_i)|^2 = \iota(\gamma_i)\overline{\iota(\gamma_i)}$ lies in the algebraically closed subfield $\iota(\overline{\mathbb{Q}}) \subset \mathbb{C}$ and thus so does $|\iota(\gamma_i)|$. Replacing G, g, f by conjugates by a suitable common permutation matrix, we suppose without loss of generality that $|\iota(\gamma_1)|$ is an eigenvalue of f of multiplicity c_1.

Lemma C.4.2. *The matrix f is a semisimple element of G such that $f - |\iota(\gamma_1)| \in \mathrm{End}(V)$ has rank at most r^2.*

Proof. For some sequence $e_1, \dots, e_n$ of tuples $e_i = (e_{i,1}, \dots, e_{i,m}) \in \mathbb{Z}^m$, the intersection of G with the subgroup of diagonal matrices in $\mathrm{GL}_R(\overline{\mathbb{Q}}_\ell)$ consists of all matrices $\mathrm{diag}(\alpha_1, \dots, \alpha_m)$ satisfying

$$\prod_{i=1}^m \alpha_i^{e_{1,i}} = \prod_{i=1}^m \alpha_i^{e_{2,i}} = \cdots = \prod_{i=1}^m \alpha_i^{e_{n,i}} = 1.$$

By hypothesis, g lies in this intersection, and thus

$$\left|\iota\left(\prod_{i=1}^m \gamma_i^{e_{1,i}}\right)\right| = \left|\iota\left(\prod_{i=1}^m \gamma_i^{e_{2,i}}\right)\right| = \cdots = \left|\iota\left(\prod_{i=1}^m \gamma_i^{e_{n,i}}\right)\right| = |\iota(1)|$$

or equivalently

$$\prod_{i=1}^m |\iota(\gamma_i)|^{e_{1,i}} = \prod_{i=1}^m |\iota(\gamma_i)|^{e_{2,i}} = \cdots = \prod_{i=1}^m |\iota(\gamma_i)|^{e_{n,i}} = 1.$$

Therefore f is a diagonal (hence semisimple) element of G as claimed. It remains to show $f - |\iota(\gamma_1)| \in \mathrm{End}(V)$ has rank at most r^2. Indeed, exactly c_1 of its eigenvalues equal $|\iota(\gamma_1)|$; hence the rank of $f - |\iota(\gamma_1)|$ is

$$R - c_1 \le \sum_{i=2}^{\mathrm{len}(c)} c_i \le r \cdot r = r^2$$

by our hypotheses on c. □

Let $[G, G]$ be the derived (i.e., commutator) subgroup of G. Observe that G acts irreducibly on $V = \overline{\mathbb{Q}}_\ell^R$ by hypothesis, so its center $Z(G)$ consists entirely of scalars and G is an almost product of $[G, G]$ and $Z(G)$. In particular, $[G, G]$ is a connected semisimple group which also acts irreducibly on V, and for some $a \in \overline{\mathbb{Q}}_\ell^\times$, the scalar multiple af lies in $[G, G]$.

Let $\mathfrak{g} \subseteq \mathfrak{gl}_R = \mathrm{End}(V)$ be the Lie algebra of $[G, G]$. We claim $\mathfrak{g}$ is simple. On one hand, $\mathfrak{g}$ is a semisimple irreducible Lie subalgebra of $\mathfrak{gl}_R$ since $[G, G]$ is semisimple and acts irreducibly on V. It also contains af, and Lemma C.4.2 implies that $\dim((af - a|\iota(\gamma_1)|)V) \le r^2$; hence the contrapositive of Proposition C.2.6 implies that V is not tensor decomposable as a representation of $\mathfrak{g}$. On the other hand, $\mathfrak{g}$ has a decomposition $\mathfrak{g} = \prod_{i=1}^n \mathfrak{g}_i$ with respect to simple Lie subalgebras $\mathfrak{g}_1, \dots, \mathfrak{g}_n \subseteq \mathfrak{g}$, and thus V has a tensor decomposition $V = \bigotimes_{i=1}^n V_i$ where $\mathfrak{g}_i$ acts faithfully on V_i. In particular, $n = 1$ since V is not tensor decomposable, and thus $\mathfrak{g}$ is simple as claimed. (Compare [Katz 2002, proof of Theorem 1.4.3].)

We now apply the following theorem to deduce that $\mathfrak{g}$ is one of $\mathfrak{sl}(V)$, $\mathfrak{so}(V)$, or $\mathfrak{sp}(V)$.

Theorem C.4.3. (Zarhin) *Let $\mathfrak{g} \subseteq \mathrm{End}(V)$ be a simple Lie subalgebra, and suppose that $\mathfrak{g}$ acts irreducibly on V. Let $(a, f) \in \overline{\mathbb{Q}}_\ell \times \mathfrak{g}$ and $r = \mathrm{rank}(f - a)$. If $R = \dim(V) > 72r^2$, then $\mathfrak{g}$ is one of $\mathfrak{sl}(V)$, $\mathfrak{so}(V)$, or $\mathfrak{sp}(V)$.*

Proof. See [Zarhin 1990, Lemma 4 and Theorem 6]. These results refer to constants D and D_2 respectively, and in the proofs one finds $D = \frac{1}{8}$ and $D_2 = 9/D = 72$ suffice. The latter is the source of the constant 72 in the hypothesis $R > 72r^2$. Compare [Katz 2002, Theorem 1.4.4]. □

To complete the proof of the theorem it suffices to rule out $\mathfrak{g} = \mathfrak{so}(V)$ and $\mathfrak{g} = \mathfrak{sp}(V)$ or equivalently to show that G preserves neither an orthogonal nor a symplectic pairing. However, our hypotheses on c, together with the contrapositive of Proposition C.3.2, imply that G preserves neither such type of pairing, so $\mathfrak{g} = \mathfrak{sl}(V)$ as claimed. That is, $[G, G]$ is $\mathrm{SL}(V)$ and G is equal to one of $\mathrm{SL}(V)$ or $\mathrm{GL}(V)$.

Appendix D: Perverse sheaves and the Tannakian monodromy group

D.1. ***Category of perverse sheaves.*** Given a smooth curve X over a perfect field $\mathbb{F}$, we can speak of the so-called derived category $D^b_c(X, \overline{\mathbb{Q}}_\ell)$. Its objects M are complexes of constructible $\overline{\mathbb{Q}}_\ell$-sheaves on X over $\mathbb{F}$ whose cohomology complex

$$\cdots \to \mathcal{H}^{-1}(M) \to \mathcal{H}^0(M) \to \mathcal{H}^1(M) \to \cdots$$

is bounded and whose cohomology sheaves $\mathcal{H}^i(M)$ are all constructible. There is a well-defined dual object DM, the Verdier dual of M. Moreover, for each $n \in \mathbb{Z}$, there is a well-defined shifted complex $M[n]$ which satisfies $\mathcal{H}^i(M[n]) = \mathcal{H}^{i+n}(M)$.

We say that M is *semiperverse* if and only if $\mathcal{H}^0(M)$ is punctual and $\mathcal{H}^i(M)$ vanishes for $i > 0$ and that M is *perverse* if and only if M and DM are semiperverse. We write $\mathrm{Perv}(X, \overline{\mathbb{Q}}_\ell)$ for the full subcategory of perverse objects in $D^b_c(X, \overline{\mathbb{Q}}_\ell)$. It is an abelian category; thus one can speak of subquotients of its objects as well as kernels and cokernels of its morphisms. It is common to call its objects perverse sheaves despite the fact that they are *complexes* of sheaves.

There is a natural functor from the category of constructible $\overline{\mathbb{Q}}_\ell$-sheaves on X over k to $D^b_c(X, \overline{\mathbb{Q}}_\ell)$: it sends a sheaf $\mathcal{F}$ to a complex concentrated at $i = 0$ and takes a morphism to the unique extension to a morphism of complexes. The image of this functor is not stable under duality though: if $\mathcal{F}^\vee$ is the dual of $\mathcal{F}$, then $D\mathcal{F}$ is isomorphic to $\mathcal{F}^\vee(1)[2]$. If instead one sends each $\mathcal{F}$ to $\mathcal{F}\left(\frac{1}{2}\right)[1]$, then self-dual objects are taken to self-dual objects and middle-extension sheaves are taken to perverse sheaves.

D.2. ***Purity.*** Let X be a smooth curve over $\mathbb{F}_q$. We say an object M in $D^b_c(X, \overline{\mathbb{Q}}_\ell)$ is *ι-mixed of weights* $\le w$ if and only if $\mathcal{H}^i(M)$ is pointwise ι-mixed of weights $\le w + i$ for every i, and then $M[n]$ is ι-mixed of weights $w + n$. We also say M is *ι-pure of weight w* if and only if M is ι-mixed of weights $\le w$ and DM is ι-mixed of weights $\le -w$, and then $M[n]$ is ι-pure of weight $w + n$. Finally, we say M is *pure of weight w* if and only if it is ι-pure of weight w for every field embedding $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$.

D.3. ***Subobjects and subquotients.*** Let $(\mathcal{C}, \oplus)$ be an abelian category, let $\mathbf{0}$ be its zero object, and let M, N be a pair of objects in $\mathcal{C}$.

We say that N is a *subobject* of M and write $N \subseteq M$ if and only if there is a monomorphism $N \hookrightarrow M$ in $\mathcal{C}$. More generally, we say N of M is a *subquotient* of M if and only if there exist an object S, a monomorphism $S \hookrightarrow M$, and an epimorphism $S \twoheadrightarrow N$ all in $\mathcal{C}$. Equivalently, N is a subquotient of M if and only if there exist an object Q, an epimorphism $M \twoheadrightarrow Q$, and a monomorphism $N \hookrightarrow Q$ all in $\mathcal{C}$.

Proposition D.3.1. *If $M \in \mathrm{Perv}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ is ι-pure of weight w, then so is every subquotient N.*

Proof. See [Beĭlinson et al. 1982, 5.3.1]. ∎

Given a pair $N_1, N_2 \subseteq M$ of subobjects, we write $N_1 \subseteq N_2 \subseteq M$ if and only if $N_1 \subseteq N_2$ and, for the corresponding monomorphisms, $N_1 \hookrightarrow M$ equals the composition $N_1 \hookrightarrow N_2 \hookrightarrow M$. We also write $N_1 = N_2 \subseteq M$ if and only if $N_1 \subseteq N_2 \subseteq M$ and $N_2 \subseteq N_1 \subseteq M$. For example, if M is an object in $\mathrm{Perv}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ and if ϕ is the Frobenius automorphism of $\overline{M}$, then the subobjects $N \subseteq M$ give rise to precisely those subobjects $\overline{N} \subseteq \overline{M}$ satisfying $\overline{N} = \phi(\overline{N}) \subseteq \overline{M}$.

D.4. ***Kummer sheaves.*** Let $\mathbb{G}_m = \mathbb{P}^1_u \setminus \{0, \infty\}$ over $\mathbb{F}_q$, and let $\pi_1^{\mathrm{t}}(\mathbb{G}_m)$ be the tame étale fundamental group, that is, the maximal quotient of $\pi_1(\mathbb{G}_m)$ whose kernel contains the p-Sylow subgroups of $I(0)$ and $I(\infty)$. It lies in an exact sequence

$$1 \to \pi_1^{\mathrm{t}}(\overline{\mathbb{G}}_m) \to \pi_1^{\mathrm{t}}(\mathbb{G}_m) \to \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to 1,$$

where $\pi_1^{\mathrm{t}}(\overline{\mathbb{G}}_m)$ is the image of $\pi_1(\overline{\mathbb{G}}_m)$ via the tame quotient $\pi_1(\mathbb{G}_m) \twoheadrightarrow \pi_1^{\mathrm{t}}(\mathbb{G}_m)$.

We say a constructible sheaf on $\overline{\mathbb{P}}^1$ is a *Kummer sheaf* if and only if it is a middle-extension sheaf which is lisse of rank 1 on $\overline{\mathbb{G}}_m$ and for which the corresponding representation factors through the quotient $\pi_1(\overline{\mathbb{G}}_m) \twoheadrightarrow \pi_1^{\mathrm{t}}(\overline{\mathbb{G}}_m)$. Equivalently, the Kummer sheaves are the middle-extension sheaves $\mathcal{L}_\rho$ on $\overline{\mathbb{P}}^1$ associated to a continuous character $\rho : \pi_1^{\mathrm{t}}(\overline{\mathbb{G}}_m) \to \overline{\mathbb{Q}}_\ell^\times$.

D.5. ***Middle convolution on $\mathcal{P}$.*** Let $\pi : \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ be the multiplication map on $\mathbb{G}_m$ over $\mathbb{F}_q$. Using it one can define two additive bifunctors on $D_c^b(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$ corresponding to two flavors of multiplicative convolution:

$$M \star_! N := R\pi_!(M \boxtimes N), \qquad M \star_* N := R\pi_*(M \boxtimes N).$$

There is a canonical map $M \star_! N \to M \star_* N$, but it need not be an isomorphism in general. However, if both convolution objects lie in $\mathrm{Perv}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$, then one can speak of the image of the map and define

$$M *_{\mathrm{mid}} N := \mathrm{Image}(M \star_! N \to M \star_* N).$$

This observation led Katz to define the full subcategory $\mathcal{P}$ of $\mathrm{Perv}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$ whose objects are all M for which $N \mapsto M \star_! N$ and $N \mapsto M \star_* N$ take perverse sheaves to perverse sheaves (see [Katz 1996, §2.6] and [Katz 2012, Chapter 2]). Among other things, it includes perverse sheaves $\mathcal{F}[1]$ for $\mathcal{F}$ a simple middle-extension sheaf on $\overline{\mathbb{G}}_m$ of generic rank at least 2. Moreover, it is an additive category with respect to the usual direct sum of sheaves. Katz called the resulting additive bifunctor on $\mathcal{P}$ middle convolution.

D.6. ***The category $\mathcal{P}_{\mathrm{arith}}$.*** Let $D_c^b(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell) \to D_c^b(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$ be the "extension of scalars" functor which sends an object of M over $\mathbb{F}_q$ to the object $\overline{M} = M \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. It maps objects of $\mathrm{Perv}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ to objects of $\mathrm{Perv}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$, and we define $\mathcal{P}_{\mathrm{arith}}$ to be the full subcategory of $\mathrm{Perv}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ whose objects M are those for which $\overline{M}$ lies in $\mathcal{P}$. Among other things, $\mathcal{P}_{\mathrm{arith}}$ contains perverse sheaves $\mathcal{F}[1]$ for $\mathcal{F}$ a geometrically simple middle-extension sheaf on $\mathbb{G}_m$ over $\mathbb{F}_q$ which is of generic rank at least 2.

Once again we have the two flavors of multiplicative convolution

$$M \star_! N := R\pi_!(M \boxtimes N), \qquad M \star_* N := R\pi_*(M \boxtimes N)$$

for any pair of objects M, N in $\mathrm{Perv}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$. We can also define middle convolution on $\mathcal{P}_{\mathrm{arith}}$ as before:

$$M *_{\mathrm{mid}} N := \mathrm{Image}(M \star_! N \to M \star_* N)$$

for any pair of objects M, N in $\mathcal{P}_{\mathrm{arith}}$.

Proposition D.6.1. *If M and N are ι-pure of weights m and n respectively, then $M *_{\mathrm{mid}} N$ is ι-pure of weight $m+n$.*

Proof. Our argument is essentially that of [Katz 2012, Chapter 4]. On one hand, $M \boxtimes N$ is ι-pure of weight $m+n$ on $\mathbb{G}_m \times \mathbb{G}_m$; hence [Deligne 1980, 3.3.1] and Proposition D.3.1 imply $M \star_! N$ and its perverse quotient $M *_{\mathrm{mid}} N$ are ι-mixed of weight $m+n$. On the other hand, DM and DN are ι-pure of weights m and n respectively, and

$$\begin{aligned} D(M *_{\mathrm{mid}} N) &= \mathrm{Image}(D(M \star_* N) \to D(M \star_! N)) \\ &= \mathrm{Image}(DM \star_! DN \to DM \star_* DN) = DM *_{\mathrm{mid}} DN; \end{aligned}$$

hence $D(M *_{\mathrm{mid}} N)$ is ι-mixed of weight $\le m+n$ (cf. [Deligne 1980, 6.2]). Thus $M *_{\mathrm{mid}} N$ is ι-pure of weight $m+n$ as claimed. □

D.7. *The category* $\mathbf{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$. Gabber and Loeser [1996, p. 529] defined an object M in $\mathrm{Perv}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$ to be *negligible* if and only if its Euler characteristic $\chi(\overline{\mathbb{G}}_m, M)$ vanishes, or equivalently, it is isomorphic to a successive extension of shifted Kummer sheaves $\mathcal{L}_\rho[1]$ (cf. [loc. cit., 3.5.3]). They showed that the full subcategory $\mathrm{Negl}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$ of $\mathrm{Perv}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$ whose objects are the negligible sheaves is a thick subcategory of the abelian category (see [loc. cit., 3.5.2]), and thus one can speak of the quotient category

$$\mathrm{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell) := \mathrm{Perv}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)/\mathrm{Negl}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell).$$

They then proceeded to show that $\mathrm{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$ is a neutral Tannakian category (see [loc. cit., 3.7.5] and [Deligne et al. 1982, II.2.19]).

Theorem D.7.1. *The composite map $\mathcal{P} \to \mathrm{Perv}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell) \to \mathrm{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$ induces an equivalence of categories such that*:

(i) *Middle convolution on $\mathcal{P}$ induces a tensor product $\otimes$ on $\mathrm{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$.*

(ii) *The unit object $\mathbf{1}$ corresponds to the skyscraper sheaf $i_*\overline{\mathbb{Q}}_\ell$ for $i : \{1\} \to \overline{\mathbb{G}}_m$ the inclusion.*

(iii) *The dual $M^\vee$ of an object M is the object $[x \mapsto 1/x]^* DM$.*

(iv) *The dimension $\dim(M)$ of an object M is $\chi(\overline{\mathbb{G}}_m, M)$.*

(v) *A fiber functor is $M \mapsto H^0(\overline{\mathbb{A}}^1_u, j_{0!}M)$ for $j_0 : \mathbb{G}_m \to \mathbb{A}^1_u$ the inclusion.*

See [Gabber and Loeser 1996, 3.7.2] and [Katz 2012, Chapters 2–3].

D.8. ***The category*** $\mathbf{Tann}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$. Let $\mathrm{Negl}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ be the full subcategory of $\mathrm{Perv}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ whose objects M are those for which $\overline{M}$ lies in $\mathrm{Negl}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$, and let

$$\mathrm{Tann}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell) := \mathrm{Perv}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)/\mathrm{Negl}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell).$$

Like $\mathrm{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$, the quotient category is an abelian category and even a neutral Tannakian category with tensor product $\otimes$ given by middle convolution. Moreover, the "extension of scalars" functor induces a functor

$$\mathrm{Tann}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell) \to \mathrm{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$$

which we also call the "extension of scalars" functor.

Proposition D.8.1. *Suppose $M, N \in \mathrm{Tann}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ are ι-pure of weights m and n respectively. Then $M^\vee$, $N^\vee$, and $M \otimes N$ are ι-pure of weights m, n, and $m+n$ respectively.*

Proof. The Verdier duals DM and DN are ι-pure of weights m and n respectively; hence so are the Tannakian duals $M^\vee = [x \mapsto 1/x]^* DM$ and $N^\vee = [x \mapsto 1/x]^* DN$. Moreover, Proposition D.6.1 implies that $M \otimes N = M *_{\mathrm{mid}} N$ is ι-pure of weight $m+n$. □

D.9. ***Semisimple abelian categories.*** We say that M is *simple* if and only if the only subobjects $N \subseteq M$ in $\mathcal{C}$ are isomorphic to $\mathbf{0}$ or M. More generally, we say that M is *semisimple* if and only if it is isomorphic to a finite direct sum $N_1 \oplus \cdots \oplus N_m$ of simple subobjects $N_1, \ldots, N_m \subseteq M$. We say that $\mathcal{C}$ is *semisimple* if and only if each of its objects is semisimple.

Proposition D.9.1. *If $M \in \mathrm{Tann}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ is ι-pure of weight zero, then $\langle \overline{M} \rangle$ is semisimple.*

Proof. If $N_1, N_2 \in \mathrm{Tann}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ are ι-pure of weight zero, then so is $N_1 \oplus N_2$. Therefore Proposition D.6.1 implies that $T^{a,b}(M)$ is pure of weight zero, for every $a, b \geq 0$, and [Beĭlinson et al. 1982, 5.3.8] implies that $T^{a,b}(\overline{M})$ is semisimple. □

D.10. ***Tannakian monodromy group.*** Let k be an algebraically closed field of characteristic zero and $\mathbf{Vec}_k$ be the category of finite-dimensional vector spaces over k. It is well known that the latter yields a rigid abelian tensor category $(\mathbf{Vec}_k, \otimes)$ with respect to the usual operators $\oplus$ and $\otimes$ of vector spaces and with unit object $\mathbf{1} = k$.

Let $(\mathcal{C}, \otimes)$ be a neutral Tannakian category over k. Thus $(\mathcal{C}, \otimes)$ is a rigid abelian tensor category whose unit object $\mathbf{1}$ satisfies $k = \mathrm{End}(\mathbf{1})$ and for which there exists a fiber functor ω, that is, an exact faithful k-linear tensor functor $\omega : \mathcal{C} \to \mathbf{Vec}_k$. For example, $\mathbf{Vec}_k$ is a neutral Tannakian category and the identity functor $\mathbf{Vec}_k \to \mathbf{Vec}_k$ is a fiber functor. More generally, given an affine group scheme G over k, the category $\mathbf{Rep}_k(G)$ of linear representations of G on finite-dimensional k-vector spaces yields a neutral Tannakian category $(\mathbf{Rep}_k(G), \otimes)$, and the forgetful functor $\mathbf{Rep}_k(G) \to \mathbf{Vec}_k$ is a fiber functor.

Given an object M of $\mathcal{C}$, its dual $M^\vee$, and nonnegative integers a, b, let

$$T^{a,b}(M) := M^{\otimes a} \oplus (M^\vee)^{\otimes b}$$

and let $\langle M\rangle$ be the full tensor subcategory of $\mathcal{C}$ whose objects consist of all subobjects of $T^{a,b}(M)$ for all $a, b \geq 0$. For each automorphism $\gamma \in \mathrm{Aut}_{\mathcal{C}}(M)$, let $\gamma^\vee \in \mathrm{Aut}_{\mathcal{C}}(M^\vee)$ be the corresponding dual automorphism and $T^{a,b}(\gamma) \in \mathrm{Aut}_{\mathcal{C}}(T^{a,b}(M))$ be the induced automorphism.

Let $\mathbf{Alg}_k$ be the category of k-algebras and **Set** be the category of sets. Given a pair ω_1, ω_2 of fiber functors $\mathcal{C} \to \mathbf{Vec}_k$ and an object M in $\mathcal{C}$, one can define a functor

$$\underline{\mathrm{Isom}}^{\otimes}(\omega_1|M, \omega_2|M) : \mathbf{Alg}_k \to \mathbf{Set}$$

by sending a k-algebra R to the set

$$\{\gamma \in \mathrm{Isom}_R(\omega_1(M)_R, \omega_2(M)_R) : T^{a,b}(\gamma)(\omega_1(N)) \subseteq \omega_2(N) \text{ for all } a, b \geq 0 \text{ and } N \subseteq T^{a,b}(M)\},$$

where $\omega_i(M)_R = \omega_i(M) \otimes_k R$ and

$$\mathrm{Isom}_R(\omega_1(M)_R, \omega_2(M)_R) = \{\gamma \in \mathrm{Hom}_R(\omega_1(M)_R, \omega_2(M)_R) : \gamma \text{ is invertible}\}.$$

Similarly, given a single fiber functor $\omega : \mathcal{C} \to \mathbf{Vec}_k$ and object M in $\mathcal{C}$, one can define a functor

$$\underline{\mathrm{Aut}}^{\otimes}(\omega \mid M) : \mathbf{Alg}_k \to \mathbf{Set}$$

as the functor $\underline{\mathrm{Isom}}^{\otimes}(\omega \mid M, \omega \mid M)$.

Theorem D.10.1. *Let ω_1, ω_2 be fiber functors $\mathcal{C} \to \mathbf{Vec}_k$ and M be an object of $\mathcal{C}$.*

(i) *$\underline{\mathrm{Aut}}^{\otimes}(\omega_i \mid M)$ is representable by an algebraic group scheme $G_{\omega_i \mid M}$ over k.*

(ii) *If $\langle M\rangle$ is semisimple, then $G_{\omega_i \mid M}$ is reductive.*

(iii) *$\underline{\mathrm{Isom}}^{\otimes}(\omega_1 \mid M, \omega_2 \mid M)$ is represented by an affine scheme over k which is a $G_{\omega_1 \mid M}$-torsor.*

See [Deligne et al. 1982, II.2.11, II.2.20, II.2.28, and II.3.2].

We call the group scheme $G_{\omega_i \mid M}$ in the theorem the *Tannakian monodromy group* of $\langle M\rangle$ with respect to ω_i.

Theorem D.10.2. *Let $\omega : \mathrm{Perv}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell) \to \mathbf{Vec}_k$ be a fiber functor over $\overline{\mathbb{F}}_q$ and $M \in \mathrm{Perv}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$. If M is pure of weight zero, then $G_{\omega \mid \overline{M}}$ is reductive.*

Proof. This follows from Proposition D.9.1 and Theorem D.10.1(ii). □

D.11. ***Geometric versus arithmetic monodromy.*** For every object M in $\mathrm{Tann}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ and all integers $a, b \geq 0$, the "extension of scalars" functor sends a subobject $N \subseteq T^{a,b}(M)$ to a subobject $\overline{N} \subseteq T^{a,b}(\overline{M})$. Moreover, composing the functor with a fiber functor ω on $\mathrm{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell)$ yields a fiber functor on $\mathrm{Tann}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ which we also denote ω. Thus there is a natural transformation

$$\underline{\mathrm{Aut}}^{\otimes}(\omega \mid \overline{M}) \to \underline{\mathrm{Aut}}^{\otimes}(\omega \mid M)$$

and a corresponding monomorphism of Tannakian monodromy groups

$$G_{\omega \mid \overline{M}} \to G_{\omega \mid M}.$$

We call $G_{\omega\,|\,\overline{M}}$ and $G_{\omega\,|\,M}$ the *geometric* and *arithmetic Tannakian monodromy groups* of M with respect to ω respectively.

Proposition D.11.1. *Suppose M is in* $\mathrm{Tann}(\mathbb{G}_m/\mathbb{F}_q, \overline{\mathbb{Q}}_\ell)$ *and is pure of weight zero. Then*:

(i) *$G_{\omega\,|\,\overline{M}}$ is a normal subgroup of $G_{\omega\,|\,M}$.*

(ii) *If M is arithmetically semisimple, then $G_{\omega\,|\,M}/G_{\omega\,|\,\overline{M}}$ is a torus, and thus $G_{\omega\,|\,M}$ is reductive.*

Proof. Proposition D.9.1 implies that $\overline{M}$ is semisimple, so part (1) follows from [Katz 2012, Theorem 6.1]. Therefore we can speak of the quotient $G_{\omega\,|\,M}/G_{\omega\,|\,\overline{M}}$, and [loc. cit., Lemmma 7.1] implies it is a quotient of M if M is arithmetically semisimple. Moreover, Theorem D.10.2 implies that $G_{\omega\,|\,\overline{M}}$ is reductive, so part (2) follows by observing that the extension of a torus by a reductive group is reductive. □

D.12. *Frobenius element.* Let ω be a fiber functor $\mathrm{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell) \to \mathbf{Vec}_k$, let $E/\mathbb{F}_q$ be a finite extension, and let M be in $\mathrm{Tann}(\mathbb{G}_m/E, \overline{\mathbb{Q}}_\ell)$. The geometric Frobenius element of $\mathrm{Gal}(\overline{\mathbb{F}}_q/E)$ induces a well-defined automorphism ϕ_E of $\overline{M}$. By applying ω, one obtains a well-defined k-linear automorphism of $\omega(\overline{M})$, that is, an element of $\mathrm{GL}(\omega(\overline{M})) = \mathrm{GL}(\omega(M))$. It is even an element of $G_{\omega\,|\,M}$ since, for every $N \subseteq T^{a,b}(M)$ and $a, b \geq 0$, one has

$$\overline{N} = T^{a,b}(\phi_E)(\overline{N}) \subseteq T^{a,b}(\overline{M})$$

and thus

$$\omega(\overline{N}) = T^{a,b}(\phi_E)(\omega(\overline{N})) \subseteq \omega(T^{a,b}(\overline{M})) = T^{a,b}(\omega(M)).$$

We call $\omega(\phi_E)$ the *geometric Frobenius element* of $G_{\omega\,|\,M}$.

D.13. *Frobenius conjugacy classes.* Let ω_1, ω_2 be fiber functors $\mathrm{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell) \to \mathbf{Vec}_k$, let M be an element of $\mathrm{Tann}(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$, and let π be an element of $\underline{\mathrm{Isom}}^{\otimes}(\omega_1 \mid M, \omega_2 \mid M)(k)$. Then Theorem D.10.1(iii) implies that the map $g \mapsto \pi g$ induces a bijection

$$G_{\omega_1\,|\,M} \to \underline{\mathrm{Isom}}^{\otimes}(\omega_1 \mid M, \omega_2 \mid M).$$

Moreover, the map $g_2 \mapsto g_2^{\pi} = \pi^{-1} g_2 \pi$ induces an isomorphism $G_{\omega_2\,|\,M} \to G_{\omega_1\,|\,M}$. While the map is not canonical (since π is not), the conjugacy class

$$\mathrm{Frob}_{\omega_2\,|\,M} = \{\omega_2(\phi)^{\pi g_1} : g_1 \in G_{\omega_1\,|\,M}(k)\} \subset G_{\omega_1\,|\,M}(k)$$

is well-defined. We call it the *geometric Frobenius conjugacy class* of $\omega_2 \mid M$ in $G_{\omega_1\,|\,M}$.

For each finite extension $E/\mathbb{F}_q$ and each character $\rho \in \Phi_E(u)$, let $\mathcal{L}_\rho$ be the corresponding Kummer sheaf on $\mathbb{G}_m$ over E and $\omega_\rho : \mathrm{Tann}(\overline{\mathbb{G}}_m, \overline{\mathbb{Q}}_\ell) \to \mathbf{Vec}_k$ be the functor given by

$$M \mapsto H^0(\bar{\mathbb{A}}^1_u, j_{0!}(M \otimes \mathcal{L}_\rho)).$$

It is a fiber functor by [Katz 2012, 3.2], and $\omega_{\mathbf{1}}$ is the fiber functor of Theorem D.7.1(v). We write

$$\mathrm{Frob}_{E,\rho} \subset G_{\omega_{\mathbf{1}}\,|\,M}$$

for the corresponding geometric Frobenius conjugacy class of $\omega_\rho \mid M_E$, where $M_E = M \times_{\mathbb{F}_q} E$.

Let $m = \dim(\omega_\rho(M))$ and $n \in \{0, 1, \ldots, m\}$. We say that $\omega_\rho(M)$ is *mixed of weights* $w_1, \ldots, w_m$ if and only if there exists an eigenvector tuple $\alpha = (\alpha_1, \ldots, \alpha_m) \in (\overline{\mathbb{Q}}_\ell^\times)^m$ of any element of $\mathrm{Frob}_{E,\rho}$ such that $\alpha \in (\overline{\mathbb{Q}}^\times)^m$ and such that

$$|\iota(\alpha_i)|^2 = (1/|E|)^{w_i} \quad \text{for } 1 \le i \le m$$

for every field embedding $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$. We also say that $\omega_\rho(M)$ is *mixed of nonzero weights* $w_1, \ldots, w_n$ if and only if it is mixed of weights $w_1, \ldots, w_m$ with $w_{n+1} = \cdots = w_m = 0$.

D.14. ***Monodromy for pure middle-extension sheaves.*** Let $U \subseteq \mathbb{G}_m$ be a dense Zariski open subset over $\mathbb{F}_q$. Let $\theta : \pi_1(U) \to \mathrm{GL}(W)$ be a continuous representation to a finite-dimensional $\overline{\mathbb{Q}}_\ell$-vector space W and $\mathcal{F}$ be the restriction to $\mathbb{G}_m$ of the associated middle-extension sheaf $\mathrm{ME}(\theta)$ on $\mathbb{P}^1_u$. Suppose that θ is pointwise pure of weight w so that $M = \mathcal{F}((1+w)/2)[1]$ is pure of weight zero. Suppose moreover that θ is geometrically simple and that it does not factor through the composed quotient $\pi_1(U) \twoheadrightarrow \pi_1(\mathbb{G}_m) \twoheadrightarrow \pi_1^{\mathrm{t}}(\mathbb{G}_m)$ so that M lies in $\mathcal{P}_{\mathrm{arith}}$.

Let $\Phi(u)$ be the dual of $\Gamma(u) = (\mathbb{F}_q[u]/u\mathbb{F}_q[u])^\times$ (cf. Section 10.2). We define the *geometric* and *arithmetic Tannakian monodromy groups* of (the Mellin transformation of) θ to be

$$\mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u)) := G_{\omega_1 \mid \overline{M}}, \quad \mathcal{G}_{\mathrm{arith}}(\theta, \Phi(u)) := G_{\omega_1 \mid M}.$$

For $u = 0, \infty$, let $W(u)$ denote W regarded as an $I(u)$-module, and let $W(u)^{\mathrm{unip}}$ be the maximal submodule of $W(u)$ where $I(u)$ acts unipotently. Moreover, let $e_{u,1}, \ldots, e_{u,d_u}$ be positive integers satisfying

$$W(u)^{\mathrm{unip}} \simeq U(e_{u,1}) \oplus \cdots \oplus U(e_{u,d_u})$$

as $I(u)$-modules, where $U(e)$ denotes the irreducible e-dimensional $I(u)$-module on which $I(u)$ acts unipotently.

Proposition D.14.1. (i) *The groups* $\mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u))$ *and* $\mathcal{G}_{\mathrm{arith}}(\theta, \Phi(u))$ *are reductive, and there is an exact sequence*

$$1 \to \mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u)) \to \mathcal{G}_{\mathrm{arith}}(\theta, \Phi(u)) \to T \to 1$$

for some torus T *over* $\overline{\mathbb{Q}}_\ell$.

(ii) *For each finite extension* $E/\mathbb{F}_q$ *and each* $\alpha \in \Phi_E(u)$, *the stalk* $\omega_\rho(M)$ *is mixed of nonzero weights* $-e_{0,1}, \ldots, -e_{0,d_0}, e_{\infty,1}, \ldots, e_{\infty,d_\infty}$.

Proof. Part (1) follows from Proposition D.11.1, and part (2) follows from [Katz 2012, Theorem 16.1]. □

Acknowledgements

We are pleased to acknowledge support under EPSRC Programme Grant EP/K034383/1 LMF: L-Functions and Modular Forms. Keating is also grateful for support through a Royal Society Wolfson Research Merit Award and a Royal Society Leverhulme Senior Research Fellowship. We thank Nick Katz, Emmanuel Kowalski, and Zeev Rudnick for discussion and helpful comments. We also gratefully acknowledge the anonymous referees for reading the drafts very carefully and providing meticulous reports.

References

[Beĭlinson et al. 1982] A. A. Beĭlinson, J. Bernstein, and P. Deligne, "Faisceaux pervers", pp. 5–171 in *Analysis and topology on singular spaces, I* (Luminy, France, 1981), Astérisque **100**, Soc. Math. France, Paris, 1982. MR Zbl

[Bosch et al. 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik (3) **21**, Springer, 1990. MR Zbl

[Bui et al. 2016] H. M. Bui, J. P. Keating, and D. J. Smith, "On the variance of sums of arithmetic functions over primes in short intervals and pair correlation for L-functions in the Selberg class", *J. London Math. Soc.* (2) **94**:1 (2016), 161–185. MR Zbl

[Carter 1985] R. W. Carter, *Finite groups of Lie type: conjugacy classes and complex characters*, Wiley, New York, 1985. MR Zbl

[Chan 2003] T. H. Chan, "More precise pair correlation of zeros and primes in short intervals", *J. London Math. Soc.* (2) **68**:3 (2003), 579–598. MR Zbl

[Cohen et al. 2006] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren (editors), *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman & Hall, Boca Raton, FL, 2006. MR Zbl

[Conrey and Snaith 2007] J. B. Conrey and N. C. Snaith, "Applications of the L-functions ratios conjectures", *Proc. Lond. Math. Soc.* (3) **94**:3 (2007), 594–646. MR Zbl

[Conrey et al. 2008] B. Conrey, D. W. Farmer, and M. R. Zirnbauer, "Autocorrelation of ratios of L-functions", *Commun. Number Theory Phys.* **2**:3 (2008), 593–636. MR Zbl

[Curtis and Reiner 1962] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure Appl. Math. **11**, Interscience, New York, 1962. MR Zbl

[Deligne 1980] P. Deligne, "La conjecture de Weil, II", *Inst. Hautes Études Sci. Publ. Math.* **52** (1980), 137–252. MR Zbl

[Deligne et al. 1982] P. Deligne, J. S. Milne, A. Ogus, and K.-y. Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Math. **900**, Springer, 1982. MR Zbl

[Diaconis and Evans 2001] P. Diaconis and S. N. Evans, "Linear functionals of eigenvalues of random matrices", *Trans. Amer. Math. Soc.* **353**:7 (2001), 2615–2633. MR Zbl

[Diaconis and Shahshahani 1994] P. Diaconis and M. Shahshahani, "On the eigenvalues of random matrices", *J. Appl. Probab.* **31A** (1994), 49–62. MR Zbl

[Friedlander and Goldston 1996] J. B. Friedlander and D. A. Goldston, "Variance of distribution of primes in residue classes", *Quart. J. Math. Oxford Ser.* (2) **47**:187 (1996), 313–336. MR Zbl

[Gabber and Loeser 1996] O. Gabber and F. Loeser, "Faisceaux pervers l-adiques sur un tore", *Duke Math. J.* **83**:3 (1996), 501–606. MR Zbl

[Goldston and Montgomery 1987] D. A. Goldston and H. L. Montgomery, "Pair correlation of zeros and primes in short intervals", pp. 183–203 in *Analytic number theory and Diophantine problems* (Stillwater, OK, 1984), edited by A. C. Adolphson et al., Progr. Math. **70**, Birkhäuser, Boston, 1987. MR Zbl

[Hall 2008] C. Hall, "Big symplectic or orthogonal monodromy modulo l", *Duke Math. J.* **141**:1 (2008), 179–203. MR Zbl

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math. **52**, Springer, 1977. MR Zbl

[Hooley 1975a] C. Hooley, "The distribution of sequences in arithmetic progressions", pp. 357–364 in *Proceedings of the International Congress of Mathematicians, I* (Vancouver, 1974), edited by R. D. James, Canad. Math. Congress, Montreal, 1975. MR Zbl

[Hooley 1975b] C. Hooley, "On the Barban–Davenport–Halberstam theorem, I", *J. Reine Angew. Math.* **274-275** (1975), 206–223. MR Zbl

[Hooley 1975c] C. Hooley, "On the Barban–Davenport–Halberstam theorem, II", *J. London Math. Soc.* (2) **9** (1975), 625–636. MR Zbl

[Katz 1988] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Ann. Math. Studies **116**, Princeton Univ. Press, 1988. MR Zbl

[Katz 1996] N. M. Katz, *Rigid local systems*, Ann. Math. Studies **139**, Princeton Univ. Press, 1996. MR Zbl

[Katz 2002] N. M. Katz, *Twisted L-functions and monodromy*, Ann. Math. Studies **150**, Princeton Univ. Press, 2002. MR Zbl

[Katz 2012] N. M. Katz, *Convolution and equidistribution*, Ann. Math. Studies **180**, Princeton Univ. Press, 2012. MR Zbl

[Katz 2013] N. M. Katz, "On a question of Keating and Rudnick about primitive Dirichlet characters with squarefree conductor", *Int. Math. Res. Not.* **2013**:14 (2013), 3221–3249. MR Zbl

[Katz and Sarnak 1999] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Amer. Math. Soc. Colloq. Publ. **45**, Amer. Math. Soc., Providence, RI, 1999. MR Zbl

[Keating and Roditty-Gershon 2016] J. P. Keating and E. Roditty-Gershon, "Arithmetic correlations over large finite fields", *Int. Math. Res. Not.* **2016**:3 (2016), 860–874. MR Zbl

[Keating and Rudnick 2014] J. P. Keating and Z. Rudnick, "The variance of the number of prime polynomials in short intervals and in residue classes", *Int. Math. Res. Not.* **2014**:1 (2014), 259–288. MR Zbl

[Keating and Rudnick 2016] J. Keating and Z. Rudnick, "Squarefree polynomials and Möbius values in short intervals and arithmetic progressions", *Algebra Number Theory* **10**:2 (2016), 375–420. MR Zbl

[Keating et al. 2018] J. P. Keating, B. Rodgers, E. Roditty-Gershon, and Z. Rudnick, "Sums of divisor functions in $\mathbb{F}_q[t]$ and matrix integrals", *Math. Z.* **288**:1-2 (2018), 167–198. MR Zbl

[Languasco et al. 2012] A. Languasco, A. Perelli, and A. Zaccagnini, "Explicit relations between pair correlation of zeros and primes in short intervals", *J. Math. Anal. Appl.* **394**:2 (2012), 761–771. MR Zbl

[Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Math. Series **33**, Princeton Univ. Press, 1980. MR Zbl

[Montgomery 1970] H. L. Montgomery, "Primes in arithmetic progressions", *Michigan Math. J.* **17** (1970), 33–39. MR Zbl

[Montgomery 1973] H. L. Montgomery, "The pair correlation of zeros of the zeta function", pp. 181–193 in *Analytic number theory* (St. Louis, 1972), edited by H. G. Diamond, Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence, RI, 1973. MR Zbl

[Montgomery and Soundararajan 2004] H. L. Montgomery and K. Soundararajan, "Primes in short intervals", *Comm. Math. Phys.* **252**:1-3 (2004), 589–617. MR Zbl

[Platonov and Rapinchuk 1994] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure Appl. Math. **139**, Academic Press, Boston, 1994. MR Zbl

[Raynaud 1966] M. Raynaud, "Caractéristique d'Euler–Poincaré d'un faisceau et cohomologie des variétés abéliennes", exposé 286 in *Séminaire Bourbaki, Vol. 9*, W. A. Benjamin, New York, 1966. Reprinted as pp. 129–147 in *Séminaire Bourbaki* **9**, Soc. Math. France, Paris, 1995. MR Zbl

[Rodgers 2018] B. Rodgers, "Arithmetic functions in short intervals and the symmetric group", *Algebra Number Theory* **12**:5 (2018), 1243–1279. MR Zbl

[Roditty-Gershon 2017] E. Roditty-Gershon, "Square-full polynomials in short intervals and in arithmetic progressions", *Res. Number Theory* **3** (2017), art. id. 3. MR Zbl

[Rosen 2002] M. Rosen, *Number theory in function fields*, Graduate Texts in Math. **210**, Springer, 2002. MR Zbl

[Rudnick 2014] Z. Rudnick, "Some problems in analytic number theory for polynomials over a finite field", pp. 443–459 in *Proceedings of the International Congress of Mathematicians, II* (Seoul, 2014), edited by S. Y. Jang et al., Kyung Moon Sa, Seoul, 2014. MR Zbl

[Serre and Tate 1968] J.-P. Serre and J. Tate, "Good reduction of abelian varieties", *Ann. of Math.* (2) **88** (1968), 492–517. MR Zbl

[SGA $4\frac{1}{2}$ 1977] P. Deligne, *Cohomologie étale* (Séminaire de Géométrie Algébrique du Bois Marie), Lecture Notes in Math. **569**, Springer, 1977. MR Zbl

[SGA 7_{I} 1972] A. Grothendieck, *Groupes de monodromie en géométrie algébrique, I: Exposés I–II, VI–IX* (Séminaire de Géométrie Algébrique du Bois Marie 1967–1969), Lecture Notes in Math. **288**, Springer, 1972. MR Zbl

[Zarhin 1990] Y. G. Zarhin, "Linear simple Lie algebras and ranks of operators", pp. 481–495 in *The Grothendieck Festschrift, III*, edited by P. Cartier et al., Progr. Math. **88**, Birkhäuser, Boston, 1990. MR

Communicated by Peter Sarnak
Received 2017-04-06 Revised 2018-08-07 Accepted 2018-09-06

chall69@uwo.ca — *Department of Mathematics, University of Western Ontario, London, ON, Canada*

j.p.keating@bristol.ac.uk — *School of Mathematics, University of Bristol, Bristol, United Kingdom*

rodittye@gmail.com — *Department of Applied Mathematics, Holon Institute of Technology, Holon, Israel*

ALGEBRA AND NUMBER THEORY 13:1 (2019)
https://doi.org/10.2140/ant.2019.13.93

Extended eigenvarieties for overconvergent cohomology

Christian Johansson and James Newton

Recently, Andreatta, Iovita and Pilloni constructed spaces of overconvergent modular forms in characteristic p, together with a natural extension of the Coleman–Mazur eigencurve over a compactified (adic) weight space. Similar ideas have also been used by Liu, Wan and Xiao to study the boundary of the eigencurve. This all goes back to an idea of Coleman.

In this article, we construct natural extensions of eigenvarieties for arbitrary reductive groups $\boldsymbol{G}$ over a number field which are split at all places above p. If $\boldsymbol{G}$ is $\mathrm{GL}_2/\mathbb{Q}$, then we obtain a new construction of the extended eigencurve of Andreatta–Iovita–Pilloni. If $\boldsymbol{G}$ is an inner form of GL_2 associated to a definite quaternion algebra, our work gives a new perspective on some of the results of Liu–Wan–Xiao.

We build our extended eigenvarieties following Hansen's construction using overconvergent cohomology. One key ingredient is a definition of locally analytic distribution modules which permits coefficients of characteristic p (and mixed characteristic). When $\boldsymbol{G}$ is GL_n over a totally real or CM number field, we also construct a family of Galois representations over the reduced extended eigenvariety.

A correction was submitted on 27 October 2020 and posted online on 27 February 2021.

1. Introduction

1.1. ***The halo conjecture.*** The *eigencurve*, introduced by Coleman and Mazur [1998], is a rigid analytic curve $\mathscr{E}^{\mathrm{rig}}$ over $\mathbb{Q}_p$ which parametrizes systems of Hecke eigenvalues of finite-slope overconvergent modular forms. It comes equipped with a morphism $\mathscr{E}^{\mathrm{rig}} \to \mathcal{W}_0^{\mathrm{rig}}$, called the weight map, whose target is known as *weight space*. $\mathcal{W}_0^{\mathrm{rig}}$ parametrizes continuous characters $\kappa : \mathbb{Z}_p^\times \to \overline{\mathbb{Q}}_p^\times$ and is a disjoint union of a finite number of open unit discs. There is also a morphism $\mathscr{E}^{\mathrm{rig}} \to \mathbb{G}_m^{\mathrm{rig}}$ which sends a system of Hecke eigenvalues to the U_p-eigenvalue; the p-adic valuation of the U_p-eigenvalue is known as the *slope*. The geometry of $\mathscr{E}^{\mathrm{rig}}$ encodes a wealth of information about congruences between finite-slope overconvergent modular forms, and it is therefore not surprising that its study remains a difficult topic. In particular, we know very little about the global geometry of $\mathscr{E}^{\mathrm{rig}}$ (for example, it is not known whether the number of irreducible components of $\mathscr{E}^{\mathrm{rig}}$ is finite or not).

Let $q = p$ if $p \neq 2$ and $q = 4$ if $p = 2$. The components of $\mathcal{W}_0^{\mathrm{rig}}$ are parametrized by the characters $(\mathbb{Z}/q\mathbb{Z})^\times \to (\mathbb{Z}/q\mathbb{Z})^\times$, and if we define $X := X_\kappa = \kappa(\exp(q)) - 1$, then X defines a parameter on each component. Very little is known about the global geometry of $\mathscr{E}^{\mathrm{rig}}$ over the centre $|X| \leq q^{-1}$ and it seems likely to be rather complicated. Near the boundary, however, the situation turns out to be rather

MSC2010: primary 11F33; secondary 11F80.
Keywords: p-adic automorphic forms, p-adic modular forms, eigenvarieties, Galois representations.

simple. Coleman and Mazur raised the question of whether the slope tends to zero as one moves along a component of $\mathscr{E}^{\mathrm{rig}}$ towards the boundary of $\mathcal{W}_0^{\mathrm{rig}}$. Buzzard and Kilford [2005] investigated this question for $p=2$ (and tame level 1) and proved a striking structure theorem: $\mathscr{E}^{\mathrm{rig}}|_{\{|X|>1/8\}}$ is a disjoint union of connected components $(E_i)_{i=0}^{\infty}$, and the weight map $E_i \to \left\{|X| > \frac{1}{8}\right\}$ is an isomorphism for every i. Moreover, the slope of a point on E_i with parameter X is $i.v_2(X)$, where v_p is the p-adic valuation (normalized so that $v_p(p)=1$). Out of this came a folklore conjecture; the following version is essentially [Liu et al. 2017, Conjecture 1.2]:

Conjecture. *For $r \in (0,1)$ sufficiently close to 1, $\mathscr{E}^{\mathrm{rig}}|_{\{|X|>r\}}$ is a disjoint union of connected components $(E_i)_{i=0}^{\infty}$ such that each E_i is finite over $\{|X|>r\}$. Moreover, there exist constants $\lambda_i \in \mathbb{R}_{\geq 0}$ for $i=0,1,\ldots$, strictly increasing and tending to infinity, such that if x is a point on E_i with weight parameter X, then the slope of x is $\lambda_i v_p(X)$. The sequence $(\lambda_i)_{i=0}^{\infty}$ is a finite union of arithmetic progressions, after perhaps removing a finite number of terms.*

We will loosely refer to this as the "halo conjecture" (the "halo" in question is the (disjoint union of) annuli $\{|X|>r\}$). Let us assume $p \neq 2$ for simplicity. If κ is a point of $\mathcal{W}_0^{\mathrm{rig}}$ then U_p acts compactly on the space of overconvergent modular forms $M_\kappa^\dagger$. The Fredholm determinants $\det(1-T.U_p \mid M_\kappa^\dagger) \in \overline{\mathbb{Q}}_p[\![T]\!]$ interpolate to an entire series $F=\sum_{n=0}^{\infty} a_n T^n$ with coefficients in $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] = \mathcal{O}(\mathcal{W}_0^{\mathrm{rig}})^\circ$. Fix a character $\eta : \mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ and consider the ideal $I_\eta = (p, [n]-\eta(n) \mid n=1,\ldots,p-1)$. The quotient ring $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]/I_\eta$ is isomorphic to $\mathbb{F}_p[\![X]\!]$ via the map sending $[\exp(p)]$ to $1+X$. We may consider the reduction $\overline{F}_\eta$ of F modulo I_η and the character

$$\bar{\kappa}_\eta : \mathbb{Z}_p^\times \to (\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]/I_\eta)^\times \cong \mathbb{F}_p[\![X]\!]^\times.$$

In an unpublished note, Coleman conjectured that there should exist an $\mathbb{F}_p((X))$-Banach space $\overline{M}_{\bar{\kappa}_\eta}^\dagger$ of "overconvergent modular forms of weight $\bar{\kappa}_\eta$" with a compact U_p-action such that $\det(1-T.U_p \mid \overline{M}_{\bar{\kappa}_\eta}^\dagger) = \overline{F}_\eta$, and promoted the idea that one should study the halo conjecture via integral models of the eigencurve near the boundary of weight space.

In [Andreatta et al. 2018], Andreatta, Iovita and Pilloni proved Coleman's conjecture on the existence of $\overline{M}_{\bar{\kappa}_\eta}^\dagger$ and constructed an integral model $\mathscr{E}'$ of $\mathscr{E}^{\mathrm{rig}}$, which lives in the category of analytic adic spaces [Huber 1994]. $\mathcal{W}_0^{\mathrm{rig}}$ has a natural formal scheme model $\operatorname{Spf} \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$, which may be viewed as an adic space $\mathfrak{W}_0$ over the affinoid ring $(\mathbb{Z}_p, \mathbb{Z}_p)$. Apart from the points corresponding to the adic incarnation of $\mathcal{W}_0^{\mathrm{rig}}$, $\mathfrak{W}_0$ contains an additional $2(p-1)$ points in characteristic p, corresponding to the characters η and $\bar{\kappa}_\eta$. The latter points are analytic in Huber's sense (the former are not) and one may consider the analytic locus $\mathcal{W}_0 = \mathcal{W}_0^{\mathrm{rig}} \cup \{\bar{\kappa}_\eta \mid \eta\}$ of $\mathfrak{W}_0$ (viewing $\mathcal{W}_0^{\mathrm{rig}}$ as an adic space). $\mathcal{W}_0$ may be viewed as a compactification of $\mathcal{W}_0^{\mathrm{rig}}$, and Coleman's idea may be interpreted as saying that one should study the behaviour of $\mathscr{E}^{\mathrm{rig}}$ near the boundary of $\mathcal{W}_0$ by extending the eigencurve to an adic space living over $\mathcal{W}_0$, turning global behaviour into local behaviour "at infinity". At a point $\bar{\kappa}_\eta$, one can no longer measure slopes using p. Instead, one has to use X. Noting that one can use X not only at $\bar{\kappa}_\eta$ but also "near" it, the halo conjecture says that the X-adic slope is constant as one approaches $\bar{\kappa}_\eta$. This supports the idea that an extension of $\mathscr{E}^{\mathrm{rig}}$ exists, and that the E_i in the halo conjecture are X-adic Coleman families (i.e., subspaces which are finite over their images in weight space, and of constant slope). In this framework, the slopes of U_p should be the λ_i, with multiplicity the degree of X_i over $\{|X| > r\}$. The halo conjecture asserts, remarkably, that a Coleman family centred at a point over $\bar{\kappa}_\eta$ extends to some locus $\{|X| > r\}$ in the component corresponding to η, where r is independent of the family (and in particular its slope).

In [Liu et al. 2017], Liu, Wan and Xiao prove the halo conjecture for eigencurves for definite quaternion algebras. Here the construction of (overconvergent) automorphic forms is of a combinatorial nature. Those authors succeeded in proving the halo conjecture by calculations on some relatively explicit ad hoc integral models of spaces of overconvergent automorphic forms. They construct one space over the whole of $\mathfrak{W}_0$, with a possibly noncompact U_p-action, and another model over $\{|X| > p^{-1}\}$ with a compact U_p-action. By the p-adic Jacquet–Langlands correspondence of [Chenevier 2005], this proves the halo conjecture for the components of the Coleman–Mazur eigencurve of (generically) Steinberg or supercuspidal type at some prime $q \neq p$.

1.2. ***Extended eigenvarieties for overconvergent cohomology.*** The main goal of this paper is to construct extensions of eigenvarieties for a very general class of connected reductive groups $\boldsymbol{G}$ over $\mathbb{Q}$. In particular, we give a new construction of the extended eigencurve $\mathscr{E}'$ appearing in [Andreatta et al. 2018]. Our construction also gives a conceptual framework for many of the results in [Liu et al. 2017] (and establishes a generalization of some of their results, which was described as an "optimistic expectation" in Remark 3.26(2) of that paper). See Theorem 6.3.4 for an interpretation of some of their results using the extended eigencurve.

Our construction of these eigenvarieties appears in Section 4.1. For the purposes of the introduction, we have the following vague statement:

Theorem A. *Let F be a number field and let $\boldsymbol{H}$ be a connected reductive group over F which is split at all places above p. Set $\boldsymbol{G} = \mathrm{Res}^F_{\mathbb{Q}} \boldsymbol{H}$. Then the eigenvarieties for $\boldsymbol{G}$ constructed in* [Hansen 2017] *naturally extend to adic spaces $\mathscr{X}_{\boldsymbol{G}}$ over the extended weight space*

$$\mathcal{W} = \mathrm{Spa}(\mathbb{Z}_p[\![T_0']\!], \mathbb{Z}_p[\![T_0']\!])^{\mathrm{an}},$$

where T_0' is a certain quotient of the $\mathbb{Z}_p$-points T_0 of a maximal torus in a suitable model of $\boldsymbol{G}$ over $\mathbb{Z}_p$.

The assumption that $\boldsymbol{H}$ is split at all places above p is made for convenience only; it makes it easy to define a "canonical" Iwahori subgroup. We believe that it should be relatively straightforward to generalize our constructions to general quasisplit $\boldsymbol{G}$ over $\mathbb{Q}$ (or to the setting of [Loeffler 2011]). The resulting theory would, however, be even more notationally cumbersome, so we have decided to stick to the simpler (but still very general) situation in this paper.

As a secondary goal, we show (Theorem 5.4.5) that when $\boldsymbol{G} = \mathrm{Res}^F_{\mathbb{Q}} \mathrm{GL}_{n/F}$, where F is a CM or totally real number field, the reduced eigenvariety that we construct carries a Galois determinant (in the language of [Chenevier 2014]) satisfying the expected compatibilities between Frobenii at unramified places and the eigenvalues of Hecke operators. This shows that, in these cases, the new systems of Hecke eigenvalues that we construct in characteristic p carry arithmetic information.

Theorem B. *There exists an n-dimensional continuous determinant D of G_F with values in $\mathcal{O}^+(\mathscr{X}_{\boldsymbol{G}}^{\mathrm{red}})$ such that*

$$D(1 - X\,\mathrm{Frob}_v) = P_v(X)$$

for unramified places v, where $P_v(X)$ is the usual Hecke polynomial (5.3.1).

Our proof of Theorem B is an adaptation of an argument due to the first author and David Hansen in the rigid setting, which will appear in a slightly refined form in [Hansen and Johansson ≥ 2019]. It crucially uses Scholze's results [2015] on Galois determinants attached to torsion classes, as well as filtrations on distribution modules constructed in [Hansen 2015].

To end our brief discussion of the results established in this paper, we explain one interpretation of the phrase "naturally extend" in Theorem A. Suppose for simplicity that $F = \mathbb{Q}$, $\boldsymbol{G}(\mathbb{R})$ is compact modulo centre, and $\boldsymbol{G}(\mathbb{Q}_p)$ may be identified with $\mathrm{GL}_n(\mathbb{Q}_p)$. We let $T_0 \subseteq \mathrm{GL}_n(\mathbb{Q}_p)$ denote the diagonal matrices with entries in $\mathbb{Z}_p$ (in this case $T_0 = T_0'$). Modules of overconvergent automorphic forms for $\boldsymbol{G}$ (and some fixed tame level, which we suppress) were constructed in [Chenevier 2004] (see also [Loeffler 2011]). If we denote by U the Hecke operator corresponding to

$$\begin{pmatrix} 1 & & & \\ & p & & \\ & & \ddots & \\ & & & p^{n-1} \end{pmatrix}$$

then this acts compactly on the spaces of overconvergent automorphic forms, and so for each continuous character $\kappa : T_0 \to \overline{\mathbb{Q}}_p^\times$ there is a characteristic power series $F_\kappa \in \overline{\mathbb{Q}}_p[\![T]\!]$ given by the determinant of $1 - TU$ on the space of overconvergent automorphic forms of weight κ. The following theorem is a consequence of our eigenvariety construction, together with Corollary 4.1.5.

Theorem C. *The characteristic power series F_κ glue together to $F_{\mathcal{W}} \in \mathcal{O}(\mathcal{W})\{\{T\}\}$, an entire function on affine 1-space over $\mathcal{W}$.*

Suppose $\bar{\kappa} : T_0 \to \mathbb{F}_q((X))^\times$ is a continuous character, with q a power of p. Then we give an interpretation of the specialization $F_{\mathcal{W},\bar{\kappa}}$ of $F_{\mathcal{W}}$ at $\bar{\kappa}$ as the characteristic power series of U acting on an $\mathbb{F}_q((X))$-Banach space of overconvergent automorphic forms of weight $\bar{\kappa}$.

The Fredholm hypersurface $\mathscr{Z}$ cut out by $F_{\mathcal{W}}$ is locally quasifinite, flat and partially proper over $\mathcal{W}$ and the eigenvariety $\mathscr{X}$ comes equipped with a finite map to $\mathscr{Z}$.

1.3. *Outline of the construction.* The eigenvarieties that we extend are those constructed using overconvergent cohomology (sometimes also referred to as overconvergent modular symbols). Overconvergent cohomology was developed in [Stevens 1994; Ash and Stevens 2008], and the eigenvarieties were constructed in [Hansen 2017]. Let us recall their construction in the special case of the Coleman–Mazur eigencurve and $p \neq 2$. Let R be an affinoid $\mathbb{Q}_p$-algebra in the sense of rigid analytic geometry and let $\kappa : \mathbb{Z}_p^\times \to R^\times$ be a continuous homomorphism. It is well known that κ is locally analytic, and in particular analytic on the cosets of $1+p^s\mathbb{Z}_p$ for all sufficiently large s. For such s, we consider the Banach R-module $\mathcal{A}_\kappa[s]$ of functions $f : p\mathbb{Z}_p \to R$ which are analytic on the cosets of $p^s\mathbb{Z}_p$. The monoid

$$\Delta = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p) \;\middle|\; p \mid c,\ a \in \mathbb{Z}_p^\times, ad-bc \neq 0 \right\}$$

acts on $\mathcal{A}_\kappa[s]$ from the right by

$$(f.\gamma)(x) = \kappa(a+bx) f\left(\frac{c+dx}{a+bx}\right).$$

We consider the dual space $\mathcal{D}_\kappa[s] = \mathrm{Hom}_{R,\mathrm{cts}}(\mathcal{A}_\kappa[s], R)$, with the dual left action of Δ. A key point is that the matrix $t = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ acts compactly on $\mathcal{D}_\kappa[s]$; it factors through the compact injection $\mathcal{D}_\kappa[s] \hookrightarrow \mathcal{D}_\kappa[s+1]$. Fix an integer $N \geq 5$ (for simplicity) which is coprime to p, and consider the congruence subgroup $\Gamma = \Gamma_1(N) \cap \Gamma_0(p) \subseteq \Delta$. We may view $\mathcal{D}_\kappa[s]$ as a local system $\widetilde{\mathcal{D}}_\kappa[s]$ on the complex modular curve $Y(\Gamma) = \Gamma \backslash \mathcal{H}$ and consider the singular cohomology group

$$H^1(Y(\Gamma), \widetilde{\mathcal{D}}_\kappa[s]) = H^1(\Gamma, \mathcal{D}_\kappa[s]),$$

where the right-hand side is group cohomology (in general we would consider cohomology in all degrees, but it turns out that $H^i(\Gamma, \mathcal{D}_\kappa[s]) = 0$ if $i \neq 1$; see Section 6.1). It carries an action of the Hecke operator U_p. Considering these spaces for varying s and $R = \mathcal{O}(\mathcal{U})$, where $\mathcal{U} \subseteq \mathcal{W}_0^{\mathrm{rig}}$ is an affinoid open subset, Hansen shows how to construct an eigenvariety from the Ash–Stevens cohomology groups by a clever adaptation of the eigenvariety construction of [Coleman 1997] (in the one-dimensional case) and [Buzzard 2007] (in the general case).[1] This eigenvariety turns out to equal the Coleman–Mazur eigencurve. To extend this construction to $\mathcal{W}_0$, the key point is to define generalizations of the modules $\mathcal{D}_\kappa[s]$ for all open affinoid subsets $\mathcal{U} \subseteq \mathcal{W}_0$. Let $R = \mathcal{O}(\mathcal{U})$ and let $\kappa : \mathbb{Z}_p^\times \to R^\times$ be the induced character. The first thing to note is that κ is continuous but need not be locally analytic anymore, so one cannot directly copy the definition of $\mathcal{D}_\kappa[s]$. One could try to instead use the space $\mathcal{A}_\kappa$ of all continuous functions $p\mathbb{Z}_p \to R$. This carries an action of Δ by the same formula, and we may consider its dual $\mathcal{D}_\kappa$. However, the action of t is no longer compact, so one has to do something different.

Let $f : p\mathbb{Z}_p \to R$ be a continuous function and let $f(x) = \sum_{n\geq 0} c_n \binom{x/p}{n}$ be its Mahler expansion. Recall that, when $\mathcal{U} \subseteq \mathcal{W}_0^{\mathrm{rig}}$ (i.e., when R is a $\mathbb{Q}_p$-algebra), a theorem of Amice (see [Colmez 2010, Théorème I.4.7]) says that f is analytic on the cosets of $p^{s+1}\mathbb{Z}_p$ if and only $|c_n| p^{n/p^s(p-1)} \to 0$ as $n \to \infty$. Here $|-|$ is any $\mathbb{Q}_p$-Banach algebra norm such that $|p| = p^{-1}$. Dually, we may identify $\mathcal{D}_\kappa$ with the ring of formal power series

$$\sum_{n\geq 0} d_n T^n,$$

where T^n is the distribution $f \mapsto c_n(f)$ and d_n is bounded as $n \to \infty$. The analytic distribution module $\mathcal{D}_\kappa[s]$ is defined by the weaker condition that $|d_n| p^{-n/p^s(p-1)}$ is bounded as $n \to \infty$. We may

[1]Note that it is not clear how to topologize the R-modules $H^1(\Gamma, \mathcal{D}_\kappa[s])$, nor that they can be made into potentially ON-able Banach R-modules, so even in this special case we are combining Hansen's eigenvariety construction with the Fredholm theory of Coleman and Buzzard, rather than using the Coleman–Mazur–Buzzard eigenvariety construction.

define norms $\|-\|_r$, for $r \in [1/p, 1)$, on $\mathcal{D}_\kappa$ by $\left\|\sum_{n\geq 0} d_n T^n\right\|_r = \sup_n |d_n| r^n$. Let $\mathcal{D}_\kappa^r$ denote the completion of $\mathcal{D}_\kappa$ with respect to $\|-\|_r$; it may be explicitly described as the ring of power series $\sum_{n\geq 0} d_n T^n$, where $|d_n| r^n \to 0$. While the $\mathcal{D}_\kappa[s]$ are not among the $\mathcal{D}_\kappa^r$, one sees that $\varprojlim_{r\to 1} \mathcal{D}_\kappa^r = \varprojlim_{s\to\infty} \mathcal{D}_\kappa[s]$, so the norms allow one to recover the space of locally analytic distributions. As an aside, we remark it is possible to recover the $\mathcal{D}_\kappa[s]$ on the nose from the $\|-\|_r$, but we will not need them for the construction of eigenvarieties.

The upshot of considering the norms $\|-\|_r$ is that they may be constructed on $\mathcal{D}_\kappa$ for any open affinoid $\mathcal{U} \subseteq \mathcal{W}_0$, by the formula given above. It is, however, not clear a priori that the norms interact well with the action of Δ. As a monoid Δ is generated by the Iwahori subgroup $I = \Delta \cap \mathrm{GL}_2(\mathbb{Z}_p)$ and the element t. The element t acts via multiplication by p on $p\mathbb{Z}_p$ and it is not too hard to see that it induces a norm-decreasing map $(\mathcal{D}_\kappa, \|-\|_r) \to (\mathcal{D}_\kappa, \|-\|_{r^{1/p}})$ and that the inclusions $\mathcal{D}_\kappa^s \subseteq \mathcal{D}_\kappa^r$ for $r < s$ are compact. Thus t induces a compact operator on $\mathcal{D}_\kappa^r$ as desired. The action of I is more complicated to analyze, but it turns out that I acts by isometries for sufficiently large r (depending only on κ). To see this, it is useful to find a different description of $\|-\|_r$. This description, which we will outline below, is one of the key technical innovations of this paper. It is the analogue, in our setting of norms, of the observation in the rigid case that if κ is s-analytic then the I-action on $\mathcal{A}_\kappa$ preserves $\mathcal{A}_\kappa[s]$.

Schneider and Teitelbaum [2003] generalized the norms defined above to the spaces $\mathcal{D}(G, L)$ of continuous distributions on a *uniform* pro-p group G [Dixon et al. 1999, Definition 4.1] valued in a finite extension L of $\mathbb{Q}_p$. To recall this construction briefly, a choice of a minimal set of topological generators of G induces an isomorphism $G \cong \mathbb{Z}_p^{\dim G}$ of p-adic manifolds and using multivariable Mahler expansions one may identify $\mathcal{D}(G, L)$ (as an L-Banach space) with $\mathcal{O}_L[\![T_1, \dots, T_{\dim G}]\!][1/p]$, and we put ($m = \dim G$)

$$\left\| \sum_{n_i \geq 0} d_{n_1,\dots,n_m} T_1^{n_1} \cdots T_m^{n_m} \right\|_r = \sup |d_{n_1,\dots,n_m}| r^{n_1+\cdots+n_m}.$$

Schneider and Teitelbaum showed that these norms are submultiplicative and independent of the choice of minimal generating set. We generalize the construction of these norms to the module $\mathcal{D}(G, R)$ of distributions on a uniform group G valued in a certain class of normed $\mathbb{Z}_p$-algebras R that we call *Banach–Tate* $\mathbb{Z}_p$*-algebras*. These include the rings $R = \mathcal{O}(\mathcal{U})$ for $\mathcal{U} \subseteq \mathcal{W}_0$ open affinoid (for a suitable choice of norm) and generalize the constructions in the previous paragraph, which was the special case $G = p\mathbb{Z}_p$. Moreover, the action of $g \in G$ on $\mathcal{D}(G, R)$ via left or right translation is an isometry for $\|-\|_r$ (for any r).

Let $B_0 = \{\gamma \in I \mid c = 0\}$ be the upper triangular Borel and let $\overline{N}_1 = \left\{\left(\begin{smallmatrix}1 & 0\\ x & 1\end{smallmatrix}\right) \,\middle|\, x \in p\mathbb{Z}_p\right\} \cong p\mathbb{Z}_p$; I has an Iwahori decomposition $I \cong \overline{N}_1 \times B_0$. Extend κ to a character of B_0 by setting $\kappa(\gamma) = \kappa(a)$. We have an I-equivariant injection $f \mapsto F$ of $\mathcal{A}_\kappa$ into the space $\mathcal{C}(I, R)$ of continuous functions $F : G \to R$ given by $F(\bar{n}b) = f(\bar{n})\kappa(b)$, with $\bar{n} \in \overline{N}_1$ and $b \in B_0$. Here I acts on $\mathcal{C}(I, R)$ via left translation. The image is the set of functions F such that $F(gb) = \kappa(b)F(g)$ for all $g \in I$ and $b \in B_0$. Dually, we obtain an I-equivariant surjection $\mathcal{D}(I, R) \to \mathcal{D}_\kappa$. If we pretend, momentarily, that I is uniform, then we may consider the quotient norm on $\mathcal{D}_\kappa$ induced from $\|-\|_r$ on $\mathcal{D}(I, R)$ and one can show that for sufficiently large r, this quotient norm agrees with the previously defined $\|-\|_r$ on $\mathcal{D}_\kappa$. This shows that I acts by isometries on $(\mathcal{D}_\kappa, \|-\|_r)$ for sufficiently large r. In reality I is not uniform, but one can adapt the argument by working with a suitable open uniform normal subgroup of I.

This summarizes our construction of the modules $\mathcal{D}_\kappa^r$ which we use to construct the eigenvariety. From the $\mathcal{D}_\kappa^r$, we construct variants $\mathcal{D}_\kappa^{<r}$ and function modules $\mathcal{A}_\kappa^r \subseteq \mathcal{A}_\kappa$ as well. When R is a Banach $\mathbb{Q}_p$-algebra, the $\mathcal{A}_\kappa[s]$ and $\mathcal{D}_\kappa[s]$ appearing in [Hansen 2017] are equal to $\mathcal{A}_\kappa^r$ and $\mathcal{D}_\kappa^{<r}$, respectively, for $r = p^{-1/p^s(p-1)}$. It is easiest, however, to use the modules $\mathcal{D}_\kappa^r$ to construct the eigenvariety since they are potentially orthonormalizable. Using the $\mathcal{D}_\kappa^r$, the construction of the eigenvariety follows [loc. cit.], and amounts largely to generalizing various well-known results from rigid geometry and nonarchimedean functional analysis. Our arguments also generalize from the case of $\boldsymbol{G} = \mathrm{GL}_{2/\mathbb{Q}}$ to the general case considered in [loc. cit.] (as stated in Theorem A). In particular, our methods work for groups that do not have Shimura varieties (such as $\boldsymbol{G} = \mathrm{Res}_{\mathbb{Q}}^F \mathrm{GL}_{n/F}$ for $n \geq 3$), which are intractable by the methods of [Andreatta et al. 2018] (see also [Andreatta et al. 2016]).

Remark 1.3.1. In independent work, Daniel Gulotta [2018] used a similar definition of distribution modules to extend Urban's construction [2011] of equidimensional eigenvarieties for reductive groups possessing discrete series.

1.4. *Questions and future work.*

Generalizations of the halo conjecture. It is interesting to consider how the halo conjecture might generalize beyond the case of $\mathrm{GL}_2/\mathbb{Q}$. For general $\boldsymbol{G}$ we raise the following questions:

Question 1.4.1. Does every irreducible component of the extended eigenvariety $\mathscr{X}_{\boldsymbol{G}}$ contain a point in the locus $p = 0$?

Question 1.4.2. Are there irreducible components of $\mathscr{X}_{\boldsymbol{G}}$ contained in the locus $p = 0$?

In the case of $\boldsymbol{G} = \mathrm{GL}_2/\mathbb{Q}$ it is a consequence of the halo conjecture that every irreducible component contains a characteristic-p point. Similarly, when $\boldsymbol{G}$ is an inner form of $\mathrm{GL}_2/\mathbb{Q}$ associated to a definite quaternion algebra over $\mathbb{Q}$, it is a consequence of the results of [Liu et al. 2017] that every irreducible component contains a characteristic-p point (see Theorem 6.3.4). In general, we regard an affirmative answer to the first question as a very weak version of the halo conjecture.

If a component has a characteristic-p point, it becomes possible to study characteristic-0 points in the component (if they exist) by passing to the characteristic-p point, or to points approximating the characteristic-p point. In the case of $\mathrm{GL}_2/\mathbb{Q}$ (or its inner forms), components which have a characteristic-p point have a Zariski dense set of points corresponding to (twists of) classical modular forms of weight 2. One argument in this spirit appears in [Pottharst and Xiao 2014], which has been used by the authors in combination with the methods of [Liu et al. 2017] to establish new cases of the parity conjecture for the Bloch–Kato Selmer groups associated to Hilbert modular forms. We essentially do this by showing that there is a classical parallel weight-2 point on every irreducible component of an eigenvariety for a definite quaternion algebra over a totally real field in which p splits completely. See [Johansson and Newton 2018] for more details.

Dimensions of irreducible components and functoriality. We note here that the theory of global irreducible components for the adic spaces we work with requires some explanation (see [Conrad 1999] for the rigid case). We have done this in a sequel to this paper [Johansson and Newton 2017], where we also generalize some of the results of [Hansen 2017]. In particular, we show that the lower bound for the dimension of irreducible components [loc. cit., Theorem 1.1.6] and (a variant of) the interpolation of Langlands functoriality [loc. cit., Theorem 5.1.6] generalize to our extended eigenvarieties.

One application of the interpolation of Langlands functoriality is that in the case of $\mathrm{GL}_{2/\mathbb{Q}}$ (or its inner forms) [Bergdall and Pollack 2016; Liu et al. 2017] show that the extended eigenvarieties contain the usual rigid eigenvarieties as a proper subspace. Applying functoriality (cyclic base change, for example) then shows that this is true for a larger class of groups. See [Johansson and Newton 2017] for more details.

Galois representations. In [Andreatta et al. 2018] the natural question is raised as to whether the Galois representations attached to characteristic-p points of the extended eigencurve are trianguline (in an appropriate sense). One can similarly ask this question for the characteristic-p Galois representations constructed in this paper. Note that in our level of generality, it is still only conjectural that the characteristic-0 Galois representations carried by the eigenvariety are trianguline, but this is known, for example, in the case where $\boldsymbol{G}$ is a definite unitary group defined with respect to a CM field. It would also be interesting to construct a "patched extended eigenvariety" in this setting, extending the construction of [Breuil et al. 2017], and we hope to study this in the near future.

1.5. ***An outline of the paper.*** Let us describe the contents of the paper. Section 2 collects what we need about the eigenvariety machine and the notion of slope decompositions, and introduces some functional-analytic terminology that we will need throughout the paper. Since the key point of the paper is the construction of certain norms, we adopt terminology that puts emphasis on the norm, as opposed to merely the underlying topology. We give a definition of a slope decomposition (a concept introduced in [Ash and Stevens 2008]) that differs slightly from the definitions that appear in the literature. This is necessary since the definition given in [loc. cit.] neither localizes nor glues well, and so is not suitable for the construction of eigenvarieties. Our definition is a formalization of an informal definition that the first author learnt from conversations with David Hansen.

In Section 3, we carry out the construction of the norms on the $\mathcal{D}_\kappa$, following the outline above. We first discuss the generalization of the Schneider–Teitelbaum norms to distributions on a uniform group G valued in a certain class of normed $\mathbb{Z}_p$-algebras that we call Banach–Tate $\mathbb{Z}_p$-algebras. These include, for example, all Banach $\mathbb{Q}_p$-algebras in the usual sense, as well as Tate rings $R = \mathcal{O}(\mathcal{U})$ with $\mathcal{U}$ an affinoid open subset of weight space (equipped with a suitable norm). We show that, in a precise sense, the completion of $\mathcal{D}(G, R)$ with respect to the family of norms $(\| - \|_r)_{r \in [1/p,1)}$ only depends on the underlying topology of R. Imposing some additional conditions on the norm (which is always possible in practice), we then construct the modules $\mathcal{D}_\kappa^r$, $\mathcal{D}_\kappa^{<r}$ and $\mathcal{A}_\kappa^r$ as outlined above.

Section 4 then uses the modules $\mathcal{D}_\kappa^r$ to construct the eigenvariety, following the strategy in [Hansen 2017]. Since the $\mathcal{D}_\kappa^r$ are potentially orthonormalizable, the construction simplifies somewhat. We end the section by generalizing the "Tor-spectral sequence" [loc. cit, Theorem 3.3.1] to our setting, which is a key tool for analyzing the geometry of eigenvarieties, and use it give a description of the "points" of the eigenvariety valued in a local field. We use this description in Section 5 when we construct Galois determinants.

In Section 6 we discuss the relationship of our work with that of [Andreatta et al. 2018; Liu et al. 2017]. We show that when $\boldsymbol{G} = \mathrm{GL}_{2/\mathbb{Q}}$, our construction, over the normalization of the weight space $\mathcal{W}_0$ discussed above, produces the same eigencurve as in [Andreatta et al. 2018] (this normalization is only different from $\mathcal{W}_0$ if $p = 2$). When $\boldsymbol{G}$ is the algebraic group over $\mathbb{Q}$ associated with the units of a definite quaternion algebra over $\mathbb{Q}$, we show that our framework gives a conceptual proof of [Liu et al. 2017, Theorem 3.16], which is a key ingredient in their proof of the halo conjecture. In essence, the numerical estimate of [loc. cit., Theorem 3.16] falls out directly from our proof of compactness of the U_p-operator. Thus, it is possible to view our proof of compactness of suitable "U_p-like" operators (known as controlling operators) as a generalization of [loc. cit., Theorem 3.16], as asked for in [loc. cit., Remark 3.26(2)]. Since this numerical estimate doesn't appear strong enough to establish the halo conjecture in more general situations, we have restricted ourselves to proving the statement in the setting of [loc. cit.] as an illustration of our method.

Finally, the Appendix proves various results that we need on the class of Tate rings whose associated affinoid adic spaces appear as the local pieces of our eigenvarieties; some of these results might be of independent interest.

2. Preliminaries

The goal of this section is to set up some functional analytic terminology and theory. Specifically, we require the results of [Buzzard 2007, §2–3] on Fredholm determinants, Riesz theory and the construction of spectral varieties in a level of generality that is intermediate between the settings of [Buzzard 2007; Coleman 1997] (see also [Andreatta et al. 2018, Appendice B]). For example, we need to work over coefficient rings arising from affinoid opens in the adic space $\mathcal{W}_0$ discussed in our Introduction. These rings are complete topological rings which are *Tate* in the language of Huber [1993, §1]. The topology on these rings is induced by a norm, and to discuss the spectral theory of compact operators it is convenient to fix such a norm. This gives rise to a class of normed rings which we call Banach–Tate rings (see Definition 2.1.2).

The proofs in [Buzzard 2007] go through with little to no change when working over Banach–Tate rings, so we will be rather brief. All norms etc. will be nonarchimedean so we will ignore this adjective. All rings will be commutative unless otherwise specified.

2.1. *Fredholm determinants over Banach–Tate rings.*

Definition 2.1.1. Let R be a ring. A function $|-| : R \to \mathbb{R}_{\geq 0}$ is called a *seminorm* if (for all $r, s \in R$)

(1) $|0| = 0$ and $|1| = 1$;

(2) $|r+s| \le \max(|r|, |s|)$;

(3) $|rs| \le |r||s|$.

If in addition $|r| = 0$ only if $r = 0$, then we say that $|-|$ is a *norm*. A ring R together with a (semi-)norm will be called a (semi-)normed ring. A normed ring R is called a Banach ring if the metric induced by the norm is complete.

If $f : R \to S$ is a morphism of normed rings, we say that f is *bounded* if there is a constant $C > 0$ such that $|f(r)| \le C|r|$ for all $r \in R$.

We say that two norms $|-|, |-|'$ on a ring R are *equivalent* if they induce the same topology. We say that they are *bounded-equivalent* if there are constants $C_1, C_2 > 0$ such that $C_1|r| \le |r|' \le C_2|r|$ for all $r \in R$ (note that this is stronger than equivalence, see Lemma 2.1.6). Let R be a normed ring. We say that $r \in R$ is *multiplicative* if $|rs| = |r||s|$ for all $s \in R$.

Definition 2.1.2. Let R be a normed ring. We say that R is *Tate* if R contains a multiplicative[2] unit ϖ such that $|\varpi| < 1$. We call such a ϖ a *multiplicative pseudouniformizer*. If R is also complete, we say that R is a *Banach–Tate ring*. If R is a Tate normed ring and ϖ is a multiplicative pseudouniformizer, then we define the corresponding valuation v_ϖ on R by $v_\varpi(r) = -\log_a |r|$, where $a = |\varpi^{-1}|$.

We remark that it is easy to see that a unit ϖ in a normed ring R is multiplicative if and only if $|\varpi^{-1}| = |\varpi|^{-1}$. A multiplicative pseudouniformizer ϖ is a uniform unit in the sense of [Kedlaya and Liu 2015, Remark 2.3.9(b)].

Remark 2.1.3. Let R be a Tate normed ring, with ϖ a multiplicative pseudouniformizer:

(1) The underlying topological ring is a Tate ring in the language of Huber; the unit ball R_0 is a ring of definition and ϖ is a topologically nilpotent unit. Conversely, assume R is a Tate ring and $\varpi \in R$ is a topologically nilpotent unit, contained in some ring of definition R_0. If $a \in \mathbb{R}_{>1}$, then we may define a norm on R by $|r| = \inf\{a^{-n} \mid r \in \varpi^n R_0,\ n \in \mathbb{Z}\}$. Equipped with this norm, R is a Tate normed ring with unit ball R_0 and ϖ is a multiplicative pseudouniformizer.

(2) A Banach–Tate ring A is the same thing as a Banach algebra A satisfying $|A^m| \ne 1$ in the language of [Coleman 1997, §1] (and what we call a Banach ring is what Coleman calls a Banach algebra). Here A^m denotes the set of multiplicative units of A. Additionally, when R is a Banach–Tate ring and R^+ is a ring of integral elements, a choice of a multiplicative pseudouniformizer ϖ may be used to identify the Gelfand spectrum $\mathcal{M}(R)$ of bounded multiplicative seminorms on R [Berkovich 1990, §1.2] with the maximal compact Hausdorff quotient of the adic spectrum $\mathrm{Spa}(R, R^+)$ [Huber 1993]; see [Kedlaya and Liu 2015, Definition 2.4.6]. Concretely, ϖ gives us a natural way of viewing a rank-1 point in $\mathrm{Spa}(R, R^+)$ as a bounded multiplicative seminorm.

Definition 2.1.4. Let R be a normed ring. A *normed R-module* is an R-module M equipped with a function $\|-\| : M \to \mathbb{R}_{\ge 0}$ such that (for all $m, n \in M$ and $r \in R$)

[2] That is, a unit which is multiplicative in the sense we just defined, as well as being a unit for multiplication!

(1) $\|m\| = 0$ if and only if $m = 0$;

(2) $\|m+n\| \le \max(\|m\|, \|n\|)$;

(3) $\|rm\| \le |r|\,\|m\|$.

We remark that if $r \in R$ is a multiplicative unit, then one sees easily that $\|rm\| = |r|\,\|m\|$ for all $m \in M$. If R is a Banach ring and M is complete, we say that M is a *Banach R-module*.

Let R be a Tate normed ring. If M and N are normed R-modules, then a homomorphism $\phi : M \to N$ is a continuous R-linear map. In this case, continuity of an R-linear map ϕ is equivalent to boundedness; i.e., there exists $C \in \mathbb{R}_{>0}$ such that $\|\phi(m)\| \le C\|m\|$ for all $m \in M$. In this case we set $|\phi| = \sup_{m \neq 0} |\phi(m)|\,|m|^{-1}$ as usual; $\mathrm{Hom}_{R,\mathrm{cts}}(M, N)$ becomes a normed R-module with respect to this norm. The open mapping theorem holds in this context; see, e.g., [Huber 1994, Lemma 2.4(i)].

Let R be a Noetherian Banach–Tate ring. The results of [Bosch et al. 1984, §3.7.2] hold in the context of Banach–Tate rings with the same proofs (thanks to the open mapping theorem), so R being Noetherian is equivalent to all ideals being closed. Moreover, the results of [loc. cit., §3.7.3] hold for *Noetherian* Banach–Tate rings with the same proofs. In particular, any finitely generated R-module carries a canonical complete topology, and any abstract R-linear map between two finitely generated R-modules is continuous and strict with respect to the canonical topology.

Definition 2.1.5. Let R be a Banach–Tate ring and let I be a set. We define $c_R(I)$ to be the set of sequences $(r_i)_{i\in I}$ in R tending to 0 (with respect to the filter of subsets of I with finite complement). It is a Banach R-module when equipped with the norm $\|(r_i)\| = \sup_{i\in I} |r_i|$.

We say that a Banach R-module M is *(potentially) orthonormalizable* (or (*potentially*) *ON-able* for short) if there exists a set I such that M is R-linearly isometric (resp. merely R-linearly homeomorphic) to $c_R(I)$. A set in M corresponding to the set $\{e_i = (\delta_{ij})_j \mid i \in I\} \subseteq c_R(I)$ under such a map is called an (*potential*) *ON-basis*.

Finally, we say that a Banach R-module M has *property* (Pr) if it is a direct summand of a potentially ON-able Banach R-module.

If $M \to N$ is a continuous morphism of ON-able Banach R-modules, then we may define its matrix for a fixed ON-basis on M and one on N as on [Buzzard 2007, p. 65], and the properties stated there hold in this situation as well. A morphism $\phi : M \to N$ between general Banach R-modules is said to be of *finite rank* if the image of ϕ is contained in a finitely generated submodule of N. More generally, ϕ is said to be *compact* (or *completely continuous*) if it is a limit of finite-rank operators in $\mathrm{Hom}_{R,\mathrm{cts}}(M, N)$. If R is Noetherian, [loc. cit., Lemma 2.3, Proposition 2.4] go through with the same proofs (using a multiplicative pseudouniformizer ϖ for what Buzzard calls ρ in the proof of Lemma 2.3) and we see that if $\phi : M \to N$ is a continuous R-linear map between ON-able Banach R-modules with matrix (a_{ij}) with respect to some bases $(e_i)_{i\in I}$ of M and $(f_j)_{j\in J}$ of N, then ϕ is compact if and only if $\lim_{j\to\infty} \sup_{i\in I} |a_{ij}| = 0$. When $M = N$ and $(e_i)_{i\in I} = (f_j)_{j\in J}$ this allows us to define the *characteristic power series*, or *Fredholm determinant*, $\det(1 - T\phi)$ of a compact ϕ using the recipe on [loc. cit., p. 67] and one sees that $\det(1-Tu) \in R\{\{T\}\}$, where

$$R\{\{T\}\} = \left\{ \sum_n a_n T^n \in R[\![T]\!] \;\middle|\; |a_m|M^m \to 0 \text{ for all } M \in \mathbb{R}_{\geq 0} \right\}$$

is the ring of entire power series in R.

Moving on, we remark that [loc. cit., Lemma 2.5, Corollary 2.6] are true in our setting with the same proofs. In particular, the notion of the Fredholm determinant extends to compact operators on potentially ON-able M, and may be computed using a potential ON-basis. It will be useful (at least psychologically) for us to know that these notions remain unchanged if we replace the norm on R by an equivalent one. First, we remark that changing the norm on R to an equivalent one doesn't change the topology on $c_R(I)$ (for I arbitrary). This can be seen directly, but it is also a consequence of the following lemma, which we will need later.

Lemma 2.1.6. *Let R be a complete Tate ring, and let $\varpi, \pi \in R$ be topologically nilpotent units. Assume that we have two equivalent norms $|-|_\varpi$ and $|-|_\pi$ on R (inducing the intrinsic topology) such that ϖ is multiplicative for $|-|_\varpi$ and π is multiplicative for $|-|_\pi$. Then we may find constants $C_1, C_2, s_1, s_2 > 0$ such that*

$$C_1 |a|_\pi^{s_1} \leq |a|_\varpi \leq C_2 |a|_\pi^{s_2}$$

for all $a \in R$.

Proof. We thank a referee for suggesting a more efficient argument for this proof. First, note that it suffices to find constants such that the inequalities hold for all nonzero $a \in R$, since it trivially holds for $a = 0$ and all choices of constants. We will first prove the second inequality. To start, pick $C' > 0$ such that $|a|_\pi \leq 1$ implies $|a|_\varpi \leq C'$ for all $a \in R$ (possible since the norms are equivalent). Since ϖ is topologically nilpotent we may find $m \in \mathbb{Z}_{\geq 1}$ such that $|\varpi^m|_\pi < 1$. It follows that $|\varpi^{-m}|_\pi \geq |\varpi^m|_\pi^{-1} > 1$.

For any nonzero $a \in R$, set

$$n = \left\lceil \frac{\log |a|_\pi}{\log |\varpi^m|_\pi^{-1}} \right\rceil.$$

We have $|\varpi^m|_\pi^n |a|_\pi \leq 1$. If $n \geq 0$, we deduce that $|\varpi^{mn} a|_\pi \leq |\varpi^m|_\pi^n |a|_\pi \leq 1$. If $n < 0$ we similarly deduce that

$$|\varpi^{mn} a|_\pi \leq |\varpi^{-m}|_\pi^{-n} |a|_\pi \leq |\varpi^m|_\pi^n |a|_\pi \leq 1.$$

Therefore we have $|\varpi^{mn} a|_\varpi \leq C'$. By multiplicativity of ϖ for $|-|_\varpi$ we get $|a|_\varpi \leq C' |\varpi|_\varpi^{-mn}$. Setting $q = |\varpi|_\varpi^{-m} > 1$, we then have

$$|a|_\varpi \leq C' q^n \leq C' q^{(\log |a|_\pi / \log |\varpi^m|_\pi^{-1}) + 1} = C' q |a|_\pi^{s_2},$$

where we have put $s_2 = (\log_q |\varpi^m|_\pi^{-1})^{-1}$; note that $s_2 > 0$. Set $C_2 = C'q$; we get

$$|a|_\varpi \leq C_2 |a|_\pi^{s_2},$$

with $C_2, s_2 > 0$ as desired.

To get the first inequality, note that by symmetry we may find $D, t > 0$ such that $|a|_\pi \leq D|a|_\varpi^t$. Rearranging we obtain

$$C_1|a|_\pi^{s_1} \leq |a|_\varpi \leq C_2|a|_\pi^{s_2}$$

as desired, where $C_1 = D^{-1/t}$ and $s_1 = 1/t$. □

Remark 2.1.7. If R has two equivalent norms $|-|$ and $|-|'$ with a common multiplicative pseudouniformizer ϖ such that $|\varpi| = |\varpi|'$, then the proof shows that $|-|$ and $|-|'$ are *bounded-equivalent*. This is also easy to see directly, and will be used freely throughout the paper.

Suppose then that $(M, |-|)$ is a Banach $(R, |-|)$-module, and $(M, |-|')$ is a Banach $(R, |-|')$-module, where $|-|$ and $|-|'$ are equivalent on both R and M. A Banach $(R, |-|)$-module isomorphism $(M, |-|) \cong (c_R(I), |-|)$ is then the same thing as a Banach $(R, |-|')$-module isomorphism $(M, |-|') \cong (c_R(I), |-|')$, since $(c_R(I), |-|) \cong (c_R(I), |-|')$ as *topological* R-modules via the identity map. Thus $(M, |-|)$ is potentially ON-able if and only if $(M, |-|')$ is potentially ON-able, and $(e_i)_{i\in I}$ is a potential ON-basis for $(M, |-|)$ if and only if it is a potential ON-basis for $(M, |-|')$. It follows, at least when R is Noetherian (which is all we need), that an operator ϕ is compact on a potentially ON-able $(M, |-|)$ if and only if it is compact on a potentially ON-able $(M, |-|')$, and the Fredholm determinant is the same.

We remark that the results [Buzzard 2007, Lemma 2.7–Corollary 2.10] hold over Noetherian Banach–Tate rings R, again with the same proofs. We can extend the notion of Fredholm determinants of compact operators on Banach R-modules with property (Pr) as on [loc. cit., pp. 72–73], and the results there hold over Noetherian Banach–Tate rings. One also sees that having property (Pr) is stable when changing the norms on (R, M) to equivalent ones, as is compactness of operators and the Fredholm determinants for compact operators are unchanged. We summarize the results of this section with the following proposition:

Proposition 2.1.8. *Let R be a Noetherian Banach–Tate ring. If M is a Banach R-module with property* (Pr) *and $\phi : M \to M$ is compact then there is a well-defined Fredholm determinant*

$$\det(1 - T\phi|M) \in R\{\{T\}\}.$$

If we change the norms on (R, M) to equivalent ones, then M still has property (Pr), *ϕ is still compact, and the Fredholm determinant is unchanged.*

2.2. ***Riesz theory, slope factorizations and slope decompositions.*** We continue to let R denote a Banach–Tate ring. If $Q \in R[T]$, we write $Q^*(T) := T^{\deg Q}Q(1/T)$. We recall the following definitions:

Definition 2.2.1. A *Fredholm series* is a formal power series $F = 1+\sum_{n\geq 1} a_nT^n \in R\{\{T\}\}$. A polynomial $Q \in R[T]$ is called *multiplicative* if the leading coefficient of Q is a unit (in other words, if $Q^*(0) \in R^\times$).

Two entire series $P, Q \in R\{\{T\}\}$ are said to be *relatively prime* if the ideal (P, Q) is equal to $R\{\{T\}\}$.

The proof of [Buzzard 2007, Theorem 3.3] goes through without changes; we state it for completeness (see also [Andreatta et al. 2018, Théoremè B.2]). Implicit in this is that [Buzzard 2007, Lemma 3.1] holds with the same proof; we will make use of this later.

Theorem 2.2.2. *Assume that R is Noetherian. Let M be a Banach R-module with property* (Pr) *and let $u : M \to M$ be a compact operator with $F = \det(1 - Tu)$. Assume that we have a factorization $F = QS$, where S is a Fredholm series, $Q \in R[T]$ is a multiplicative polynomial, and Q and S are relatively prime in $R\{\{T\}\}$. Then $\operatorname{Ker} Q^*(u) \subseteq M$ is finitely generated and projective and has a unique u-stable closed complement N such that $Q^*(u)$ is invertible on N. The idempotent projectors $M \to \operatorname{Ker} Q^*(u)$ and $M \to N$ lie in the closure of $R[u] \subseteq \operatorname{End}_{R,\mathrm{cts}}(M)$. The rank of $\operatorname{Ker} Q^*(u)$ is $\deg Q$, and $\det(1 - Tu \mid \operatorname{Ker} Q^*(u)) = Q$. Moreover, u is invertible on $\operatorname{Ker} Q^*(u)$, and $\det(1 - Tu \mid N) = S$.*

Proof. Apart from the last sentence, this is (a minor reformulation of) [Buzzard 2007, Theorem 3.3]. To see that u is invertible on $\operatorname{Ker} Q^*(u)$, note that

$$\det(u \mid \operatorname{Ker} Q^*(u)) = Q^*(0) \in R^\times.$$

To see that $\det(1 - Tu \mid N) = S$, write $S' = \det(1 - Tu \mid N)$ and note that

$$F = \det(1 - Tu \mid \operatorname{Ker} Q^*(u)) \det(1 - Tu \mid N) = QS'.$$

Hence $Q(S - S') = 0$, and Q is not a zero divisor since $Q(0) = 1$, so $S = S'$. □

The following lemma may be extracted from the proof of [loc. cit., Lemma 5.6]; we give the short proof for completeness.

Lemma 2.2.3. *Assume that R is Noetherian. Let M and M' be two Banach R-modules with property* (Pr) *and assume that we have a continuous R-linear map $v : M \to M'$ and a compact R-linear map $i : M' \to M$. Set $u = iv$ and $u' = vi$. Then u and u' are both compact and $\det(1 - Tu) = \det(1 - Tu')$; call this entire power series F. If $F = QS$ is a factorization as in Theorem 2.2.2, then i restricts to an isomorphism between $\operatorname{Ker} Q^*(u')$ and $\operatorname{Ker} Q^*(u)$.*

Proof. Compactness of u and u' and the equality of their Fredholm determinants follows from [loc. cit., Proposition 2.7]. Now assume we have a factorization $F = QS$. If $x' \in \operatorname{Ker} Q^*(u')$, then $Q^*(u)(i(x')) = i(Q^*(u')(x')) = 0$ so $i(\operatorname{Ker} Q^*(u')) \subseteq \operatorname{Ker} Q^*(u)$. Furthermore, if $i(x') = 0$ then $u'(x') = 0$, so $Q^*(u')(x') = Q^*(0).x' = 0$ and hence $x' = 0$, so i is injective on $\operatorname{Ker} Q^*(u')$. For surjectivity onto $\operatorname{Ker} Q^*(u)$, let $x \in \operatorname{Ker} Q^*(u)$ and choose $y \in \operatorname{Ker} Q^*(u)$ with $u(y) = x$ (possible by Theorem 2.2.2). Then one checks, similarly to the computation above, that $v(y) \in \operatorname{Ker} Q^*(u')$, and hence $i(v(y)) = u(y) = x$, which gives us surjectivity and finishes the proof. □

Next, we let K be a field, complete with respect to a nontrivial nonarchimedean absolute value. We briefly define the Newton polygon of a power series $F \in K[\![T]\!]$, following [Ash and Stevens 2008, §4.2] (in this special case). A subset $\mathcal{N} \subseteq \mathbb{R}^2$ is said to be *sup-convex* if it is convex and, if a point (a, b) is in $\mathcal{N}$, then $\mathcal{N}$ contains the whole half-line $\{(a, b + t) \mid t \geq 0\}$ above it. Given an arbitrary subset $S \subseteq \mathbb{R}^2$, there is a unique smallest sup-convex set containing S, which we will denote by $\mathcal{H}_+(S)$. If $I \subseteq \mathbb{Z}_{\geq 0}$ and $\omega : I \to \mathbb{R}$ is a function, then any set of the form $\mathcal{H}_+(\{(n, \omega(n)) \mid n \in I\})$ is called a *Newton polygon*. We refer to [loc. cit., §4.2] for the notions of vertices, edges and slopes of a Newton polygon.

Definition 2.2.4. Let $F = \sum_{n\geq 0} a_n T^n \in K[\![T]\!]$. Fix a pseudouniformizer $\varpi \in K$ and consider the corresponding valuation v_ϖ. The *Newton polygon of F* is the Newton polygon $\mathcal{H}_+(\mathcal{S}(F))$, where

$$\mathcal{S}(F) = \{(n, v_\varpi(a_n)) \mid n \in I_F\} \subseteq \mathbb{R}^2,$$

with $I_F = \{n \in \mathbb{Z}_{\geq 0} \mid a_n \neq 0\}$.

Let $h \in \mathbb{R}$. We say that a power series $F \in K[\![T]\!]$ has slope $\leq h$ (or $> h$) if all slopes of its Newton polygon are $\leq h$ (or $> h$). Now consider a Banach–Tate ring R with a multiplicative pseudouniformizer ϖ. We say that $F \in R[\![T]\!]$ has slope $\leq h$ (or $> h$) if, for any x in the Gelfand spectrum $\mathcal{M}(R)$ with residue field K_x, the specialization $F_x \in K_x[\![T]\!]$ has slope $\leq h$ (or $> h$).

Definition 2.2.5. Let R be a Banach–Tate ring with a fixed multiplicative pseudouniformizer ϖ. Let $F \in R\{\{T\}\}$ be a Fredholm series and let $h \in \mathbb{R}$. A *slope $\leq h$-factorization* of F is a factorization $F = QS$ in $R\{\{T\}\}$, where Q is a multiplicative polynomial of slope $\leq h$ and S is a Fredholm series of slope $> h$.

Remark 2.2.6. If R is a complete Tate ring with a fixed topologically nilpotent unit ϖ, then the notions of slope factorizations and slope $\leq h$ or $> h$ are independent of the choice of a norm on R with ϖ multiplicative. Moreover, one can define all these notions directly without choosing a norm on R.

Recall that an element $a \in R$ is called *quasinilpotent* if its spectral seminorm[3] $|a|_{\mathrm{sp}}$ is 0. This is equivalent to $|a|_x = 0$ for all $x \in \mathcal{M}(R)$ by [Berkovich 1990, Corollary 1.3.2]. The set of quasinilpotent elements forms an ideal of R, which is the kernel of the Gelfand transform $R \to \prod_{x \in \mathcal{M}(R)} K_x$. We note that it is easy to see that a quasinilpotent element is topologically nilpotent. For the kinds of rings R which appear in practice in this paper, the quasinilpotent elements are just the nilpotent elements (this follows from Theorem A.7), and the proof of the following lemma is simpler. However, we will avoid imposing additional technical assumptions at this stage.

Lemma 2.2.7. *Let R be a Banach–Tate ring with a fixed multiplicative pseudouniformizer ϖ and let $h \in \mathbb{Q}_{\geq 0}$. Let S be a Fredholm series of slope $> h$ and Q a multiplicative polynomial of slope $\leq h$. Then Q and S are relatively prime.*

Proof. We will use Coleman's resultant Res, for which we refer to [Coleman 1997, §A3] (the reader may also benefit from the discussion on [Buzzard 2007, p. 74]). By [Coleman 1997, Lemma A3.7] it suffices to prove that $\mathrm{Res}(Q, S)$ is a unit in $R\{\{T\}\}$. Pick $x \in \mathcal{M}(R)$ and specialize to K_x. Then $\mathrm{Res}(Q, S)_x = \mathrm{Res}(Q_x, S_x)$ and since Q_x has slope $\leq h$ and S_x has slope $> h$ we see that $\mathrm{Res}(Q, S)_x \in K_x\{\{T\}\}^\times = K_x^\times$. By [Berkovich 1990, Corollary 1.2.4] we see that $\mathrm{Res}(Q, S) = a_0 + T.F(T)$, where $a_0 \in R^\times$ and $F(T) \in R\{\{T\}\}$ has quasinilpotent coefficients. Multiplying by a_0^{-1} we see that it suffices to prove that if $F \in R\{\{T\}\}$ has quasinilpotent coefficients, then $1 - T.F(T) \in R\{\{T\}\}^\times$.

To prove this, we use an argument suggested to us by a referee, which is more efficient than our original argument. First note that the formal inverse of $1 - T.F(T)$ is $G(T) = \sum_{n\geq 0} T^n.F(T)^n$, so we need to show that this is entire. Setting $H(T) = T.F(T)$, it suffices to show that if $H(T)$ is any entire power

[3] The definition of the spectral seminorm is recalled in the Appendix.

series with $H(0) = 0$ and with quasinilpotent coefficients, then $\sum_{n\geq 0} H(T)^n$ converges and is entire. In fact, it suffices to prove that $\sum_{n\geq 0} H(T)^n \in R\langle T\rangle$, since if we have proved this we can apply this to $H(\varpi^{-N}T)$ for all N (which still has quasinilpotent coefficients) to deduce that $\sum_{n\geq 0} H(T)^n$ is entire.

So, to show this, it suffices to show that $H(T)$ is topologically nilpotent in $R\langle T\rangle$, where we equip $R\langle T\rangle$ with the Gauss norm coming from the norm on R. Since the coefficients of H tend to 0, we may write $H(T) = \sum_{n=1}^{N} h_n T^n + \sum_{n>N} h_n T^n$, with $|h_n| < 1$ for $n > N$. Then the tail $\sum_{n>N} h_n T^n$ is topologically nilpotent (it has Gauss norm < 1) and the terms $h_n T^n$ are topologically nilpotent for all n since h_n is quasinilpotent (and hence topologically nilpotent). So $H(T)$ is a finite sum of topologically nilpotent elements, and hence topologically nilpotent. □

Continue to let R be a Banach–Tate ring with a fixed multiplicative pseudouniformizer ϖ. The following is a minor variation of [Ash and Stevens 2008, Definition 4.6.1].

Definition 2.2.8. Let M be an (abstract) R-module, let $u : M \to M$ be an R-linear map and let $h \in \mathbb{Q}$. An element $m \in M$ is said to have slope $\leq h$ with respect to u if there is a multiplicative polynomial $Q \in R[T]$ such that

(1) $Q^*(u).m = 0$;

(2) the slope of Q is $\leq h$.

We let $M_{\leq h} \subseteq M$ denote the subset of elements of slope $\leq h$.

Lemma 2.2.9 [Ash and Stevens 2008, Proposition 4.6.2]. *$M_{\leq h}$ is an R-submodule of M, which is stable under u.*

Proof. It is clear from the definition that $M_{\leq h}$ is closed under multiplication, and stable under u. It therefore suffices to prove that it is closed under addition, for which it suffices to prove that if Q_1 and Q_2 are two multiplicative polynomials of slope $\leq h$, then so is $Q_1 Q_2$. To see this it suffices to specialize to the case when R is a field and the norm is an absolute value. The assertion is then well known (for example, the argument in the proof of [loc. cit., Proposition 4.6.2] carries over without change). □

Definition 2.2.10 [Ash and Stevens 2008, Definition 4.6.3]. Let M be an R-module with an R-linear map $u : M \to M$ and let $h \in \mathbb{Q}$. A slope $\leq h$-decomposition of M is an $R[u]$-module decomposition $M = M_h \oplus M^h$ such that

(1) M_h is a finitely generated R-submodule of $M_{\leq h}$;

(2) for every multiplicative polynomial $Q \in R[T]$ of slope $\leq h$, the map $Q^*(u) : M^h \to M^h$ is an isomorphism of R-modules.

Proposition 2.2.11. *We keep the above notation. If M has a slope $\leq h$-decomposition $M_h \oplus M^h$, then it is unique, and $M_h = M_{\leq h}$ (in particular the latter is finitely generated over R). We will from now on write $M_{>h}$ for the unique complement. Moreover, slope decompositions satisfy the following functorial properties*:

(1) *Let $f : M \to N$ be a morphism of $R[u]$-modules with slope $\leq h$-decompositions. Then $f(M_{\leq h}) \subseteq N_{\leq h}$ and $f(M_{>h}) \subseteq N_{>h}$. Moreover, both* $\mathrm{Ker}(f)$ *and* $\mathrm{Im}(f)$ *have slope $\leq h$-decompositions.*

(2) *Let $C^\bullet$ be a complex of $R[u]$-modules and suppose that each C^i has a slope $\leq h$-decomposition. Then every $H^i(C^\bullet)$ has a slope $\leq h$-decomposition, explicitly given by $H^i(C^\bullet) = H^i(C^\bullet_{\leq h}) \oplus H^i(C^\bullet_{>h})$.*

Proof. The proof is identical to that of [Ash and Stevens 2008, Lemma 4.6.4]: one equates slope $\leq h$-decompositions with $\mathcal{S}$-decompositions (as defined and studied in [loc. cit., §4.1]) for the set $\mathcal{S} \subseteq R[u]$ of all $Q^*(u)$, where Q is a multiplicative polynomial of slope $\leq h$. The properties then stated follow from general facts about $\mathcal{S}$-decompositions, recorded in [loc. cit., Proposition 4.1.2]. ☐

Definition 2.2.12. Let R be a Banach–Tate ring with a fixed multiplicative pseudouniformizer ϖ and let M be a Banach R-module. Assume that M has a slope $\leq h$-decomposition $M = M_{\leq h} \oplus M_{>h}$. If $f : R \to S$ is a bounded morphism of Banach–Tate rings such that $f(\varpi)$ is a multiplicative pseudouniformizer in S, we say that the slope $\leq h$-decomposition is *functorial for* $R \to S$ if $M \widehat{\otimes}_R S = (M_{\leq h} \otimes_R S) \oplus (M_{>h} \widehat{\otimes}_R S)$ is a slope $\leq h$-decomposition of $M \widehat{\otimes}_R S$ (using $f(\varpi)$ to define slopes for S). We say that the slope $\leq h$-decomposition is *functorial* if it is functorial for all such bounded homomorphisms of Banach–Tate rings out of R.

Theorem 2.2.13. *Let R be a Noetherian Banach–Tate ring with a fixed multiplicative pseudouniformizer ϖ, and let M be a Banach R-module with property* (Pr). *Let u be a compact R-linear operator on M, with Fredholm determinant $F(T) = \det(1 - Tu)$. If M has a slope $\leq h$-decomposition which is functorial with respect to $R \to K_x$ for all $x \in \mathcal{M}(R)$, then F has a slope $\leq h$-factorization. Conversely, if F has a slope $\leq h$-factorization, then M has a functorial slope $\leq h$-decomposition.*

Proof. Assume that M has a slope $\leq h$-decomposition $M = M_{\leq h} \oplus M_{>h}$ which is functorial with respect to $R \to K_x$ for all $x \in \mathcal{M}(R)$. Then both of these spaces satisfy property (Pr) and are u-stable, and hence we have

$$F = \det(1 - Tu \mid M_{\leq h}) \det(1 - Tu \mid M_{>h}).$$

We claim that this is a slope $\leq h$-factorization. Put $Q = \det(1 - Tu \mid M_{\leq h})$, $S = \det(1 - Tu \mid M_{>h})$. Pick $x \in \mathcal{M}(R)$ with residue field K_x and specialize. We have $Q_x = \det(1 - Tu \mid M_{\leq h} \otimes_R K_x)$ and $S_x = \det(1 - Tu \mid M_{>h} \widehat{\otimes}_R K_x)$. By assumption $M \widehat{\otimes}_R K_x = (M_{\leq h} \otimes_R K_x) \oplus (M_{>h} \widehat{\otimes}_R K_x)$ is a slope $\leq h$-decomposition, so Q_x has slopes $\leq h$ and S_x has slopes $> h$ and so $F = QS$ is a slope $\leq h$-factorization.

Conversely, assume that F has a slope $\leq h$-factorization $F = QS$. By Lemma 2.2.7 Q and S are relatively prime, so we may apply Theorem 2.2.2 to get a u-stable decomposition $M = \mathrm{Ker}\, Q^*(u) \oplus N$. It is easy to see that this decomposition is functorial, as is a slope $\leq h$-factorization, so it suffices to prove that this decomposition is a slope $\leq h$-decomposition. First, since Q has slope $\leq h$ we see that $\mathrm{Ker}\, Q^*(u) \subseteq M_{\leq h}$ (and we know it's finitely generated). It remains to show that for every multiplicative polynomial P of slope $\leq h$, $P^*(u)$ is invertible on N. By Lemma 2.2.7 P and S are relatively prime. Since $S = \det(1 - Tu \mid N)$ (by Theorem 2.2.2), it follows from [Buzzard 2007, Lemma 3.1] that P^* is invertible on N, as desired. ☐

Corollary 2.2.14. *With notation and assumptions as in the theorem, a slope $\leq h$-decomposition of M is functorial if and only if it is functorial for the natural map $R \to K_x$ for all $x \in \mathcal{M}(R)$.*

2.3. *Fredholm hypersurfaces.* In this section we discuss the notion of Fredholm hypersurfaces and relate this to slope factorizations and decompositions. We will use Huber's adic spaces as our framework for nonarchimedean geometry, and we will use standard notions and notation from this theory freely, referring to the basic references [Huber 1994; 1996].

Any Tate ring R with a Noetherian ring of definition has an associated affinoid adic space $\mathrm{Spa}(R, R^+)$, for any ring of integral elements R^+, by [Huber 1994, Theorem 2.5]. Fix an R^+ and consider $X = \mathrm{Spa}(R, R^+)$. We will frequently be interested in affine 1-space over X. As an adic space over $(\mathbb{Z}, \mathbb{Z})$, we have $\mathbb{A}^1 = \mathrm{Spa}(\mathbb{Z}[T], \mathbb{Z})$; it represents the functor $X \mapsto \mathcal{O}(X)$ on the category of adic spaces (we note that the functor $X \mapsto \mathcal{O}^+(X)$ is represented by the "closed unit disc" $\mathrm{Spa}(\mathbb{Z}[T], \mathbb{Z}[T])$). The fibre product $\mathbb{A}^1_X := X \times_{\mathrm{Spa}(\mathbb{Z},\mathbb{Z})} \mathbb{A}^1$ exists, but it is no longer affinoid. Indeed, if we pick a topologically nilpotent unit $\varpi \in R$, it can be checked that the fibre product is given by

$$\mathbb{A}^1_X = \bigcup_{m \geq 0} \mathrm{Spa}(R\langle \varpi^m T \rangle, R^+\langle \varpi^m T \rangle)$$

with respect to the transition maps coming from the natural inclusions. The ring of global functions on $\mathbb{A}^1_X$ is the ring of entire power series $R\{\{T\}\}$. Pick a topologically nilpotent unit $\varpi \in R$. If $h \in \mathbb{Q}$ then, writing $h = m/n$ with $m \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 1}$, we define an affinoid subset $\mathbb{B}_{X,h} \subseteq \mathbb{A}^1_X$ by

$$\mathbb{B}_{X,h} = \{|T^n| \leq |\varpi^{-m}|\} \subseteq \mathbb{A}^1_X.$$

We have $\mathbb{A}^1_X = \bigcup_{h \in \mathbb{Q}} \mathbb{B}_{X,h}$.

Let R be a complete Tate ring with a Noetherian ring of definition and let $F \in R\{\{T\}\}$ be a Fredholm series. Put $X = \mathrm{Spa}(R, R^\circ)$. The closed subvariety $Z(F) := \{F = 0\} \subseteq \mathbb{A}^1_X$ is called the *Fredholm hypersurface* of F, or sometimes the *spectral variety* of F. It carries a projection map $Z(F) \to X$, which is flat, locally quasifinite and partially proper by [Andreatta et al. 2018, Théoremè B.1].

Definition 2.3.1. Let R be a complete Tate ring with a Noetherian ring of definition, and pick a topologically nilpotent unit $\varpi \in R$. Let F be a Fredholm series with Fredholm hypersurface $Z = Z(F) \subseteq \mathbb{A}^1_X$, where $X = \mathrm{Spa}(R, R^\circ)$. Let $h \in \mathbb{Q}_{\geq 0}$ and let $U \subseteq X$ be an open affinoid in X; put $Z_{U,h} = Z \cap \mathbb{B}_{U,h} \subseteq \mathbb{A}^1_X$ (this is an open affinoid subset of Z). We say that the pair (U, h) is a *slope datum* for (X, F) if $Z_{U,h} \to U$ is finite of constant degree (if the pair (X, F) is clear form the context, we occasionally just say that (U, h) is a slope datum).

Theorem 2.3.2. *Let R be a complete Tate ring with a Noetherian ring of definition, and pick a topologically nilpotent unit $\varpi \in R$. Let F be a Fredholm series over R with spectral variety $Z = Z(F) \subseteq \mathbb{A}^1_X$, where $X = \mathrm{Spa}(R, R^\circ)$. Let $U \subseteq X$ be an open affinoid and let $h \in \mathbb{Q}_{\geq 0}$. Then*:

(1) *(U, h) is a slope datum for (X, F) if and only if F has a slope $\leq h$-factorization in $\mathcal{O}_X(U)\{\{T\}\}$.*

(2) *The collection of all $Z_{U,h}$ for all slope data (U, h) is an open cover of Z.*

Proof. This follows almost directly from [Andreatta et al. 2018, Théoremè B.1, Corollaire B.1]. The second assertion is shown by tracing through the proof of [loc. cit., Lemme B.1, Théoremè B.1]; adapting the proof of [loc. cit., Théoremè B.1] slightly one sees that one may take the sets to be of the form $Z_{U,h}$ (the degree is locally constant on U, so constancy of the degree can be arranged). For the first assertion, the statement that if (U, h) is a slope datum then F has a slope $\leq h$-factorization in $\mathcal{O}_X(U)\{\{T\}\}$ is [loc. cit., Corollaire B.1]. Conversely, if $F = QS$ is a slope $\leq h$-factorization in $\mathcal{O}_X(U)\{\{T\}\}$, then S is a unit in $\mathcal{O}(\mathbb{B}_{U,h})$. Therefore $\mathcal{O}(Z_{U,h}) = \mathcal{O}(\mathbb{B}_{U,h})/(F) = \mathcal{O}(\mathbb{B}_{U,h})/(Q)$ is finite of constant degree equal to $\deg Q$ over U, and hence $Z_{U,h} \to U$ is finite of constant degree. □

More generally, let X be an analytic adic space locally of the form $\mathrm{Spa}(R, R^\circ)$ for R a complete Tate ring with a Noetherian ring of definition, and let F be a Fredholm series over X with Fredholm hypersurface Z. If $U \subseteq X$ is an open affinoid and $h \in \mathbb{Q}_{\geq 0}$, we say that (U, h) is a slope datum for (X, F) if $\mathcal{O}(U)$ is Tate and there is a topologically nilpotent unit $\varpi \in \mathcal{O}(U)$ such that $Z_{U,h}$, defined using this choice of ϖ, is finite flat of constant degree over U.

When constructing eigenvarieties, it will be useful to consider a slightly more general notion. Let X be an analytic adic space as above and let F be a Fredholm series over X, with associated hypersurface Z. Write $\pi : Z \to X$ for the projection. We let $\mathscr{C}ov(Z)$ denote the set of all open affinoid $V \subseteq Z$ such that $\pi(V) \subseteq X$ is open affinoid, $\mathcal{O}(\pi(V))$ is Tate, and the map $\pi|_V : V \to \pi(V)$ is finite of constant degree. Then we have the following theorem.

Theorem 2.3.3. *Keep the notation and assumptions of the paragraph above. Then $\mathscr{C}ov(Z)$ is an open cover of Z. If $V \in \mathscr{C}ov(Z)$, then there exists a factorization $F = QS$ in $\mathcal{O}(\pi(V))\{\{T\}\}$, where Q is a multiplicative polynomial of degree $\deg \pi|_V$, S is a Fredholm series, Q and S are relatively prime, and we have*

$$\mathcal{O}(V) = \mathcal{O}(\pi(V))[T]/(Q) \quad \textit{and} \quad \mathcal{O}^+(V) = (\mathcal{O}(\pi(V))[T]/(Q))^\circ.$$

Conversely, if such a factorization of F exists in $\mathcal{O}(U)\{\{T\}\}$, where $U \subseteq X$ is open affinoid and $\mathcal{O}(U)$ is Tate, then $V = \mathrm{Spa}\big(\mathcal{O}(U)[T]/(Q), (\mathcal{O}(U)[T]/(Q))^\circ\big)$ is naturally an element of $\mathscr{C}ov(Z)$.

Proof. The assertions about rings of integral elements follow immediately from the rest by Lemma A.3. The first two parts are [Andreatta et al. 2018, Théoremè B.1, Corollaire B.1]. Note that if $\pi : V \to U$ is a finite flat morphism, with $U \subset X$ and $V \subset Z$ open affinoid, then π is open by [Huber 1996, Lemma 1.7.9]. For the last part, it is clear that $V \to U$ is finite and surjective of constant degree $\deg Q$, so it remains to see that V is naturally an open subset of Z. For this we may work locally over U. Set $B = \mathcal{O}(U)$. For each n we have compatible morphisms

$$B[T]/(Q) \to B\langle \varpi^n T\rangle/(Q) \leftarrow B\langle \varpi^n T\rangle/(F).$$

The second map is the projection onto the first factor in the decomposition

$$B\langle \varpi^n T\rangle/(F) \cong B\langle \varpi^n T\rangle/(Q) \times B\langle \varpi^n T\rangle/(S)$$

which results from the fact that Q and S are relatively prime. Thus $\{Q=0\} \subseteq Z$ is open and closed in Z. Moreover, when n is sufficiently large, we claim that the first map is an isomorphism. To see this, consider the quotient map $p : B[T] \to B[T]/(Q)$ and equip the target with a submultiplicative norm that induces the canonical topology. For large enough n we will have $|p(\varpi^n T)| \leq 1$ and hence $p(B_0[\varpi^n T]) \subseteq (B[T]/(Q))_0$ (here we are using $-_0$ to denote unit balls), so p is continuous for the topology on $B[T]$ coming from the inclusion $B[T] \subseteq B\langle \varpi^n T\rangle$, and we may complete to obtain a morphism $B\langle \varpi^n T\rangle \to B[T]/(Q)$ with kernel $QB\langle \varpi^n T\rangle$. This gives an inverse to the map $B[T]/(Q) \to B\langle \varpi^n T\rangle/(Q)$, proving the claim. Thus we may identify V with $\{Q=0\} \subseteq Z$, which shows that V is naturally an open subset of Z. □

3. Relative distribution algebras

3.1. ***Relative distribution algebras and norms.*** A p-adic analytic group will in this paper always mean a $\mathbb{Q}_p$-analytic group. Let R be a Banach–Tate ring. We denote the unit ball of R by R_0. If there exists a norm-decreasing homomorphism $\mathbb{Z}_p \to R$, where we equip $\mathbb{Z}_p$ with the usual norm $|x|_p = p^{-\mathrm{ord}_p(x)}$, we call such an R (together with the map $\mathbb{Z}_p \to R$) a *Banach–Tate $\mathbb{Z}_p$-algebra*. The goal of this section is to extend some of the constructions of [Schneider and Teitelbaum 2003, §4] to the case of continuous functions and distributions valued in such R. In particular, we construct R-valued analogues of (locally) analytic distribution algebras for compact p-adic analytic groups. We begin with a lemma on the existence of Banach–Tate $\mathbb{Z}_p$-algebra norms.

Lemma 3.1.1. *Let R be a Noetherian Banach–Tate ring with norm $|-|$ and a multiplicative pseudouniformizer ϖ. Assume that there exists a continuous homomorphism $\mathbb{Z}_p \to R$ (necessarily unique). Then there exists a Banach-Tate $\mathbb{Z}_p$-algebra norm $|-|'$ on R which is bounded-equivalent to $|-|^s$ for some $s>0$, and such that ϖ is a multiplicative pseudouniformizer for $|-|'$.*

Proof. Note first that a norm $|-|'$ on R is a Banach–Tate $\mathbb{Z}_p$-algebra norm if and only if $|p|' \leq p^{-1}$, so we need to check this. By continuity of $\mathbb{Z}_p \to R$ we have $p \in R^{\circ\circ}$. Choose $m \in \mathbb{Z}_{\geq 1}$ such that $|p|_{\mathrm{sp}} < |\varpi|^{2/m}$ and consider the finite free R-algebra

$$S = R[\varpi^{1/m}] = R[X]/(X^m - \varpi).$$

We equip S with its canonical topology as a finite R-module; then the induced subspace topology on $R \subseteq S$ agrees with the original topology on S. Thus we have $p, \varpi^{1/m} \in S^{\circ\circ}$. Now equip S with a submultiplicative R-Banach module norm $|-|_S$ that induces the canonical topology. Note that ϖ is a multiplicative pseudouniformizer for $|-|_S$ with $|\varpi|_S = |\varpi|$, and that $(R, |-|) \to (S, |-|_S)$ is norm-decreasing. We then have $|p\varpi^{-1/m}|_{S,\mathrm{sp}} < |\varpi|^{1/m} < 1$ by construction, so $p\varpi^{-1/m}$ is topologically nilpotent in S. We can then choose a ring of definition S_2 of S containing $\varpi^{1/m}$ and $p\varpi^{-1/m}$ and consider the norm

$$|s|_2 = \inf\{|\varpi|^{k/m} \mid s \in \varpi^{k/m} S_2\}.$$

Since $p \in \varpi^{1/m} S_2$ we have $|p|_2 < 1$, and we may hence find $s > 0$ such that $|p|_2^s \leq p^{-1}$. Restricting the norm $|-|' := |-|_2^s$ to $R \subseteq S$ then gives the desired norm. □

Definition 3.1.2. Let X be a compact topological space and let A be a topological $\mathbb{Z}_p$-algebra:

(1) We let $\mathcal{C}(X, A)$ denote the A-module of all continuous A-valued functions on X, and let $\mathcal{C}_{\mathrm{sm}}(X, A)$ denote the subspace of all locally constant functions.

(2) We put $\mathcal{D}(X, A) = \mathrm{Hom}_{A,\mathrm{cts}}(\mathcal{C}(X, A), A)$.

When A is a normed ring, we may topologize $\mathcal{C}(X, A)$ and $\mathcal{C}_{\mathrm{sm}}(X, A)$ using the supremum norm, and we may give $\mathcal{D}(X, A)$ the corresponding dual/operator norm. If A is complete, this makes $\mathcal{C}(X, A)$ into a complete A-module. When the topology on X is profinite, $\mathcal{C}_{\mathrm{sm}}(X, A)$ is dense in $\mathcal{C}(X, A)$ and, if R is a Banach–Tate $\mathbb{Z}_p$-algebra, the natural map $\mathcal{C}(X, \mathbb{Z}_p)\widehat{\otimes}_{\mathbb{Z}_p} R \to \mathcal{C}(X, R)$ is a topological isomorphism. Similarly $\mathcal{C}(X, \mathbb{Z}_p)\widehat{\otimes}_{\mathbb{Z}_p} R_0 \cong \mathcal{C}(X, R_0)$, where R_0 is the unit ball of R.

Continue to let X be a profinite set and R a Banach–Tate $\mathbb{Z}_p$-algebra with unit ball R_0 and a multiplicative pseudouniformizer ϖ. Note that $\mathcal{D}(X, R_0) = \mathrm{Hom}_{R_0}(\mathcal{C}(X, R_0), R_0)$ (i.e., continuity with respect to the ϖ-adic topology is automatic) and that this is the unit ball in $\mathcal{D}(X, R)$. We may equip $\mathcal{D}(X, R_0)$ with the weak topology coming from the family of maps $\mathcal{D}(X, R_0) \to R_0$ given by $\mu \mapsto \mu(f)$ for $f \in \mathcal{C}(X, R_0)$ and the ϖ-adic topology on R_0. We will refer to this topology as the *weak-star topology* on $\mathcal{D}(X, R_0)$. When $X = G$ is a profinite group, $\mathcal{D}(G, R)$ carries a convolution product

$$(\mu * \nu)(f) = \mu(g \mapsto \nu(h \mapsto f(gh))).$$

One checks directly that $\delta_g * \delta_h = \delta_{gh}$ for all $g, h \in G$, where δ_g denotes the Dirac distribution at g. This product preserves $\mathcal{D}(G, R_0)$. We sum up some basic properties of the weak-star topology.

Lemma 3.1.3. *If X is finite (hence discrete) the weak-star topology on $\mathcal{D}(X, R_0)$ coincides with the ϖ-adic topology. In general, if $X = \varprojlim_n X_n$ is an inverse limit of finite sets X_n, we have a natural isomorphism $\mathcal{D}(X, R_0) \cong \varprojlim_n \mathcal{D}(X_n, R_0)$ which identifies the weak-star topology on the source with the inverse limit topology, where $\mathcal{D}(X_n, R_0)$ is equipped with the ϖ-adic topology. When $X = G$ is a profinite group this is a ring homomorphism, and multiplication on $\mathcal{D}(G, R_0)$ is jointly continuous with respect to the weak-star topology.*

Proof. The first assertion is straightforward. For the second, note that the formation of $\mathcal{D}(X, R_0)$ is covariantly functorial in X, so the maps $X \to X_n$ induce a natural map $\mathcal{D}(X, R_0) \to \varprojlim_n \mathcal{D}(X_n, R_0)$ which is continuous by the first assertion when we equip the source and the target with the topologies in the statement of the lemma. Moreover it is easily checked to be a ring homomorphism when $X = G$ is a profinite group. Unraveling, we see that this morphism is the natural morphism

$$\mathrm{Hom}_{R_0}(\mathcal{C}(X, R_0), R_0) \to \mathrm{Hom}_{R_0}(\mathcal{C}_{\mathrm{sm}}(X, R_0), R_0)$$

induced by the inclusion $\mathcal{C}_{\mathrm{sm}}(X, R_0) \subseteq \mathcal{C}(X, R_0)$. Since this subspace is dense for the ϖ-adic topology, we see that the map is an isomorphism. To check that it also a homeomorphism, note first that by the same density one may define the weak-star topology using only locally constant functions. It is then straightforward to check that all basic opens from locally constant functions come by pullback from basic opens on the $\mathcal{D}(X_n, R_0)$, which implies that the map is a homeomorphism. Finally, multiplication is jointly continuous for the ϖ-adic topology on $\mathcal{D}(G_n, R_0)$ for all n, and hence jointly continuous on the inverse limit. This implies the last assertion. □

Let $X = \varprojlim_n X_n$ be a countable inverse limit of finite sets, viewed as a profinite set. We define $R_0[\![X]\!] := \varprojlim_n R_0[X_n]$ and $R[\![X]\!] := (\varprojlim_n R_0[X_n])[1/\varpi]$; these are R_0- and R-modules, respectively, and independent of the choice of the X_n's (here, if B is a ring and S is a finite set, $B[S]$ denotes the free B-module generated by the set S). If the X_n are groups (so X is a profinite group) then they carry natural algebra structures. We may topologize $R_0[\![X]\!]$ in two ways; either giving it the natural inverse limit topology or the ϖ-adic topology. We give $R[\![X]\!]$ the topology induced from the ϖ-adic topology on $R_0[\![X]\!]$, which is compatible with viewing $R[\![X]\!]$ as an R-Banach module with unit ball $R_0[\![X]\!]$.

Proposition 3.1.4. *Let $X = \varprojlim_n X_n$ be a profinite set. There is a natural R-Banach module isomorphism $R[\![X]\!] \to \mathcal{D}(X, R)$ sending $[x]$ to δ_x. It restricts to an R_0-module isomorphism $R_0[\![X]\!] \to \mathcal{D}(X, R_0)$ which identifies the inverse limit topology on the source with the weak-star topology on the target. If $X = G$ is a profinite group, then these maps are ring homomorphisms.*

Proof. Define compatible maps $R_0[X_n] \to \mathrm{Hom}_{R_0}(\mathcal{C}(X_n, R_0), R_0)$ by $[x] \mapsto \delta_x$; one checks directly that this is an isomorphism of topological R_0-modules, and that it is a ring homomorphism when X is a profinite group. Taking inverse limits we get

$$R_0[\![X]\!] \xrightarrow{\sim} \mathrm{Hom}_{R_0}(\mathcal{C}_{\mathrm{sm}}(X, R_0), R_0) = \mathcal{D}(X, R_0).$$

Lemma 3.1.3 shows that this identifies the inverse limit topology on the source with the weak-star topology on the target. Inverting ϖ we get the desired isomorphism $R[\![X]\!] \to \mathcal{D}(X, R)$, which is clearly a Banach module isomorphism since it identifies the respective unit balls $R_0[\![X]\!]$ and $\mathcal{D}(X, R_0)$. □

Recall the notion of a uniform pro-p group from [Dixon et al. 1999, Definition 4.1]. When G is a uniform pro-p group, $\mathbb{Z}_p[\![G]\!]$ may be identified with a ring of noncommutative formal power series

$$\left\{ \sum_{\alpha} d_\alpha \boldsymbol{b}^\alpha \,\middle|\, d_\alpha \in \mathbb{Z}_p \right\},$$

where d is the dimension of G, $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Z}^d_{\geq 0}$ is a multi-index, $g_1, \ldots, g_d$ is a minimal set of topological generators of G, $b_i = [g_i] - 1$ and $\boldsymbol{b}^\alpha := b_1^{\alpha_1} \cdots b_d^{\alpha_d}$. Our next goal is to show that the analogous description holds for $R_0[\![G]\!]$, with the same commutation relations between the $\boldsymbol{b}^\alpha$.

Proposition 3.1.5. *Let $G = \mathbb{Z}_p^d$. For $\alpha \in \mathbb{Z}^d_{\geq 0}$, let $E_\alpha : \mathbb{Z}_p^d \to \mathbb{Z}_p$ denote the function*

$$E_\alpha(x_1, \ldots, x_d) = \binom{x_1}{\alpha_1} \cdots \binom{x_d}{\alpha_d}.$$

Then the Amice transform

$$\mu \mapsto \sum_{\alpha} \mu(E_\alpha) T_1^{\alpha_1} \cdots T_d^{\alpha_d}$$

defines an algebra isomorphism $\mathcal{D}(\mathbb{Z}_p^d, R_0) \xrightarrow{\sim} R_0[\![T_1, \dots, T_d]\!]$ *which identifies the weak-star topology on the source with the product topology* $R_0[\![T_1, \dots, T_d]\!] = \prod_\alpha R_0.T_1^{\alpha_1} \cdots T_d^{\alpha_d}$ *on the target.*

Proof. Once again this is a simple extension of a well-known result, so we content ourselves with a sketch. The key observation is that $\mathcal{C}(\mathbb{Z}_p^d, R_0) \cong \mathcal{C}(\mathbb{Z}_p^d, \mathbb{Z}_p)\widehat{\otimes}_{\mathbb{Z}_p} R_0$. Then it is clear that

$$\mathcal{D}(\mathbb{Z}_p^d, R_0) \xrightarrow{\sim} \prod_\alpha R_0$$

via $\mu \mapsto (\mu(E_\alpha))_\alpha$ and it is straightforward to check that this identifies the weak topology on the source with the product topology on the target (it is the statement that the E_α suffice to define the weak-star topology). To finish, we remark that the computation that the algebra structures match up is identical to the well-known one in the case $R_0 = \mathbb{Z}_p$. □

Note that the topology on $R_0[\![T_1, \dots, T_d]\!]$ described in the proposition is equal to the $(\varpi, T_1, \dots, T_d)$-adic topology. Let us return to the case of a general uniform pro-p group G. The ring $\mathbb{Z}_p[\![G]\!]$ is described by formal power series as above. Following [Schneider and Teitelbaum 2003], let us define elements $c_{\beta\gamma,\alpha} \in \mathbb{Z}_p$ by

$$\boldsymbol{b}^\beta \boldsymbol{b}^\gamma = \sum_\alpha c_{\beta\gamma,\alpha} \boldsymbol{b}^\alpha. \tag{3.1.1}$$

We remark that, for fixed α, $c_{\beta\gamma,\alpha} \to 0$ as $|\beta| + |\gamma| \to +\infty$ (here and elsewhere, for a multi-index α we define $|\alpha| = \alpha_1 + \cdots + \alpha_d$). This follows from [loc. cit., Lemma 4.1(ii)].

Proposition 3.1.6. *Let G be a uniform pro-p group and use the notation above. Then $R_0[\![G]\!]$ may be identified with the ring of formal power series*

$$\left\{ \sum_\alpha d_\alpha \boldsymbol{b}^\alpha \,\middle|\, d_\alpha \in R_0 \right\}$$

with multiplication given by

$$\left(\sum_\beta d_\beta \boldsymbol{b}^\beta\right)\left(\sum_\gamma e_\gamma \boldsymbol{b}^\gamma\right) = \sum_\alpha \left(\sum_{\beta,\gamma} d_\beta e_\gamma c_{\beta\gamma,\alpha}\right) \boldsymbol{b}^\alpha.$$

Proof. The choice $g_1, \dots, g_d$ of a minimal (ordered) set of topological generators identifies G, as p-adic analytic manifold, with $\mathbb{Z}_p^d$. Thus we get a topological isomorphism $R_0[\![G]\!] \cong R_0[\![\mathbb{Z}_p^d]\!]$ of R_0-modules (for both the weak-star and the ϖ-adic topology). Proposition 3.1.5 then implies the description in terms of power series. To see that the multiplication works out as described, note that the natural map $\mathbb{Z}_p[\![G]\!] \to R_0[\![G]\!]$ is an algebra homomorphism; hence the above formula is true for products of monomials. We can then deduce the formula in general by noting that R_0 is central in $R_0[\![G]\!]$ and that the subring generated by R_0 and the image of $\mathbb{Z}_p[\![G]\!]$ (for which the formula holds) is dense in $R_0[\![G]\!]$ with respect to the weak-star topology, and that multiplication is jointly continuous for the weak-star topology. □

Inverting ϖ we get an explicit description of $R[\![G]\!]$ when G is uniform. Using this we may now define a family of norms on $R[\![G]\!]$ following [Schneider and Teitelbaum 2003, §4]. We continue to fix a minimal ordered set of topological generators $g_1, \dots, g_d$.

Definition 3.1.7. Let $r \in [1/p, 1)$. We define the r-norm $\| - \|_r$ on $R[\![G]\!]$ by the formula

$$\left\| \sum_{\alpha} d_\alpha \boldsymbol{b}^\alpha \right\|_r = \sup_\alpha |d_\alpha| r^{|\alpha|}.$$

Recall that we have fixed a choice of norm $| - |$ on R such that $|z| \le |z|_p$ for all $z \in \mathbb{Z}_p$. This will be convenient for some calculations. Note that the definition of $\| - \|_r$ a priori depends on the choice of generators. We remark that for all $r \in [1/p, 1)$, $\| - \|_r$ induces the weak-star topology on $R_0[\![G]\!]$ by Proposition 3.1.5 and a straightforward calculation. It follows that any homomorphism $G \to H$ of uniform groups induces a continuous homomorphism $R_0[\![G]\!] \to R_0[\![H]\!]$ when the source and target are equipped with (any) r-norms, since this is true for the weak-star topology using the characterization in Lemma 3.1.3.

Proposition 3.1.8. *The norm $\| - \|_r$ is independent of the choice of minimal ordered set of topological generators for G, and is submultiplicative. Finally, if we replace the norm $| - |$ on R by a bounded-equivalent $\mathbb{Z}_p$-algebra norm $| - |'$, then the resulting norm $\| - \|'_r$ is bounded-equivalent to $\| - \|_r$.*

Proof. For the proof of independence, we follow the discussion after the proof of [Schneider and Teitelbaum 2003, Theorem 4.10]. Let $g'_1, \dots, g'_d$ be a different choice and set $b'_i = [g'_i] - 1 \in \mathbb{Z}_p[\![G]\!]$ etc., and let $\| - \|'_r$ denote the r-norm with respect to this choice. We may write

$$\boldsymbol{b}'^\beta = \sum_\alpha c_{\beta,\alpha} \boldsymbol{b}^\alpha$$

in $\mathbb{Z}_p[\![G]\!]$, and one has $|c_{\beta,\alpha}|_p r^{|\alpha|} \le r^{|\beta|}$ (see [loc. cit.]). Transporting this to $R[\![G]\!]$ we have the same identity, and the inequality $|c_{\beta,\alpha}| r^{|\alpha|} \le r^{|\beta|}$ (since $|c_{\beta,\alpha}| \le |c_{\beta,\alpha}|_p$). Expanding out a general element $\mu \in R[\![G]\!]$ we then have

$$\mu = \sum_\beta d'_\beta \boldsymbol{b}'^\beta = \sum_\alpha \left(\sum_\beta d'_\beta c_{\beta,\alpha} \right) \boldsymbol{b}^\alpha.$$

We then have

$$\|\mu\|_r \le \sup_{\beta,\alpha} |d'_\beta| |c_{\beta,\alpha}| r^{|\alpha|} \le \sup_\beta |d'_\beta| r^{|\beta|} = \|\mu\|'_r.$$

By symmetry, we must have equality.

To prove submultiplicativity, we follow the proof of [Schneider and Teitelbaum 2003, Proposition 4.2]. Recall the $c_{\beta\gamma,\alpha}$ from (3.1.1). By [loc. cit., Lemma 4.1(ii)] we have $|c_{\beta\gamma,\alpha}| r^{|\alpha|} \le |c_{\beta\gamma,\alpha}|_p r^{|\alpha|} \le r^{|\beta|+|\gamma|}$ for all α, β, γ. Let $\mu = \sum_\beta d_\beta \boldsymbol{b}^\beta$ and $\nu = \sum_\gamma e_\gamma \boldsymbol{b}^\gamma$ be elements of $R[\![G]\!]$; then we have

$$\mu * \nu = \sum_\alpha \left(\sum_{\beta,\gamma} d_\beta e_\gamma c_{\beta\gamma,\alpha} \right) \boldsymbol{b}^\alpha$$

and we can calculate

$$\|\mu\nu\|_r = \sup_\alpha \left| \sum_{\beta,\gamma} d_\beta e_\gamma c_{\beta\gamma,\alpha} \right| r^{|\alpha|} \le \sup_{\beta,\gamma} |d_\beta| |e_\gamma| r^{|\beta|+|\gamma|} = \|\mu\|_r \|\nu\|_r,$$

where we use submultiplicativity and $|c_{\beta\gamma,\alpha}|r^{|\alpha|} \le r^{|\beta|+|\gamma|}$ to obtain the middle inequality. This finishes the proof of submultiplicativity.

Finally, suppose we have $C_1|x| \le |x|' \le C_2|x|$ for all $x \in R$. Then $C_1|d_\alpha|r^{|\alpha|} \le |d_\alpha|'r^{|\alpha|} \le C_2|d_\alpha|r^{|\alpha|}$ for all α which implies

$$C_1\left\|\sum_\alpha d_\alpha \boldsymbol{b}^\alpha\right\|_r \le \left\|\sum_\alpha d_\alpha \boldsymbol{b}^\alpha\right\|_r' \le C_2\left\|\sum_\alpha d_\alpha \boldsymbol{b}^\alpha\right\|_r$$

as desired. □

Before moving on to general compact p-adic analytic G, we record a few properties of the r-norms.

Lemma 3.1.9. *Let $r \in [1/p, 1)$. If $g \in G$, then $\|[g]\|_r = 1$ and $\|[g]\mu\|_r = \|\mu[g]\|_r = \|\mu\|_r$ for all $\mu \in R[\![G]\!]$. Moreover, if ϕ is an automorphism of G (of p-adic analytic groups), then ϕ induces an automorphism of $R[\![G]\!]$ satisfying $\|\phi(\mu)\|_r = \|\mu\|_r$ for all $\mu \in R[\![G]\!]$.*

Proof. The first statement follows from the fact that the expansion of $[g]$ has coefficients in $\mathbb{Z}_p$ and the constant term is 1. The second is an easy consequence of the first and submultiplicativity (since $[g]^{-1} = [g^{-1}]$ also has norm 1).

For the final statement, observe that if $g_1, \ldots, g_d$ is a set of topological generators then so are $\phi(g_1), \ldots, \phi(g_d)$. Since the r-norms are independent of the choice of generators, we conclude that if $\mu = \sum_\alpha d_\alpha \boldsymbol{b}^\alpha$, then

$$\|\phi(\mu)\|_r = \left\|\sum_\alpha d_\alpha(\phi(\boldsymbol{b}))^\alpha\right\|_r = \sup_\alpha |d_\alpha|r^{|\alpha|} = \|\mu\|_r. \qquad \square$$

We will use the last property mostly in the case when H is a compact p-adic analytic group, $N \subseteq H$ is a uniform open normal subgroup, and ϕ is the automorphism of N given by conjugation by some $h \in H$.

Now let G be an arbitrary compact p-analytic group. Pick a uniform open normal subgroup N and a set $h_1, \ldots, h_t$ of coset representatives of G/N. Any $\mu \in R[\![G]\!]$ may be written uniquely as $\mu = \sum_i [h_i]\mu_i$ with $\mu_i \in R[\![N]\!]$, and we define a norm $\|-\|_{N,r}$ on $R[\![G]\!]$ by

$$\|\mu\|_{N,r} = \sup_i \|\mu_i\|_r.$$

We could alternatively take a right coset decomposition $\mu = \sum_i \nu_i[h_i]$ with $\nu_i \in R[\![N]\!]$, and define $\|-\|_{N,r}^{\mathrm{right}}$ on $R[\![G]\!]$ by

$$\|\mu\|_{N,r}^{\mathrm{right}} = \sup_i \|\nu_i\|_r.$$

Proposition 3.1.10. *We have $\|-\|_{N,r} = \|-\|_{N,r}^{\mathrm{right}}$. The definition is also independent of the choice of coset representatives. Moreover, $\|-\|_{N,r}$ is submultiplicative and satisfies $\|[g]\|_{N,r} = 1$ and $\|[g]\mu\|_{N,r} = \|\mu[g]\|_{N,r} = \|\mu\|_{N,r}$ for all $g \in G$ and $\mu \in R[\![G]\!]$.*

Proof. For left/right independence, note that $\mu = \sum_i([h_i]\mu_i[h_i^{-1}])[h_i]$ and hence

$$\|\mu\|_{N,r}^{\mathrm{right}} = \sup_i \|[h_i]\mu_i[h_i^{-1}]\|_r = \sup_i \|\mu_i\|_r = \|\mu\|_{N,r}$$

by Lemma 3.1.9. For independence of the coset representatives, suppose we have h_i' a different set with $h_i = h_i' n_i$; then $\mu = \sum_i [h_i']([n_i]\mu_i)$ and hence

$$\|\mu\|'_{N,r} = \sup_i \|[n_i]\mu_i\|_r = \sup_i \|\mu_i\|_r = \|\mu\|_{N,r}$$

by Lemma 3.1.9 again. Next we prove submultiplicativity. Define $k(i,j)$ by $h_i h_j = h_{k(i,j)} n_{ij}$. For $\mu = \sum_i [h_i]\mu_i$ and $\nu = \sum_j [h_j]\nu_j$ in $R[\![G]\!]$, we have

$$\mu\nu = \sum_k [h_k]\Bigg(\sum_{i,j:k(i,j)=k} [n_{ij}]([h_j^{-1}]\mu_i[h_j])\nu_j\Bigg).$$

Using Lemma 3.1.9 and submultiplicativity for $\| - \|_r$ on N one then sees easily that $\|\mu\nu\|_{N,r} \leq \|\mu\|_{N,r}\|\nu\|_{N,r}$.

Next, let $g \in G$. Writing $g = h_i n$ for some i and $n \in N$, we see that $\|[g]\|_{N,r} = \|[n]\|_r = 1$ by Lemma 3.1.9. Finally, the last property then follows by the same argument as in the proof of Lemma 3.1.9. □

As the notation suggests, $\| - \|_{N,r}$ *does* depend on the choice of N. For a study of how the completions change when one changes the subgroup in certain situations, see [Ardakov and Wadsley 2013, §10.6–10.8].

3.2. *Completions.* In this section we study the case when G is a uniform pro-p group in more detail. Let R be a Banach–Tate $\mathbb{Z}_p$-algebra with multiplicative pseudouniformizer ϖ as usual.

Definition 3.2.1. For $r \in [1/p, 1)$, define $\mathcal{D}^r(G, R)$ to be the completion of $\mathcal{D}(G, R)$ with respect to the norm $\| - \|_r$, and we let $\mathscr{D}(G, R)$ denote the completion of $\mathcal{D}(G, R)$ with respect to the entire family of norms $(\| - \|_r)_{r\in[1/p,1)}$.

Remark 3.2.2. Note that if we change the norm on R to a bounded-equivalent one, then the completion $\mathcal{D}^r(G, R)$ is unchanged, by Proposition 3.1.8.

The motivation for this definition is that if R is a Banach $\mathbb{Q}_p$-algebra, $\mathscr{D}(G, R)$ is naturally isomorphic to the space of locally analytic R-valued distributions on G, by Proposition 3.2.9.

Note that there are natural norm-decreasing injective maps $\mathcal{D}^s(G, R) \to \mathcal{D}^r(G, R)$ whenever $r \leq s$ (which we will think of as inclusions), and that they fit together into an inverse system with limit $\mathscr{D}(G, R)$. The explicit description of $\mathcal{D}(G, R)$ from Proposition 3.1.6 gives us an explicit formal power series description

$$\mathcal{D}^r(G, R) = \left\{ \sum_\alpha d_\alpha \boldsymbol{b}^\alpha \;\middle|\; d_\alpha \in R,\ |d_\alpha| r^{|\alpha|} \to 0 \right\}$$

and the norm is still given by $\left\|\sum d_\alpha \boldsymbol{b}^\alpha\right\|_r = \sup |d_\alpha| r^{|\alpha|}$. We see that, unlike $\mathcal{D}(G, R)$, the $\mathcal{D}^r(G, K)$ are naturally potentially ON-able, with a potential ON-basis given by the elements $\varpi^{-n(r,\varpi,\alpha)}\boldsymbol{b}^\alpha$, where

$$n(r, \varpi, \alpha) = \left\lfloor \frac{|\alpha| \log_p r}{\log_p |\varpi|} \right\rfloor. \tag{3.2.1}$$

Lemma 3.2.3. *If $r < s$ then the inclusion $\iota : \mathcal{D}^s(G, R) \hookrightarrow \mathcal{D}^r(G, R)$ is a compact map of R-Banach modules.*

Proof. For simplicity set $\mathcal{D}^r := \mathcal{D}^r(G, R)$ etc. for the duration of this proof. Choose a minimal set of topological generators $g_1, \dots, g_d$ of G and set $b_i = [g_i] - 1$ as usual. For $n \geq 1$ define $T_n : \mathcal{D}^s \to \mathcal{D}^r$ by

$$T_n\Big(\sum_\alpha d_\alpha \boldsymbol{b}^\alpha\Big) = \sum_{|\alpha|<n} d_\alpha \boldsymbol{b}^\alpha.$$

By definition we see that T_n is of finite rank. Then if $\sum_\alpha d_\alpha \boldsymbol{b}^\alpha$ is in the unit ball of $\mathcal{D}^s$, i.e., $|d_\alpha| s^{|\alpha|} \leq 1$ for all α, we have

$$\Big\|(\iota - T_n)\Big(\sum_\alpha d_\alpha \boldsymbol{b}^\alpha\Big)\Big\|_r = \Big\|\sum_{|\alpha|\geq n} d_\alpha \boldsymbol{b}^\alpha\Big\|_r \leq (r/s)^n.$$

Thus $\|\iota - T_n\| \leq (r/s)^n$, where $\| - \|$ is the operator norm on $\mathrm{Hom}_{R,\mathrm{cts}}(\mathcal{D}^s, \mathcal{D}^r)$, and hence $T_n \to \iota$ as $n \to \infty$, so ι is compact. ☐

Lemma 3.2.4. *Let G and H be two uniform pro-p groups and assume that $f : G \to H$ is a homomorphism of p-adic analytic groups such that $f(G) \subseteq H^{p^n}$ for some $n \geq 0$. Then the induced map $f_* : \mathcal{D}(G, R) \to \mathcal{D}(H, R)$ is norm-decreasing when we equip $\mathcal{D}(G, R)$ with $\| - \|_r$ and $\mathcal{D}(H, R)$ with $\| - \|_{r^{1/p^n}}$. As a consequence, we get an induced map*

$$f_* : \mathcal{D}^r(G, R) \to \mathcal{D}^r(H, R)$$

which factors through the natural map $\mathcal{D}^{r^{1/p^n}}(H, R) \to \mathcal{D}^r(H, R)$. In particular, when $n \geq 1$, f_* is compact.

Proof. We start with the first assertion. Note that the general case follows from two special cases: $n = 0$, f arbitrary, and $n = 1$, $G = H^p$ with f the inclusion. Indeed the general case can be written as a composition of these cases.

So, suppose first that $n = 0$. Scaling by powers of ϖ, it suffices to prove this for $\mathcal{D}(G, R_0)$. The map f_* is continuous with respect to the norm $\| - \|_r$ (see the discussion after Definition 3.1.7). Let $g_1, \dots, g_d$ be a minimal set of topological generators for G and let $b_i = [g_i] - 1$ as usual. Using that $\|[h] - 1\|_r \leq r$ for all $h \in H$, we see that

$$\Big\|f_*\Big(\sum d_\alpha \boldsymbol{b}^\alpha\Big)\Big\|_r = \Big\|\sum d_\alpha f_*(\boldsymbol{b})^\alpha\Big\|_r \leq \sup |d_\alpha| r^{|\alpha|} = \Big\|\sum d_\alpha \boldsymbol{b}^\alpha\Big\|_r$$

as desired, using continuity of f_*. This completes the proof of the first special case.

Next, we consider the second case $G = H^p \subseteq H$. Let $s = r^{1/p}$; since $r \geq p^{-1}$ we have $s \geq p^{-1/p} > p^{-1/(p-1)}$. Let $h_1, \dots, h_d$ be a minimal set of topological generators for H. Then $h_1^p, \dots, h_1^d$ form a minimal set of topological generators for H^p. Set $b_i = [h_i^p] - 1$ and $b_i' = [h_i] - 1$ (apologies for the mild abuse of notation). Then, inside $\mathcal{D}(H, R)$, we have

$$\|b_i\|_s = \|(1 + b_i')^p - 1\|_s = \Big\|\sum_{k=1}^{p} \binom{p}{k} (b_i')^k\Big\|_s = s^p = r$$

using $s > p^{-1/(p-1)}$ and $|p| \leq |p|_p = p^{-1}$. Thus, if $\sum d_\alpha \boldsymbol{b}^\alpha \in \mathcal{D}(H^p, R)$, then inside $\mathcal{D}(H, R)$ we have

$$\left\| \sum d_\alpha \boldsymbol{b}^\alpha \right\|_s \leq \sup |d_\alpha| r^\alpha,$$

which is equal to $\left\| \sum d_\alpha \boldsymbol{b}^\alpha \right\|_r$ computed inside $\mathcal{D}(H^p, R)$. This finishes the proof of first assertion. The remaining assertions are then easily verified (using Lemma 3.2.3 for last one). □

Before discussing what happens when one changes the norm on R, we record the following important base change lemma.

Lemma 3.2.5. *Let R and S be Banach–Tate $\mathbb{Z}_p$-algebras, and let $f : R \to S$ be a bounded ring homomorphism. Suppose that there is a multiplicative pseudouniformizer $\varpi \in R$ such that $f(\varpi)$ is also multiplicative. Let $r \in [1/p, 1)$. Then the natural map $\mathcal{D}^r(G, R)\widehat{\otimes}_R S \to \mathcal{D}^r(G, S)$ is an isomorphism of Banach S-modules.*

Proof. Note that (since f is bounded) the fact that ϖ and $f(\varpi)$ are both multiplicative implies that $|\varpi| = |f(\varpi)|$. We recall the potential ON-bases $(\varpi^{-n(r,\varpi,\alpha)}\boldsymbol{b}^\alpha)_\alpha$ and $(f(\varpi)^{-n(r,f(\varpi),\alpha)}\boldsymbol{b}^\alpha)_\alpha$ of $\mathcal{D}^r(G, R)$ and $\mathcal{D}^r(G, S)$, respectively. It is straightforward to check that the tensor product norm on

$$\left(\bigoplus_\alpha R(\varpi^{-n(r,\varpi,\alpha)}\boldsymbol{b}^\alpha) \right) \otimes_R S = \bigoplus_\alpha S(f(\varpi^{-n(r,\varpi,\alpha)})\boldsymbol{b}^\alpha)$$

induced by $\| - \|_r$ on $\mathcal{D}^r(G, R)$ and the norm on S is bounded-equivalent to the norm induced by $\| - \|_r$ on $\mathcal{D}^r(G, S)$, and so we obtain isomorphic completions, which gives the desired statement. □

Our next goal is to prove that $\mathscr{D}(G, R)$ is independent, as a topological R-module, of the choice of norm on R. Recall that we only consider norms for which there exists a multiplicative pseudouniformizer, and such that the natural map $\mathbb{Z}_p \to R$ is norm-decreasing.

Proposition 3.2.6. *$\mathscr{D}(G, R)$ is independent of the choice of norm on R.*

Proof. Let $| - |$ and $| - |'$ be two equivalent such norms on R; for $r \in [1/p, 1)$ we get the corresponding r-norms $\| - \|_r$ and $\| - \|'_r$ on $\mathcal{D}(G, R)$. Let $\mu = \sum_\alpha d_\alpha \boldsymbol{b}^\alpha \in \mathcal{D}(G, R)$ be an arbitrary element and use Lemma 2.1.6 to find constants $C_1, C_2, s_1, s_2 > 0$ such that

$$C_1|a|^{s_1} \leq |a|' \leq C_2|a|^{s_2}$$

for all $a \in R$. Then

$$C_1|d_\alpha|^{s_1} r^{|\alpha|} \leq |d_\alpha|' r^{|\alpha|} \leq C_2|d_\alpha|^{s_2} r^{|\alpha|}$$

for all α and hence

$$C_1\|\mu\|^{s_1}_{r^{1/s_1}} \leq \|\mu\|'_r \leq C_2\|\mu\|^{s_2}_{r^{1/s_2}}$$

for all r such that $r, r^{1/s_1}, r^{1/s_2} \in [1/p, 1)$. It follows that the families $(\| - \|_r)$ and $(\| - \|'_r)$ define the same topology on $\mathcal{D}(G, R)$, and hence the same completion, as required. □

We now introduce a variant of the $\mathcal{D}^r(G, R)$, which, when R is a Banach $\mathbb{Q}_p$-algebra, recovers the analytic distribution algebra (with fixed radius of analyticity). Although we do not use this variant in our construction of eigenvarieties, it is used in Section 5 to construct Galois representations.

Let $r > s \geq 1/p$. Let $\mathcal{D}^{r,\circ}(G, R) = \{\sum d_\alpha \boldsymbol{b}^\alpha \mid |d_\alpha| r^{|\alpha|} \leq 1\}$ denote the unit ball of $\mathcal{D}^r(G, R)$. We define $\mathcal{D}^{<r,\circ}(G, R)$ to be the closure of $\mathcal{D}^{r,\circ}(G, R)$ in $\mathcal{D}^s(G, R)$. Note that $\mathcal{D}^{<r,\circ}(G, R)$ is an R_0-module, a priori depending on s, which carries two natural topologies (the ϖ-adic topology and the subspace topology coming from $\mathcal{D}^s(G, R)$).

Proposition 3.2.7. *We have*

$$\mathcal{D}^{<r,\circ}(G, R) = \left\{ \sum_\alpha d_\alpha \boldsymbol{b}^\alpha \in \mathcal{D}^s(G, R) \;\middle|\; |d_\alpha| r^{|\alpha|} \leq 1 \right\}$$

as a subset of $\mathcal{D}^s(G, R)$. Thus $\mathcal{D}^{<r,\circ}(G, R)$ is independent of s. The subspace topology corresponds to the weak topology with respect to the family of maps $(\mu \mapsto d_\alpha(\mu))_\alpha$ on the right-hand side (and is therefore also independent of s). The ϖ-adic topology is induced by the norm

$$\left\| \sum d_\alpha \boldsymbol{b}^\alpha \right\|_r = \sup_\alpha |d_\alpha|' r^{|\alpha|}$$

and is separated and complete.

Proof. Let $W = \left\{ \sum d_\alpha \boldsymbol{b}^\alpha \in \mathcal{D}^s(G, R) \;\middle|\; |d_\alpha| r^{|\alpha|} \leq 1 \right\}$. Since the maps $\mu \mapsto d_\alpha(\mu)$ are continuous we see that W is closed. On other hand, any finite truncation of an element in W is in $\mathcal{D}^{r,\circ}(G, R)$, so $\mathcal{D}^{r,\circ}(G, R)$ is dense in W. It follows that $W = \mathcal{D}^{<r,\circ}(G, R)$. The subspace topology is given by the norm $\| - \|_s$, and one checks easily that this agrees with the weak topology in the statement of the proposition. The final statement is similarly easy to check; we leave it to the reader. □

We then set $\mathcal{D}^{<r}(G, R) = \mathcal{D}^{<r,\circ}(G, R)[1/\varpi]$; this is naturally a Banach R-module which embeds into $\mathcal{D}^s(G, R)$ for all $s \in [1/p, r)$. The $(\mathcal{D}^{<r}(G, R))_{r>1/p}$ form an inverse system and the natural map $\mathcal{D}^r(G, R) \to \mathcal{D}^s(G, R)$ factors over $\mathcal{D}^{<r}(G, R)$, so we therefore have

$$\mathscr{D}(G, R) = \varprojlim_r \mathcal{D}^{<r}(G, R)$$

as well. Recall the potential ON-basis $(\varpi^{-n(r,\varpi,\alpha)} \boldsymbol{b}^\alpha)_\alpha$ of $\mathcal{D}^r(G, R)$; we have

$$\mathcal{D}^{<r}(G, R) = \left\{ \sum_\alpha d_\alpha \boldsymbol{b}^\alpha \;\middle|\; |d_\alpha| r^{|\alpha|} \text{ bounded} \right\} = \left(\prod_\alpha R_0 . \varpi^{-n(r,\varpi,\alpha)} \boldsymbol{b}^\alpha \right) \left[\frac{1}{\varpi} \right].$$

We remark that if $(\varpi^{-n(r,\varpi,\alpha)} \boldsymbol{b}^\alpha)_\alpha$ is an ON-basis, we have $\mathcal{D}^{<r,\circ}(G, R) = \prod_\alpha R_0 . \varpi^{-n(r,\varpi,\alpha)} \boldsymbol{b}^\alpha$ and the weak topology on the left-hand side is equal to the product topology on the right-hand side. Next, we define some function modules in a similar fashion. We put

$$\mathcal{C}^{<r,\circ}(G, R) = \{ f \in \mathcal{C}(G, R) \mid |\mu(f)| \leq 1 \text{ for all } \mu \in \mathcal{D}(G, R) \cap \mathcal{D}^{r,\circ}(G, R) \}$$

and set $\mathcal{C}^{<r}(G,R)=\mathcal{C}^{<r,\circ}(G,R)[1/\varpi]\subseteq\mathcal{C}(G,R)$. We note that $f=\sum_\alpha c_\alpha E_\alpha\in\mathcal{C}^{<r}(G,R)$ if and only if $\varpi^{-n(r,\varpi,\alpha)}\boldsymbol{b}^\alpha(f)=c_\alpha\varpi^{-n(r,\varpi,\alpha)}$ is bounded as $\alpha\to\infty$; from this one sees that

$$\mathcal{C}^{<r}(G,R)=\left(\prod_\alpha R_0.\varpi^{n(r,\varpi,\alpha)}E_\alpha\right)\left[\frac{1}{\varpi}\right]$$

and that it is the dual space of $\mathcal{D}^r(G,R)$, and that the dual norm is given by $\left\|\sum_\alpha c_\alpha E_\alpha\right\|_r=\sup_\alpha|c_\alpha|r^{-|\alpha|}$. When $r>s\geq 1/p$, we let $\mathcal{C}^r(G,R)$ denote the closure of $\mathcal{C}^{<s}(G,R)$ inside $\mathcal{C}^{<r}(G,R)$. Tracing through the definitions we get an explicit description

$$\mathcal{C}^r(G,R)=\left\{\sum_\alpha c_\alpha E_\alpha\;\middle|\;|c_\alpha|r^{-|\alpha|}\to 0\right\}=\widehat{\bigoplus_\alpha}R.\varpi^{n(r,\varpi,\alpha)}E_\alpha$$

and see that the dual space of $\mathcal{C}^r(G,R)$ is $\mathcal{D}^{<r}(G,R)$.

Remark 3.2.8. The reader should compare our description of $\mathcal{C}^r(G,R)$ with the construction of [Liu et al. 2017, Section 5.4]. Here, the authors give a definition of a "modified" space of continuous functions on $\mathbb{Z}_p$ with values in $\mathbb{Z}_p[\![T,pT^{-1}]\!]$ which is morally (apart from the slight difference in coefficients and the fact that we have only defined $\mathcal{C}^r(G,R)$ for $r>1/p$) the space $\mathcal{C}^{1/p}(\mathbb{Z}_p,R)$, where R is the Tate ring obtained as the rational localization

$$\mathbb{Z}_p[\![T]\!]\left\langle\frac{p}{T}\right\rangle\left[\frac{1}{T}\right]$$

of $\mathbb{Z}_p[\![T]\!]$. We give R the norm with unit ball $\mathbb{Z}_p[\![T]\!]\langle p/T\rangle$ and $|T|=1/p$, defined as in Remark 2.1.3. The definition which appears in [loc. cit.] is therefore a useful motivation for the general constructions of this article, although we will not use the modules $\mathcal{C}^r(G,R)$ in this article. We will see in Theorem 6.3.4 that one may use the module $\mathcal{D}^{1/p}(\mathbb{Z}_p,R)$ (which is defined) to prove the main results of [loc. cit.].

To finish this section we discuss the relationship between our constructions and the spaces of locally analytic functions or distributions when R is a Banach $\mathbb{Q}_p$-algebra. We may and do assume that $\mathbb{Q}_p$ is isometrically embedded into R and that $|p|=1/p$. Recall that the atlas on G induced from our choice of a topological basis identifies G^{p^n} with $(p^n\mathbb{Z}_p)^{\dim G}$. Amice's theorem [Colmez 2010, Théorème I.4.7] tells us that the space of n-analytic functions on G with respect to this atlas is explicitly given as

$$\mathcal{C}^{n\text{-an}}(G,\mathbb{Q}_p)=\widehat{\bigoplus_\alpha}\mathbb{Q}_p.k_\alpha E_\alpha,$$

where $k_\alpha:=\lfloor p^{-n}\alpha_1\rfloor!\cdots\lfloor p^{-n}\alpha_{\dim G}\rfloor!$. The space of n-analytic R-valued functions on G is then

$$\mathcal{C}^{n\text{-an}}(G,R)=\widehat{\bigoplus_\alpha}R.k_\alpha E_\alpha\subseteq\mathcal{C}(G,R).$$

It is well known that $|k_\alpha|\sim r_n^{|\alpha|}$ with $r_n=p^{-1/p^n(p-1)}$, and it follows that $\mathcal{C}^{n\text{-an}}(G,R)=\mathcal{C}^{r_n}(G,R)$ as $\mathbb{Q}_p$-Banach spaces. Since $r_n\to 1$ from below as $n\to\infty$ it follows that $\mathscr{C}(G,R)$ is the space of locally analytic R-valued functions on G, with its usual locally convex topology. Dually, $\mathscr{D}(G,R)$ is then the space of locally analytic R-valued distributions with its usual locally convex topology. We sum up this discussion in a proposition.

Proposition 3.2.9. *When R is Banach $\mathbb{Q}_p$-algebra, $\mathscr{C}(G, R)$ is canonically the space of locally analytic R-valued functions on G and $\mathscr{D}(G, R)$ is dually the space of locally analytic R-valued distributions on G.*

3.3. ***Ash–Stevens distribution modules for Banach–Tate $\mathbb{Z}_p$-algebras.*** While the definitions in this subsection will be of a local nature, let us nevertheless start by introducing the global setup that we will need to define eigenvarieties. Let F be a number field. We put $\boldsymbol{G} = \mathrm{Res}^F_{\mathbb{Q}} \boldsymbol{H}$, where $\boldsymbol{H}$ is a connected reductive group over F split at all places $v \mid p$. $\boldsymbol{G}$ is then a connected reductive group over $\mathbb{Q}$. When $v \mid p$ we write $\boldsymbol{H}_{\mathcal{O}_{F_v}}$ for a split model of $\boldsymbol{H}_{F_v}$ over $\mathcal{O}_{F_v}$ and choose a Borel subgroup $\boldsymbol{B}_v$ (with unipotent radical $\boldsymbol{N}_v$) and a maximal torus $\boldsymbol{T}_v \subseteq \boldsymbol{B}_v$ of $\boldsymbol{H}_{\mathcal{O}_{F_v}}$. Set

$$\boldsymbol{G}_{\mathbb{Z}_p} = \prod_{v \mid p} \mathrm{Res}^{\mathcal{O}_{F_v}}_{\mathbb{Z}_p} \boldsymbol{H}_{\mathcal{O}_{F_v}}, \quad \boldsymbol{B} = \prod_{v \mid p} \mathrm{Res}^{\mathcal{O}_{F_v}}_{\mathbb{Z}_p} \boldsymbol{B}_v, \quad \boldsymbol{T} = \prod_{v \mid p} \mathrm{Res}^{\mathcal{O}_{F_v}}_{\mathbb{Z}_p} \boldsymbol{T}_v$$

and also put $\boldsymbol{N} = \prod_{v \mid p} \mathrm{Res}^{\mathcal{O}_{F_v}}_{\mathbb{Z}_p} \boldsymbol{N}_v$. We use overlines to denote opposite groups; e.g., $\overline{\boldsymbol{B}} = \prod_{v \mid p} \mathrm{Res}^{\mathcal{O}_{F_v}}_{\mathbb{Z}_p} \overline{\boldsymbol{B}}_v$, where the $\overline{\boldsymbol{B}}_v$ are the opposite Borels of $\boldsymbol{B}_v$.

We will also need notation for various subgroups of $G := \boldsymbol{G}(\mathbb{Q}_p)$. Set $G_0 = \boldsymbol{G}_{\mathbb{Z}_p}(\mathbb{Z}_p)$, $B_0 = \boldsymbol{B}(\mathbb{Z}_p)$, $T_0 = \boldsymbol{T}(\mathbb{Z}_p)$, and $N_0 = \boldsymbol{N}(\mathbb{Z}_p)$. We let I denote the Iwahori subgroup of G defined as the preimage of $\boldsymbol{B}(\mathbb{F}_p)$ under the reduction map $G_0 \to \boldsymbol{G}_{\mathbb{Z}_p}(\mathbb{F}_p)$, and we let $K_s = \mathrm{Ker}(G_0 \to \boldsymbol{G}_{\mathbb{Z}_p}(\mathbb{Z}/p^s))$ be the s-th principal congruence subgroup of G_0 for $s \geq 1$. Again for $s \geq 1$, set

$$\begin{aligned} T_s &= \mathrm{Ker}(T_0 \to \boldsymbol{T}(\mathbb{Z}/p^s\mathbb{Z})), \\ N_s &= \mathrm{Ker}(N_0 \to \boldsymbol{N}(\mathbb{Z}/p^s\mathbb{Z})), \\ \overline{N}_s &= \mathrm{Ker}(\overline{\boldsymbol{N}}(\mathbb{Z}_p) \to \overline{\boldsymbol{N}}(\mathbb{Z}/p^s\mathbb{Z})). \end{aligned}$$

Set $B_s = T_s N_s$ for $s \geq 0$. We have Iwahori decompositions $I = \overline{N}_1 T_0 N_0$ and $K_s = \overline{N}_s T_s N_s$. Next, choose a splitting $T := \boldsymbol{T}(\mathbb{Q}_p) \to T_0$ of the inclusion $T_0 \subseteq T$ and put $\Sigma = \mathrm{Ker}(T \to T_0)$. We set

$$\begin{aligned} \Sigma^+ &= \{t \in \Sigma \mid t\overline{N}_1 t^{-1} \subseteq \overline{N}_1\}, \\ \Sigma^{\mathrm{cpt}} &= \{t \in \Sigma \mid t\overline{N}_1 t^{-1} \subseteq \overline{N}_2\}. \end{aligned}$$

We may then define $\Delta_p = I\Sigma^+ I$; this is a monoid and (Δ_p, I) is a Hecke pair (which means that I and $\delta I \delta^{-1}$ are commensurable for all $\delta \in \Delta_p$). The corresponding Hecke algebra (defined over $\mathbb{Z}_p$) will be denoted by $\mathbb{T}(\Delta_p, I)$.

With these preparations let us now move on to the definition of analytic and locally analytic distribution modules for general Banach–Tate $\mathbb{Z}_p$-algebras R. When R is a Banach $\mathbb{Q}_p$-algebra, these were defined in [Ash and Stevens 2008] using (locally) analytic functions on I. Recasting this in terms of the norms of the previous section, we are able to extend the definition to all Banach–Tate $\mathbb{Z}_p$-algebras.

Let $\kappa : T_0 \to R^\times$ be a continuous character. We will put some restrictions on the choice of norm on R, according to the following lemma. We set $\epsilon = 1$ if $p \neq 2$ and $\epsilon = 2$ if $p = 2$, and put $q = p^\epsilon$.

Lemma 3.3.1. *Keep the above notation and assume that R is Noetherian. Write $|-|$ for the given norm on R and let ϖ be a multiplicative pseudouniformizer. Then there exists a Banach–Tate $\mathbb{Z}_p$-algebra norm $|-|'$ on R, bounded-equivalent to $|-|^s$ for some $s > 0$, such that $|\kappa(t)|' \le 1$ for all $t \in T_0$, $|\kappa(t) - 1|' < 1$ for all $t \in T_\epsilon$, and ϖ is a multiplicative pseudouniformizer for $|-|'$.*

Proof. The proof is similar to that of Lemma 3.1.1. Let $t_1, \dots, t_a$ be a set of topological generators of T_0 and let $t_{a+1}, \dots, t_b$ be a set of topological generators for T_ϵ; it suffices to find $|-|'$ such that $|\kappa(t_i)|' \le 1$ for $i = 1, \dots, a$, $|\kappa(t_i) - 1| < 1$ for $i = a+1, \dots, b$, and $|p|' \le p^{-1}$, which is bounded-equivalent to $|-|^s$ for some $s > 0$.

Since T_0 is compact, $\kappa(T_0)$ is bounded, and hence t_i is powerbounded for all i. Moreover, T_ϵ is pro-p and $R^\circ/R^{\circ\circ}$ is a reduced discrete ring of characteristic p, so the continuous homomorphism $T_\epsilon \to (R^\circ/R^{\circ\circ})^\times$ induced from κ is trivial. We conclude that $\kappa(T_\epsilon) \subseteq 1 + R^{\circ\circ}$ and hence $\kappa(t_i) - 1 \in R^{\circ\circ}$ for $i = a+1, \dots, b$. We may now choose m such that $|\kappa(t_i) - 1|_{\mathrm{sp}} < |\varpi|^{2/m}$ for $i = a+1, \dots, b$ and $|p|_{\mathrm{sp}} < |\varpi|^{2/m}$. Arguing with $S = R[\varpi^{1/m}]$ as in Lemma 3.1.1 we may construct a norm $|-|_2$ on R for which ϖ is a multiplicative pseudouniformizer with $|\varpi|_2 = |\varpi|$, $|\kappa(t_i)|_2 \le 1$ for $i = 1, \dots, a$, $|\kappa(t_i) - 1|_2 < 1$ for $i = a+1, \dots, b$, and $|p|_2 < 1$. Setting $|-|' := |-|_2^s$ for s sufficiently large then gives the desired norm. □

Definition 3.3.2. Let R be a Banach–Tate $\mathbb{Z}_p$-algebra and $\kappa : T_0 \to R^\times$ a continuous character. We will say that the norm of R is *adapted to* κ if $\kappa(T_0) \subseteq R_0$ and $|\kappa(t) - 1| < 1$ for all $t \in T_\epsilon$. Note that then $|\kappa(t)| = 1$ for all $t \in T_0$ and there exists an $r < 1$ such that $|\kappa(t) - 1| \le r$ for all $t \in T_\epsilon$.

For the rest of the subsection we consider a Banach–Tate $\mathbb{Z}_p$-algebra R and character $\kappa : T_0 \to R$ such that the norm on R is adapted to κ. We extend κ to a character of B_0 by making it trivial on N_0. We define $\mathcal{A}_\kappa \subseteq \mathcal{C}(I, R)$ to be the subset of functions such that $f(gb) = \kappa(b)f(g)$ for all $g \in I$ and $b \in B_0$. $\mathcal{A}_\kappa$ is naturally a Banach R-module and carries a continuous right action of I by left translation. Restricting a function from I to $\overline{N}_1$ gives a topological isomorphism $\mathcal{A}_\kappa \cong \mathcal{C}(\overline{N}_1, R)$. By definition, Σ^+ acts on the left on $\overline{N}_1$ by conjugation, and via the previous isomorphism this induces a right action of Σ^+ on $\mathcal{A}_\kappa$. These actions fit together into a right action of Δ_p on $\mathcal{A}_\kappa$. We let $\mathcal{D}_\kappa$ denote the dual $\mathrm{Hom}_{R,\mathrm{cts}}(\mathcal{A}_\kappa, R)$, equipped with the dual left Δ_p-action. Since $\mathcal{A}_\kappa$ is the set of B_0-invariants of $\mathcal{C}(I, R)$ with respect to the action $(f.b)(g) = \kappa(b)^{-1} f(gb)$ ($b \in B_0$, $g \in I$), $\mathcal{D}_\kappa$ is the Hausdorff B_0-coinvariants of $\mathcal{D}(I, R)$ with respect to the dual (right) action. We record a more precise statement for future use:

Proposition 3.3.3. *The natural surjection $\mathcal{D}(I, R) \to \mathcal{D}_\kappa$ is equivariant for the natural left I-actions on both sides. Identifying $\mathcal{D}_\kappa$ with $\mathcal{D}(\overline{N}_1, R)$, the map is given by $\delta_{\bar{n}b} \mapsto \kappa(b)\delta_{\bar{n}}$.*

Proof. The inverse to the restriction map $\mathcal{A}_\kappa \to \mathcal{C}(\overline{N}_1, R)$ is given by $f \mapsto (\bar{n}b \mapsto \kappa(b)f(\bar{n}))$ (here and above $\bar{n} \in \overline{N}_1$ and $b \in B_0$). From this one sees directly that the dual map sends $\delta_{\bar{n}b}$ to $\kappa(b)\delta_{\bar{n}}$. That this characterizes the maps follows from R-linearity and continuity for the weak-star topology. □

To apply the results from the previous subsection we will need to know that some groups are uniform. The following result is presumably well known to experts but we have been unable to find a suitable reference. The proof we give is due to Konstantin Ardakov, and we thank him for allowing us to include it here (any errors are due to the authors).

Proposition 3.3.4. *K_s and $\overline{N}_s$ are uniform for $s \geq \epsilon$.*

Proof. By construction the groups are products $K_s = \prod_{v\,|\,p} K_{s,v}$, and similarly for $\overline{N}_{s,v}$, in a natural way, so it suffices to prove that each $K_{s,v}$ and each $\overline{N}_{s,v}$ is uniform. Fix $v \,|\, p$ and let $s \geq \epsilon$. First assume that $\boldsymbol{H}_v = \mathrm{GL}_{n/\mathcal{O}_{F_v}}$. Then we have the usual matrix logarithm $\log : K_{s,v} \to p^s M_n(\mathcal{O}_{F_v})$ and exponential $\exp : p^s M_n(\mathcal{O}_{F_v}) \to K_{s,v}$. They converge and are inverse to each other (by our assumption on s) and the Lie algebra $p^s M_n(\mathcal{O}_{F_v})$ is easily seen to be powerful by assumption, so by the definition of the correspondence between powerful Lie algebras and uniform pro-p groups [Dixon et al. 1999, Theorem 9.10] via the Campbell–Hausdorff series we see that $K_{s,v}$ is the uniform group corresponding to $p^s M_n(\mathcal{O}_{F_v})$. To get the result for $\overline{N}_{s,v}$ we may by conjugation assume that $\overline{\boldsymbol{N}}_v$ is the group of lower triangular unipotent matrices; the corresponding Lie algebra is that of lower triangular nilpotent matrices and we then argue similarly.

Now let $\boldsymbol{H}_v$ be arbitrary and choose a closed immersion $\boldsymbol{H}_v \hookrightarrow \mathrm{GL}_{n/\mathcal{O}_{F_v}}$ for some n. We thereby identify $\boldsymbol{H}_v$ with a closed subgroup of $\mathrm{GL}_{n/\mathcal{O}_{F_v}}$. Writing $\boldsymbol{B}'_v$ for the upper triangular Borel of $\mathrm{GL}_{n/\mathcal{O}_{F_v}}$, $\boldsymbol{N}'_v$ for its unipotent radical, $\overline{\boldsymbol{N}}'_v$ for the opposite of $\boldsymbol{N}'_v$ and $\boldsymbol{T}'_v$ for the diagonal torus, we may assume, after conjugating if necessary, that $\boldsymbol{T}_v \subseteq \boldsymbol{T}'_v$ etc. We write $K'_{s,v}$ etc. for the corresponding principal congruence subgroups. With this setup, we now give the rest of the proof for the $K_{s,v}$ only; the proof for $\overline{N}_{s,v}$ proceeds in the same way. Note that $K_{s,v} = \boldsymbol{H}_v(\mathcal{O}_{F_v}) \cap K'_{s,v}$. By [Dixon et al. 1999, Theorem 4.5] we see that $K'_{s,v}$ is torsion-free and that it suffices to prove that $K_{s,v}$ is powerful, i.e., that $[K_{s,v}, K_{s,v}] \subseteq K^q_{s,v}$, where $[K_{s,v}, K_{s,v}]$ is the derived subgroup of $K_{s,v}$ and $K^q_{s,v}$ is the subgroup generated by the q-th powers of elements in $K_{s,v}$ (any compact p-adic analytic group is topologically finitely generated). We remark that it is easy to see that $[K'_{s,v}, K'_{s,v}] \subseteq K'_{s+\epsilon,v} = (K'_{s,v})^q$. Using this and $K_{s,v} = \boldsymbol{H}_v(\mathcal{O}_{F_v}) \cap K'_{s,v}$, we see that $[K_{s,v}, K_{s,v}] \subseteq K'_{s+\epsilon,v} \cap \boldsymbol{H}_v(\mathcal{O}_{F_v}) = K_{s+\epsilon,v}$ and $K^q_{s,v} \subseteq K_{s+\epsilon,v}$.

It remains to prove that $K_{s+\epsilon,v} \subseteq K^q_{s,v}$. We have $T_{s+\epsilon,v} = T^q_{s,v}$ using the logarithm and exponential ($\boldsymbol{T}_v$ is a split torus). We have an isomorphism of $\mathcal{O}_{F_v}$-schemes $\prod_\alpha x_\alpha : \prod_\alpha \mathbb{G}_a \xrightarrow{\sim} \boldsymbol{N}_v$, where α ranges through the roots of $\boldsymbol{H}_v$ whose root subgroups are contained in $\boldsymbol{N}_v$, and x_α is a corresponding root homomorphism. Under this isomorphism $N_{s,v}$ corresponds to $\prod_\alpha p^s \mathcal{O}_{F_v}$, and by standard properties of x_α one has $x_\alpha(q.(p^s a)) = x_\alpha(p^s a)^q$ for any $a \in \mathcal{O}_{F_v}$. It follows that $N_{s+\epsilon,v} = N^q_{s,v}$. Similarly $\overline{N}_{s+\epsilon,v} = \overline{N}^q_{s,v}$. By the Iwahori decomposition we then see that $K_{s+\epsilon,v} \subseteq K^q_{s,v}$ as desired. □

Remark 3.3.5. Note that the argument in the final paragraph of the above proof also implies that, for arbitrary p and $s \geq 1$, we have $\overline{N}_{s+1,v} = \overline{N}^p_{s,v}$.

Definition 3.3.6. Let $r \in [1/p, 1)$:

(1) We define a norm $\|-\|^{\mathrm{sub}}_r$ on $\mathcal{D}_\kappa$ by transporting the norm $\|-\|_{\overline{N}_\epsilon, r}$ (defined before Proposition 3.1.10) on $\mathcal{D}(\overline{N}_1, R)$ to $\mathcal{D}_\kappa$ via the isomorphism $\mathcal{D}(\overline{N}_1, R) \cong \mathcal{D}_\kappa$ obtained by restriction of functions from I to $\overline{N}_1$.

(2) We define a norm $\| - \|_r^{\mathrm{quot}}$ on $\mathcal{D}_\kappa$ as the quotient norm induced from $\| - \|_{K_\epsilon, r}$ (defined before Proposition 3.1.10) via the natural surjection $\mathcal{D}(I, R) \to \mathcal{D}_\kappa$.

Note that $\| - \|_r^{\mathrm{quot}}$ is I-invariant; this follows from I-equivariance of the surjection and from Proposition 3.1.10. The following is the key result of this subsection:

Proposition 3.3.7. *Suppose that $|\kappa(t) - 1| \le r$ for all $t \in T_\epsilon$. Then $\| - \|_r^{\mathrm{quot}} = \| - \|_r^{\mathrm{sub}}$ on $\mathcal{D}_\kappa$.*

Proof. Let us first assume that $p \neq 2$. First we claim that $\| - \|_r^{\mathrm{quot}}$ is equal to the quotient norm on $\mathcal{D}_\kappa$ coming from the surjection $\mathcal{D}(K_1, R) \to \mathcal{D}_\kappa$ and the norm $\| - \|_r$ on the source. To see this, pick a set $(b_i)_i$ of coset representatives of I/K_1 lying in B_0 and define a map $\pi_\kappa : \mathcal{D}(I, R) = \bigoplus_i \delta_{b_i} \mathcal{D}(K_1, R) \to \mathcal{D}(K_1, R)$ by

$$(\delta_{b_i} \mu_i)_i \mapsto \sum_i \kappa(b_i) \mu_i .$$

We remark that composing this map with the natural surjection $\mathcal{D}(K_1, R) \to \mathcal{D}_\kappa$ gives the natural surjection $\mathcal{D}(I, R) \to \mathcal{D}_\kappa$ (this follows from the explicit formula in Proposition 3.3.3). To prove the claim, it then suffices to prove that $\| - \|_r$ is the quotient norm of $\| - \|_{K_1, r}$ via π_κ. Write $\| - \|_r'$ for this quotient norm. For simplicity assume that 1 is one of the coset representatives b_i. Then our map is a section of the inclusion $\mathcal{D}(K_1, R) \subseteq \mathcal{D}(I, R)$. It is then clear that $\| - \|_r' \le (\| - \|_{K_1, r})|_{\mathcal{D}(K_1, r)} = \| - \|_r$. Conversely, if $\mu = \sum_i \kappa(b_i) \mu_i \in \mathcal{D}(K_1, R)$ is the image of $\sum_i \delta_{b_i} \mu_i \in \mathcal{D}(I, R)$, then

$$\|\mu\|_r \le \sup_i \|\kappa(b_i)\mu_i\|_r \le \sup_i \|\mu_i\|_r = \left\| \sum_i \delta_{b_i} \mu_i \right\|_{K_1, r} .$$

Taking the infimum over such presentations we obtain $\| - \|_r \le \| - \|_r'$, and hence equality.

Next, let $\bar{n}_1, \dots, \bar{n}_k$ (resp. $n_1, \dots, n_k$) be a minimal set of topological generators of $\overline{N}_1$ (resp. N_1), and let $t_1, \dots, t_l$ be a set of topological generators of T_1. Put $\boldsymbol{n}^\alpha = \prod_i (\delta_{n_i} - 1)^{\alpha_i}$ and similarly for T_1 and $\overline{N}_1$. By Proposition 3.3.3, the map $\mathcal{D}(K_1, R) \to \mathcal{D}_\kappa$ is then given by

$$\sum_{\alpha,\beta,\gamma} d_{\alpha,\beta,\gamma} \bar{\boldsymbol{n}}^\alpha \boldsymbol{t}^\beta \boldsymbol{n}^\gamma \mapsto \sum_\alpha \left(\sum_\beta d_{\alpha,\beta,\underline{0}} \prod_i (\kappa(t_i) - 1)^{\beta_i} \right) \bar{\boldsymbol{n}}^\alpha .$$

We then make a computation similar to the one in the proof of the claim above. First, it's clear that $\| - \|_r^{\mathrm{quot}} \le \| - \|_r^{\mathrm{sub}}$ since restricting $\| - \|_r$ on $\mathcal{D}(K_1, R)$ to $\mathcal{D}(\overline{N}_1, R)$ gives (the intrinsically defined) $\| - \|_r$, and the composition $\mathcal{D}(\overline{N}_1, R) \to \mathcal{D}(K_1, R) \to D_\kappa \cong \mathcal{D}(\overline{N}_1, R)$ is the identity. Second, if

$$\sum_\alpha e_\alpha \bar{\boldsymbol{n}}^\alpha = \sum_\alpha \left(\sum_\beta d_{\alpha,\beta,\underline{0}} \prod_i (\kappa(t_i) - 1)^{\beta_i} \right) \bar{\boldsymbol{n}}^\alpha ,$$

then

$$\left\| \sum_\alpha e_\alpha \bar{\boldsymbol{n}}^\alpha \right\|_r \le \sup_{\alpha,\beta} \left(|d_{\alpha,\beta,\underline{0}}| \prod_i |\kappa(t_i) - 1|^{\beta_i} r^{|\alpha|} \right) \le \sup_{\alpha,\beta} |d_{\alpha,\beta,\underline{0}}| r^{|\alpha|+|\beta|} \le \left\| \sum_{\alpha,\beta,\gamma} d_{\alpha,\beta,\gamma} \bar{\boldsymbol{n}}^\alpha \boldsymbol{t}^\beta \boldsymbol{n}^\gamma \right\|_r ,$$

where we have used the assumption $|\kappa(t_i) - 1| \le r$ for all i to obtain the second inequality. Hence, taking the infimum over such presentations, we see that $\| - \|_r^{\mathrm{sub}} \le \| - \|_r^{\mathrm{quot}}$ and equality follows.

The case $p=2$ is similar. We identify $\mathcal{D}_\kappa$ with $\mathcal{D}(\overline{N}_1, R)$ and consider the subspace $\mathcal{D}(\overline{N}_2, R)$. It carries the norm $\|-\|_r$ and also receives a quotient norm from the norm $\|-\|_r$ on $\mathcal{D}(K_2, R)$ via the surjection $\varphi : \mathcal{D}(K_2, R) \to \mathcal{D}(\overline{N}_2, R)$. These two norms are equal by the same type of argument as in the second part above. We then equip $\mathcal{D}(I, R)$ with the norm $\|-\|_{K_2,r}$ and $\mathcal{D}(\overline{N}_1, R)$ with the norm $\|-\|_r^{\mathrm{sub}}$. Pick coset representatives $(\bar{n}_i)_i$ of $\overline{N}_1/\overline{N}_2$ and $(b_j)_j$ of B_0/B_2, both containing 1. We may then write the map $\mathcal{D}(I, R) \to \mathcal{D}(\overline{N}_1, R)$ as

$$\bigoplus_{i,j} \delta_{\bar{n}_i b_j} \mathcal{D}(K_2, R) \to \bigoplus_i \delta_{\bar{n}_i} \mathcal{D}(\overline{N}_2, R), \quad (\delta_{\bar{n}_i b_j} \mu_{ij})_{i,j} \mapsto \Bigl(\delta_{\bar{n}_i} \sum_j \kappa(b_j)\varphi(\mu_{ij})\Bigr)_i.$$

By a computation similar to that in the first part of the proof in the case $p \neq 2$ (using additionally the equality of the two norms on $\mathcal{D}(\overline{N}_2, R)$ asserted above) the norm $\|-\|_r^{\mathrm{quot}}$ agrees with the norm $\|-\|_r^{\mathrm{sub}}$, as desired. □

Remark 3.3.8. It might happen that $\overline{N}_1$ is uniform when $p=2$ (e.g., when $\boldsymbol{G} = \mathrm{Res}_{\mathbb{Q}}^F \mathrm{GL}_{2/F}$). In this case, the norm $\|-\|_r^{\mathrm{sub}}$ is bounded-equivalent to $\|-\|_{r^{1/2}}$ on $\mathcal{D}(\overline{N}_1, R)$.

Definition 3.3.9. Write r_κ for the minimal $r \in [1/p, 1)$ such that $|\kappa(t)-1| \leq r$ for all $t \in T_\epsilon$. When $r \geq r_\kappa$, we write $\|-\|_r$ for the norm $\|-\|_r^{\mathrm{sub}} = \|-\|_r^{\mathrm{quot}}$ on $\mathcal{D}_\kappa$ (we will never consider these norms when $r < r_\kappa$).

Let $r \geq r_\kappa$. We define $\mathcal{D}_\kappa^r$ to be the completion of $\mathcal{D}_\kappa$ with respect to $\|-\|_r$, and let $\mathscr{D}_\kappa = \varprojlim_r \mathcal{D}_\kappa^r$.

$\mathcal{D}_\kappa^r$ is a Banach R-module with respect to its induced norm, and carries a left I-action (since I acts on $\mathcal{D}_\kappa$ by $\|-\|_r$-isometries, the action extends to the completion). When R is a Banach $\mathbb{Q}_p$-algebra, it follows from Proposition 3.2.9 that $\mathscr{D}_\kappa$ is the locally analytic distribution module used in [Ash and Stevens 2008; Hansen 2017]. We will also need to extend the action of Σ^+ to these modules, and prove that elements of Σ^{cpt} give compact operators. For this, it is convenient to use the definition of $\|-\|_r$ as $\|-\|_r^{\mathrm{sub}}$. We have a natural identification $\mathcal{D}_\kappa^r \cong \mathcal{D}^r(\overline{N}_1, R)$ when $p \neq 2$; when $p=2$ we have $\mathcal{D}_\kappa^r \cong \bigoplus_{\bar{n}_i \in \overline{N}_1/\overline{N}_2} \delta_{\bar{n}_i} \mathcal{D}^r(\overline{N}_2, R)$.

Corollary 3.3.10. *If $t \in \Sigma^+$, then the action of t on $\mathcal{D}_\kappa$ is norm-decreasing with respect to $\|-\|_r$ for any $r \geq r_\kappa$, and hence the action of t extends to $\mathcal{D}_\kappa^r$. If $t \in \Sigma^{\mathrm{cpt}}$, then t acts compactly on $\mathcal{D}_\kappa^r$. Moreover, in this case the action of t is given by the composition of a norm-decreasing map*

$$\mathcal{D}_\kappa^r \to \mathcal{D}_\kappa^{r^{1/p}}$$

with the compact (norm-decreasing) inclusion

$$\mathcal{D}_\kappa^{r^{1/p}} \hookrightarrow \mathcal{D}_\kappa^r.$$

Proof. We use the identification $\mathcal{D}_\kappa \cong \mathcal{D}(\overline{N}_1, R)$, with regards to which t acts by the map induced from the homomorphism $\overline{N}_1 \to \overline{N}_1$ given by $\bar{n} \mapsto t\bar{n}t^{-1}$. First assume $p \neq 2$. The first assertion follows directly from Lemma 3.2.4. The second assertion follows from the third, so it remains to prove the third assertion. If $t \in \Sigma^{\mathrm{cpt}}$ we have $t\overline{N}_1 t^{-1} \subseteq \overline{N}_2 = (\overline{N}_1)^p$ by the definition of Σ^{cpt} and Remark 3.3.5, so the third assertion follows from Lemmas 3.2.3 and 3.2.4.

Now assume $p=2$ and let $(\bar{n}_i)_i$ be a set of coset representatives of $\overline{N}_1/\overline{N}_2$. We have $t\overline{N}_2t^{-1} \subseteq \overline{N}_2$ and $\bar{n} \mapsto t\bar{n}t^{-1}$ induces a map $\overline{N}_1/\overline{N}_2 \to \overline{N}_1/\overline{N}_2$; moreover if $t \in \Sigma^{\mathrm{cpt}}$ then $t\overline{N}_2t^{-1} \subseteq \overline{N}_3$, by Remark 3.3.5. Writing $\mathcal{D}(\overline{N}_1, R) = \bigoplus_i \delta_{\bar{n}_i}\mathcal{D}(\overline{N}_2, R)$ we see that t acts by a sum of maps of the form $\mathcal{D}(\overline{N}_2, R) \to \mathcal{D}(\overline{N}_2, R)$ induced by $\bar{n} \mapsto t\bar{n}t^{-1}$, and the proof now proceeds as in the case when $p \neq 2$. □

Continue to assume $r \geq r_\kappa$. In the rest of this subsection, for simplicity of notation we will assume $p \neq 2$ in the discussion, but everything we do works for $p=2$ as well after minor adjustments, writing $\mathcal{D}_\kappa^r \cong \bigoplus_i \delta_{\bar{n}_i}\mathcal{D}^r(\overline{N}_2, R)$. Let $\bar{n}_1, \dots, \bar{n}_t$ be a topological basis of $\overline{N}_1$ and set $\boldsymbol{n}_i = [\bar{n}_i] - 1 \in \mathcal{D}_\kappa$ as usual. Then the description

$$\mathcal{D}^r(\overline{N}_1, R) = \widehat{\bigoplus_\alpha} R.\varpi^{-n(r,\varpi,\alpha)}\boldsymbol{n}^\alpha$$

gives us an explicit description of $\mathcal{D}_\kappa^r$ via the identification $\mathcal{D}_\kappa^r \cong \mathcal{D}^r(\overline{N}_1, R)$. In particular we remark that the $\mathcal{D}_\kappa^r$ are potentially ON-able with a countable potential ON-basis that we can actually write down. This is in contrast with the compact distribution modules considered in [Ash and Stevens 2008], which are potentially ON-able but one cannot write down an explicit basis (and the dimension is uncountable), as well as the distribution modules considered in [Hansen 2017], which are not known to be potentially ON-able in general. Our next goal is to introduce variants of the modules $\mathcal{D}_\kappa^r$, as well as modules $\mathcal{A}_\kappa^r \subseteq \mathcal{A}_\kappa$, which are analogous to those considered in [loc. cit.].

Let $r > r_\kappa$ and pick $s \in [r_\kappa, r)$. The unit ball $\mathcal{D}_\kappa^{r,\circ}$ of $\mathcal{D}_\kappa^r$ is Δ-stable since Δ acts by norm-decreasing operators. The natural map $\mathcal{D}_\kappa^r \to \mathcal{D}_\kappa^s$ is injective, and may naturally be thought of as an inclusion. Doing so, we define $\mathcal{D}_\kappa^{<r,\circ}$ to be the closure of $\mathcal{D}_\kappa^{r,\circ}$ inside $\mathcal{D}_\kappa^s$. It is a ϖ-torsion free R_0-module and we set $\mathcal{D}_\kappa^{<r} = \mathcal{D}_\kappa^{<r,\circ}[1/\varpi]$; this is an R-module which naturally embed into $\mathcal{D}_\kappa^s$. Since $\mathcal{D}_\kappa^{r,\circ} \subseteq \mathcal{D}_\kappa^s$ is Δ-stable we see that $\mathcal{D}_\kappa^{<r,\circ}$ and $\mathcal{D}_\kappa^{<r}$ are as well. We may then define

$$\mathcal{A}_\kappa^{<r,\circ} = \{f \in \mathcal{A}_\kappa \mid |\mu(f)| \leq 1 \text{ for all } \mu \in \mathcal{D}_\kappa \cap \mathcal{D}_\kappa^{r,\circ}\}$$

and $\mathcal{A}_\kappa^{<r} = \mathcal{A}_\kappa^{<r,\circ}[1/\varpi] \subseteq \mathcal{A}_\kappa$. Then $\mathcal{A}_\kappa^{<r}$ is the dual space of $\mathcal{D}_\kappa^r$. We equip it with the norm dual to $\|-\|_r$, and define $\mathcal{A}_\kappa^r \subseteq \mathcal{A}_\kappa^{<r}$ to be the closure of $\mathcal{A}_\kappa^{<s} \subseteq \mathcal{A}_\kappa^{<r}$ with respect to this norm. These spaces are Δ-stable since $\mathcal{D}_\kappa \cap \mathcal{D}_\kappa^{r,\circ}$ is. Note that we have natural identifications

$$\mathcal{D}_\kappa^{<r} \cong \mathcal{D}^{<r}(\overline{N}_1, R), \quad \mathcal{A}_\kappa^{<r} \cong \mathcal{C}^{<r}(\overline{N}_1, R), \quad \mathcal{A}_\kappa^r \cong \mathcal{C}^r(\overline{N}_1, R),$$

so the discussion in Section 3.2 applies to give explicit descriptions of these spaces, and show that they are independent of the choice of s.

4. Overconvergent cohomology and eigenvarieties

In this section we establish the basic results on overconvergent cohomology needed to construct and analyze eigenvarieties. We retain the notation from Section 3.3, but we will change our point of view slightly, from a functional-analytic point of view to a geometric one. Instead of working with Banach–Tate $\mathbb{Z}_p$-algebras, we will work with complete Tate $\mathbb{Z}_p$-algebras, which we will always assume to have a

Noetherian ring of definition. A *weight* will therefore be a continuous homomorphism $\kappa : T_0 \to R^\times$, where R is a complete Tate $\mathbb{Z}_p$-algebra with a Noetherian ring of definition. We follow the strategy of [Hansen 2017, §3–4] to construct our eigenvarieties. A similar construction was also carried out in [Xiang 2012].

4.1. ***Eigenvarieties.*** We retain the global setup from the beginning of Section 3.3. To construct our eigenvarieties, we will need some more notation as well as some concepts from [Ash and Stevens 2008; Hansen 2017]. First, let us fix a compact open subgroup $K_\ell = K_\ell \subseteq \boldsymbol{G}(\mathbb{Q}_\ell)$, for each prime $\ell \neq p$, which is hyperspecial for all but finitely many ℓ, and set $K^p = \prod_{\ell \neq p} K_\ell$ (the tame level) and $K = K^p I$. We assume that K is neat (which is the case when K^p is sufficiently small).[4] Let $\boldsymbol{Z}$ denote the centre of $\boldsymbol{G}$ and put $Z(K) = \boldsymbol{Z}(\mathbb{Q}) \cap K$. All weights in this section will be assumed to be trivial on $\overline{Z(K)} \subseteq T_0$.

We also fix a monoid $\Delta_\ell \subseteq \boldsymbol{G}(\mathbb{Q}_\ell)$ containing K_ℓ, which is equal to $\boldsymbol{G}(\mathbb{Q}_\ell)$ when K_ℓ is hyperspecial, such that (Δ_ℓ, K_ℓ) is a Hecke pair and the ℓ-Hecke algebra $\mathbb{T}(\Delta_\ell, K_\ell)$ (defined over $\mathbb{Z}_p$) is commutative. Set $\Delta^p = \prod' \Delta_\ell$ (restricted product with respect to the K_ℓ) and $\Delta = \Delta^p \Delta_p$ (recall that $\Delta_p = I \Sigma^+ I$). Next, as in [Hansen 2017, §2.1], we fix a choice $C_\bullet(K, -)$ of an *augmented Borel–Serre complex* and for any left Δ-module M we define $C^\bullet(K, M)$. Note that $C^\bullet(K, M)$ carries an action of the Hecke algebra $\mathbb{T}(\Delta, K)$. In general, if $C^\bullet$ is a cochain complex we let $C^* = \bigoplus_{i \in \mathbb{Z}} C^i$ and, similarly, we use H^* to denote the direct sum of all cohomology groups when cohomology makes sense.

Fix once and for all an element $t \in \Sigma^{\mathrm{cpt}}$. Let $\kappa : T_0 \to R^\times$ be a weight, and choose a Banach–Tate $\mathbb{Z}_p$-algebra norm on R which is adapted to κ. We let $\widetilde{U}_{\kappa,r} = \widetilde{U}_{t,\kappa,r}$ denote the corresponding Hecke operator on $C^\bullet(K, \mathcal{D}_\kappa^r)$ (here $r \geq r_\kappa$). This operator is compact and we let

$$F_\kappa^r(T) = \det(1 - T\widetilde{U}_{\kappa,r} \mid C^*(K, \mathcal{D}_\kappa^r))$$

denote its Fredholm determinant, which exists since $C^*(K, \mathcal{D}_\kappa^r)$ is potentially ON-able (by basic properties of Borel–Serre complexes). Before proceeding, let us recall the definition of weight space.

Definition 4.1.1. Suppose (A, A^+) is a complete sheafy affinoid $(\mathbb{Z}_p, \mathbb{Z}_p)$-algebra. The functor

$$(A, A^+) \mapsto \mathrm{Hom}_{\mathrm{cts}}(T_0/\overline{Z(K)}, A^\times)$$

from complete sheafy affinoid $(\mathbb{Z}_p, \mathbb{Z}_p)$-algebras (A, A^+) to sets is representable by the affinoid ring $(\mathbb{Z}_p[\![T_0/\overline{Z(K)}]\!], \mathbb{Z}_p[\![T_0/\overline{Z(K)}]\!])$, and we let $\mathfrak{W}$ denote the corresponding adic space. We remark that any continuous homomorphism $T_0/\overline{Z(K)} \to A^\times$ automatically lands in $(A^+)^\times$. To see this, note that T_0 is noncanonically isomorphic to $F \times \mathbb{Z}_p^r$ as a p-adic Lie group, where F is a finite group and $r \in \mathbb{Z}_{\geq 0}$. The image of F lands in the roots of unity $\mu_\infty(A)$ in A, and the image of $\mathbb{Z}_p^r$ lands in $1 + A^{\circ\circ}$. Since A^+ is open and integrally closed in A (which is complete), $\mu_\infty(A)$ and $1 + A^{\circ\circ}$ are both subsets of $(A^+)^\times$.

We let $\mathcal{W}$ denote the *analytic* locus of $\mathfrak{W}$; this is an open subset. For any weight $\kappa : T_0 \to R^\times$ and ring of integral elements $R^+ \subseteq R^\circ$, we obtain a map $\mathcal{U} = \mathrm{Spa}(R, R^+) \to \mathcal{W}$. If this map is an open immersion (so in particular we have $R^+ = R^\circ$, by Corollary A.6), we will conflate the weight κ and the open subset $\mathcal{U} \subseteq \mathcal{W}$ and refer to $\mathcal{U}$ as an *open* weight. In this case, we will also replace κ by $\mathcal{U}$ in our notation, writing $\mathcal{D}_\mathcal{U}$ etc.

[4] In fact it suffices to assume that K contains a neat open normal subgroup with index prime to p.

Proposition 4.1.2. *Let κ be a weight and choose an adapted Banach–Tate $\mathbb{Z}_p$-algebra norm on R. Then F_κ^r is independent of $r \geq r_\kappa$.*

Proof. Let $r_\kappa \leq r < s$; we wish to prove that $F_\kappa^r = F_\kappa^s$. Note that the general case follows from the case $s \leq r^{1/p}$, so we may assume this. Then, by Corollary 3.3.10, $\widetilde{U}_{\kappa,r}$ factors as

$$C^*(K, \mathcal{D}_\kappa^r) \xrightarrow{\Phi} C^*(K, \mathcal{D}_\kappa^s) \xrightarrow{\iota} C^*(K, \mathcal{D}_\kappa^r),$$

where ι is induced by the natural compact inclusion $\mathcal{D}_\kappa^s \hookrightarrow \mathcal{D}_\kappa^r$. We have $\widetilde{U}_{\kappa,s} = \Phi \circ \iota$, so the result follows from [Buzzard 2007, Lemma 2.7]. □

In light of this we will from now on drop r from the notation and simply write F_κ. We remark that it currently depends on a choice of norm on R.

Proposition 4.1.3. *Let $\kappa : T_0 \to R^\times$ be a weight and choose an adapted Banach–Tate $\mathbb{Z}_p$-algebra norm on R. Let ϖ be a multiplicative pseudouniformizer in R:*

(1) *Assume that F_κ has a factorization $F_\kappa = QS$, where Q is a multiplicative polynomial, S is a Fredholm series, and Q and S are relatively prime. Let $s > r \geq r_\kappa$. The inclusion $C^\bullet(K, \mathcal{D}_\kappa^s) \subseteq C^\bullet(K, \mathcal{D}_\kappa^r)$ induces an equality* $\mathrm{Ker}^\bullet\, Q^*(\widetilde{U}_{\kappa,s}) = \mathrm{Ker}^\bullet\, Q^*(\widetilde{U}_{\kappa,r})$ *(here and elsewhere we write* $\mathrm{Ker}^\bullet\, Q^*(\widetilde{U}_{\kappa,r})$ *for the complex with i-th term being the kernel of $Q^*(\widetilde{U}_{\kappa,r})$ acting on $C^i(K, \mathcal{D}_\kappa^r)$).*

(2) *Let R' be a complete Tate ring with a Noetherian ring of definition, which we assume to be equipped with a Banach–Tate $\mathbb{Z}_p$-algebra norm $|-|'$ which induces the topology. Assume that we have a bounded homomorphism $\phi : R \to R'$ such that $|-|'$ is adapted to $\kappa' = \kappa \circ \phi$ and $\phi(\varpi)$ is multiplicative for $|-|'$. Then $F_{\kappa'} = \phi(F_\kappa)$.*

If we assume moreover that F_κ has a factorization as in the previous part, we have a canonical isomorphism $(\mathrm{Ker}^\bullet\, Q^*(\widetilde{U}_{\kappa,r})) \otimes_R R' \cong \mathrm{Ker}^\bullet\, Q^*(\widetilde{U}_{\kappa',r})$.

Proof. For assertion (1), we note that the general case follows from the case $s \leq r^{1/p}$, and then writing $\widetilde{U}_{\kappa,r}$ and $\widetilde{U}_{\kappa,s}$ as in the proof of Proposition 4.1.2 the result follows from Lemma 2.2.3. For part (2), the first assertion follows from Lemma 3.2.5 and [Buzzard 2007, Lemma 2.13], and the second assertion follows from Lemma 3.2.5 upon writing $C^\bullet(K, \mathcal{D}_\kappa^r) = \mathrm{Ker}^\bullet\, Q^*(\widetilde{U}_{\kappa,r}) \oplus N^\bullet$ as in Theorem 2.2.2 since $Q^*(\widetilde{U}_{\kappa,r})$ is invertible on $N^\bullet$. □

We can now prove that F_κ is independent of the choice of norm on R.

Proposition 4.1.4. *F_κ is independent of the choice of adapted Banach–Tate $\mathbb{Z}_p$-algebra norm on R.*

Proof. Let $|-|$ and $|-|'$ be two different such norms on R and denote the constructions coming from $|-|$ as usual and the constructions coming from $|-|'$ by adding a prime. By Lemma 2.1.6, we may find constants $C_1, C_2, s_1, s_2 > 0$ such that $C_1|a|^{s_1} \leq |a|' \leq C_2|a|^{s_2}$ for all $a \in R$, which, as in the proof of Proposition 3.2.6, implies that $\mathcal{D}_\kappa^{r^{1/s_2}} \subseteq \mathcal{D}_\kappa^{r,\prime} \subseteq \mathcal{D}_\kappa^{r^{1/s_1}}$ for r suitably close to 1. Assume first that $s_2/s_1 < p$, or in other words that $r^{p/s_2} < r^{1/s_1}$. Then $\widetilde{U}_{\kappa,r^{1/s_1}}$ factors through $\mathcal{D}_\kappa^{r^{1/s_2}}$, and hence through $\mathcal{D}_\kappa^{r,\prime}$. Decreasing s_1 if necessary (still making sure that $s_2/s_1 \leq p$), the inclusion $\mathcal{D}_\kappa^{r,\prime} \subseteq \mathcal{D}_\kappa^{r^{1/s_1}}$ is compact, and we may now argue as in the proof of Proposition 4.1.2.

We now do the general case. Choose multiplicative pseudouniformizers ϖ and ϖ' for $|-|$ and $|-|'$ respectively. Put $X = \mathrm{Spa}(R, R^\circ)$ and let $U \subseteq X$ be a rational subdomain. Write $R_U := \mathcal{O}_X(U)$ and ϕ_U for the natural map $R \to R_U$. Then it is easy to see, by (the proof of) Lemma 3.3.1, that we may find a Banach–Tate norm $|-|_U$ on R_U such that $\phi_U : (R, |-|) \to (R_U, |-|_U)$ is bounded, ϖ is a multiplicative pseudouniformizer for $|-|_U$, and for all t_U sufficiently large, $|-|_U^{t_U}$ is a Banach–Tate $\mathbb{Z}_p$-algebra norm on R_U which is adapted for $\kappa_U := \phi_U \circ \kappa$. We may find a norm $|-|'_U$ with the same properties in relation to $|-|'$ etc. By Proposition 4.1.3(2) we then have $F_{\kappa_U} = \phi_U(F_\kappa)$ and $F'_\kappa = \phi_U(F'_\kappa)$, using that changing a norm by raising it to a real positive power only reindexes the $\mathcal{D}^r$, and hence does not change the Fredholm determinant by Proposition 4.1.2. We also remark that raising $|-|$ and $|-|'$ to the same power $t > 0$ does not change the quantity s_2/s_1. Thus, we aim to find an open cover $(U_i)_i$ of $\mathrm{Spa}(R, R^\circ)$ consisting of rational subdomains, such that, writing $R_i = \mathcal{O}(U_i)$ and equipping with norms of the form described above, the quantity s_1/s_2 is $< p$ for each i. This would then finish the proof.

It remains to construct the cover $(U_i)_i$. We recall from the proof of Lemma 2.1.6 that we may take

$$s_1 = \frac{\log|\varpi^m|'}{\log|\varpi^m|}, \qquad s_2 = \frac{\log|(\varpi')^m|'}{\log|(\varpi')^m|}$$

for any m sufficiently large that $|\varpi^m|', |(\varpi')^m| < 1$. Let $\delta > 0$ be small, and choose m sufficiently large that $(|\varpi^m|')^{1/m} - |\varpi|'_{\mathrm{sp}} \le \delta$ and $|(\varpi')^m|^{1/m} - |\varpi'|_{\mathrm{sp}} \le \delta$. There is a continuous real-valued function Φ on $\mathcal{M}(R)$ given by

$$x \mapsto \Phi(x) = \frac{\log|\varpi'|' \log|\varpi|}{\log|\varpi'|_x \log|\varpi|'_x} = \frac{\log|\varpi'|'_x \log|\varpi|_x}{\log|\varpi'|_x \log|\varpi|'_x}.$$

Note the similarity between s_2/s_1 and Φ. We recall here that $\mathcal{M}(R)$ is the maximal Hausdorff quotient of $\mathrm{Spa}(R, R^\circ)$, and hence it does not depend on whether we used $|-|$ or $|-|'$ to construct it (though of course the functions $x \mapsto |-|_x$ and $x \mapsto |-|'_x$ are in general different). We compose this function with the projection $\mathrm{Spa}(R, R^\circ) \to \mathcal{M}(R)$ to get a function on $\mathrm{Spa}(R, R^\circ)$. We claim that it is constant and equal to 1. To see this, fix x and note that there is an $s > 0$ such that $|-|'_x = |-|^s_x$; one then checks easily that $\Phi(x) = 1$. Fix $x \in \mathrm{Spa}(R, R^\circ)$. Let U be a rational subdomain containing x and give $\mathcal{O}(U)$ two norms $|-|$ and $|-|'$ constructed as for R_i above. If U is small, $|\varpi|'_{\mathrm{sp}} = \sup_{y \in \mathcal{M}(\mathcal{O}(U)) \subseteq \mathcal{M}(R)} |\varpi|'_y$ is close to $|\varpi|'_x$, and similarly for $|\varpi'|_{\mathrm{sp}}$. Choosing δ small, we may then ensure that the quantity s_2/s_1 is close to $\Phi(x) = 1$ for U small; in particular it is $< p$ as desired. Picking such a U for every x gives the desired cover. □

From the preceding two propositions, we can immediately deduce the following corollary.

Corollary 4.1.5. *Let $\mathcal{U}_1 \subseteq \mathcal{U}_2$ be open weights and let $\phi : \mathcal{O}_{\mathcal{W}}(\mathcal{U}_2) \to \mathcal{O}_{\mathcal{W}}(\mathcal{U}_1)$ be the induced map. Then $\phi(F_{\mathcal{U}_2}) = F_{\mathcal{U}_1}$. Therefore, the Fredholm determinants $(F_{\mathcal{U}})_{\mathcal{U}}$, where $\mathcal{U}$ ranges over all open weights, glue together to a Fredholm series $F_{\mathcal{W}} \in \mathcal{O}(\mathcal{W})\{\{T\}\} = \mathcal{O}(\mathbb{A}^1_{\mathcal{W}})$.*

We write $\widetilde{U}_\kappa$ for the Hecke operator on $C^\bullet(K, \mathscr{D}_\kappa)$ coming from our fixed $t \in \Sigma^{\mathrm{cpt}}$.

Proposition 4.1.6. *Let $\kappa : T_0 \to R^\times$ be a weight. Assume that F_κ has a factorization $F_\kappa = QS$, where Q is a multiplicative polynomial, S is a Fredholm series, and Q and S are relatively prime. Then* $\mathrm{Ker}^\bullet\, Q^*(\widetilde{U}_\kappa)$ *is a complex of projective R-modules. If $\phi : R \to R'$ is a continuous homomorphism, where R' is a complete Tate ring with a Noetherian ring of definition, then we have a canonical isomorphism* $(\mathrm{Ker}^\bullet\, Q^*(\widetilde{U}_\kappa)) \otimes_R R' \cong \mathrm{Ker}^\bullet\, Q^*(\widetilde{U}_{\kappa'})$*, where $\kappa' = \kappa \circ \phi$.*

Proof. We have $C^\bullet(K, \mathscr{D}_\kappa) = \varprojlim_{r \geq r_\kappa} C^\bullet(K, \mathcal{D}_\kappa^r)$. Since $\widetilde{U}_\kappa = \varprojlim_{r \geq r_\kappa} \widetilde{U}_{\kappa,r}$ the result follows from Proposition 4.1.3 upon noting that we may choose a topologically nilpotent unit $\varpi \in R$ and norms on R and R' such that ϕ and ϖ satisfies the assumptions of that proposition. □

Next we study what happens when the factorization of F_κ changes. Keep the notation of Proposition 4.1.6. We make $\mathrm{Ker}^\bullet\, Q^*(\widetilde{U}_\kappa)$ into a complex of $R[T]/(Q(T))$-modules by letting T act as $\widetilde{U}_\kappa^{-1}$.

Proposition 4.1.7. *Let $\kappa : T_0 \to R^\times$ be a weight. Assume that F_κ has two factorizations $F_\kappa = Q_1 S_1 = Q_2 S_2$, where the Q_i are multiplicative polynomials, the S_i are Fredholm series, and for each i the Q_i and S_i are relatively prime. Assume further that $Q_1 \mid Q_2$. Then we have a canonical isomorphism*

$$\mathrm{Ker}^\bullet\, Q_2^*(\widetilde{U}_\kappa) \otimes_{R[T]/(Q_2)} R[T]/(Q_1) \cong \mathrm{Ker}^\bullet(Q_1^*(\widetilde{U}_\kappa)).$$

Proof. Let P be such that $Q_2 = PQ_1$; P is then a multiplicative polynomial and one checks that it is relatively prime to Q_1, so we may find polynomials $A, B \in R[T]$ such that $PA + Q_1 B = 1$. We then have $R[T]/(Q_2) \cong R[T]/(Q_1) \times R[T]/(P)$ and $PA \in R[T]/(Q_2)$ corresponds to $(1, 0) \in R[T]/(Q_1) \times R[T]/(P)$. The proposition now amounts to showing that $PA.\, \mathrm{Ker}^\bullet\, Q_2^*(\widetilde{U}_\kappa) = \mathrm{Ker}^\bullet\, Q_1^*(\widetilde{U}_\kappa)$. If $x \in \mathrm{Ker}^\bullet\, Q_2^*(\widetilde{U}_\kappa)$, then

$$Q_1^*(\widetilde{U}_\kappa).PAx = \widetilde{U}_\kappa^{\deg Q_1} A Q_2 x = 0,$$

which gives us one inclusion. For the other, assume that $y \in \mathrm{Ker}^\bullet\, Q_1^*(\widetilde{U}_\kappa)$. Note that $\deg PA = \deg Q_1 B$. Then

$$y = \widetilde{U}_\kappa^{-\deg PA}\big(P^*(\widetilde{U}_\kappa)A^*(\widetilde{U}_\kappa) + B^*(\widetilde{U}_\kappa)Q_1^*(\widetilde{U}_\kappa)\big)y = P^*(\widetilde{U}_\kappa)A^*(\widetilde{U}_\kappa)\widetilde{U}_\kappa^{-\deg PA} y,$$

which gives us the other inclusion. □

We now return to the Fredholm series $F_{\mathcal{W}}$ from Corollary 4.1.5. Let $\mathscr{Z} \subseteq \mathbb{A}^1_{\mathcal{W}}$ denote its Fredholm hypersurface. Consider $\mathscr{C}ov(\mathscr{Z})$, the set of all open affinoid $V \subseteq Z$ such that $\pi(V) \subseteq X$ is open affinoid, $\mathcal{O}(\pi(V))$ is Tate, and the map $\pi|_V : V \to \pi(V)$ is finite of constant degree, where $\pi : \mathscr{Z} \to \mathcal{W}$ is the projection map. For $V \in \mathscr{C}ov(\mathscr{Z})$, let us write $F_{\mathcal{W}} = Q_V S_V$ for the associated factorization of $F_{\mathcal{W}}$ from Theorem 2.3.3.

Corollary 4.1.8. *The assignment $V \mapsto \mathrm{Ker}^\bullet\, Q_V^*(\widetilde{U}_{\pi(V)})$, with $V \in \mathscr{C}ov(\mathscr{Z})$, defines a bounded complex of coherent sheaves $\mathscr{K}^\bullet$ on $\mathscr{Z}$.*

Proof. $\mathscr{C}ov(\mathscr{Z})$ is an open cover of $\mathscr{Z}$ so we need to prove that whenever $V_1 \subseteq V_2$ are elements of $\mathscr{C}ov(\mathscr{Z})$, we have $(\mathrm{Ker}^\bullet\, Q_{V_2}^*(\widetilde{U}_{\pi(V_2)})) \otimes_{\mathcal{O}(V_2)} \mathcal{O}(V_1) \cong \mathrm{Ker}^\bullet\, Q_{V_1}^*(\widetilde{U}_{\pi(V_1)})$ canonically. Define $V_3 = \pi|_{V_2}^{-1}(\pi(V_1))$. Then we have $V_1 \subseteq V_3 \subseteq V_2$, so it suffices to treat the inclusions $V_1 \subseteq V_3$ and $V_3 \subseteq V_2$. In the first case we have $\pi(V_1)=\pi(V_3)$ and the result follows from Proposition 4.1.7, since $V_1\subseteq V_3$ forces $Q_{V_1}\mid Q_{V_3}$. For the second we have $V_3=V_2\times_{\pi(V_2)}\pi(V_1)$ and the result follows from Proposition 4.1.6. □

This allows us to finish the construction of the eigenvariety. We define $\mathscr{H}^*=H^*(\mathscr{K}^\bullet)$; this is a coherent sheaf on $\mathscr{Z}$. Since the projectors $C^\bullet(K,\mathscr{D}_{\pi(V)})\to \operatorname{Ker}^\bullet Q_V^*(\widetilde{U}_{\pi(V)})$ commute with the action of $\mathbb{T}(\Delta^p,K^p)$ (by construction, using the assertion about the projectors in Theorem 2.2.2), we get an induced action $\mathbb{T}(\Delta^p,K^p)\to \mathscr{E}nd_{\mathscr{Z}}(\mathscr{H}^*)$. Let $\mathscr{T}\subseteq \mathscr{E}nd_{\mathscr{Z}}(\mathscr{H}^*)$ denote the sub-presheaf generated over $\mathcal{O}_{\mathscr{Z}}$ by the image of $\mathbb{T}(\Delta^p,K^p)$. It is a sheaf by flatness of rational localization, hence a coherent sheaf of $\mathcal{O}_{\mathscr{Z}}$-algebras, and we define the eigenvariety $\mathscr{X}=\mathscr{X}_{\boldsymbol{G},K^p}$ to be the relative $\underline{\operatorname{Spa}}(\mathscr{T},\mathscr{T}^\circ)\to\mathscr{Z}$ (note that the sheaf of integral elements is determined by Lemma A.3). The morphism $q:\mathscr{X}\to\mathscr{Z}$ is finite by construction, and we have

$$\mathcal{O}(q^{-1}(V))=\operatorname{Im}\big(\mathbb{T}(\Delta^p,K^p)\otimes_{\mathbb{Z}_p}\mathcal{O}(V)\to \operatorname{End}_{\mathcal{O}(V)}(H^*(\operatorname{Ker}^\bullet Q_V^*))\big)$$

for all $V\in\mathscr{C}ov(\mathscr{Z})$. In particular, if $(\mathcal{U},h)$ is a slope datum for $(\mathcal{W},F_{\mathcal{W}})$, we write $\mathscr{T}_{\mathcal{U},h}=\mathcal{O}(q^{-1}(\mathscr{Z}_{\mathcal{U},h}))$ and have

$$\mathscr{T}_{\mathcal{U},h}=\operatorname{Im}\big(\mathbb{T}(\Delta^p,K^p)\otimes_{\mathbb{Z}_p}\mathcal{O}(\mathscr{Z}_{\mathcal{U},h})\to \operatorname{End}_{\mathcal{O}(\mathscr{Z}_{\mathcal{U},h})}(H^*(K,\mathscr{D}_{\mathcal{U}})_{\leq h})\big).$$

Remark 4.1.9. Our eigenvariety $\mathscr{X}$ contains the eigenvariety constructed in [Hansen 2017, §4] as the open subset $\{p\neq 0\}$. Indeed, our construction specializes to his over Banach $\mathbb{Q}_p$-algebras, with the minor difference that we use the complexes $C^\bullet(K,\mathcal{D}_{\mathcal{U}}^r)$ to construct the auxiliary Fredholm hypersurface $\mathscr{Z}$, whereas the complexes $C_\bullet(K,\mathscr{A}_{\mathcal{U}}^r)$ (in our notation) are used in [loc. cit.], giving a different auxiliary Fredholm hypersuface. However, working over the union of the two Fredholm hypersurfaces, one sees that the coherent sheaf $\mathscr{H}^*$ on $\mathbb{A}^1_{\mathcal{W}^{\mathrm{rig}}}$, with its $\mathbb{T}(\Delta^p,K^p)$-action, is equal to the sheaf $\mathscr{M}^*$ on $\mathbb{A}^1_{\mathcal{W}^{\mathrm{rig}}}$ (in the notation of [loc. cit., §4.3]), with its $\mathbb{T}(\Delta^p,K^p)$-action (here we have used $\mathcal{W}^{\mathrm{rig}}$ to denote the locus $\{p\neq 0\}\subseteq\mathcal{W}$).

Remark 4.1.10. Like the other constructions, our construction of overconvergent cohomology and eigenvarieties has numerous variations, which are sometimes useful to keep in mind. For example, one may use compactly supported cohomology, homology or Borel–Moore homology instead (see [loc. cit., §3.3]), and/or one could use the modules $\mathscr{A}_\kappa$ instead of the $\mathscr{D}_\kappa$. One can also add (or remove) Hecke operators, or work over some restricted family of weights, rather than the universal one.

4.2. ***The Tor-spectral sequence.*** We now give the analogue of the Tor spectral sequence in [Hansen 2017, Theorem 3.3.1], which is a key tool in analyzing the eigenvarieties. We phrase it in terms of slope decompositions and Banach–Tate rings, though we could have formulated it more generally for elements in $\mathscr{C}ov(\mathscr{Z})$.

Theorem 4.2.1. *Let $h\in\mathbb{Q}_{\geq 0}$ and let $\kappa:T_0\to R^\times$ be a weight. We fix an adapted Banach–Tate $\mathbb{Z}_p$-algebra norm on R, and suppose that $C^\bullet(K,\mathcal{D}_\kappa^r)$ has a slope $\leq h$-decomposition for some $r\geq r_\kappa$. Let $R\to S$ be a bounded homomorphism of Banach–Tate $\mathbb{Z}_p$-algebras with adapted norms and write κ_S for the induced* *weight $T_0 \to S^\times$. Then there is a convergent Hecke-equivariant (cohomological) second quadrant spectral sequence*

$$E_2^{ij} = \mathrm{Tor}_{-i}^R(H^j(K, \mathscr{D}_\kappa)_{\le h}, S) \Longrightarrow H^{i+j}(K, \mathscr{D}_{\kappa_S})_{\le h}.$$

Proof. We follow the proof of [Hansen 2017, Theorem 3.3.1]. Define a chain complex $\mathscr{C}_\bullet$ by $\mathscr{C}_i = C^{-i}(K, \mathscr{D}_\kappa)_{\le h}$ and the obvious differentials (i.e., we are just reindexing and viewing $C^\bullet(K, \mathscr{D}_\kappa)_{\le h}$ as a chain complex). This is a bounded chain complex of finite projective R-modules. Thus

$$\mathbf{Tor}_{i+j}^R(\mathscr{C}_\bullet, S) = H_{i+j}(\mathscr{C}_\bullet \otimes_R S),$$

where **Tor** denotes hyper-Tor. The hyper-Tor spectral sequence then gives us a homological spectral sequence

$$E_{ij}^2 = \mathrm{Tor}_i^R(H_j(\mathscr{C}_\bullet), S) \Longrightarrow H_{i+j}(\mathscr{C}_\bullet \otimes_R S)$$

which is concentrated in the fourth quadrant. Reindexing we may turn this into a cohomological spectral sequence (see [Weibel 1994, Dual definition 5.2.3])

$$E_2^{ij} = \mathrm{Tor}_{-i}^R(H_{-j}(\mathscr{C}_\bullet), S) \Longrightarrow H_{-i-j}(\mathscr{C}_\bullet \otimes_R S)$$

which is concentrated in the second quadrant. Since $H_{-j}(\mathscr{C}_\bullet) = H^j(K, \mathscr{D}_\kappa)_{\le h}$ (by definition) and $H_{-i-j}(\mathscr{C}_\bullet \otimes_R S) \cong H^{i+j}(K, \mathscr{D}_{\kappa_S})_{\le h}$ (canonically, by our previous results) this gives the desired spectral sequence. Finally, Hecke-equivariance follows from the functoriality of the hyper-Tor spectral sequence. $\square$

As an application, we prove the following analogue of [Hansen 2017, Theorem 4.3.3]. We will use it in the next section when we construct Galois representations.

Proposition 4.2.2. *Let $(\mathcal{U}, h)$ be a slope datum and let $\mathfrak{m} \subseteq \mathcal{O}_{\mathcal{W}}(\mathcal{U})$ be a maximal ideal corresponding to a weight $\kappa : T_0 \to L^\times$, where $L = \mathcal{O}_{\mathcal{W}}(\mathcal{U})/\mathfrak{m}$; this is a local field by Lemma A.12. Fix an absolute value on L with $|p| \le p^{-1}$ (i.e., an adapted Banach–Tate $\mathbb{Z}_p$-algebra norm). Let $\mathbb{T} \subseteq \mathbb{T}(\Delta, K)$ be a $\mathbb{Z}_p$-subalgebra and put*

$$\mathbb{T}_{\kappa,h} = \mathrm{Im}(\mathbb{T} \otimes_{\mathbb{Z}_p} L \to \mathrm{End}_L(H^*(K, \mathscr{D}_\kappa)_{\le h})),$$
$$\mathbb{T}_{\mathcal{U},h} = \mathrm{Im}(\mathbb{T} \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathcal{W}}(\mathcal{U}) \to \mathrm{End}_{\mathcal{O}_W(\mathcal{U})}(H^*(K, \mathscr{D}_{\mathcal{U}})_{\le h})).$$

Then there is a natural isomorphism $(\mathbb{T}_{\mathcal{U},h} \otimes_{\mathcal{O}_{\mathcal{W}}(\mathcal{U})} L)^{\mathrm{red}} \cong \mathbb{T}_{\kappa,h}^{\mathrm{red}}$.

Proof. By the Tor-spectral sequence we see that, if $T \in \mathbb{T}$ acts as 0 on $H^*(K, \mathscr{D}_{\mathcal{U}})_{\le h}$, then it acts nilpotently on $H^*(K, \mathscr{D}_\kappa)_{\le h}$. It follows that we have a surjection $\mathbb{T}_{\mathcal{U},h} \otimes_{\mathcal{O}_{\mathcal{W}}(\mathcal{U})} L \twoheadrightarrow \mathbb{T}_{\kappa,h}^{\mathrm{red}}$ of finite-dimensional commutative L-algebras. To finish the proof it suffices to show that if $\mathfrak{q}$ is a maximal ideal of $\mathbb{T}_{\mathcal{U},h} \otimes_{\mathcal{O}(\mathcal{U})} L$ then the localization $(\mathbb{T}_{\kappa,h})_{\mathfrak{q}}$ is nonzero. Let j be maximal such that $(H^j(K, \mathscr{D}_{\mathcal{U}})_{\le h})_{\mathfrak{q}} \neq 0$ and localize the entire Tor-spectral sequence with respect to $\mathfrak{q}$. Then the entry $(E_2^{0,j})_{\mathfrak{q}}$ is stable (i.e., $(E_2^{0,j})_{\mathfrak{q}} = (E_\infty^{0,j})_{\mathfrak{q}}$) and it follows that $(H^j(K, \mathscr{D}_\kappa)_{\le h})_{\mathfrak{q}} \neq 0$. Thus we must have $(\mathbb{T}_{\kappa,h})_{\mathfrak{q}} \neq 0$ as desired. $\square$

Corollary 4.2.3. *We retain the notation of Proposition 4.2.2. If we let U_t be the double coset operator $[KtK] \in \mathbb{T}(\Delta, K)$ for our fixed $t \in \Sigma^{\mathrm{cpt}}$, consider the commutative subalgebra $\mathbb{T}(\Delta^p, K^p)[U_t] \subseteq \mathbb{T}(\Delta, K)$. Then we have a natural isomorphism $(\mathscr{T}_{\mathcal{U},h} \otimes_{\mathcal{O}(\mathcal{U})} L)^{\mathrm{red}} \cong \mathbb{T}(\Delta^p, K^p)[U_t]_{\kappa,h}^{\mathrm{red}}$.*

Proof. By Proposition 4.2.2 we have a natural isomorphism

$$(\mathbb{T}(\Delta^p, K^p)[U_t]_{\mathcal{U},h} \otimes_{\mathcal{O}(\mathcal{U})} L)^{\mathrm{red}} \cong \mathbb{T}(\Delta^p, K^p)[U_t]^{\mathrm{red}}_{\kappa,h}$$

so it suffices to show that $\mathscr{T}_{\mathcal{U},h} \cong \mathbb{T}(\Delta^p, K^p)[U_t]_{\mathcal{U},h}$, which is clear from the definitions (note that $\mathrm{End}_{\mathcal{O}(\mathscr{Z}_{\mathcal{U},h})}(H^*(K, \mathscr{D}_{\mathcal{U}})_{\leq h}) \subseteq \mathrm{End}_{\mathcal{O}(\mathcal{U})}(H^*(K, \mathscr{D}_{\mathcal{U}})_{\leq h})$). □

5. Galois representations

We continue to assume that all weights are trivial on $\overline{Z(K)}$. Let $\boldsymbol{G} = \mathrm{Res}^F_{\mathbb{Q}} \mathrm{GL}_{n/F}$, with F a totally real or CM field. In this section we construct a Galois determinant (in the language of [Chenevier 2014]) valued in the global sections of the *reduced* extended eigenvariety, satisfying the expected compatibility between Hecke eigenvalues and the characteristic polynomial of Frobenius at all unramified primes. The construction is an adaptation of a construction due to the first author and David Hansen, to appear in [Hansen and Johansson ≥ 2019] (in a slightly refined form), which produces a Galois determinant over the reduced rigid eigenvariety as constructed in [Hansen 2017]. The key step is to produce the desired Galois determinant for all "points" of the extended eigenvariety. In the rigid analytic setting one can then glue these individual determinants together by an argument due to Bellaïche and Chenevier; we prove a version of this gluing technique in our setting. We will not assume that $\boldsymbol{G} = \mathrm{Res}^F_{\mathbb{Q}} \mathrm{GL}_{n/F}$ until Section 5.3.

5.1. *Filtrations.* Let $\kappa : T_0 \to L^\times$ be a weight, where L is a local field equipped with an adapted absolute value; we let ϖ be a uniformizer of L. Let $r > r_\kappa$ and choose an auxiliary $s \in (r_\kappa, r)$. In this subsection, we construct a filtration on the unit ball $\mathcal{D}^{<r,\circ}_\kappa$ of $\mathcal{D}^{<r}_\kappa$ with finite graded pieces, generalizing the filtrations constructed in [Hansen 2015]. We define

$$\mathrm{Fil}^j \mathcal{D}^{<r,\circ}_\kappa := \mathcal{D}^{<r,\circ}_\kappa \cap \varpi^j \mathcal{D}^{s,\circ}_\kappa.$$

When κ and r are clear from the context we will simply write Fil^j for $\mathrm{Fil}^j \mathcal{D}^{<r,\circ}_\kappa$ (we will always omit the choice of s). By the definitions the Fil^j are open and closed in the subspace topology on $\mathcal{D}^{<r,\circ}_\kappa$ coming from $\mathcal{D}^s_\kappa$ (we recall that $\mathcal{D}^{<r,\circ}_\kappa$ is compact with respect to this subspace topology since $\mathcal{O}_L$ is compact). Therefore the $\mathcal{D}^{<r,\circ}_\kappa / \mathrm{Fil}^j$ are finite discrete $\mathcal{O}_L$-torsion modules and we have $\mathcal{D}^{<r,\circ}_\kappa = \varprojlim_j \mathcal{D}^{<r,\circ}_\kappa / \mathrm{Fil}^j$ topologically. Note that Fil^j is Δ-stable (being the intersection of two Δ-stable subsets in $\mathcal{D}^s_\kappa$), so the $\mathcal{O}_L$-torsion modules $\mathcal{D}^{<r,\circ}_\kappa / \mathrm{Fil}^j$ inherit a Δ-action and the equality in the previous sentence is Δ-equivariant. We also record the following lemma.

Lemma 5.1.1. *We have*

$$H^i(K, \mathcal{D}^{<r,\circ}_\kappa) = \varprojlim_j H^i(K, \mathcal{D}^{<r,\circ}_\kappa / \mathrm{Fil}^j) \quad \textit{for all } i.$$

Proof. On Borel–Serre complexes we have $C^\bullet(K, \mathcal{D}^{<r,\circ}_\kappa) = \varprojlim_j C^\bullet(K, \mathcal{D}^{<r,\circ}_\kappa / \mathrm{Fil}^j)$ and these are bounded complexes of compact abelian Hausdorff groups. This category is abelian and has exact inverse limits (e.g., by [Neukirch 1999, Proposition IV.2.7]), which gives us the result. □

We remark that $C^\bullet(K, \mathcal{D}_\kappa^{<r})$ has a slope $\leq h$-decomposition for any $h \in \mathbb{Q}_{\geq 0}$ (since we are working over the field L) and $C^\bullet(K, \mathcal{D}_\kappa^{<r})_{\leq h} = C^\bullet(K, \mathcal{D}_\kappa^{r})_{\leq h}$ (since it is sandwiched between $C^\bullet(K, \mathcal{D}_\kappa^{r})_{\leq h}$ and $C^\bullet(K, \mathcal{D}_\kappa^{s})_{\leq h}$, and these are equal). Thus, we may use the $\mathcal{D}_\kappa^{<r}$ instead of the $\mathcal{D}_\kappa^{r}$ to define overconvergent cohomology. We will do this to define Galois representations because of the fact that $\mathcal{D}_\kappa^{<r,\circ}$ is profinite with respect to topology coming from the Fil^j.

5.2. ***A morphism of Hecke algebras.*** We continue with the notation of the previous subsection. In this subsection we will fix a $\mathbb{Z}_p$-subalgebra $\mathbb{T} \subseteq \mathbb{T}(\Delta, K)$ and, if A is any $\mathbb{Z}_p$-algebra, we will write $\mathbb{T}_A$ for $\mathbb{T} \otimes_{\mathbb{Z}_p} A$. Then $\mathbb{T}_{\mathcal{O}_L}$ acts on $H^*(K, \mathcal{D}_\kappa^{<r,\circ}/\mathrm{Fil}^j)$ for all r and j and we set

$$\mathbb{T}_{\kappa,j}^r = \mathrm{Im}\big(\mathbb{T}_{\mathcal{O}_L} \to \mathrm{End}_{\mathcal{O}_L}(H^*(K, \mathcal{D}_\kappa^{<r,\circ}/\mathrm{Fil}^j))\big),$$
$$\mathbb{T}_{\kappa,\mathrm{Fil}}^r = \mathrm{Im}\Big(\mathbb{T}_{\mathcal{O}_L} \to \prod_j \mathbb{T}_{\kappa,j}^r\Big).$$

We equip each $\mathbb{T}_{\kappa,j}^r$ with the discrete topology (they are finite rings) and give $\prod_j \mathbb{T}_{\kappa,j}^r$ the product topology; we then give $\mathbb{T}_{\kappa,\mathrm{Fil}}^r$ the subspace topology. We let $\widehat{\mathbb{T}}_{\kappa,\mathrm{Fil}}^r$ denote the completion of $\mathbb{T}_{\kappa,\mathrm{Fil}}^r$ in $\prod_j \mathbb{T}_{\kappa,j}^r$; this is a compact Hausdorff ring.

Fix $h \in \mathbb{Q}_{\geq 0}$. We have natural maps $H^*(K, \mathcal{D}_\kappa^{<r,\circ}) \to H^*(K, \mathcal{D}_\kappa^{<r}) \to H^*(K, \mathcal{D}_\kappa^{<r})_{\leq h}$ and we define $H^*(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}$ to be the image of the composition.

Lemma 5.2.1. *$H^*(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}$ is an open and bounded $\mathcal{O}_L$-submodule of $H^*(K, \mathcal{D}_\kappa^{<r})_{\leq h}$ (and hence a finite free $\mathcal{O}_L$-module).*

Proof. It is an $\mathcal{O}_L$-submodule which spans $H^*(K, \mathcal{D}_\kappa^{<r})_{\leq h}$ essentially by construction, so it suffices to show that it is finitely generated. The morphisms $H^*(K, \mathcal{D}_\kappa^{<r,\circ}) \to H^*(K, \mathcal{D}_\kappa^{<r}) \to H^*(K, \mathcal{D}_\kappa^{<r})_{\leq h}$ are induced by the morphisms

$$C^\bullet(K, \mathcal{D}_\kappa^{<r,\circ}) \to C^\bullet(K, \mathcal{D}_\kappa^{<r}) \to C^\bullet(K, \mathcal{D}_\kappa^{<r})_{\leq h}$$

of complexes. Let $C^\bullet(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}$ denote the image of the composition. Note that each $C^i(K, \mathcal{D}_\kappa^{<r,\circ})$ is bounded in $C^i(K, \mathcal{D}_\kappa^{<r})$, so $C^i(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}$ is bounded in $C^i(K, \mathcal{D}_\kappa^{<r})_{\leq h}$ by continuity of the projection. Thus $C^\bullet(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}$ is a bounded complex of finite free $\mathcal{O}_L$-modules. Since $H^*(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h} \subseteq \mathrm{Im}(H^*(C^\bullet(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}) \to H^*(K, \mathcal{D}_\kappa^{<r})_{\leq h})$, finite generation of the former follows. ☐

We define

$$\mathbb{T}_{\kappa,\leq h}^{r,\circ} = \mathrm{Im}(\mathbb{T}_{\mathcal{O}_L} \to \mathrm{End}_{\mathcal{O}_L}(H^*(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}));$$

by the above lemma this is a finite $\mathcal{O}_L$-algebra and hence naturally a compact Hausdorff ring. Note that if $T \in \mathbb{T}_{\mathcal{O}_L}$ is 0 in $\mathbb{T}_{\kappa,\mathrm{Fil}}^r$, i.e., acts as 0 on all $H^*(K, \mathcal{D}_\kappa^{<r,\circ}/\mathrm{Fil}^j)$, then it acts as 0 on $H^*(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}$ and so is 0 in $\mathbb{T}_{\kappa,\leq h}^{r,\circ}$. In other words we have a natural (surjective) map $\mathbb{T}_{\kappa,\mathrm{Fil}}^r \to \mathbb{T}_{\kappa,\leq h}^{r,\circ}$. The goal of this section is to show that this map is continuous and so extends to the completion $\widehat{\mathbb{T}}_{\kappa,\mathrm{Fil}}^r$.

To do this we introduce some special open sets. Let $\mathrm{pr}_j : \mathbb{T}_{\kappa,\mathrm{Fil}}^r \to \mathbb{T}_{\kappa,j}^r$ denote the projection. We put $U_j = \mathrm{Ker}(\mathrm{pr}_j)$; this is an open ideal of $\mathbb{T}_{\kappa,\mathrm{Fil}}^r$. On $\mathbb{T}_{\kappa,\leq h}^{r,\circ}$ the opens that we will use are more delicate to construct. We have a commutative diagram

$$\begin{array}{ccc} H^*(K, \mathcal{D}_\kappa^{<r,\circ}) & \longrightarrow & H^*(K, \mathcal{D}_\kappa^{<r})_{\leq h} \\ \downarrow & & \downarrow \\ H^*(K, \mathcal{D}_\kappa^{s,\circ}) & \longrightarrow & H^*(K, \mathcal{D}_\kappa^{s})_{\leq h} \end{array}$$

where the right vertical map is an isomorphism, which we think of as an equality (the reader may trace through the definitions and see that this is a natural thing to do). Defining $H^*(K, \mathcal{D}_\kappa^{s,\circ})_{\leq h}$ to be the image of $H^*(K, \mathcal{D}_\kappa^{s,\circ}) \to H^*(K, \mathcal{D}_\kappa^{s})_{\leq h}$ we see that $H^*(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h} \subseteq H^*(K, \mathcal{D}_\kappa^{s,\circ})_{\leq h}$ are both open lattices in $H^*(K, \mathcal{D}_\kappa^{<r})_{\leq h} = H^*(K, \mathcal{D}_\kappa^{s})_{\leq h}$ (Lemma 5.2.1 holds for $H^*(K, \mathcal{D}_\kappa^{s,\circ})_{\leq h}$ as well, with the same proof).

Lemma 5.2.2. *The ideals*

$$V_j = \{T \in \mathbb{T}_{\kappa,\leq h}^{r,\circ} \mid T(H^*(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}) \subseteq \varpi^j H^*(K, \mathcal{D}_\kappa^{s,\circ})_{\leq h}\}$$

form a basis of open neighbourhoods of 0 *in* $\mathbb{T}_{\kappa,\leq h}^{r,\circ}$.

Proof. It's easy to check that the V_j are ideals. By the preceding remarks the subgroups $\varpi^j H^*(K, \mathcal{D}_\kappa^{s,\circ})_{\leq h}$ form a basis of neighborhoods of 0 in $H^*(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}$ (for $j \gg 0$). Using this the lemma is elementary. □

We may now prove continuity. Denote the map $\mathbb{T}_{\kappa,\mathrm{Fil}}^{r} \to \mathbb{T}_{\kappa,\leq h}^{r,\circ}$ by ϕ.

Proposition 5.2.3. *We have* $\phi(U_j) \subseteq V_j$. *Thus* ϕ *is continuous and extends to a continuous map* $\widehat{\mathbb{T}}_{\kappa,\mathrm{Fil}}^{r} \to \mathbb{T}_{\kappa,\leq h}^{r,\circ}$.

Proof. The second statement follows directly from the first (by general properties of linearly topologized groups and the fact that $\mathbb{T}_{\kappa,\leq h}^{r,\circ}$ is complete). The first statement amounts, by the definitions, to proving that if T acts as 0 on $H^*(K, \mathcal{D}_\kappa^{<r,\circ}/\,\mathrm{Fil}^j)$, then it maps $H^*(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h}$ into $\varpi^j H^*(K, \mathcal{D}_\kappa^{s,\circ})_{\leq h}$, or in other words that T acts as 0 on

$$\mathrm{Im}(H^*(K, \mathcal{D}_\kappa^{<r,\circ})_{\leq h} \to H^*(K, \mathcal{D}_\kappa^{s,\circ})_{\leq h}/\varpi^j).$$

By definition this image is equal to

$$\mathrm{Im}(H^*(K, \mathcal{D}_\kappa^{<r,\circ}) \to H^*(K, \mathcal{D}_\kappa^{s,\circ})_{\leq h}/\varpi^j).$$

Assume now that T acts as 0 on $H^*(K, \mathcal{D}_\kappa^{<r,\circ}/\,\mathrm{Fil}^j)$. We may factor $H^*(K, \mathcal{D}_\kappa^{<r,\circ}) \to H^*(K, \mathcal{D}_\kappa^{s,\circ})_{\leq h}/\varpi^j$ through $H^*(K, \mathcal{D}_\kappa^{s,\circ})/\varpi^j$ so it suffices to prove that T acts as 0 on

$$\mathrm{Im}(H^*(K, \mathcal{D}_\kappa^{<r,\circ}) \to H^*(K, \mathcal{D}_\kappa^{s,\circ})/\varpi^j).$$

From the long exact sequence attached to the short exact sequence

$$0 \to \mathcal{D}_\kappa^{s,\circ} \xrightarrow{\varpi^j} \mathcal{D}_\kappa^{s,\circ} \to \mathcal{D}_\kappa^{s,\circ}/\varpi^j \to 0$$

we see that

$$H^*(K, \mathcal{D}_\kappa^{s,\circ})/\varpi^j \hookrightarrow H^*(K, \mathcal{D}_\kappa^{s,\circ}/\varpi^j).$$

By definition, we have a natural map $\mathcal{D}_\kappa^{<r,\circ}/\operatorname{Fil}^j \to \mathcal{D}_\kappa^{s,\circ}/\varpi^j$. Assembling the last few sentences, we have a commutative diagram

$$\begin{array}{ccc} H^*(K,\mathcal{D}_\kappa^{<r,\circ}) & \longrightarrow & H^*(K,\mathcal{D}_\kappa^{s,\circ})/\varpi^j \\ \downarrow & & \downarrow \\ H^*(K,\mathcal{D}_\kappa^{<r,\circ}/\operatorname{Fil}^j) & \longrightarrow & H^*(K,\mathcal{D}_\kappa^{s,\circ}/\varpi^j) \end{array}$$

where the right vertical map is injective. By assumption T acts as 0 on $H^*(K,\mathcal{D}_\kappa^{<r,\circ}/\operatorname{Fil}^j)$; hence it acts as 0 on $\operatorname{Im}(H^*(K,\mathcal{D}_\kappa^{<r,\circ}) \to H^*(K,\mathcal{D}_\kappa^{s,\circ}/\varpi^j))$. But, since the right vertical map is injective, this image is isomorphic to $\operatorname{Im}(H^*(K,\mathcal{D}_\kappa^{<r,\circ}) \to H^*(K,\mathcal{D}_\kappa^{s,\circ})/\varpi^j)$. Thus T acts as 0 on this, which is what we wanted to prove. □

5.3. *Galois representations.* We now specialize to the case $G = \operatorname{Res}^F_{\mathbb{Q}} \operatorname{GL}_{n/F}$, where F is a totally real or CM number field, and $n \geq 2$. When discussing Galois representations we will, for simplicity of referencing, use the same conventions as in [Scholze 2015, §5]. Let S' denote the set of places w of $\mathbb{Q}$ such that either $w = \infty$, or if w is finite then K_w is *not* hyperspecial. This is a finite set containing p and the primes which ramify in F. We let S denote the set of places in F lying above those in S'. We set

$$\mathbb{T} = \bigotimes_{v \notin S} \mathbb{T}_v,$$

where $\mathbb{T}_v = \mathbb{Z}_p[\operatorname{GL}_n(F_v)//\operatorname{GL}_n(\mathcal{O}_{F_v})]$ is the usual spherical Hecke algebra (we assume that $K \subseteq \operatorname{GL}_n(\mathcal{O}_F \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})$). We have $\mathbb{T} \subseteq \mathbb{T}(\Delta, K)$ and we will use the notation and results of the previous subsection for this choice of $\mathbb{T}$. Let q_v be the size of the residue field at v. We have the (unnormalized) Satake isomorphism

$$\mathbb{T}_v[q_v^{1/2}] \cong \mathbb{Z}_p[q_v^{1/2}][x_1^{\pm 1}, \dots, x_n^{\pm 1}]^{S_n},$$

where S_n is the symmetric group on $\{1, \dots, n\}$ permuting the variables $x_1, \dots, x_n$. If we let $T_{i,v}$ denote the i-th elementary symmetric polynomial in $x_1, \dots, x_n$, then $q_v^{i(n+1)/2} T_{i,v} \in \mathbb{T}_v$ and we define

$$P_v(X) = 1 - q_v^{(n+1)/2} T_{1,v} X + q_v^{n+1} T_{2,v} X^2 - \cdots + (-1)^n q_v^{n(n+1)/2} T_{n,v} X^n \in \mathbb{T}_v[X]. \tag{5.3.1}$$

The following theorem is essentially a special case of [Scholze 2015, Theorem 5.4.1]. We let $G_{F,S}$ denote the Galois group of the maximal algebraic extension of F unramified outside S. For the notion of a determinant we refer to [Chenevier 2014].

Theorem 5.3.1. (*Scholze*) *There exists an integer M depending only on $[F:\mathbb{Q}]$ and n such that the following is true*: *for any j and r there exists an ideal $I^r_{\kappa,j} \subseteq \mathbb{T}^r_{\kappa,j}$ with $(I^r_{\kappa,j})^M = 0$ and an n-dimensional continuous determinant D of $G_{F,S}$ with values in $\mathbb{T}^r_{\kappa,j}/I^r_{\kappa,j}$ such that*

$$D(1 - X \operatorname{Frob}_v) = P_v(X)$$

for all $v \notin S$.

We remark that the local systems corresponding to the $\mathcal{D}_\kappa^{<r,\circ}/\operatorname{Fil}^j$ are not necessarily included in the formulation of [Scholze 2015, Theorem 5.4.1], but the proof works the same: one first applies the Hochschild–Serre spectral sequence to reduce to the case of a trivial local system.

Corollary 5.3.2. *Keep the notation of Theorem 5.3.1:*

(1) *There exists a closed ideal $I \subseteq \widehat{\mathbb{T}}^r_{\kappa,\mathrm{Fil}}$ such that $I^M = 0$ and an n-dimensional continuous determinant D of $G_{F,S}$ with values in $\widehat{\mathbb{T}}^r_{\kappa,\mathrm{Fil}}/I$ such that $D(1 - X\operatorname{Frob}_v) = P_v(X)$ for all $v \notin S$.*

(2) *Let $h \in \mathbb{Q}_{\geq 0}$. Then there exists a closed ideal $J \subseteq \mathbb{T}^{r,\circ}_{\kappa,\leq h}$ such that $J^M = 0$ and an n-dimensional continuous determinant D of $G_{F,S}$ with values in $\mathbb{T}^{r,\circ}_{\kappa,\leq h}/J$ such that $D(1 - X\operatorname{Frob}_v) = P_v(X)$ for all $v \notin S$.*

Proof. Part (1) follows from the theorem and the definition and compactness of $\widehat{\mathbb{T}}^r_{\kappa,\mathrm{Fil}}$ via [Chenevier 2014, Example 2.32]; one sets $I = \widehat{\mathbb{T}}^r_{\kappa,\mathrm{Fil}} \cap \prod_j I^r_{\kappa,j}$. Assertion (2) then follows from (1) and Proposition 5.2.3. □

5.4. ***Gluing over the reduced eigenvariety.*** We now finish our construction of a Galois determinant over the reduced eigenvariety $\mathscr{X}^{\mathrm{red}} = \mathscr{X}^{\mathrm{red}}_{\boldsymbol{G}}$. See Definition A.10 for the definition of the reduced subspace. Keep the notation of the previous subsection. Let $(\mathcal{U}, h)$ be a slope datum. We have a corresponding open affinoid $\mathscr{X}_{\mathcal{U},h} \subseteq \mathscr{X}$. If $\mathfrak{m}_\kappa$ is a maximal ideal of $\mathcal{O}(\mathcal{U})$ corresponding to the weight $\kappa : T_0 \to L^\times$ with $L = \mathcal{O}(\mathcal{U})/\mathfrak{m}_\kappa$ a local field, then Corollary 4.2.3 gives us a natural identification

$$(\mathcal{O}(\mathscr{X}_{\mathcal{U},h})/\mathfrak{m}_\kappa)^{\mathrm{red}} = (\mathcal{O}(\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h})/\mathfrak{m}_\kappa)^{\mathrm{red}} \cong \mathbb{T}(\Delta^p, K^p)[U_t]^{\mathrm{red}}_{\kappa,h}.$$

Fix r. Note that $\mathbb{T}^r_{\kappa,\leq h} = \mathbb{T}^{r,\circ}_{\kappa,\leq h}[1/\varpi]$ is naturally a closed L-subalgebra of $\mathbb{T}(\Delta^p, K^p)[U_t]_{\kappa,h}$. From Corollary 5.3.2 it follows that we have a Galois determinant into $\mathbb{T}(\Delta^p, K^p)[U_t]^{\mathrm{red}}_{\kappa,h}$ and therefore into $(\mathcal{O}(\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h})/\mathfrak{m}_\kappa)^{\mathrm{red}}$. We record this discussion in the following convenient form:

Lemma 5.4.1. *Let $(\mathcal{U}, h)$ be a slope datum and let $\mathfrak{m}$ be a maximal ideal of $\mathcal{O}(\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h})$. Then there exists an n-dimensional continuous determinant D of $G_{F,S}$ with values in $\mathcal{O}(\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h})/\mathfrak{m}$ such that $D(1 - X\operatorname{Frob}_v) = P_v(X)$ for all $v \notin S$.*

Proof. This follows from the discussion above since the map $\operatorname{Spec}\mathcal{O}(\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h}) \to \operatorname{Spec}\mathcal{O}(\mathcal{U})$ sends maximal ideals to maximal ideals (the map is finite). □

Before we can glue we need some preparations. Let A be a reduced $\mathbb{Z}_p$-algebra which is finite and free as a $\mathbb{Z}_p$-module; we equip it with the p-adic topology. Consider the adic space $Z^{\mathrm{an}} = \mathbb{A}^1_{S^{\mathrm{an}}}$, where $S = \operatorname{Spa}(A[\![X_1, \dots, X_d]\!], A[\![X_1, \dots, X_d]\!])$; here $A[\![X_1, \dots, X_d]\!]$ carries the $(p, X_1, \dots, X_d)$-adic topology. Fix an index $i \in \{1, \dots, d\}$. Let T be a coordinate on $\mathbb{A}^1_{S^{\mathrm{an}}}$. We are interested in the open affinoid subsets $V_m = \{|p^m|, |X_1^m|, \dots, |X_d^m| \leq |X_i| \neq 0,\ |X_i^m T| \leq 1\}$ of Z^{an} for $m \in \mathbb{Z}_{\geq 1}$. Note that the union of the V_m is the locus $V = \{|X_i| \neq 0\} \subseteq Z^{\mathrm{an}}$. The ring $\mathcal{O}(V_m)$ has a ring of definition

$$R_m = A[\![X_1, \dots, X_d]\!]\left\langle \frac{p^m}{X_i}, \frac{X_1^m}{X_i}, \dots, \frac{X_d^m}{X_i} \right\rangle \langle X_i^m T \rangle$$

(with the X_i-adic topology), and we have natural maps $R_{m+1} \to R_m$ for all m. Note that $\mathcal{O}(V_m) = R_m[1/X_i]$ and that $\mathcal{O}^+(V_m)$ is the integral closure of R_m in $\mathcal{O}(V_m)$. By Theorem A.5 (and its proof), in fact we have $\mathcal{O}^+(V_m) = \mathcal{O}(V_m)^\circ$ and $\mathcal{O}(V_m)^\circ$ is a finite R_m-algebra.

Lemma 5.4.2. *The image of R_{m+1} in R_m/X_i^n is finite for all m and n. More generally, if M is a finitely generated R_{m+1}-module, then the image of M in $M \otimes_{R_{m+1}} R_m/X_i^n$ is finite.*

Proof. Fix m and n. We start with the first assertion. It suffices to check that the kernel contains the ideal

$$I = \left(p^{mn}, X_1^{mn}, \ldots, X_d^{mn}, \left(\frac{p^{m+1}}{X_i}\right)^{mn}, \left(\frac{X_1^{m+1}}{X_i}\right)^{mn}, \ldots, \left(\frac{X_d^{m+1}}{X_i}\right)^{mn}, (X_i^{m+1}T)^n\right)$$

since it's straightforward to check that R_{m+1}/I is finite. It's also straightforward to check that the given generators of I are in the kernel. This finishes the (sketch of) proof of the first assertion. For the second, there is an integer $q \geq 0$ and a surjection $R_{m+1}^q \twoheadrightarrow M$ of R_{m+1}-modules, which gives us a commuting diagram

$$\begin{array}{ccc} R_{m+1}^q & \longrightarrow & R_m^q/X_i^n \\ \downarrow & & \downarrow \\ M & \longrightarrow & M \otimes_{R_{m+1}} R_m/X_i^n \end{array}$$

where the vertical maps are surjections, and the second assertion then follows from the first. □

Proposition 5.4.3. *With notation as above, let $Y \to V = \{|X_i| \neq 0\} \subset Z^{\mathrm{an}}$ be a finite morphism of adic spaces, and assume that Y is reduced. Then $\mathcal{O}^+(Y)$ is compact.*

Proof. Write Y_m for the pullback of V_m; these form an increasing cover of Y consisting of open affinoids. Since $Y_m \to V_m$ is finite and $\mathcal{O}^+(V_m) = \mathcal{O}(V_m)^\circ$ we know that $\mathcal{O}^+(Y_m)$ is integral over $\mathcal{O}(V_m)^\circ$ (by definition of a finite morphism). Since $\mathcal{O}(Y_m)$ is reduced and $\mathcal{O}(V_m)^\circ$ is Nagata (it is finite over R_m, which is Nagata by the proof of Theorem A.5) it follows that $\mathcal{O}^+(Y_m)$ is finite over $\mathcal{O}(V_m)^\circ$. In particular, $\mathcal{O}^+(Y_m)$ is finite over R_m, and hence Noetherian. We may also deduce from Lemma A.2 that $\mathcal{O}^+(Y_m) = \mathcal{O}(Y_m)^\circ$.

For any n the map $\mathcal{O}^+(Y_{m+1}) \to \mathcal{O}^+(Y_m)/X_i^n$ factors through $\mathcal{O}^+(Y_{m+1}) \otimes_{R_{m+1}} R_m/X_i^n$ and hence the image is finite by Lemma 5.4.2. It follows that $\mathcal{O}^+(Y_{m+1})$, when equipped with the weak topology with respect to the map $\mathcal{O}^+(Y_{m+1}) \to \mathcal{O}^+(Y_m)$, is compact. We deduce that $\mathcal{O}^+(Y) = \varprojlim_m \mathcal{O}^+(Y_m)$ is compact, as desired. □

Corollary 5.4.4. *Assume that $X \to Z^{\mathrm{an}}$ is a finite morphism of adic spaces, with X reduced. Then $\mathcal{O}^+(X)$ is compact.*

Proof. For each $i \in \{1, \ldots, d\}$ consider the locus $Z_i = \{|X_i| \neq 0\} \subseteq Z^{\mathrm{an}}$ (i.e., what was previously denoted by V) and set $Z_0 = \{|p| \neq 0\}$. Let X_i, for $i \in \{0, \ldots, d\}$, denote the corresponding pullbacks to X. Then we have a strict inclusion $\mathcal{O}^+(X) \subseteq \prod_{i=0}^d \mathcal{O}^+(X_i)$ with closed image and the $\mathcal{O}^+(X_i)$ are compact (for $i = 1, \ldots, d$ this is Proposition 5.4.3 and for $i = 0$ this is [Bellaïche and Chenevier 2009, Lemma 7.2.11]; note that X_0 is nested in the terminology of that paper), so $\mathcal{O}^+(X)$ is compact as well. □

We may then prove the main result of this section.

Theorem 5.4.5. *There is an n-dimensional continuous determinant D of $G_{F,S}$ with values in $\mathcal{O}^+(\mathscr{X}^{\mathrm{red}})$ such that*

$$D(1 - X\,\mathrm{Frob}_v) = P_v(X)$$

for all $v \notin S$.

Proof. Fix a collection $\{(\mathcal{U}, h)\}$ of slope data such that the $\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h}$ cover $\mathscr{X}^{\mathrm{red}}$. We then have injections

$$\mathcal{O}^+(\mathscr{X}^{\mathrm{red}}) \hookrightarrow \prod_{(\mathcal{U},h)} \mathcal{O}(\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h}) \hookrightarrow \prod_{(\mathcal{U},h)} \prod_{\mathfrak{m}} \mathcal{O}(\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h})/\mathfrak{m},$$

where the $\mathfrak{m}$ range over all maximal ideals of $\mathcal{O}(\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h})$. Note that we have an injection $\mathcal{O}(\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h}) \hookrightarrow \prod_{\mathfrak{m}} \mathcal{O}(\mathscr{X}^{\mathrm{red}}_{\mathcal{U},h})/\mathfrak{m}$ by Lemma A.1, so the second morphism really is an injection. Then note that $\mathcal{O}^+(\mathscr{X}^{\mathrm{red}})$ is compact; since $\mathscr{X}^{\mathrm{red}}$ is finite over $\mathrm{Spa}(\mathbb{Z}_p[\![T_0]\!], \mathbb{Z}_p[\![T_0]\!])^{\mathrm{an}} \times \mathbb{A}^1$ this follows from Corollary 5.4.4. To see that $\mathbb{Z}_p[\![T_0]\!]$ is of the form $A[\![X_1, \dots, X_d]\!]$, we write $T_0 \cong T_0^{\mathrm{tor}} \times T_0^{\mathrm{free}}$, where T_0^{tor} is the torsion subgroup of T_0 (which is finitely generated) and $T_0^{\mathrm{free}} \cong \mathbb{Z}_p^{\dim T_0}$ is a free complement (see, e.g., [Neukirch 1999, Proposition II.5.7]). Set $A = \mathbb{Z}_p[T_0^{\mathrm{tor}}]$; then

$$\mathbb{Z}_p[\![T_0]\!] \cong A \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![T_0^{\mathrm{free}}]\!] \cong A[\![X_1, \dots, X_d]\!].$$

Thus we may glue the determinants from Lemma 5.4.1 into the desired determinant using [Chenevier 2014, Example 2.32]. □

6. The Coleman–Mazur eigencurve

In this section we give a short discussion of the special case of the Coleman–Mazur eigencurve and the relationship between our work and that of Andreatta, Iovita and Pilloni [Andreatta et al. 2018] and Liu, Wan and Xiao [Liu et al. 2017].

6.1. ***The case $G = \mathrm{GL}_{2/\mathbb{Q}}$.*** Let us consider the special case $G = \mathrm{GL}_{2/\mathbb{Q}}$. We begin by fixing choices of groups and Hecke algebras/operators. Let B be the upper triangular Borel, I the corresponding Iwahori and T the diagonal torus. We use the element $t = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \in \Sigma^{\mathrm{cpt}}$; the corresponding Hecke operator is the U_p-operator. We choose the tame level

$$K_1(N) = \left\{ g \in \mathrm{GL}_2(\widehat{\mathbb{Z}}^p) \;\middle|\; g \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \bmod N \right\},$$

with $N \in \mathbb{Z}_{\geq 5}$ prime to p. Put

$$\Delta_\ell = \begin{cases} \mathrm{GL}_2(\mathbb{Q}_\ell) & \text{if } \ell \nmid N, \\ \mathrm{GL}_2(\mathbb{Z}_\ell) & \text{if } \ell \mid N. \end{cases}$$

With these choices, everything else is determined and we use the notation of the main part of the paper.

In this case, overconvergent modular symbols were first constructed in [Stevens 1994], and the corresponding eigencurve was constructed and shown to agree with the Coleman–Mazur eigencurve in [Bellaïche 2010]. Stevens and Bellaïche worked with the compactly supported cohomology H^1_c, which admits a very explicit description in this case (it is given by the functor denoted by Symb in [Bellaïche 2010; Stevens 1994]). Ordinary cohomology was first considered in [Hansen 2017]. For ordinary cohomology, one has

$$H^*(K, \mathscr{D}_\kappa) = H^1(K, \mathscr{D}_\kappa)$$

for all weights κ, upon noting that the H^i vanish automatically for all $i \geq 2$ and that H^0 vanishes by (a simpler version of) the argument in the proof of [Chojecki et al. 2017, Lemma 5.4]. A consequence is the following lemma:

Lemma 6.1.1. *Let $\kappa : T_0 \to R^\times$ be a weight, and assume that F_κ has a slope $\leq h$-factorization for some $h \in \mathbb{Q}_{\geq 0}$ (slopes with respect to some multiplicative pseudouniformizer $\varpi \in R$). Then $H^1(K, \mathscr{D}_\kappa)_{\leq h}$ is a finite projective R-module and is compatible with arbitrary base change.*

Proof. Let $f : R \to S$ be a continuous homomorphism of complete Tate rings and equip S with a Banach–Tate $\mathbb{Z}_p$-algebra norm such that $f(\varpi)$ is a multiplicative pseudouniformizer. Put $\kappa_S = f \circ \kappa$. By the vanishing of the H^i for $i \neq 1$ the Tor-spectral sequence collapses and gives us that

$$H^1(K, \mathscr{D}_\kappa)_{\leq h} \otimes_R S = H^1(K, \mathscr{D}_{\kappa_S})_{\leq h},$$
$$\mathrm{Tor}_1^R(H^1(K, \mathscr{D}_\kappa)_{\leq h}, S) = 0.$$

The first line is compatibility with base change. Putting $S = R/J$ for an arbitrary ideal $J \subseteq R$ (automatically closed) we see from the second line that $H^1(K, \mathscr{D}_\kappa)_{\leq h}$ is a finite flat R-module, and hence is finite projective. □

If $\kappa : T_0 \to R^\times$ is a weight, we write κ_i, $i = 1, 2$, for the characters $\mathbb{Z}_p^\times \to R^\times$ defined by

$$\kappa\left(\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\right) = \kappa_1(a)\kappa_2(d)$$

and we identify $\overline{N}_1$ with $p\mathbb{Z}_p$ via $\left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) \mapsto x$. If we consider the eigenvariety $\mathscr{X}^{\mathrm{rig}} = \mathscr{X}_{\boldsymbol{G}}^{\mathrm{rig}}$ constructed in [Hansen 2017], then it is equidimensional of dimension 2 by Proposition B.1 of that paper since $H^* = H^1$. This object is usually referred to as the "eigensurface". If we instead do the eigenvariety construction over the part $\mathcal{W}_0^{\mathrm{rig}}$ of weight space where $\kappa_2 = 1$, we obtain an eigenvariety that turns out to equal the Coleman–Mazur eigencurve; it is in particular reduced, equidimensional of dimension 1, and flat over $\mathcal{W}_0^{\mathrm{rig}}$. Let us denote this eigenvariety by $\mathscr{E}^{\mathrm{rig}}$; the properties of $\mathscr{E}^{\mathrm{rig}}$ stated in the previous sentence are presumably well known to experts but we will give a brief sketch of the proofs below. To begin with, it is equidimensional of dimension 1 (by the same argument as above for $\mathscr{X}^{\mathrm{rig}}$). For weights with $\kappa_2 = 1$ we conflate κ and κ_1, and we may write the action on $\mathscr{A}_\kappa$ explicitly as

$$(f.\gamma)(x) = \kappa(a + bx) f\left(\frac{c + dx}{a + bx}\right)$$

for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}_p)$ such that $a \in \mathbb{Z}_p^\times$, $c \in p\mathbb{Z}_p$ (this defines the submonoid $\Delta_{p,0}$ of Δ_p generated by I and t), and $x \in p\mathbb{Z}_p$ [Hansen 2017, §2.2]. Using the anti-involution

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & c/p \\ pb & d \end{pmatrix}$$

on $\Delta_{p,0}$ and rescaling f by p^{-1} in the argument to a function on $\mathbb{Z}_p$ one sees this right action corresponds to the left action defined in [Stevens 1994]. To prove that $\mathscr{E}^{\mathrm{rig}}$ is reduced one uses a criterion of [Chenevier 2005, Proposition 3.9]; see [Bellaïche 2010, Theorem IV.2.1] for the analogous statement for the H_c^1. Unfortunately, the notion of a "classical structure" in [Chenevier 2005] is based on the input data for the eigenvariety construction in [Buzzard 2007] and is therefore not directly applicable to the situation in [Hansen 2017]. Let us state a version of [Chenevier 2005, Proposition 3.9] applicable to the situation in [Hansen 2017, Definition 4.2.1]. We use the notation and terminology of [Hansen 2017, §4–5] freely; in particular we use the language of classical rigid geometry for this proposition.

Proposition 6.1.2. *Let $\mathfrak{D} = (\mathscr{W}, \mathscr{Z}, \mathscr{M}, \boldsymbol{T}, \psi)$ be an eigenvariety datum. If (U, h) is a slope datum, assume that $\mathscr{M}(\mathscr{Z}_{U,h})$ is a projective $\mathcal{O}(U)$-module. Assume moreover that there exists a very Zariski dense set $\mathscr{W}^{cl} \subseteq \mathscr{W}$ such that, if (U, h) is a slope datum, there is a Zariski open and dense subset $W_{U,h}$ of $\mathscr{W}^{cl} \cap U$ such that $\mathscr{M}(\mathscr{Z}_{U,h})_x$ is a semisimple $\boldsymbol{T}[T^{-1}]$-module. Here T is the parameter on $\mathbb{A}^1_{\mathscr{W}}$, which naturally acts invertibly on $\mathscr{M}(\mathscr{Z}_{U,h})$, and the set $\mathscr{W}^{cl}$ is given the Zariski topology. Then the eigenvariety $\mathscr{X}_{\mathfrak{D}}$ is reduced.*

The proof is virtually identical to that of [Chenevier 2005, Proposition 3.9]; we omit it. Using this, one proves that $\mathscr{E}^{\mathrm{rig}}$ is reduced in the same way as in the proof of [Bellaïche 2010, Theorem IV.2.1(i)], using the control theorem of Stevens (see [Hansen 2017, Theorem 3.2.5]); recall that our Hecke algebra $\mathbb{T}(\Delta^p, K^p)$ contains no Hecke operators at primes dividing N. That $\mathscr{E}^{\mathrm{rig}}$ is equal to the Coleman–Mazur eigencurve is then proved using the control theorems of Coleman and Stevens and the Eichler–Shimura isomorphism together with [Hansen 2017, Theorem 5.1.2] (this type of argument is well known to experts; see for example the proof of [Bellaïche 2010, Theorem IV.2.1(i)]). The argument for flatness will be given below. This finishes our review of the basic properties of $\mathscr{E}^{\mathrm{rig}}$.

Let us now return to the constructions of this paper. Our eigenvariety construction gives an extension $\mathscr{E}$ of $\mathscr{E}^{\mathrm{rig}}$ defined over the locus $\mathcal{W}_0 \subseteq \mathcal{W}$ where $\kappa_2 = 1$. Another such extension $\mathscr{E}'$ was constructed by Andreatta, Iovita and Pilloni [Andreatta et al. 2018]. Note that $\mathcal{W}_0$ is naturally the analytic locus of the formal weight space $\mathfrak{W}_0$ with $\kappa_2 = 1$. We have

$$\mathfrak{W}_0 \cong \mathrm{Spa}(\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!], \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]).$$

When $p \neq 2$, $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$ is a regular ring. When $p = 2$ this is no longer the case; we have $\mathbb{Z}_2[\![\mathbb{Z}_2^\times]\!] \cong \mathbb{Z}_2[\mathbb{Z}/2][\![X]\!]$ and $\mathbb{Z}_2[\mathbb{Z}/2]$ is not regular. We will instead work over the normalization A of $\mathbb{Z}_2[\![\mathbb{Z}_2^\times]\!]$, which is isomorphic to $\mathbb{Z}_2[\![X]\!] \times \mathbb{Z}_2[\![X]\!]$. The normalization map

$$\mathbb{Z}_2[\mathbb{Z}/2][\![X]\!] \to \mathbb{Z}_2[\![X]\!] \times \mathbb{Z}_2[\![X]\!]$$

is explicitly given by

$$\sum_{n\geq 0}(a_n+b_n g)X^n \mapsto \left(\sum_{n\geq 0}(a_n+b_n)X^n, \sum_{n\geq 0}(a_n-b_n)X^n\right),$$

where $a_n, b_n \in \mathbb{Z}_2$ and $g \in \mathbb{Z}/2$ is the nontrivial element. Using this map we get a weight into A, and we let $\widetilde{\mathfrak{W}}_0 = \mathrm{Spa}(A, A)$ and put $\widetilde{\mathcal{W}}_0 = \widetilde{\mathfrak{W}}_0^{\mathrm{an}}$. We remark that $\widetilde{\mathcal{W}}_0^{\mathrm{rig}} \cong \mathcal{W}_0^{\mathrm{rig}}$ canonically via the normalization map. To make our notation uniform, we set $\widetilde{\mathcal{W}}_0 = \mathcal{W}_0$ when $p \neq 2$. We may perform our construction over $\widetilde{\mathcal{W}}_0$, and one may pull back the Banach modules that are used to construct the eigencurve in [Andreatta et al. 2018] to $\widetilde{\mathcal{W}}_0$, and construct the eigencurve over $\widetilde{\mathcal{W}}_0$ instead. Let us denote the corresponding eigenvarieties by $\tilde{\mathscr{E}}$ and $\tilde{\mathscr{E}}'$, though we hasten to remark that these should *not* be thought of as normalizations of $\mathscr{E}$ and $\mathscr{E}'$.

Lemma 6.1.3. *Let $\mathcal{U} \subset \widetilde{\mathcal{W}}_0$ be a connected open affinoid subset such that $\mathcal{O}(U)$ is a Tate ring. Then $\mathcal{O}(\mathcal{U})$ is a Dedekind domain.*

Proof. We first show that $\mathcal{O}(\mathcal{U})$ is regular of Krull dimension 1. The connected components of $\widetilde{\mathcal{W}}_0$ are isomorphic to $\mathrm{Spa}(\mathbb{Z}_p[\![X]\!], \mathbb{Z}_p[\![X]\!])$ so we may take $\mathcal{U}$ to be an open affinoid subset of $\mathrm{Spa}(\mathbb{Z}_p[\![X]\!], \mathbb{Z}_p[\![X]\!])$. Let $\mathfrak{q}$ be a maximal ideal of $\mathcal{O}(\mathcal{U})$ and let $\mathfrak{p}$ be its preimage in $A = \mathbb{Z}_p[\![X]\!]$. By Proposition A.15 the natural map $A_{\mathfrak{p}} \to \mathcal{O}(\mathcal{U})_{\mathfrak{q}}$ induces an isomorphism on completions. By Lemma A.13 $\mathfrak{p}$ defines a closed point of $\mathrm{Spec}\, A \setminus \{(p, X)\}$. Since A is a regular local ring of dimension 2, it follows that $A_{\mathfrak{p}}$ is a regular local ring of dimension 1, and hence the same is true for $\mathcal{O}(\mathcal{U})_{\mathfrak{q}}$ (since if R is a Noetherian local ring with completion $\widehat{R}$, then R is regular if and only if $\widehat{R}$ is regular, and $\dim R = \dim \widehat{R}$). It follows that $\mathcal{O}(\mathcal{U})$ is a product of regular integral domains of dimension 1. Since $\mathcal{U}$ is connected $\mathcal{O}(\mathcal{U})$ does not contain any nontrivial idempotents, so $\mathcal{O}(\mathcal{U})$ is an integral domain. □

Let $(\mathcal{U}, h)$ be a connected slope datum for $\tilde{\mathscr{E}}$ (by which we mean a slope datum for the construction that produces $\tilde{\mathscr{E}}$ such that $\mathcal{U}$ is connected; we will use the terminology "(connected) slope datum for $\tilde{\mathscr{E}}'$" similarly). Then $\mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U},h})$ is, by definition, an $\mathcal{O}(\mathcal{U})$-submodule of $\mathrm{End}_{\mathcal{O}(\mathcal{U})}(H^1(K, \mathscr{D}_{\mathcal{U}})_{\leq h})$. The latter is projective by Lemma 6.1.1, so the former is also projective since $\mathcal{O}(\mathcal{U})$ is Dedekind. Thus the natural map $\tilde{\mathscr{E}}_{\mathcal{U},h} \to \mathcal{U}$ is finite flat, and hence $\tilde{\mathscr{E}} \to \widetilde{\mathcal{W}}_0$ is flat. The same applies to $\tilde{\mathscr{E}}'$.

Now let $(\mathcal{U}, h)$ be a slope datum for $\tilde{\mathscr{E}}$ *and* $\tilde{\mathscr{E}}'$. Let $(\mathcal{U}_i)_{i\in I}$ be an open affinoid cover of $\mathcal{U}^{\mathrm{rig}}$. Then the natural map $\mathcal{O}(\mathcal{U}) \to \prod_{i\in I} \mathcal{O}(\mathcal{U}_i)$ is an injection (since $\mathcal{U} \setminus \mathcal{U}^{\mathrm{rig}}$ does not contain any open subset of $\mathcal{U}$) so tensoring with the finite projective $\mathcal{O}(\mathcal{U})$-module $\mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U},h})$ we get an injection

$$\mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U},h}) \hookrightarrow \left(\prod_{i\in I} \mathcal{O}(\mathcal{U}_i)\right) \otimes_{\mathcal{O}(\mathcal{U})} \mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U},h}) \cong \prod_{i\in I} \mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U}_i,h}),$$

which in particular shows that $\mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U},h})$ is reduced. The image of $\mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U},h})$ inside $\prod_{i\in I} \mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U}_i,h})$ is equal to the $\mathcal{O}(\mathcal{U})$-span of the image of $\mathbb{T}(\Delta^p, K^p)[U_p]$ in $\prod_{i\in I} \mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U}_i,h})$. The same holds replacing $\tilde{\mathscr{E}}$ by $\tilde{\mathscr{E}}'$, so since we have canonical isomorphisms

$$\mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U}_i,h}) \cong \mathcal{O}(\tilde{\mathscr{E}}'_{\mathcal{U}_i,h}),$$

we obtain a canonical isomorphism $\mathcal{O}(\tilde{\mathscr{E}}_{\mathcal{U},h}) \cong \mathcal{O}(\tilde{\mathscr{E}}'_{\mathcal{U},h})$, compatible with the way the eigencurves are built. As a result we have a canonical isomorphism $\tilde{\mathscr{E}} \cong \tilde{\mathscr{E}}'$ extending the canonical isomorphism $\tilde{\mathscr{E}}^{\mathrm{rig}} \cong (\tilde{\mathscr{E}}')^{\mathrm{rig}}$. We summarize the discussion above in the following theorem:

Theorem 6.1.4. *The eigenvariety $\tilde{\mathscr{E}}$ is reduced and flat over $\widetilde{\mathcal{W}}_0$. Moreover, it is canonically isomorphic to the eigencurve $\tilde{\mathscr{E}}'$ constructed by Andreatta, Iovita and Pilloni* [Andreatta et al. 2018].

Remark 6.1.5. In fact, it is possible to show that $\mathscr{E}$ and $\mathscr{E}'$ are isomorphic for all p (i.e., including $p=2$), using the interpolation theorem [Johansson and Newton 2017, Theorem 3.2.1], since both $\mathscr{E}$ and $\mathscr{E}'$ are reduced with Zariski dense sets of classical points which naturally match up.

Fix a character $\eta : (\mathbb{Z}/q)^\times \to \mathbb{F}_p^\times$ (recall that $q=4$ if $p=2$ and $q=p$ otherwise). We have a natural isomorphism $\mathbb{Z}_p^\times \cong (\mathbb{Z}/q)^\times \times (1+q\mathbb{Z}_p)$ defined by $z \mapsto (\bar{z}, z/\omega(\bar{z}))$, where an overline denotes reduction modulo q and ω denotes the Teichmüller lift. Let us write $\langle z\rangle := z/\omega(\bar{z})$. Then we may define a character $\kappa_\eta : \mathbb{Z}_p^\times \to \mathbb{Z}_p[\![X]\!]^\times$ by

$$\kappa_\eta(z) = \omega(\eta(\bar{z})) \sum_{n=0}^{\infty} \binom{p^{-1}\log\langle z\rangle}{n} X^n.$$

We let $\bar{\kappa}_\eta$ denote its reduction modulo p. This is a character $\mathbb{Z}_p^\times \to \mathbb{F}_p((X))^\times$ which we may think of as a character $T_0 \to \mathbb{F}_p((X))^\times$ with $\kappa_2 = 1$. We remark that if $p=2$ then η, and hence $\bar{\kappa}_\eta$, is unique.

Corollary 6.1.6. *There are infinitely many (nonordinary) finite-slope U_p-eigenvectors in $H^1(K, \mathscr{D}_{\bar{\kappa}_\eta})$.*

Proof. By Corollary 4.2.3, its analogue for $\tilde{\mathscr{E}}'$ (which is simpler, and is essentially [Buzzard 2007, Lemma 5.9]) and Theorem 6.1.4 we see that $H^1(K, \mathscr{D}_{\bar{\kappa}_\eta})$ and the module $\overline{M}^\dagger_{\bar{\kappa}_\eta}(N)$ of overconvergent modular forms of weight $\bar{\kappa}_\eta$ and tame level N constructed in [Andreatta et al. 2018] contain the same finite-slope systems of Hecke eigenvalues. By [Bergdall and Pollack 2016, Corollary A.1], $\overline{M}^\dagger_{\bar{\kappa}_\eta}(N)$ has infinitely many finite-slope U_p-eigenvectors, so we are done. ☐

Remark 6.1.7. It is possible to prove Corollary 6.1.6 directly from [Bergdall and Pollack 2016, Theorem A] (using the observation in the remark following [loc. cit., Corollary A.2]) without any reference to [Andreatta et al. 2018].

6.2. ***Estimates for the Newton polygon of U_p.*** In this and the following section we give a short proof of the estimates obtained in [Liu et al. 2017, Theorem 3.16] for the Newton polygon of U_p acting on spaces of overconvergent automorphic forms for a definite quaternion algebra over $\mathbb{Q}$.

We fix an odd prime p and assume that we are in the setting of Section 3.3. Suppose that $\overline{N}_1 \cong \mathbb{Z}_p$ and fix a topological generator $\bar{\mathfrak{n}}$. Let f be a norm-decreasing R-linear map

$$f : \bigoplus_{i=1}^{t} \mathcal{D}_\kappa^r \to \bigoplus_{i=1}^{t} \mathcal{D}_\kappa^{r^{1/p}}$$

and recall that we have a compact inclusion

$$\iota : \bigoplus_{i=1}^{t} \mathcal{D}_\kappa^{r^{1/p}} \hookrightarrow \bigoplus_{i=1}^{t} \mathcal{D}_\kappa^{r}.$$

We set $U = \iota \circ f$. Then U is a compact endomorphism of $M = \bigoplus_{i=1}^{t} \mathcal{D}_\kappa^r$. Recall that we have a potential ON-basis for $\mathcal{D}_\kappa^r$ given by the elements $e_{r,\alpha} := \varpi^{-n(r,\varpi,\alpha)} \bar{\mathfrak{n}}^\alpha$ for $\alpha \in \mathbb{Z}_{\geq 0}$.

We consider the potential ON-basis for M given by

$$e_{r,0}^1 = (e_{r,0}, 0, \ldots, 0), \quad \ldots, \quad e_{r,0}^t = (0, \ldots, 0, e_{r,0}), \quad e_{r,1}^1 = (e_{r,1}, 0, \ldots, 0), \quad \ldots.$$

Lemma 6.2.1. *Assume that there is no $x \in R$ with $1 < |x| < |\varpi|^{-1}$. Then U maps $e_{r,\alpha}^i$ to a sum $\sum_{j,\beta} a_\beta^j e_{r,\beta}^j$ with*

$$|a_\beta^j| \leq |\varpi|^{n(r,\varpi,\beta) - n(r^{1/p},\varpi,\beta)}.$$

If we define

$$\lambda(0) = 0, \quad \lambda(i+1) = \lambda(i) + n(r, \varpi, \lfloor i/t \rfloor) - n(r^{1/p}, \varpi, \lfloor i/t \rfloor),$$

the Fredholm series

$$\det(1 - TU|M) = \sum_{n \geq 0} c_n T^n \in R\{\{T\}\}$$

satisfies $|c_n| \leq |\varpi|^{\lambda(n)}$.

Proof. We first prove the estimate on the matrix coefficients of U. Apply f to $e_{r,\alpha}^i$. We get a sum $\sum_{j,\beta} b_\beta^j e_{r^{1/p},\beta}^j$, and the fact that f is norm-decreasing is equivalent to

$$|b_\beta^j| \leq |\varpi|^{n(r^{1/p},\varpi,\beta) - n(r,\varpi,\alpha)} r^{|\alpha| - |\beta|/p}$$

for all j, β. Since $|\varpi| < |\varpi|^{-n(r,\varpi,\alpha)} r^{|\alpha|}$, $|\varpi|^{-n(r^{1/p},\varpi,\beta)} r^{|\beta|/p} \leq 1$ by construction, we deduce that $|b_\beta^j| < |\varpi|^{-1}$ for all j, β. By our assumption on R, it follows that $|b_\beta^j| \leq 1$ for all j, β. We then have

$$e_{r^{1/p},\beta}^j = \varpi^{-n(r^{1/p},\varpi,\beta)} \bar{\mathfrak{n}}^\beta = \varpi^{n(r,\varpi,\beta) - n(r^{1/p},\varpi,\beta)} e_{r,\beta}^j$$

so we conclude that

$$U e_{r,\alpha}^i = \sum_{j,\beta} a_\beta^j e_{r,\beta}^j,$$

where $a_\beta^j = \varpi^{n(r,\varpi,\beta) - n(r^{1/p},\varpi,\beta)} b_\beta^j$, and therefore

$$|a_\beta^j| \leq |\varpi|^{n(r,\varpi,\beta) - n(r^{1/p},\varpi,\beta)}.$$

In other words, the i-th row of the matrix for U (we begin indexing rows at $i = 0$) has entries with norm $\leq |\varpi|^{n(r,\varpi,\lfloor i/t \rfloor) - n(r^{1/p},\varpi,\lfloor i/t \rfloor)}$. We deduce immediately that $|c_n| \leq |\varpi|^{\lambda(n)}$, since c_n is an alternating sum of products of matrix entries coming from n distinct rows [Serre 1962, Proposition 7], and each of these products has norm $\leq |\varpi|^{\lambda(n)}$. □

6.3. *Definite quaternion algebras over* $\mathbb{Q}$. As an application of Lemma 6.2.1, we give a new proof of [Liu et al. 2017, Theorem 3.16]. In this section we assume that p is odd. We need to set up things so that we can apply the machinery of Sections 3.3 and 4. Let $D/\mathbb{Q}$ be a definite quaternion algebra, split at p, and let $\boldsymbol{G}$ be the reductive group over $\mathbb{Q}$ defined by $\boldsymbol{G}(R) = (D \otimes_{\mathbb{Q}} R)^\times$, for $\mathbb{Q}$-algebras R. We fix an isomorphism $D_p \cong M_2(\mathbb{Q}_p)$ and henceforth identify D_p with $M_2(\mathbb{Q}_p)$ via this isomorphism. Let $\boldsymbol{G}_{\mathbb{Z}_p}$ be the $\mathbb{Z}_p$-model for $\boldsymbol{G}$ given by $\boldsymbol{G}_{\mathbb{Z}_p}(R) = (M_2(\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} R)^\times$ for $\mathbb{Z}_p$-algebras R. We let $\boldsymbol{B}$ be the upper triangular Borel in $\boldsymbol{G}_{\mathbb{Z}_p}$ and let $\boldsymbol{T}$ be the diagonal maximal torus.

Fix a tame level $K^p = \prod_{l \neq p} K_l$ with $K_l \subset \boldsymbol{G}(\mathbb{Q}_l)$ compact open, let $K = K^p I$, and assume that K is neat.

Fix a character $\eta : \mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ and let $\Lambda = \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$. We have an induced map $\pi_\eta : \Lambda \to \mathbb{F}_p$ and we denote its kernel by $\mathfrak{m}_\eta$. We write Λ_η for the localization $\Lambda_{\mathfrak{m}_\eta}$. We have a universal character

$$[\,\cdot\,]_\eta : \mathbb{Z}_p^\times \to \Lambda_\eta^\times.$$

We give the complete local ring Λ_η the $\mathfrak{m}_\eta$-adic topology. Fixing a topological generator γ of $1 + p\mathbb{Z}_p$ gives an isomorphism

$$\mathbb{Z}_p[\![X]\!] \to \Lambda_\eta, \quad X \mapsto [\gamma]_\eta - 1.$$

Let $\mathfrak{W}_\eta = \mathrm{Spa}(\Lambda_\eta, \Lambda_\eta)$, denote its analytic locus by $\mathcal{W}_\eta$ and let $\mathcal{U}_1 \subset \mathcal{W}_\eta$ be the rational subdomain of $\mathfrak{W}_\eta$

$$\mathcal{U}_1 = \{|p| \le |X| \neq 0\}.$$

Pulling back $\mathcal{U}_1$ to the open unit disc $\mathcal{W}_\eta^{\mathrm{rig}}$ gives the "boundary annulus" $|X|_p \ge p^{-1}$.

We let $R_\eta = \mathcal{O}(\mathcal{U}_1)$. More explicitly, $R_\eta = R_\eta^\circ[1/X]$, where R_η° is a ring of definition for R_η, given by the X-adic completion of $\mathbb{Z}_p[\![X]\!][p/X]$, with the X-adic topology.

Even more explicitly, we can describe the elements of R_η° as formal power series

$$\left\{ \sum_{n \in \mathbb{Z}} a_n X^n \;\middle|\; a_n \in \mathbb{Z}_p,\ |a_n|_p p^{-n} \le 1,\ |a_n|_p p^{-n} \to 0 \text{ as } n \to -\infty \right\}$$

X is a topologically nilpotent unit in R_η and so equipping R_η with the norm

$$|r| = \inf\{p^{-n} \mid r \in X^n R_\eta^\circ,\ n \in \mathbb{Z}\}$$

makes R_η into a Banach–Tate $\mathbb{Z}_p$-algebra. This norm has the explicit description

$$\left| \sum_{n \in \mathbb{Z}} a_n X^n \right| = \sup\{|a_n|_p p^{-n}\}. \tag{6.3.1}$$

Note that if $r \in \Lambda_\eta$, we have $|r| = \inf\{p^{-n} \mid r \in \mathfrak{m}_\eta^n, n \in \mathbb{Z}\}$.

We now define a continuous character

$$\kappa_\eta : T_0 \to R_\eta^\times$$

by

$$\kappa_\eta \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = [a]_\eta.$$

Lemma 6.3.1. *The norm we have defined on R_η is adapted to κ_η. Moreover, for $t \in T_1$ we have $|\kappa_\eta(t) - 1| \le 1/p$.*

Proof. If $t \in T_1$ we have $\kappa(t) - 1 = (1+X)^\alpha - 1 = \sum_{n \ge 1} \binom{\alpha}{n} X^n$ for some $\alpha \in \mathbb{Z}_p$. So $|\kappa_\eta(t) - 1| \le 1/p$. $\square$

We can now apply the theory of Section 4 to the space of overconvergent automorphic forms $H^0(K, \mathcal{D}^{1/p}_{\kappa_\eta})$. Note that we have the concrete description

$$H^0(K, \mathcal{D}^{1/p}_{\kappa_\eta}) = \{f : D^\times \backslash (D \otimes \mathbb{A}^f)^\times / K^p \to \mathcal{D}^{1/p}_{\kappa_\eta} \mid f(gk) = k^{-1} f(g) \text{ for } k \in I\}$$

and $H^0(K, \mathcal{D}^{1/p}_{\kappa_\eta})$ is a Banach R_η-module with norm $|f| = \sup_{g \in (D\otimes\mathbb{A}^f)^\times} \|f(g)\|_{1/p}$.

In particular, we consider the action on $H^0(K, \mathcal{D}^{1/p}_{\kappa_\eta})$ of the Hecke operator U_{κ_η} attached to the element $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \in \Sigma^{\text{cpt}}$. As a simple consequence of our results, we obtain the following theorem, which is essentially due to Liu–Wan–Xiao — compare with [Liu et al. 2017, Theorem 3.16, §5.4].

Theorem 6.3.2. *The Hecke operator U_{κ_η} is compact. Consider the Fredholm series*

$$F_{\kappa_\eta}(T) = \sum_{n \geq 0} c_n T^n = \det(1 - T U_{\kappa_\eta} | H^0(K, \mathcal{D}^{1/p}_{\kappa_\eta})).$$

Let $t = |D^\times \backslash (D \otimes \mathbb{A}^f)^\times / K|$. We have $c_n \in \Lambda_\eta$ and moreover we have

$$c_n \in \mathfrak{m}_\eta^{\lambda(n)} \quad \text{for } n \in \mathbb{Z}_{\geq 0},$$

where $\lambda(0) = 0, \lambda(1), \ldots$ is a sequence of integers determined by

$$\lambda(0) = 0, \quad \lambda(i+1) = \lambda(i) + \lfloor i/t \rfloor - \lfloor i/pt \rfloor.$$

Proof. Compactness of U_{κ_η} follows from Corollary 3.3.10. The fact that $c_n \in \Lambda_\eta$ follows from Corollary 4.1.5, since $F_{\kappa_\eta}(T)$ extends to a Fredholm series over $\mathcal{W}_\eta$, and $\mathcal{O}(\mathcal{W}_\eta) = \Lambda_\eta$.

The rest of the theorem follows from Lemma 6.2.1 (note that the norm on R_η satisfies the assumption of that lemma), using the fact that if we choose representatives $g_1, \ldots, g_t$ for the double cosets $D^\times \backslash (D \otimes \mathbb{A}^f)^\times / K$ and $r \in [p^{-1}, 1)$ we have an isomorphism of potentially ON-able R_η-modules:

$$H^0(K, \mathcal{D}^r_{\kappa_\eta}) \cong \bigoplus_{i=1}^{t} \mathcal{D}^r_{\kappa_\eta}, \qquad f \mapsto (f(g_i))_{i=1}^t.$$

We take $\varpi = X$, and compute that

$$n(p^{-1}, X, \lfloor i/t \rfloor) = \lfloor i/t \rfloor,$$
$$n(p^{-1/p}, X, \lfloor i/t \rfloor) = \lfloor 1/p \lfloor i/t \rfloor \rfloor = \lfloor i/pt \rfloor. \qquad \square$$

As in Section 6.1, our eigenvariety construction, applied to the modules $H^0(K, \mathcal{D}^r_\kappa)$ with $\kappa_2 = 1$, gives an eigenvariety $\mathscr{E}_\eta$ which is flat over $\mathcal{W}_\eta$. The open subspace $\mathscr{E}^{\text{rig}}_\eta$ defined by $|p| \neq 0$ is the eigenvariety constructed in [Buzzard 2004].

We end this section with our interpretation of [Liu et al. 2017, Theorems 1.3 and 1.5]. First we need some extra notation. For $m \leq n$ positive integers we define

$$\mathcal{U}_{m/n} = \{|p^m| \leq |X^n| \neq 0\} \subseteq \mathcal{W}_\eta.$$

We set $\mathcal{U} = \mathcal{U}_1$.

For a real number $\alpha \in (0, 1]$ we denote by $\mathcal{W}_\eta^{>p^{-\alpha}}$ the open subspace of $\mathcal{W}_\eta$ obtained as the union of open affinoids

$$\mathcal{W}_\eta^{>p^{-\alpha}} = \bigcup_{m/n<\alpha} \mathcal{U}_{m/n}.$$

Note that X is a topologically nilpotent unit in $\mathcal{O}(\mathcal{U}_{m/n})$ for all m, n. We denote the pullback of $\mathscr{E}_\eta$ to $\mathcal{W}_\eta^{>p^{-\alpha}}$ by $\mathscr{E}_\eta^{>p^{-\alpha}}$. The eigenvariety $\mathscr{E}_\eta$ comes equipped with a map to the spectral variety $Z(F_{\kappa_\eta})$, and therefore it comes equipped with a map to $\mathbb{A}^1_{\mathcal{U}}$. For $h = m/n \in \mathbb{Q}$ with $m \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 1}$ we define an affinoid subspace $\mathbb{B}_{\mathcal{U},=h} \subset \mathbb{A}^1_{\mathcal{U}}$ by

$$\mathbb{B}_{\mathcal{U},=h} = \{|T^n| = |X^{-m}|\}.$$

Similarly, if $h = m/n \leq h' = m'/n$ are rational numbers, we define

$$\mathbb{B}_{\mathcal{U},[h,h']} = \{|X^{-m}| \leq |T^n| \leq |X^{-m'}|\}.$$

Lemma 6.3.3. *Let $L/\mathbb{Q}_p$ be a finite extension and let $x \in L$ with $|x|_p = p^{-\alpha}$, where $0 < \alpha \leq 1$. Consider the closed immersion $\iota : \mathrm{Spa}(L, \mathcal{O}_L) \hookrightarrow \mathcal{U}$ induced by the continuous $\mathbb{Z}_p$-algebra map $R_\eta \to L$ sending X to x. Let $\mathbb{B}_{x,=h}$ be the pullback of $\mathbb{B}_{\mathcal{U},=h}$ along ι. Then $\mathbb{B}_{x,=h} \hookrightarrow \mathbb{A}^1_L$ is the affinoid open defined by*

$$\mathbb{B}_{x,=h} = \{|T|_p = p^{-\alpha h}\}.$$

Proof. The affinoid $\mathbb{B}_{x,=h}$ is given by $\{|T^n| = |x^{-m}| = |p^{\alpha m}|\} \subset \mathbb{A}^1_L$. □

Theorem 6.3.4 [Liu et al. 2017]. *The space $\mathscr{E}_\eta^{>p^{-1}}$ is a disjoint countable union of adic spaces finite and flat over $\mathcal{W}_\eta^{>p^{-1}}$.*

Moreover, there is an explicit α depending only on K^p, with $0 < \alpha < 1$, such that

$$\mathscr{E}_\eta^{>p^{-\alpha}} = \coprod_{i \geq 0} \mathscr{X}_{\eta,i}$$

with $\mathscr{X}_{\eta,i}$ finite flat over $\mathcal{W}_\eta^{>p^{-\alpha}}$ and each piece $\mathscr{X}_{\eta,i}$ of the eigenvariety has constant slope, in the sense that each map $\mathscr{X}_{\eta,i} \to \mathbb{A}^1_{\mathcal{U}}$ factors through the affinoid subspace $\mathbb{B}_{\mathcal{U},=h_i} \subset \mathbb{A}^1_{\mathcal{U}}$ for some $h_i \in \mathbb{Q}_{\geq 0}$. In particular, if we measure slopes on $\mathscr{X}_{\eta,i}^{\mathrm{rig}}$ with the usual p-adic valuation, then the slope of a point in $\mathscr{X}_{\eta,i}^{\mathrm{rig}}$ is given by $h_i v_p(T)$.

Proof. This follows from Theorems 1.3, 1.5 and Remark 3.25 of [Liu et al. 2017]. Remark 3.25 shows that, after restricting to $\mathcal{W}_\eta^{>p^{-1}}$, the Fredholm series F_{κ_η} factorizes as a countable product of multiplicative polynomials $\prod_{i\geq 0} P_i$, with each finite product $\prod_{i\geq 0}^N P_i$ a factor in a slope factorization over every affinoid subspace of $\mathcal{W}_\eta^{>p^{-1}}$. This establishes the claim about $\mathscr{E}_\eta^{>p^{-1}}$. Theorem 1.5 shows moreover that (for some explicit α) the restriction of F_{κ_η} to $\mathcal{W}_\eta^{>p^{-\alpha}}$ factorizes as $\prod_{i\geq 0} Q_i$, such that the specialization of Q_i at every classical rigid analytic point of $\mathcal{W}_\eta^{>p^{-\alpha}}$ has constant slope equal to h_i for some $h_i \in \mathbb{Q}_{\geq 0}$ (independent of the specialization). We obtain a decomposition of $Z(F_{\kappa_\eta})$ as a disjoint union of spaces Z_i, finite flat over $\mathcal{W}_\eta^{>p^{-\alpha}}$, such that every classical rigid analytic point of Z_i is contained in $\mathbb{B}_{\mathcal{U},=h_i}$. The space $\mathscr{X}_{\eta,i}$ is defined to be the inverse image of Z_i in $\mathscr{E}_\eta^{>p^{-\alpha}}$. It now remains to show that every point of Z_i is contained in $\mathbb{B}_{\mathcal{U},=h_i}$. First we check this for rank-1 points: a rank-1 point of Z_i which is not in $\mathbb{B}_{\mathcal{U},=h_i}$ is contained in $\mathbb{B}_{\mathcal{U},[h,h']}$ for some interval $[h, h']$ which does not contain h_i. But then $\mathbb{B}_{\mathcal{U},[h,h']} \cap Z_i$ is a nonempty open subset in Z_i which contains no classical rigid analytic point, which is impossible since Z_i is finite flat over $\mathcal{W}_\eta^{>p^{-\alpha}}$ (in particular the map $Z_i \to \mathcal{W}_\eta^{>p^{-\alpha}}$ is open). Let V be an affinoid open in $\mathcal{W}_\eta^{>p^{-\alpha}}$. Then $Z_i|_V \cap \mathbb{B}_{\mathcal{U},=h_i}$ is an affinoid open in $Z_i|_V$ such that the complement contains no rank-1 point. We have $Z_i|_V = \mathrm{Spa}(A, A^\circ)$ for some Tate ring A with a Noetherian ring of definition. So [Huber 1993, Lemma 3.4] (see the proof of Corollary 4.2 of that paper) implies that rank-1 points are dense in the constructible topology of $\mathrm{Spa}(A, A^\circ)$ and we deduce that $Z_i|_V \cap \mathbb{B}_{\mathcal{U},=h_i} = Z_i|_V$. Therefore Z_i is contained in $\mathbb{B}_{\mathcal{U},=h_i}$, as desired. The final sentence of the theorem follows from Lemma 6.3.3. □

Note that [Liu et al. 2017] proves moreover that the slopes appearing in the above theorem (with multiplicities) are given by a finite union of arithmetic progressions.

Appendix: Some algebraic properties of Tate rings

In this section we prove some properties of the kinds of Tate rings and adic spaces that we need. We start with a ring-theoretic lemma.

Lemma A.1. *Let R be a complete Tate ring with a Noetherian ring of definition R_0. Then R is Jacobson.*

Proof. Let $\varpi \in R_0$ be a topologically nilpotent unit in R. Because R_0 is a Zariski ring when equipped with its ϖ-adic topology (since it is complete), $\mathrm{Spec}\, R_0 \setminus \{\varpi = 0\}$ is a Jacobson scheme by [EGA IV$_3$ 1966, (10.5.7)]. But $\mathrm{Spec}\, R_0 \setminus \{\varpi = 0\} = \mathrm{Spec}\, R$, so R is Jacobson as desired. □

We record another simple lemma that will prove to be useful.

Lemma A.2. *Let R be a complete Tate ring with a Noetherian ring of definition R_0. If $S \subseteq R$ is an open and bounded subring (i.e., a ring of definition) containing R_0, then S is a finitely generated R_0-module, hence Noetherian, and integral over R_0. Moreover, R° is the integral closure of R_0 in R.*

Proof. Pick a topologically nilpotent unit $\varpi \in R$ contained in R_0. Since S is bounded we have $S \subseteq \varpi^{-N} R_0$ for some N, and hence S is an R_0-submodule of the cyclic R_0-module $\varpi^{-N} R_0$. The lemma now follows since R_0 is Noetherian. For the last assertion, first note that the integral closure is contained in R°. Since R° is the union of all open and bounded subrings and any two open bounded subrings are contained in a third, the assertion follows from the first part. □

One consequence of the above lemma is a version for Tate rings (with our Noetherian hypothesis) of [Bosch et al. 1984, 6.3.4/Proposition 1]:

Lemma A.3. *Let R be a complete Tate ring with a Noetherian ring of definition. Let S be a finite R-algebra, equipped with the natural R-module topology. Then S is a complete Tate ring with a Noetherian ring of definition.*

Moreover, the integral closure of R° in S is equal to S°. In particular, the morphism $(R, R^\circ) \to (S, S^\circ)$ is a finite morphism of affinoid rings (see [Huber 1996, 1.4.2]) *and* $\mathrm{Spa}(S, S^\circ) \to \mathrm{Spa}(R, R^\circ)$ *is a finite morphism of adic spaces* (see [loc. cit., 1.4.4]).

Proof. We let R_0 denote a Noetherian ring of definition for R, let ϖ denote a topologically nilpotent unit in R and let $s_1, \ldots, s_n$ denote R-module generators of S. Each s_i is integral over R, and multiplying by a large enough power of ϖ we may assume that each s_i is integral over R_0. Let S_0 be the subring of S generated by R_0 and $s_1, \ldots, s_n$. Now S_0 is a finite R_0-module and is in particular a Noetherian ring. Moreover S_0 with the ϖ-adic topology is an open subring of S. In particular, S is an f-adic topological ring, and since ϖ is a topologically nilpotent unit we see that S is a Tate ring with a Noetherian ring of definition. Completeness of S follows from completeness of finitely generated modules over Noetherian adic rings (this is [Huber 1994, Lemma 2.3(ii)]).

Finally we show that the integral closure R° in S is equal to S°. It is clear from the definition of the topology on S that R° maps to S° so the integral closure of R° in S is contained in S°. Conversely, by Lemma A.2, S° is the integral closure of S_0 in S. Since S_0 is integral over R_0, we see that S° is integral over R_0, and therefore it is integral over R°. □

Next we recall the notion of uniformity. If R is a normed ring, then the spectral seminorm $|-|_{\mathrm{sp}}$ on R is defined by $|r|_{\mathrm{sp}} = \lim_{n\to\infty} |r^n|^{1/n}$. It is well known that this limit exists and defines a power-multiplicative seminorm. Whenever it is a norm, we will refer to it as the spectral norm on R. Conversely, if we mention "the spectral norm of R", we are implicitly stating (or assuming) that the spectral seminorm is a norm.

Definition A.4. Let R be a complete Tate ring. We say that R is *uniform* if the set of power-bounded elements R° is bounded. We say that R is *stably uniform* if any rational localization of R is also uniform. If R is a Banach–Tate ring, we say that R is *uniform* if the norm is power-multiplicative.

Note that, if R is Banach–Tate ring whose underlying complete Tate ring is uniform, then the given norm on R is equivalent to the corresponding spectral norm, which is power-multiplicative. In this case, [Berkovich 1990, Theorem 1.3] says that the spectral norm is equal to the Gelfand norm $\sup_{x\in\mathcal{M}(R)} |-|_x$. If R is in addition stably uniform, then if $\varpi \in R$ is a multiplicative pseudouniformizer and $U \subseteq X = \mathrm{Spa}(R, R^+)$ is a rational subdomain, we may equate $\mathcal{M}(\mathcal{O}_X(U))$ with the rank-1 points in U using ϖ and equip $\mathcal{O}_X(U)$ with the corresponding Gelfand norm.

We may extend the definition of stable uniformity to arbitrary *analytic* adic spaces, i.e., those that are locally the adic spectra of complete Tate rings. We say that such an X is stably uniform if there is a cover of open affinoid subsets $U_i \subseteq X$ such that $\mathcal{O}_X(U)$ is stably uniform. We remark that if R is a complete sheafy Tate ring such that $\mathrm{Spa}(R, R^+)$ is stably uniform, then R is stably uniform (this is a short argument; see [Kedlaya and Liu 2015, Remark 2.8.12]). When R has a Noetherian ring of definition, many naturally occurring complete Tate rings are stably uniform. Below we will prove some results in this direction.

Theorem A.5. *Let A be a reduced quasiexcellent ring. Let I be an ideal of A and give A the I-adic topology. If U is a rational subdomain of $X = \mathrm{Spa}(A, A)$ and $\mathcal{O}_X(U)$ is Tate, then $\mathcal{O}_X(U)$ is uniform. In other words, the analytic locus $X^{\mathrm{an}} \subseteq X$ is stably uniform. We also have $\mathcal{O}_X^+(U) = \mathcal{O}_X(U)^\circ$.*

Moreover, if $U \subset X^{\mathrm{an}}$ is an arbitrary open affinoid then $\mathcal{O}^+_{X^{\mathrm{an}}}(U) = \mathcal{O}_{X^{\mathrm{an}}}(U)^\circ$ and $\mathcal{O}_{X^{\mathrm{an}}}(U)^\circ$ is bounded in $\mathcal{O}_{X^{\mathrm{an}}}(U)$.

Proof. Let $f_1, \dots, f_n, g \in A$ such that $f_1, \dots, f_n$ generate an open ideal and let

$$U = \{|f_1|, \dots, |f_n| \le |g| \ne 0\}.$$

Put $R = \mathcal{O}_X(U)$; recall that R may be constructed as completion of the f-adic ring $T = A[1/g]$ with ring of definition $T_0 = A[f_1/g, \dots, f_n/g] \subseteq T$ and ideal of definition $J = I[f_1/g, \dots, f_n/g] \subseteq T_0$. Let R_0 be the J-adic completion of T_0; this is a ring of definition of R, with ideal of definition JR_0. Since A is reduced, so is T and hence T_0; moreover T_0 is quasiexcellent since it is finitely generated over A. Recall that a Noetherian ring is reduced if and only if Serre's conditions R_0 and S_1 hold (we apologize for the unfortunate clash of notations). By [EGA IV$_2$ 1965, (7.8.3.1)], R_0 inherits these properties from T_0 and is therefore reduced. Moreover, T_0, and hence $T_0/J = R_0/JR_0$, are Nagata (since they are finitely generated over A, which is quasiexcellent, and hence Nagata). By [Marot 1975, Proposition 2.3], R_0 is Nagata (note that there is a trivial misprint in the reference).

Pick a topologically nilpotent unit $\varpi \in R$ (recall that R is Tate by assumption); without loss of generality assume $\varpi \in R_0$. Then $R = R_0[1/\varpi]$, so R is contained in the total ring of fractions $Q(R_0)$ of R_0. Since R_0 is reduced and Nagata, it follows that the integral closure R' of R_0 in R is a finitely generated R_0-module, and hence is bounded. Now $R' = R^\circ$ by Lemma A.2, so R° is bounded as desired.

For the assertion about $\mathcal{O}_X^+(U)$, let T^+ denote the integral closure of T_0 in T. By definition, the completion of T^+ is $R^+ := \mathcal{O}_X^+(U)$. In particular, R^+ contains R_0 and the assertion now follows from Lemma A.2.

To check the assertion about an open affinoid $U = \operatorname{Spa}(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$, note that U has a finite cover by Tate rational subdomains $(U_i)_{i\in I}$ of X. Since the maps $\mathcal{O}(U) \to \mathcal{O}(U_i)$ are bounded (the U_i are also rational subdomains of U), the strict embedding

$$\mathcal{O}(U) \hookrightarrow \prod_{i\in I} \mathcal{O}(U_i)$$

induces an embedding

$$\mathcal{O}(U)^\circ \hookrightarrow \mathcal{O}(U) \cap \prod_{i\in I} \mathcal{O}(U_i)^\circ$$

but the right-hand side equals

$$\mathcal{O}(U) \cap \prod_{i\in I} \mathcal{O}^+(U_i) = \mathcal{O}^+(U)$$

by the first part of the theorem, so we are done because by definition $\mathcal{O}^+(U) \subseteq \mathcal{O}(U)^\circ$, which implies that we have equality. Finally, the boundedness of $\mathcal{O}_{X^{\mathrm{an}}}(U)^\circ$ follows from the boundedness of the $\mathcal{O}(U_i)^\circ$. □

Corollary A.6. *Let $\mathcal{O}$ be a complete discrete valuation ring and let A be a reduced complete Noetherian adic ring formally of finite type over $\mathcal{O}$, i.e., such that $A/A^{\circ\circ}$ is a finitely generated $\mathcal{O}$-algebra. Then the analytic locus $X^{\mathrm{an}} \subseteq X$ is stably uniform. Moreover, if $U \subset X^{\mathrm{an}}$ is an open affinoid subspace then $\mathcal{O}^+_{X^{\mathrm{an}}}(U) = \mathcal{O}_{X^{\mathrm{an}}}(U)^\circ$ and $\mathcal{O}_{X^{\mathrm{an}}}(U)^\circ$ is bounded in $\mathcal{O}_{X^{\mathrm{an}}}(U)$.*

Proof. A is excellent by [Valabrega 1975, Proposition 7; 1976, Theorem 9] (see [Conrad 1999], near the end of the Introduction). Thus, Theorem A.5 applies. □

We also note that the proof of Theorem A.5 applies essentially verbatim to prove the following similar result.

Theorem A.7. *Let R be a complete Tate ring and assume that R has a ring of definition R_0 which is quasiexcellent and reduced. Then R is stably uniform. Moreover, if $X = \mathrm{Spa}(R, R^\circ)$, and $U \subset X$ is an open affinoid subspace, then $\mathcal{O}_X^+(U) = \mathcal{O}_X(U)^\circ$ and $\mathcal{O}_X(U)^\circ$ is bounded in $\mathcal{O}_X(U)$. In particular, $\mathcal{O}_X(U)$ is reduced.*

This theorem also allows us to develop the theory of the nilreduction of an adic space. We only give a sketch here — one can check that everything in [Bosch et al. 1984, §9.5.1] works in our setting.

Definition A.8. Let X be an adic space. Define the *nilradical* $\mathrm{rad}\,\mathcal{O}_X$ to be the sheaf associated to the presheaf $U \mapsto \mathrm{rad}(\mathcal{O}_X(U))$, where $\mathrm{rad}(\mathcal{O}_X(U))$ is the nilradical of the ring $\mathcal{O}_X(U)$.

Proposition A.9. *Let R be a complete Tate ring and assume that R has a ring of definition R_0 which is quasiexcellent. Let $X = \mathrm{Spa}(R, R^\circ)$. Then $\mathrm{rad}\,\mathcal{O}_X \subset \mathcal{O}_X$ is a coherent $\mathcal{O}_X$-ideal, associated to the ideal $\mathrm{rad}(R)$ of R.*

More generally, if X is an adic space which is locally of the form $\mathrm{Spa}(R, R^\circ)$ where R is a complete Tate ring with a quasiexcellent ring of definition, then $\mathrm{rad}\,\mathcal{O}_X$ is a coherent $\mathcal{O}_X$-ideal.

Proof. The key point is that if $U \subset X = \mathrm{Spa}(R, R^\circ)$ is a rational subdomain, then

$$\mathrm{Spa}\big(\mathcal{O}_X(U)/\mathrm{rad}(R), (\mathcal{O}_X(U)/\mathrm{rad}(R))^\circ\big) \to \mathrm{Spa}(R^{\mathrm{red}}, (R^{\mathrm{red}})^\circ)$$

is a rational subdomain, so Theorem A.7 implies that $\mathcal{O}_X(U)/\mathrm{rad}(R)$ is reduced, which implies that $\mathrm{rad}(\mathcal{O}_X(U)) = \mathrm{rad}(R)\mathcal{O}_X(U)$. □

Definition A.10. Let X be an adic space which is locally of the form $\mathrm{Spa}(R, R^\circ)$, where R is a complete Tate ring with a quasiexcellent ring of definition. Then we define X^{red} to be the closed subspace of X cut out by $\mathrm{rad}\,\mathcal{O}_X$ (see [Huber 1996, 1.4]).

In this paper the analytic adic spaces encountered will locally be of the form $\mathrm{Spa}(R, R^\circ)$, where R is a complete Tate ring with a ring of definition R_0 which is formally of finite type over $\mathbb{Z}_p$. We will need a few properties of these rings, all of which follow from the material in [Abbes 2010]. We recall the following definition from that paper, specialized to our Noetherian situation.

Definition A.11. A Noetherian adic ring B is called a 1-*valuative order* if it is an integral domain which is local of Krull dimension 1, and has no J-torsion, where J is an ideal of definition (this is independent of the choice of ideal of definition).

This is [Abbes 2010, Definition 1.11.1], except that we demand that B is Noetherian. If B is a 1-valuative order, then the integral closure $\overline{B}$ in $L = \mathrm{Frac}(B)$ is finite over B and is a complete discrete valuation ring, so L is a complete discrete valuation field [loc. cit., Proposition 1.11.4]. If A is any

Noetherian adic ring with an ideal of definition I and $\mathfrak{p} \in \operatorname{Spec} A$, then $A/\mathfrak{p}$ is a 1-valuative order if and only if $\mathfrak{p}$ is a closed point in $\operatorname{Spec} A \setminus V(I)$ [loc. cit., Proposition 1.11.8].

Lemma A.12. *Let R be a complete Tate ring with a ring of definition R_0 which is formally of finite type over $\mathbb{Z}_p$, and let $\mathfrak{m} \subseteq R$ be a maximal ideal. Then $R/\mathfrak{m}$ is a local field.*

Proof. Let $\mathfrak{p} = R_0 \cap \mathfrak{m}$ and let $\varpi \in R_0$ be a topologically nilpotent unit. Then $\mathfrak{p}$ is a closed point in $\operatorname{Spec} R_0 \setminus V((\varpi)) = \operatorname{Spec} R$, so $R_0/\mathfrak{p}$ is a 1-valuative order and hence its fraction field $R/\mathfrak{m}$ is a complete discrete valuation field. It remains to prove that the residue field is finite. For this, it suffices to show that the residue field of the local ring $R_0/\mathfrak{p}$ is finite since the integral closure of $R_0/\mathfrak{p}$ in $R/\mathfrak{m}$ is finite over $R_0/\mathfrak{p}$. Pick an adic surjection $A = \mathbb{Z}_p[[T_1, \dots, T_m]]\langle X_1, \dots, X_n\rangle \twoheadrightarrow R_0$ for some $m, n \in \mathbb{Z}_{\geq 0}$. The maximal ideal of $R_0/\mathfrak{p}$ is open and so corresponds to an open maximal ideal of A, and hence to a maximal ideal of $\mathbb{F}_p[X_1, \dots, X_n]$ in a way that preserves residue fields. It follows that $R_0/\mathfrak{p}$ is finite as desired. □

Lemma A.13. *Let $f : A \to B$ be a morphism of topologically finite type between Noetherian adic rings. Let I be an ideal of definition of A and assume that A/I is Jacobson. Let $J = IB$; this is an ideal of definition of B. If $\mathfrak{q} \in \operatorname{Spec} B \setminus V(J)$ is a closed point, then $\mathfrak{p} = f^{-1}(\mathfrak{q})$ is a closed point in $\operatorname{Spec} A \setminus V(I)$.*

Proof. The morphism $A \to B/\mathfrak{q}$ is topologically of finite type and $B/\mathfrak{q}$ is a 1-valuative order, so by [Abbes 2010, Proposition 1.11.2] $A \to B/\mathfrak{q}$ is finite. It is then easy to check that this forces $A/\mathfrak{p}$ to be a 1-valuative order as well, and hence $\mathfrak{p}$ to be closed in $\operatorname{Spec} A \setminus V(I)$ by [loc. cit., Proposition 1.11.8]. □

Corollary A.14. *Let $g : R \to S$ be a continuous morphism between two complete Tate rings with a ring of definition that is formally of finite type over $\mathbb{Z}_p$. Then g is topologically of finite type*[5] *and pulls back maximal ideals to maximal ideals.*

Proof. Choose a ring of definition R_0 for R which is formally of finite type over $\mathbb{Z}_p$. By [Huber 1993, Proposition 1.10] g is adic, and therefore $g(R_0)$ is contained in a ring of definition for S. Since any two rings of definition are contained in another, we can find a ring of definition S_0 for S such that $g(R_0) \subseteq S_0$ and S_0 contains a ring of definition S_1 which is formally of finite type over $\mathbb{Z}_p$. It follows from Lemma A.2 that S_0 is finite over S_1, and hence S_0 is also formally of finite type over $\mathbb{Z}_p$.

Let $\varpi \in R_0$ be a topologically nilpotent unit in R. Then $I = \varpi R_0$ and $J = g(\varpi)S_0$ are ideals of definition, and $R_0/I \to S_0/J$ is of finite type. Therefore $R_0 \to S_0$ is topologically of finite type; hence so is g. This proves the first assertion. The second then follows from Lemma A.13, since maximal ideals of R and S correspond to closed points in $\operatorname{Spec} R = \operatorname{Spec} R_0 \setminus V(I)$ and $\operatorname{Spec} S = \operatorname{Spec} S_0 \setminus V(J))$ respectively. □

Proposition A.15. *Let S be a complete Tate ring with a Noetherian ring of definition S_0 and a topologically nilpotent unit $\pi \in S_0$ such that $S_0/\pi S_0$ is Jacobson:*

(1) *Let A be a Noetherian adic ring with an ideal of definition I such that A/I is Jacobson. Let $f : A \to S$ be a continuous morphism such that the induced map $\operatorname{Spa}(S, S^\circ) \to \operatorname{Spa}(A, A)$ is an open immersion,*

[5] That is, g factors through a surjective, continuous and open morphism $R\langle X_1, \dots, X_n\rangle \to S$; see [Huber 1994, Lemma 3.3].

and let $\mathfrak{q}$ *be a maximal ideal of* S *with preimage* $\mathfrak{p} = f^{-1}(\mathfrak{q})$ *in* A. *Then the natural map* $A_{\mathfrak{p}} \to S_{\mathfrak{q}}$ *induces an isomorphism on completions* (*with respect to the maximal ideals*).

(2) *Let* R *be a complete Tate ring with a Noetherian ring of definition* R_0 *and a topologically nilpotent unit* $\varpi \in R_0$ *such that* R_0/ϖ *is Jacobson. Let* $h : R \to S$ *be a continuous morphism such that the induced map* $\mathrm{Spa}(S, S^\circ) \to \mathrm{Spa}(R, R^\circ)$ *is an open immersion, and let* $\mathfrak{q}'$ *be a maximal ideal of* S *with preimage* $\mathfrak{p}' = h^{-1}(\mathfrak{q}')$ *in* R. *Then the natural map* $R_{\mathfrak{p}'} \to S_{\mathfrak{q}'}$ *induces an isomorphism on completions* (*with respect to the maximal ideals*).

Proof. We prove part (1); the proof of part (2) is virtually identical. Since $S/\mathfrak{q}$ is a complete discretely valued field it defines a point v in $\mathrm{Spa}(S, S^\circ) \subseteq \mathrm{Spa}(A, A)$; let $U = \{|f_1|, \dots, |f_n| \le |g| \ne 0\}$ be a rational subdomain of $\mathrm{Spa}(A, A)$ which contains this point and is contained in $\mathrm{Spa}(S, S^\circ)$. Let

$$T = A[f_1/g, \dots, f_n/g] \subseteq A[1/g]$$

and let $\widehat{T}$ be the IT-adic completion of T. Since $\widehat{T}[1/g] = \mathcal{O}(U)$ we see that the valuation v extends to a valuation w on $\widehat{T}[1/g]$, and hence $\mathfrak{q}$ extends to a maximal ideal $\mathfrak{r} = \mathrm{Ker}\, w$ of $\widehat{T}[1/g]$. We will abuse notation and let $\mathfrak{r}$ denote its preimage in any of the rings T, $T[1/g]$ and $\widehat{T}$ as well; then $\mathfrak{r}$ is a closed point in $\mathrm{Spec}\,\widehat{T} \setminus V(I\widehat{T})$.

By [Abbes 2010, Proposition 1.12.18], the natural map $T_{\mathfrak{r}} \to \widehat{T}_{\mathfrak{r}}$ induces an isomorphism of completions. We claim that the natural maps $A_{\mathfrak{p}} \to T_{\mathfrak{r}}$ and $\widehat{T}_{\mathfrak{r}} \to \widehat{T}[1/g]_{\mathfrak{r}}$ are isomorphisms. For the second map this is clear (by the general fact that if B is any ring, $f \in B$, and $P \in \mathrm{Spec}\, B[1/f] \subseteq \mathrm{Spec}\, B$, then the natural map $B_P \to B[1/f]_P$ is an isomorphism). For the first map, we have natural maps $A_{\mathfrak{p}} \to T_{\mathfrak{r}} \to T[1/g]_{\mathfrak{r}} = A[1/g]_{\mathfrak{r}}$ and it is clear that the second map and the composite are isomorphisms, so the first map is an isomorphism as well. Summing up, we see that the natural map $A_{\mathfrak{p}} \to \mathcal{O}(U)_{\mathfrak{r}}$ induces an isomorphism on completions. By an almost identical argument, the natural map $S_{\mathfrak{q}} \to \mathcal{O}(U)_{\mathfrak{r}}$ induces an isomorphism on completions. It then follows that the natural map $A_{\mathfrak{p}} \to S_{\mathfrak{q}}$ induces an isomorphism on completions, as desired. □

Acknowledgments

This paper was inspired by [Andreatta et al. 2018], and Johansson wishes to thank Vincent Pilloni for some interesting discussions on that paper and David Hansen for innumerable and invaluable discussions on overconvergent cohomology and eigenvarieties. He would also like to thank Konstantin Ardakov for patiently answering several questions, and both authors would like to thank him for providing us with a proof of Proposition 3.3.4, and allowing us to include it here. We wish to thank John Bergdall and Kevin Buzzard for various conversations about the boundary of the eigencurve, as well as helpful comments on an earlier version of this paper. Finally, we wish to thank the anonymous referees for their careful reading and helpful comments. Johansson was supported by NSF grant DMS-1128155 during the main work on this paper, and by the Herchel Smith Foundation during the revision. Newton was supported by ERC Starting Grant 306326. Work on this project was also supported by the EPSRC Platform Grant EP/I019111.

References

[Abbes 2010] A. Abbes, *Éléments de géométrie rigide, I: Construction et étude géométrique des espaces rigides*, Progr. Math. **286**, Springer, 2010. MR Zbl

[Andreatta et al. 2016] F. Andreatta, A. Iovita, and V. Pilloni, "The adic, cuspidal, Hilbert eigenvarieties", *Res. Math. Sci.* **3** (2016), art. id. 34. MR Zbl

[Andreatta et al. 2018] F. Andreatta, A. Iovita, and V. Pilloni, "Le halo spectral", *Ann. Sci. Éc. Norm. Supér.* (4) **51**:3 (2018), 603–655. MR Zbl

[Ardakov and Wadsley 2013] K. Ardakov and S. Wadsley, "On irreducible representations of compact p-adic analytic groups", *Ann. of Math.* (2) **178**:2 (2013), 453–557. MR Zbl

[Ash and Stevens 2008] A. Ash and G. Stevens, "p-adic deformations of arithmetic cohomology", preprint, 2008, available at http://math.bu.edu/people/ghs/preprints/Ash-Stevens-02-08.pdf.

[Bellaïche 2010] J. Bellaïche, "Eigenvarieties and p-adic L-functions", preprint, 2010, available at http://people.brandeis.edu/~jbellaic/preprint/coursebook.pdf.

[Bellaïche and Chenevier 2009] J. Bellaïche and G. Chenevier, *Families of Galois representations and Selmer groups*, Astérisque **324**, Société Mathématique de France, Paris, 2009. MR Zbl

[Bergdall and Pollack 2016] J. Bergdall and R. Pollack, "Arithmetic properties of Fredholm series for p-adic modular forms", *Proc. Lond. Math. Soc.* (3) **113**:4 (2016), 419–444. MR Zbl

[Berkovich 1990] V. G. Berkovich, *Spectral theory and analytic geometry over non-Archimedean fields*, Math. Surveys and Monographs **33**, Amer. Math. Soc., Providence, RI, 1990. MR Zbl

[Bosch et al. 1984] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean analysis: a systematic approach to rigid analytic geometry*, Grundlehren der Math. Wissenschaften **261**, Springer, 1984. MR Zbl

[Breuil et al. 2017] C. Breuil, E. Hellmann, and B. Schraen, "Une interprétation modulaire de la variété trianguline", *Math. Ann.* **367**:3-4 (2017), 1587–1645. MR Zbl

[Buzzard 2004] K. Buzzard, "On p-adic families of automorphic forms", pp. 23–44 in *Modular curves and abelian varieties* (Bellaterra, Spain, 2002), edited by J. Cremona et al., Progr. Math. **224**, Birkhäuser, Basel, 2004. MR Zbl

[Buzzard 2007] K. Buzzard, "Eigenvarieties", pp. 59–120 in *L-functions and Galois representations* (Durham, 2004), edited by D. Burns et al., London Math. Soc. Lecture Note Ser. **320**, Cambridge Univ. Press, 2007. MR Zbl

[Buzzard and Kilford 2005] K. Buzzard and L. J. P. Kilford, "The 2-adic eigencurve at the boundary of weight space", *Compos. Math.* **141**:3 (2005), 605–619. MR Zbl

[Chenevier 2004] G. Chenevier, "Familles p-adiques de formes automorphes pour GL_n", *J. Reine Angew. Math.* **570** (2004), 143–217. MR Zbl

[Chenevier 2005] G. Chenevier, "Une correspondance de Jacquet–Langlands p-adique", *Duke Math. J.* **126**:1 (2005), 161–194. MR Zbl

[Chenevier 2014] G. Chenevier, "The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings", pp. 221–285 in *Automorphic forms and Galois representations, I* (Durham, 2011), edited by F. Diamond et al., London Math. Soc. Lecture Note Ser. **414**, Cambridge Univ. Press, 2014. MR Zbl

[Chojecki et al. 2017] P. Chojecki, D. Hansen, and C. Johansson, "Overconvergent modular forms and perfectoid Shimura curves", *Doc. Math.* **22** (2017), 191–262. MR Zbl

[Coleman 1997] R. F. Coleman, "p-adic Banach spaces and families of modular forms", *Invent. Math.* **127**:3 (1997), 417–479. MR Zbl

[Coleman and Mazur 1998] R. Coleman and B. Mazur, "The eigencurve", pp. 1–113 in *Galois representations in arithmetic algebraic geometry* (Durham, 1996), edited by A. J. Scholl and R. L. Taylor, London Math. Soc. Lecture Note Ser. **254**, Cambridge Univ. Press, 1998. MR Zbl

[Colmez 2010] P. Colmez, "Fonctions d'une variable p-adique", pp. 13–59 Astérisque **330**, Société Mathématique de France, Paris, 2010. MR Zbl

[Conrad 1999] B. Conrad, "Irreducible components of rigid spaces", *Ann. Inst. Fourier* (*Grenoble*) **49**:2 (1999), 473–541. MR Zbl

[Dixon et al. 1999] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p-groups*, 2nd ed., Cambridge Studies in Adv. Math. **61**, Cambridge Univ. Press, 1999. MR Zbl

[EGA IV_2 1965] A. Grothendieck, "Eléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, II", *Inst. Hautes Études Sci. Publ. Math.* **24** (1965), 5–231. MR Zbl

[EGA IV_3 1966] A. Grothendieck, "Eléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, III", *Inst. Hautes Études Sci. Publ. Math.* **28** (1966), 5–255. MR Zbl

[Gulotta 2018] D. R. Gulotta, *Equidimensional adic eigenvarietes for groups with discrete series*, Ph.D. thesis, Columbia University, 2018, available at https://search.proquest.com/docview/2031119725.

[Hansen 2015] D. Hansen, "Iwasawa theory of overconvergent modular forms, I: Critical p-adic L-functions", preprint, 2015. arXiv

[Hansen 2017] D. Hansen, "Universal eigenvarieties, trianguline Galois representations, and p-adic Langlands functoriality", *J. Reine Angew. Math.* **730** (2017), 1–64. MR Zbl

[Hansen and Johansson $\geq$ 2019] D. Hansen and C. Johansson, "Completed and overconvergent cohomology", in preparation.

[Huber 1993] R. Huber, "Continuous valuations", *Math. Z.* **212**:3 (1993), 455–477. MR Zbl

[Huber 1994] R. Huber, "A generalization of formal schemes and rigid analytic varieties", *Math. Z.* **217**:4 (1994), 513–551. MR Zbl

[Huber 1996] R. Huber, *Étale cohomology of rigid analytic varieties and adic spaces*, Aspects of Math. **E30**, Vieweg, Wiesbaden, 1996. MR Zbl

[Johansson and Newton 2017] C. Johansson and J. Newton, "Irreducible components of extended eigenvarieties and interpolating Langlands functoriality", 2017. To appear in *Math. Res. Lett.* arXiv

[Johansson and Newton 2018] C. Johansson and J. Newton, "Parallel weight 2 points on Hilbert modular eigenvarieties and the parity conjecture", preprint, 2018. arXiv

[Kedlaya and Liu 2015] K. S. Kedlaya and R. Liu, *Relative p-adic Hodge theory: foundations*, Astérisque **371**, Société Mathématique de France, Paris, 2015. MR Zbl arXiv

[Liu et al. 2017] R. Liu, D. Wan, and L. Xiao, "The eigencurve over the boundary of weight space", *Duke Math. J.* **166**:9 (2017), 1739–1787. MR Zbl

[Loeffler 2011] D. Loeffler, "Overconvergent algebraic automorphic forms", *Proc. Lond. Math. Soc.* (3) **102**:2 (2011), 193–228. MR Zbl

[Marot 1975] J. Marot, "Sur les anneaux universellement japonais", *Bull. Soc. Math. France* **103**:1 (1975), 103–111. MR Zbl

[Neukirch 1999] J. Neukirch, *Algebraic number theory*, Grundlehren der Math. Wissenschaften **322**, Springer, 1999. MR Zbl

[Pottharst and Xiao 2014] J. Pottharst and L. Xiao, "On the parity conjecture in finite-slope families", preprint, 2014. arXiv

[Schneider and Teitelbaum 2003] P. Schneider and J. Teitelbaum, "Algebras of p-adic distributions and admissible representations", *Invent. Math.* **153**:1 (2003), 145–196. MR Zbl

[Scholze 2015] P. Scholze, "On torsion in the cohomology of locally symmetric varieties", *Ann. of Math.* (2) **182**:3 (2015), 945–1066. MR Zbl

[Serre 1962] J.-P. Serre, "Endomorphismes complètement continus des espaces de Banach p-adiques", *Inst. Hautes Études Sci. Publ. Math.* **12** (1962), 69–85. MR Zbl

[Stevens 1994] G. Stevens, "Rigid analytic modular symbols", preprint, 1994, available at http://math.bu.edu/people/ghs/research.d/RigidSymbs.pdf.

[Urban 2011] E. Urban, "Eigenvarieties for reductive groups", *Ann. of Math.* (2) **174**:3 (2011), 1685–1784. MR Zbl

[Valabrega 1975] P. Valabrega, "On the excellent property for power series rings over polynomial rings", *J. Math. Kyoto Univ.* **15**:2 (1975), 387–395. MR Zbl

[Valabrega 1976] P. Valabrega, "A few theorems on completion of excellent rings", *Nagoya Math. J.* **61** (1976), 127–133. MR Zbl

[Weibel 1994] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Adv. Math. **38**, Cambridge Univ. Press, 1994. MR Zbl

[Xiang 2012] Z. Xiang, "A construction of the full eigenvariety of a reductive group", *J. Number Theory* **132**:5 (2012), 938–952. MR Zbl

Communicated by Bjorn Poonen
Received 2017-06-15 Revised 2018-06-28 Accepted 2018-09-25

chrjohv@chalmers.se *Department of Mathematical Sciences, Chalmers University of Technology and the University of Gothenburg, Gothenburg, Sweden*

j.newton@kcl.ac.uk *Department of Mathematics, King's College London, London, United Kingdom*

ALGEBRA AND NUMBER THEORY 13:1 (2019)
dx.doi.org/10.2140/ant.2019.13.159

A tubular variant of Runge's method in all dimensions, with applications to integral points on Siegel modular varieties

Samuel Le Fourn

Runge's method is a tool to figure out integral points on algebraic curves effectively in terms of height. This method has been generalized to varieties of any dimension, but unfortunately the conditions needed to apply it are often too restrictive. We provide a further generalization intended to be more flexible while still effective, and exemplify its applicability by giving finiteness results for integral points on some Siegel modular varieties. As a special case, we obtain an explicit finiteness result for integral points on the Siegel modular variety $A_2(2)$.

Introduction

One of the major motivations of number theory is the description of rational or integral solutions of diophantine equations, which from a geometric perspective amounts to understanding the behavior of rational or integral points on algebraic varieties. In dimension one, several fundamental results provide a good overview of the situation, including the famous Faltings' theorem (for genus ≥ 2 and algebraic points) or Siegel's theorem (for integral points and a function with at least three poles). Nevertheless, the quest for general *effectivity* (meaning a bound on the height on these points, or hopefully complete

The author is supported by the European Union's Horizon 2020 research and programme under the Marie Sklodowska-Curie grant agreement No 793646, titled *LowDegModCurve*.
MSC2010: primary 11G35; secondary 11G10, 14G05, 14G35.
Keywords: Runge's method, integral points on varieties, abelian varieties.

determination of the points) is still ongoing, and effective methods are quite different from these two powerful theoretical theorems.

On the other hand, there is major interest in the study of algebraic torsion points of elliptic curves, or more generally abelian varieties, defined over a given number field. In many situations, it amounts to understanding the algebraic points of so-called *modular spaces*, parametrizing isomorphism classes of abelian varieties with additional datum. For modular curves (i.e., modular spaces of elliptic curves), the existing techniques are numerous and far-reaching (for example, with Merel's uniform boundedness theorem [1996] or Mazur's isogeny theorem [1977]), but the world of higher-dimensional abelian varieties is far less known.

We thus focus in this paper on a method for integral points on curves called *Runge's method*, and its generalizations to algebraic varieties and applications for Siegel modular varieties. This introduction is twofold: first, we give the guiding principles behind our approach and second, we flesh out the precise structure of the article and indicate where to find the details for each claim made.

Runge's method for algebraic varieties. On a smooth algebraic projective curve C over a number field K, Runge's method proceeds as follows. Let $\phi \in K(C)$ be a nonconstant rational function on C. For any finite extension L/K, we denote by M_L the set of places of L (and by M_L^∞ the archimedean ones). For S_L, a finite set of places of L containing M_L^∞, we denote the ring of S_L-integers of L by

$$\mathcal{O}_{L,S_L} = \{x \in L : |x|_v \leq 1 \text{ for all } v \in M_L \backslash S_L\}.$$

Now, let r_L be the number of orbits of poles of ϕ under the action of $\mathrm{Gal}(\bar{L}/L)$. The *Runge condition* on a pair (L, S_L) is the inequality

$$|S_L| < r_L. \tag{1}$$

Then, Bombieri's generalization [Bombieri and Gubler 2006, paragraph 9.6.5 and Theorem 9.6.6] of Runge's old theorem [1887] states that given such C and ϕ, there is an *absolute* bound B such that for every pair (L, S_L) satisfying the Runge condition and every point $P \in C(L)$ such that $\phi(P) \in \mathcal{O}_{L,S_L}$,

$$h(\phi(P)) \leq B,$$

where h is the Weil height. In short, as long as the point $\phi(P)$ has few nonintegrality places (the exact condition being (1)), there is an absolute bound on the height of $\phi(P)$. When applicable, this method has two important assets: it gives good bounds and is uniform in the pairs (L, S_L), which for example is not true for Baker's method [Bilu 1995].

Our first goal was to transpose the ideas for Runge's method on curves to higher-dimensional varieties. First, let us recall a previous generalization of Bombieri's theorem in higher dimensions obtained by Levin [2008, Theorem 4] under a simplified form. On a projective smooth variety X, the analogues of poles of ϕ are effective divisors $D_1, \ldots, D_r$. We have to fix a smooth integral model $\mathcal{X}$ of X on $\mathcal{O}_K$, and denote by $\mathcal{D}_1, \ldots, \mathcal{D}_r$ the Zariski closures of the divisors in this model, of union $\mathcal{D}$, so our integral points here are the points of $(\mathcal{X} \backslash \mathcal{D})(\mathcal{O}_{L,S_L})$. There are two major changes in higher dimension. Firstly, the divisors have to be ample (or at least big) to obtain finiteness results (this was automatic for dimension 1). Secondly, instead of the condition $|S_L| < r$ as for curves, the *higher-dimensional Runge condition* is

$$m|S_L| < r, \tag{2}$$

where m is the smallest number such that any $(m+1)$ divisors amongst $D_1, \ldots, D_r$ have empty common intersection. Levin's theorem states in particular that when the divisors are ample,

$$\left(\bigcup_{\substack{(L,S_L) \\ m|S_L|<r}} (\mathcal{X} \backslash \mathcal{D})(\mathcal{O}_{L,S_L}) \right) \text{ is (effectively) finite.}$$

The issue with (2) is that the maximal number $|S_L|$ satisfying this condition is lowered by m, since the ample (or big) hypothesis tends to give a lower bound on m, condition (2) is impossible to satisfy (remember that S_L contains archimedean places, so $|S_L| \geq [L:\mathbb{Q}]/2$). This was the initial motivation for a generalization of this theorem, called "tubular Runge's theorem", designed to be more flexible in terms of the Runge condition. Let us explain its principle below.

In addition to X and $D_1, \ldots, D_r$, we fix a closed subvariety Y of X which is meant to be "where the divisors $D_1, \ldots, D_r$ intersect a lot". More precisely, let m_Y be the smallest number such that for any $(m_Y + 1)$ distinct divisors amongst $D_1, \ldots, D_r$, their common intersection is included in Y. In particular, $m_Y \leq m$, and the goal is to have m_Y as small as possible without asking Y to be too large. Now, we fix a "tubular neighborhood" of Y, which is the datum of a family $\mathcal{V} = (V_v)_v$ where v goes through the places v of $\overline{K}$, every V_v is a neighborhood of Y in the v-adic topology, and this family is uniformly not too small in some sense. As the main example, if $\mathcal{Y}$ is the Zariski closure of Y in $\mathcal{X}$, we can define at a finite place v the neighborhood V_v to be the set of points of $\mathcal{X}(\overline{K_v})$ reducing in $\mathcal{Y}$ modulo v. A point $P \in X(\overline{K})$ does *not* belong to $\mathcal{V}$ if $P \notin V_v$ for every place v of $\overline{K}$, and intuitively, this means that P is v-adically far away from Y for *every* place v of $\overline{K}$. Now, assume our integral points are *not* in $\mathcal{V}$. It implies that at most m_Y divisors amongst $D_1, \ldots, D_r$ can be v-adically close to them, hence using the same principles of proof as Levin, this gives the *tubular Runge condition*

$$m_Y |S_L| < r. \tag{3}$$

With this additional data, one can now sketch our tubular Runge's theorem.

Theorem (simplified version of the "tubular Runge's theorem" (Theorem 5.1)). *For X, $\mathcal{X}$, $D_1, \ldots, D_r$, Y, m_Y and a tubular neighborhood $\mathcal{V}$ of Y as in the paragraph above, let $(\mathcal{X} \backslash \mathcal{D})(\mathcal{O}_{L,S_L}) \backslash \mathcal{V}$ be the set of points of $(\mathcal{X} \backslash \mathcal{D})(\mathcal{O}_{L,S_L})$ which do not belong to $\mathcal{V}$. Then, if $D_1, \ldots, D_r$ are ample, for every such tubular neighborhood, the set*

$$\left(\bigcup_{\substack{(L,S_L) \\ m_Y|S_L|<r}} (\mathcal{X} \backslash \mathcal{D})(\mathcal{O}_{L,S_L}) \backslash \mathcal{V} \right) \textit{ is finite,}$$

and bounded in terms of some auxiliary height.

As the implicit bound on the height is parametrized by the tubular neighborhood $\mathcal{V}$, this theorem can be seen as a *concentration result* rather than a finiteness one; essentially, it states that the points of $(\mathcal{X}\backslash\mathcal{D})(\mathcal{O}_{L,S_L})$ concentrate near the closed subset Y. As such, we have compared it to theorems of [Corvaja et al. 2009], notably Autissier's theorem and the CLZ theorem, in Section 5 (in particular, our version is made to be effective, whereas these results are based on Schmidt's subspace theorem, of which no effective proof is known yet). On the other hand, there is an interesting (and genuine finiteness result) variant only using the tubular neighborhood at finite places: under all above assumptions, we also have finiteness of the union of all the $(\mathcal{X}\backslash\mathcal{D})(\mathcal{O}_{L,S_L})$ minus all the points reducing in Y at some finite place, where the pairs (L, S_L) satisfy the *mixed tubular Runge condition*

$$m|M_L^\infty| + m_Y|S_L\backslash M_L^\infty| < r, \tag{4}$$

and this will be straightforward given the proof of the theorem.

In the second part of our paper, we apply the method to Siegel modular varieties, both as a proof of principle and because integral points on these varieties are not very well understood, apart from the Shafarevich conjecture proved by Faltings. As we will see below, this is also a case where a candidate for Y presents itself, thus giving tubular neighborhoods a natural interpretation.

For $n \geq 2$, the variety denoted by $A_2(n)$ is the variety over $\mathbb{Q}(\zeta_n)$ parametrizing triples (A, λ, α_n) where (A, λ) is a principally polarized abelian variety of dimension 2 and α_n is a symplectic level n structure on (A, λ). It is a quasiprojective algebraic variety of dimension 3, and its Satake compactification (which is a projective algebraic variety) is denoted by $A_2(n)^S$, the boundary being $\partial A_2(n) = A_2(n)^S\backslash A_2(n)$. The extension of scalars $A_2(n)_{\mathbb{C}}$ is the quotient of the half-superior Siegel space $\mathcal{H}_2$ by the natural action of the symplectic congruence subgroup $\Gamma_2(n)$ of $\mathrm{Sp}_4(\mathbb{Z})$ made up with the matrices congruent to the identity modulo n. Now, we consider some divisors ($n^4/2+2$ of them) defined by the vanishing of some modular forms, specifically *theta functions*. One finds that they intersect a lot on the boundary $\partial A_2(n)$ (m comparable to n^4), but when we fix $Y = \partial A_2(n)$, we get $m_Y \leq (n^2-3)$ hence giving the *tubular Runge condition*

$$(n^2-3)|S_L| < \tfrac{1}{2}n^4 + 2.$$

The application of our tubular Runge's theorem gives for every even $n \geq 2$ a finiteness result for the integral points for these divisors and some tubular neighborhoods associated to potentially bad reduction for the finite places; this is Theorem 7.12. In the special case $n = 2$, we made this result completely explicit in Theorem 8.2. A simplified case of this theorem (using (4)) is the following result.

Theorem (Theorem 8.2, simplified case). *Let K be either $\mathbb{Q}$ or a quadratic imaginary field.*

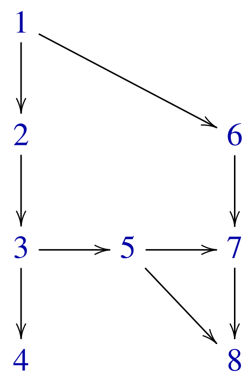
Let A be a principally polarized abelian surface defined over K, whose full 2-torsion is also defined over K and having potentially good reduction at all finite places of K.

Then, if the semistable reduction of A is a product of elliptic curves at most at 3 finite places of K, we have the explicit bound

$$h_{\mathcal{F}}(A) \leq 828,$$

where $h_{\mathcal{F}}$ is the stable Faltings height. In particular, there are only finitely many such abelian surfaces.

Let us finally explain the structure of the paper.



Section 1 is devoted to the notations used throughout the paper, including heights, M_K-constants and bounded sets. We advise the reader to pay particular attention to its reading as it introduces notations which are ubiquitous in the rest of the paper. Section 2 is where the exact definition and basic properties of tubular neighborhoods are given. In Section 3, we prove the key result for the tubular Runge's theorem (Proposition 3.1), essentially relying on a well-applied Nullstellensatz. In Section 4, we reprove Bombieri's theorem for curves with Bilu's idea, as it is not yet published to our knowledge (although this is exactly the principle behind Runge's method in [Bilu and Parent 2011] for example). Finally, we prove and discuss our tubular Runge's theorem (Theorem 5.1) in Section 5.

For the applications to Siegel modular varieties, Section 6 gathers the necessary notations and reminders on these varieties (Section 6A), their integral models and their properties (Section 6B) and the key notion of theta divisors on abelian varieties and their link with classical theta functions (Section 6C). The theta functions are essential because they define the divisors we use in our applications of the tubular Runge's theorem.

In Section 7, we focus on the case of abelian surfaces (the one we are interested in), especially regarding the behavior of theta divisors (Section 7A) and state in Section 7B the applications of our tubular Runge's theorem for the varieties $A_2(n)^S$ and the divisors mentioned above (Theorems 7.11 and 7.12).

Finally, in Section 8, we make explicit Theorem 7.11 by computations on the ten fourth powers of even characteristic theta constants. To do this, the places need to be split into three categories. The finite places not above 2 are treated by the theory of algebraic theta functions in Section 8A, the archimedean places by estimates of Fourier expansions in Section 8B and the finite places above 2 (the hardest case) by the theory of Igusa invariants and with polynomials built from our ten theta constants in Section 8C. The final estimates are given as Theorem 8.2 in Section 8D, both in terms of a given embedding of $A_2(2)$ and in terms of Faltings height.

The main results of this paper have been announced in the recently published note [Le Fourn 2017], and apart from Section 8 and some improvements can be found in the author's thesis manuscript [Le Fourn 2015] (both in French).

1. Notations and preliminary notions

The following notations are classical and given below for clarity. They will be used throughout the paper.

• K is a number field, M_K and M_K^∞ are the set of places and archimedean places of K, respectively. We also denote by $M_{\overline{K}}$ the set of places of $\overline{K}$.

• $|\cdot|_\infty$ is the usual absolute value on $\mathbb{Q}$, and $|\cdot|_p$ is the place associated to p prime, whose absolute value is normalized by

$$|x|_p = p^{-\operatorname{ord}_p(x)},$$

where $\operatorname{ord}_p(x)$ is the unique integer such that $x = p^{\operatorname{ord}_p(x)}\frac{a}{b}$ with $p \nmid ab$ (by convention, $|0|_p = 0$). Similarly, $|\cdot|_v$ is the absolute value on K associated to $v \in M_K$, normalized to extend $|\cdot|_{v_0}$ when v is above $v_0 \in M_{\mathbb{Q}}$, and the local degree is $n_v = [K_v : \mathbb{Q}_{v_0}]$. For every $x \in K^*$, one has the classical product formula

$$\prod_{v \in M_K} |x|_v^{n_v} = 1.$$

When v comes from a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we indifferently write $|\cdot|_v$ and $|\cdot|_{\mathfrak{p}}$.

• For any place v of K, one defines the sup norm on K^{n+1} by

$$\|(x_0, \ldots, x_n)\|_v = \max_{0 \le i \le n} |x_i|_v.$$

• Every set of places $S \subset M_K$ considered is finite and contains M_K^∞. The ring of S-integers is

$$\mathcal{O}_{K,S} = \{x \in K : |x|_v \le 1 \text{ for every } v \in M_K \backslash S\}.$$

• For every $P \in \mathbb{P}^n(K)$, we denote by $x_P = (x_{P,0}, \ldots, x_{P,n}) \in K^{n+1}$ any possible choice of projective coordinates for P, this choice being of course fixed for consistency when used in a formula or a proof. The logarithmic Weil height of P is defined by

$$h(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v \log\|x_P\|_v, \tag{1-1}$$

this does not depend on the choice of x_P nor on the number field, and satisfies the Northcott property.

• For every $n \ge 1$ and every $i \in \{0, \ldots, n\}$, the i-th coordinate open subset U_i of $\mathbb{P}^n$ is the affine subset defined as

$$U_i = \{(x_0 : \cdots : x_n) \mid x_i \neq 0\}. \tag{1-2}$$

The normalization function $\varphi_i : U_i \to \mathbb{A}^{n+1}$ is then defined by

$$\varphi_i(x_0 : \cdots : x_n) = \left(\frac{x_0}{x_i}, \ldots, 1, \ldots \frac{x_n}{x_i}\right). \tag{1-3}$$

For most of our results, we need to formalize the notion that some families of sets indexed by the places $v \in M_K$ are "uniformly bounded". To this end, we recall some classical definitions (see [Bombieri and Gubler 2006, §2.6]).

Definition 1.1 (M_K-constants and M_K-bounded sets). • An M_K*-constant* is a family $\mathcal{C} = (c_v)_{v \in M_K}$ of real numbers such that $c_v = 0$ except for a finite number of places $v \in M_K$. The set of M_K-constants is stable by finite sum and finite maximum on each coordinate, a fact which we will often use without further mention.

• Let L/K be a finite extension. For an M_K-constant $(c_v)_{v \in M_K}$, we define (with abuse of notation) an M_L-constant $(c_w)_{w \in M_L}$ by $c_w := c_v$ if $w \mid v$. Conversely, if $(c_w)_{w \in M_L}$ is an M_L-constant, we define (again with abuse of notation) $(c_v)_{v \in M_K}$ by $c_v := \max_{w \mid v} c_w$, and get in both cases the inequality

$$\frac{1}{[L:\mathbb{Q}]} \sum_{w \in M_L} n_w c_w \leq \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v c_v. \tag{1-4}$$

• If U is an affine variety over K and $E \subset U(\overline{K}) \times M_{\overline{K}}$, a regular function $f \in \overline{K}[U]$ is M_K*-bounded on* E if there is a M_K-constant $\mathcal{C} = (c_v)_{v \in M_K}$ such that for every $(P, w) \in E$ with w above v in M_K,

$$\log |f(P)|_w \leq c_v.$$

• An M_K*-bounded subset of* U is, by abuse of definition, a subset E of $U(\overline{K}) \times M_{\overline{K}}$ such that every regular function $f \in \overline{K}[U]$ is M_K-bounded on E.

Remark 1.2. (a) In the projective space $\mathbb{P}^n_K$, for every $i \in \{0, \ldots, n\}$, consider the set

$$E_i = \{(P, w) \in \mathbb{P}^n(\overline{K}) \times M_{\overline{K}} : |x_{P,i}|_w = \|x_P\|_w\}. \tag{1-5}$$

The regular functions x_j/x_i $(j \neq i)$ on $\overline{K}[U_i]$ (notation (1-2)) are trivially M_K-bounded (by the zero M_K-constant) on E_i, hence E_i is M_K-bounded in U_i. Notice that the E_i cover $\mathbb{P}^n(\overline{K}) \times M_{\overline{K}}$.

(b) With notations (1-1), (1-2) and (1-3), for a subset E of $U_i(\overline{K})$, if the coordinate functions of U_i are M_K-bounded on $E \times M_{\overline{K}}$, the height $h \circ \varphi_i$ is straightforwardly bounded on E in terms of the involved M_K-constants. This simple observation will be the basis of our finiteness arguments.

The following lemma allows us to split M_K-bounded sets in an affine cover.

Lemma 1.3. *Let U be an affine variety and E an M_K-bounded set. If $(U_j)_{j \in J}$ is a finite affine open cover of U, there exists a cover $(E_j)_{j \in J}$ of E such that every E_j is M_K-bounded in U_j.*

Proof. This is Lemma 2.2.10 together with Remark 2.6.12 of [Bombieri and Gubler 2006]. □

Let us now recall some notions about integral points on schemes and varieties.

For a finite extension L of K, a point $P \in \mathbb{P}^n(L)$ and a nonzero prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ of residue field $k(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$, the point P extends to a unique morphism $\operatorname{Spec} \mathcal{O}_{L,\mathfrak{P}} \to \mathbb{P}^n_{\mathcal{O}_K}$, and the image of its special point is *the reduction of P modulo* $\mathfrak{P}$, denoted by $P_{\mathfrak{P}} \in \mathbb{P}^n(k(\mathfrak{P}))$. More explicitly, after normalization of the coordinates x_P of P so that they all belong to $\mathcal{O}_{L,\mathfrak{P}}$ and one of them to $\mathcal{O}^*_{L,\mathfrak{P}}$, one has

$$P_{\mathfrak{P}} = (x_{P,0} \bmod \mathfrak{P} : \cdots : x_{P,n} \bmod \mathfrak{P}) \in \mathbb{P}^n_{k(\mathfrak{P})}. \tag{1-6}$$

The following (easy) proposition expresses scheme-theoretic reduction in terms of functions (there will be another in Proposition 3.4). We write it below as it is the inspiration behind the notion of tubular neighborhood in Section 2.

Proposition 1.4. *Let S be a finite set of places of K containing M_K^∞, and $\mathcal{X}$ be a projective scheme on $\mathcal{O}_{K,S}$, seen as a closed subscheme of $\mathbb{P}^n_{\mathcal{O}_{K,S}}$.*

Let $\mathcal{Y}$ be a closed sub-$\mathcal{O}_{K,S}$-scheme of $\mathcal{X}$.

Consider $g_1, \ldots, g_s \in \mathcal{O}_{K,S}[X_0, \ldots, X_n]$ homogeneous generators of the ideal of definition of $\mathcal{Y}$ in $\mathbb{P}^n_{\mathcal{O}_{K,S_0}}$. For every nonzero prime $\mathfrak{P}$ of $\mathcal{O}_L$ not above S and every point $P \in \mathcal{X}(L)$, the reduction $P_\mathfrak{P}$ belongs to $\mathcal{Y}_\mathfrak{p}(k(\mathfrak{P}))$ (with $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$) if and only if $\forall j \in \{1, \ldots, s\}$

$$|g_j(x_P)|_\mathfrak{P} < \|x_P\|_\mathfrak{P}^{\deg g_j}. \tag{1-7}$$

Proof. For every $j \in \{1, \ldots, s\}$, by homogeneity of g_j, for a choice x_P of coordinates for P belonging to $\mathcal{O}_{L,\mathfrak{P}}$ with one of them in $\mathcal{O}^*_{L,\mathfrak{P}}$, the inequality (1-7) amounts to

$$g_j(x_{P,0}, \ldots, x_{P,n}) = 0 \bmod \mathfrak{P}.$$

On the other hand, the reduction of P modulo $\mathfrak{P}$ belongs to $\mathcal{Y}_\mathfrak{p}(\overline{k(\mathfrak{P})})$ if and only if its coordinates satisfy the equations defining $\mathcal{Y}_\mathfrak{p}$ in $X_\mathfrak{p}$, but these are exactly the equations $g_1, \ldots, g_s$ modulo $\mathfrak{p}$. This remark immediately gives the proposition by (1-6). □

2. Definition and properties of tubular neighborhoods

The explicit expression (1-7) is the motivation for our definition of *tubular neighborhood*, at the core of our results. This definition is meant to be used by exclusion; with the same notations as Proposition 1.4, we want to say that a point $P \in X(L)$ is *not* in some tubular neighborhood of $\mathcal{Y}$ if it *never* reduces in $\mathcal{Y}$, whatever the prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ is.

The main interest of this notion is that it provides us with a convenient alternative to the reduction assumption for the places in S (which are the places where the reduction is not well defined, including the archimedean places), and also allows us to loosen up this reduction hypothesis in a nice fashion. Moreover, as the definition is function-theoretic, we only need to consider the varieties over a base field, keeping in mind that Proposition 1.4 makes the link with reduction at finite places.

Definition 2.1 (tubular neighborhood). Let X be a projective variety over K and Y be a closed K-subscheme of X.

We choose an embedding $X \subset \mathbb{P}^n_K$, a set of homogeneous generators $g_1, \ldots, g_s$ in $K[X_0, \ldots, X_n]$ of the homogeneous ideal defining Y in $\mathbb{P}^n$ and an M_K-constant $\mathcal{C} = (c_v)_{v \in M_K}$.

The *tubular neighborhood of Y in X associated to $\mathcal{C}$ and $g_1, \ldots, g_s$* (the embedding made implicit) is the family $\mathcal{V} = (V_w)_{w \in M_{\overline{K}}}$ of subsets of $X(\overline{K})$ defined as follows.

For every $w \in M_{\overline{K}}$ above some $v \in M_K$, V_w is the set of points $P \in X(\overline{K})$ such that, $\forall j \in \{1, \ldots, s\}$,

$$\log|g_j(x_P)|_w < \deg(g_j) \cdot \log\|x_P\|_w + c_v. \tag{2-1}$$

As we said before, this definition will be ultimately used by exclusion:

Definition 2.2. Let X be a projective variety over K and Y be a closed K-subscheme of X.

For any tubular neighborhood $\mathcal{V} = (V_w)_{w \in M_{\overline{K}}}$ of Y, we say that a point $P \in X(\overline{K})$ *does not belong to* $\mathcal{V}$ (and we denote it by $P \notin \mathcal{V}$) if, $\forall w \in M_{\overline{K}}$,

$$P \notin V_w.$$

Remark 2.3. (a) A tubular neighborhood of Y can also be seen as a family of open subsets defined by bounding strictly a global height function relative to Y coming from arithmetic distance functions (see [Vojta 1987], paragraph 2.5 or the original article [Silverman 1987] for more details on arithmetic distance functions). In particular, functoriality of global height functions (Theorem 2.1(h) of [Vojta 1987] for example) implies that if one fixes a second embedding $X \subset \mathbb{P}^m_K$, any tubular neighborhood of Y defined using this embedding can be put between two tubular neighborhoods defined using the original embedding, and conversely. The notion of tubular neighborhood is thus essentially independent of the choice of embedding (which is there to make things as explicit as needed).

(b) Comparing (1-7) and (2-1), for the M_K-constant $\mathcal{C} = 0$ and with the notations of Proposition 1.4, at the finite places w not above S, the tubular neighborhood V_w is exactly the set of points $P \in X(\overline{K})$ reducing in $\mathcal{Y}$ modulo w.

(c) If Y is an ample divisor of X and $\mathcal{V}$ is a tubular neighborhood of Y, one easily sees that if $P \notin \mathcal{V}$ then $h(\psi(P))$ is bounded for some embedding ψ associated to Y, from which we get the finiteness of the set of points P of bounded degree outside of $\mathcal{V}$. This illustrates why such an assumption is only really relevant when Y is of small dimension.

Example 2.4. We have drawn in Figures 1, 2 and 3 three different pictures of tubular neighborhoods in $\mathbb{P}^2(\mathbb{R})$, at the usual archimedean norm. The coordinates are x, y, z, the affine open subset U_z defined by $z \neq 0$, and E_x, E_y, E_z the respective sets such that $|x|, |y|, |z| = \max(|x|, |y|, |z|)$. These different tubular neighborhoods are drawn in U_z, and the contribution of the different parts E_x, E_y and E_z is made clear.

3. Key results

We will now prove the key result for Runge's method, as a consequence of the Nullstellensatz. We only use the projective case in the rest of the paper but the affine case is both necessary for its proof and enlightening for the method we use.

Proposition 3.1 (key proposition). (a) (*Affine version*) *Let U be an affine variety over K, Y a closed subset of U, $g_1, \dots, g_r \in K[U]$ whose set of common zeroes is Y and $h_1, \dots, h_s \in K[U]$ all vanishing on Y. For every M_K-bounded set E of U and every M_K-constant $\mathcal{C}_0$, there is an M_K-constant $\mathcal{C}$ such that for every $(P, w) \in E$ with w above $v \in M_K$, one has the following dichotomy*:

$$\max_{1 \le \ell \le r} \log|g_\ell(P)|_w \ge c_v \quad \textit{or} \quad \max_{1 \le j \le s} \log|h_j(P)|_w < c_{0,v}. \tag{3-1}$$

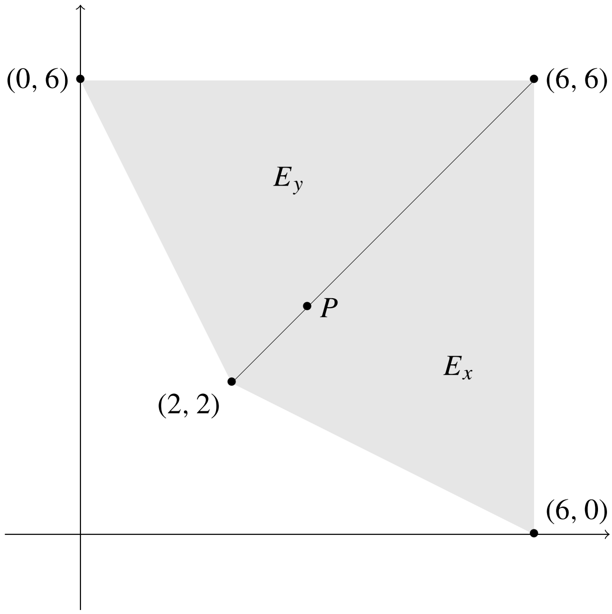


Figure 1. Tubular neighborhood of the point $P = (3:3:1)$ associated to the inequality $\max(|x-3y, y-3z|) < \frac{1}{2}\max(|x|, |y|, |z|)$.

(b) (*Projective version*) *Let X be a normal projective variety over K and $\phi_1, \dots, \phi_r \in K(X)$. Let Y be the closed subset of X defined as the intersection of the supports of the* (*Weil*) *divisors of poles of the ϕ_i. For every tubular neighborhood $\mathcal{V}$ of Y* (*Definition 2.1*), *there is an M_K-constant $\mathcal{C}$ depending on $\mathcal{V}$ such that for every $w \in M_{\overline{K}}$* (*above $v \in M_K$*) *and every $P \in X(\overline{K})$,*

$$\min_{1 \le \ell \le r} \log|\phi_\ell(P)|_w \le c_v \quad \textit{or} \quad P \in V_w. \tag{3-2}$$

This result has an immediate corollary when $Y = \varnothing$:

Corollary 3.2 [Levin 2008, Lemma 5]. *Let X be a normal projective variety over K and $\phi_1, \dots, \phi_r \in K(X)$ having globally no common pole. Then, there is an M_K-constant $\mathcal{C}$ such that for every $w \in M_{\overline{K}}$* (*above $v \in M_K$*) *and every $P \in X(\overline{K})$,*

$$\min_{1 \le \ell \le r} \log|\phi_\ell(P)|_w \le c_v. \tag{3-3}$$

Remark 3.3. (a) As will become clear in the proof, part (b) is actually part (a) applied to a good cover of X by M_K-bounded subsets of affine open subsets of X (inspired by the natural example of Remark 1.2(a)).

(b) Besides the fact that the results must be uniform in the places (hence the M_K-constants), the principle of (a) and (b) is simple. For (a), we would like to say that if the first part of the dichotomy is not satisfied, the point P must be close to each set of zeroes of the g_ℓ hence to their intersection Y. Consequently, the functions vanishing on Y must be small at P (second part of the dichotomy). This is not immediately true yet (take for example functions vanishing respectively on one hyperbola and one of its axes on the

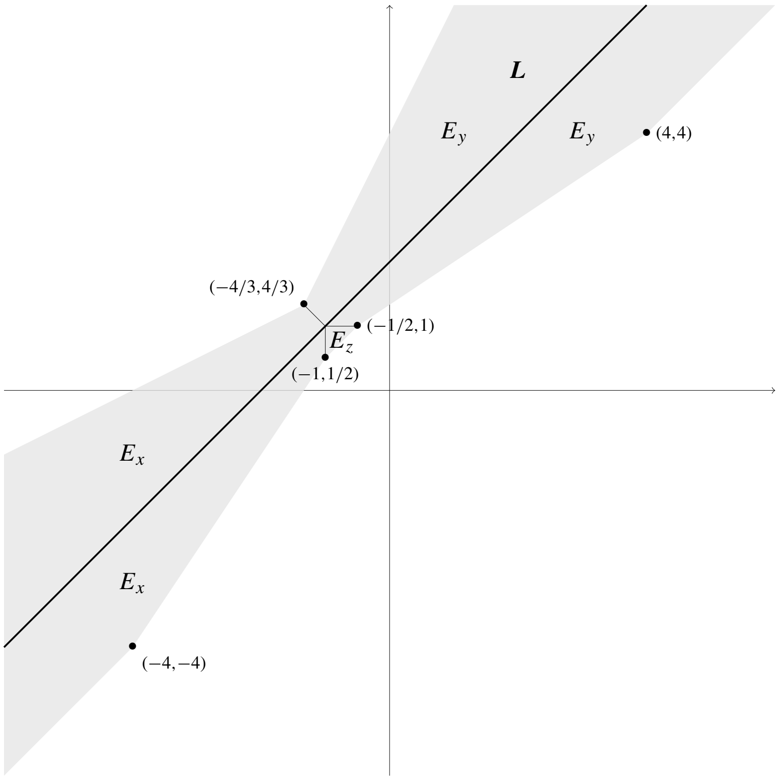


Figure 2. Tubular neighborhood of the line $D : y - x + 2z = 0$ associated to the inequality $\max(|x - y + 2z|) < \frac{1}{2}\max(|x|, |y|, |z|)$. The boundary of the neighborhood is made up with segments between the indicated points.

affine plane). Indeed, one needs to restrict to bounded sets to compactify the situation, which is also why it works in the projective case as the closed sets are then compact.

(c) Corollary 3.2 is the key for Runge's method in the case of curves in Section 4. Notice that Lemma 5 of [Levin 2008] assumed X smooth, but the proof is actually exactly the same for X normal. Moreover, the argument below follows the structure of Levin's proof.

(d) If we replace Y by $Y' \supset Y$ and $\mathcal{V}$ by a tubular neighborhood $\mathcal{V}'$ of Y', the result remains true with the same proof, which is not surprising because tubular neighborhoods of Y' are larger than tubular neighborhoods of Y.

Proof of Proposition 3.1.

(a) By the Nullstellensatz applied to $K[U]$, there are $p \in \mathbb{N}_{\geq 1}$ and regular functions $f_{\ell,m} \in K[U]$ such that for every $m \in \{1, \ldots, s\}$,

$$\sum_{1 \leq \ell \leq r} g_\ell f_{\ell,m} = h_m^p.$$

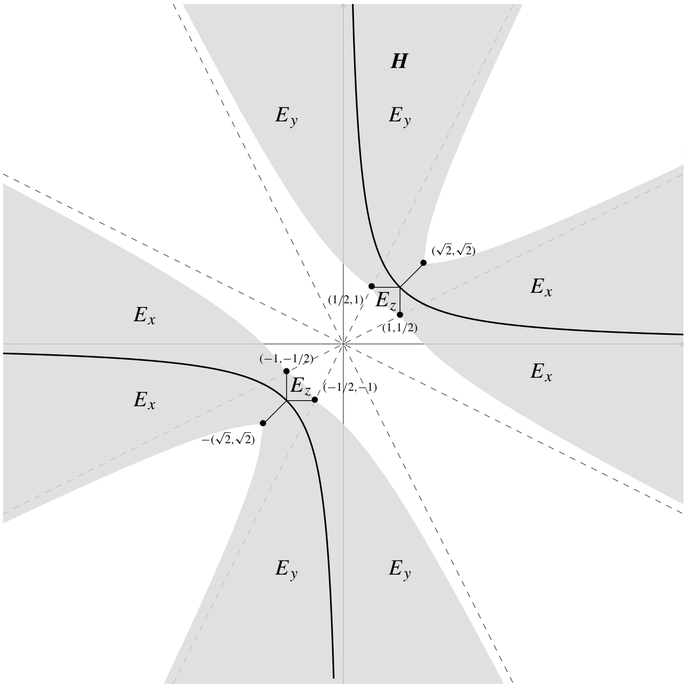


Figure 3. Tubular neighborhood of the hyperbola $H : xy - z^2 = 0$ given by the inequality $|xy - z^2| < \frac{1}{2}\max(|x|, |y|, |z|)$. The boundary is made up with arcs of hyperbola between the indicated points.

As E is M_K-bounded on U, all the $f_{\ell,m}$ are M_K-bounded on E hence there is an auxiliary M_K-constant $\mathcal{C}_1$ such that for all $(P, w) \in E$,

$$\max_{\substack{1 \le \ell \le r \\ 1 \le m \le s}} \log|f_{\ell,m}(P)|_w \le c_{1,v},$$

therefore

$$|h_m(P)^p|_w = \left| \sum_{1 \le \ell \le r} g_\ell(P) f_{\ell,m}(P) \right|_w \le r^{\delta_v} e^{c_{1,v}} \max_{1 \le \ell \le r} |g_\ell(P)|_w,$$

where δ_v is 1 if v is archimedean and 0 otherwise. For fixed w and P, either $\log|h_m(P)|_w < c_{0,v}$ for all $m \in \{1, \dots, s\}$ (second part of dichotomy (3-1)) or the above inequality applied to some $m \in \{1, \dots, s\}$ gives

$$p \cdot c_{0,v} \le \delta_v \log(r) + c_{1,v} + \max_{1 \le \ell \le r} \log|g_{\ell,j}(P)|_w,$$

which is equivalent to

$$\max_{1 \le \ell \le r} \log|g_\ell(P)|_w \ge p \cdot c_{0,v} - \delta_v \log(r) - c_{1,v}$$

and taking the M_K-constant defined by $c_v := c_{1,v} + \delta_v \log(r) - p \cdot c_{0,v}$ for every $v \in M_K$ gives exactly the first part of (3-1).

(b) We consider X as embedded in some $\mathbb{P}^n_K$ so that $\mathcal{V}$ is exactly the tubular neighborhood of Y in X associated to an M_K-constant $\mathcal{C}_0$ and generators $g_1, \dots, g_s$ for this embedding. Let us define $X_i := X \cap U_i$ for every $i \in \{0, \dots, n\}$ (see notations (1-2), (1-3) and (1-5)). The following argument is designed to make Y appear as a common zero locus of regular functions built from the ϕ_ℓ.

For every $\ell \in \{1, \dots, r\}$, let D_ℓ be the positive Weil divisor of zeroes of ϕ_ℓ on X. For every $i \in \{0, \dots, n\}$, let $I_{\ell,i}$ be the ideal of $K[X_i]$ made up with the regular functions h on the affine variety X_i such that $\operatorname{div}(h) \geq (D_\ell)_{|X_i}$, and we choose generators $h_{\ell,i,1}, \dots, h_{\ell,i,j_{\ell,i}}$ of this ideal. The functions $h_{\ell,i,j}/(\phi_\ell)_{|X_i}$ are then regular on X_i and $\forall j \in \{1, \dots, j_{\ell,i}\}$,

$$\operatorname{div}\left(\frac{h_{\ell,i,j}}{(\phi_\ell)_{|X_i}}\right) \geq (\phi_{\ell,i})_\infty$$

(the divisor of poles of ϕ_ℓ on X_i). By construction of $I_{\ell,i}$, the minimum (prime Weil divisor by prime Weil divisor) of the $\operatorname{div}(h_{\ell,i,j})$ is exactly $(D_\ell)_{|X_i}$; indeed, for every finite family of distinct prime Weil divisors $D'_1, \dots, D'_s, D''$ on X_i, there is a uniformizer h for D'' of order 0 for each of the D'_k, otherwise the prime ideal associated to D'' in X_i would be included in the finite union of the others. This allows us to build for every prime divisor D' of X_i not in the support of $(D_\ell)_{|X_i}$ a function $h \in I_{\ell,i}$ of order 0 along D' (and of the proper order for every D' in the support of $(D_\ell)_{|X_i}$). Consequently, the minimum of the divisors of the $h_{\ell,i,j}/(\phi_\ell)_{|X_i}$, being naturally the minimum of the divisors of the $h/(\phi_\ell)_{|X_i}$ (for $h \in K[X_i]$), is exactly $(\phi_{\ell,i})_\infty$.

Thus, by definition of Y, for fixed i, the set of common zeroes of the regular functions $h_{\ell,i,j}/(\phi_\ell)_{|X_i}$ (for $1 \leq \ell \leq r$ and $1 \leq j \leq j_{\ell,i}$) on X_i is $Y \cap X_i$, so they generate an ideal whose radical is the ideal of definition of $Y \cap X_i$. We apply part (a) of this proposition to the $h_{\ell,i,j}/(\phi_\ell)_{|X_i}$ (for $1 \leq \ell \leq r$ and $1 \leq j \leq j_{\ell,i}$), the $g_j \circ \varphi_i$ (for $1 \leq j \leq s$) and the M_K-constant $\mathcal{C}_0$, which gives us an M_K-constant $\mathcal{C}'_i$ and the following dichotomy on X_i for every $(P, w) \in E_i$:

$$\max_{\substack{1 \leq \ell \leq r \\ 1 \leq j \leq s_i}} \log\left|\frac{h_{\ell,i,j}}{\phi_\ell}(P)\right|_w \geq c'_{i,v} \quad \text{or} \quad \max_{1 \leq j \leq s} \log|g_j \circ \varphi_i(P)|_w < c_{0,v}.$$

Now, the $h_{\ell,i,j}$ are regular on X_i hence M_K-bounded on E_i, therefore there is a second M_K-constant $\mathcal{C}''_i$ such that for every $(P, w) \in E_i$

$$\max_{\substack{1 \leq \ell \leq r \\ 1 \leq j \leq s_i}} \log\left|\frac{h_{\ell,i,j}}{\phi_\ell}(P)\right|_w \geq c'_{i,v} \Longrightarrow \min_{1 \leq \ell \leq r} \log|\phi_\ell(P)|_w \leq c''_{i,v}.$$

Taking $\mathcal{C}$ as the maximum of the M_K-constants $\mathcal{C}''_i$, $0 \leq i \leq n$, for every $(P, w) \in X(\overline{K}) \times M_{\overline{K}}$, we choose i such that $(P, w) \in E_i$ and then we have the dichotomy (3-2) by definition of the tubular neighborhood V_w. □

To finish this section, we will give the explicit link between integral points on a projective scheme (relative to a divisor) and integral points relative to rational functions on the scheme. This will also tie our notion of integer points with that of [Levin 2008, Section 2], showing that the two can be treated exactly in the same way.

Proposition 3.4. *Let $\mathcal{X}$ be a normal projective scheme over $\mathcal{O}_{K,S}$.*

(a) *If $\mathcal{Y}$ is an effective Cartier divisor on $\mathcal{X}$ such that $\mathcal{Y}_K$ is an ample (Cartier) divisor of $\mathcal{X}_K$, there is a projective embedding $\psi : \mathcal{X}_K \to \mathbb{P}^n_K$ and an M_K-constant $\mathcal{C}$ such that the pullback by ψ of the hyperplane of equation $x_0 = 0$ in $\mathbb{P}^n_K$ is $\mathcal{Y}_K$, and for any finite extension L of K and any $w \in M_L$ not above S, $\forall P \in (\mathcal{X} \backslash \mathcal{Y})(\mathcal{O}_{L,w})$,*

$$\log\|x_{\psi(P)}\|_w \leq c_v + \log|x_{\psi(P),0}|_w. \tag{3-4}$$

(b) *If $\mathcal{Y}$ is an effective Cartier divisor on $\mathcal{X}$ such that $\mathcal{Y}_K$ is a big (Cartier) divisor of $\mathcal{X}_K$, there is a strict Zariski closed subset Z_K of $\mathcal{X}_K$, a closed immersion $\psi : \mathcal{X}_K \backslash Z_K \to \mathbb{P}^n_K \backslash \{x_0 = 0\}$ and an M_K-constant $\mathcal{C}$ such that for any finite extension L of K and any $w \in M_L$ not above S, formula (3-4) holds outside Z_K.*

Proof of Proposition 3.4. (a) and (b) come from the classical link between integral points in terms of a scheme and integral points in terms of local heights (proven in Lemma 1.4.6 and Proposition 1.4.7 of [Vojta 1987] for instance), combined with the properties of the morphisms associated to (very) ample or big divisors. □

Remark 3.5. (a) This proposition is formulated to avoid the use of local heights, but the idea is exactly that under the hypotheses above, if $P \in (\mathcal{X} \backslash \mathcal{Y})(\mathcal{O}_{L,w})$, the local height at w of P for the divisor $\mathcal{Y}$ is strictly bounded.

(b) The hypotheses on ampleness (or "bigness") are only necessary at the generic fiber. Once again, the auxiliary functions replace the need for a complete understanding of what happens at the finite places.

4. The case of curves revisited

In this section, we reprove the generalization of an old theorem of Runge [1887], obtained by Bombieri [1983, p. 305] (also rewritten as [Bombieri and Gubler 2006, Theorem 9.6.6]), following an idea explained by Bilu in an unpublished note and mentioned for the case $K = \mathbb{Q}$ by [Schoof 2008, Chapter 5]. The aim of this section is to give a general understanding of this idea (quite different from the original proof of Bombieri), as well as explain how it actually gives a *method* to bound heights of integral points on curves. It is also a good start to understand how the intuition behind this result can be generalized to higher dimension, which will be done in the next section.

Proposition 4.1 (Bombieri, 1983). *Let C be a smooth projective algebraic curve defined over a number field K and $\phi \in K(C)$ not constant.*

For any finite extension L/K, let r_L be the number of orbits of the natural action of $\mathrm{Gal}(\overline{L}/L)$ over the poles of ϕ. For any set of places S_L of L containing M_L^∞, we say that (L, S_L) satisfies the ***Runge condition*** *if*

$$|S_L| < r_L. \tag{4-1}$$

Then, the union

$$\bigcup_{(L,S_L)} \{P \in C(L) \mid \phi(P) \in \mathcal{O}_{L,S_L}\}, \tag{4-2}$$

where (L, S_L) *runs through all the pairs satisfying the Runge condition, is* ***finite*** *and can be explicitly bounded in terms of the height* $h \circ \phi$.

Example 4.2. As a concrete example, consider the modular curve $X_0(p)$ for p prime and the j-invariant function. This curve is defined over $\mathbb{Q}$ and j has two rational poles (which are the cusps of $X_0(p)$), hence $r_L = 2$ for any choice of L, and we need to ensure $|M_L^\infty| \leq |S_L| < 2$. The only possibilities satisfying the Runge condition are thus imaginary quadratic fields L with $S_L = \{|\cdot|_\infty\}$.

We proved in [Le Fourn 2016] that for any imaginary quadratic field L and any $P \in X_0(p)(L)$ such that $j(P) \in \mathcal{O}_L$, one has

$$\log|j(P)| \leq 2\pi\sqrt{p} + 6\log(p) + 8.$$

The method for general modular curves is carried out in [Bilu and Parent 2011] and gives explicit estimates on the height for integral points satisfying the Runge condition. This article uses the theory of modular units and implicitly the same proof of Bombieri's result as the one we explain below.

Remark 4.3. (a) The claim of an explicit bound deserves a clarification: it can actually be made explicit when one knows well enough the auxiliary functions involved in the proof below (which is possible in many cases, e.g., for modular curves thanks to the modular units). Furthermore, even as the theoretical proof makes use of M_K-constants and results of Section 3, they are frequently implicit in practical cases.

(b) Despite the convoluted formulation of the proof below and the many auxiliary functions to obtain the full result, its principle is as described in the introduction. It also gives the framework to apply Runge's method to a given couple (C, ϕ).

Proof of Proposition 4.1. We fix K' a finite Galois extension of K on which every pole of ϕ is defined. For any two distinct poles Q and Q' of ϕ, we choose by the Riemann–Roch theorem a function $g_{Q,Q'} \in K'(C)$ whose only pole is Q and which vanishes at Q'. For every point P of $C(\overline{K})$ which is not a pole of ϕ, one has $\mathrm{ord}_P(g_{Q,Q'}) \geq 0$ thus $g_{Q,Q'}$ belongs to the intersection of the discrete valuation rings of $\overline{K}(C)$ containing ϕ and $\overline{K}$ [Hartshorne 1977, proof of Lemma I.6.5], which is exactly the integral closure of $K[\phi]$ in $\overline{K}(C)$ [Atiyah and Macdonald 1969, Corollary 5.22]. Hence, the function $g_{Q,Q'}$ is integral on $K[\phi]$ and up to multiplication by some nonzero integer, we can and will assume it is integral on $\mathcal{O}_K[\phi]$.

For any fixed finite extension L of K included in $\overline{K}$, we define $f_{Q,Q',L} \in L(C)$ the product of the conjugates of $g_{Q,Q'}$ by $\mathrm{Gal}(\overline{L}/L)$. If Q and Q' belong to distinct orbits of poles for $\mathrm{Gal}(\overline{L}/L)$, the set of poles of $f_{Q,Q',L}$ is exactly the orbit of Q by $\mathrm{Gal}(\overline{K}/L)$, and its set of zeroes contains all the orbit of Q' by $\mathrm{Gal}(\overline{K}/L)$. Notice that we thus built only finitely many different functions (even with L running through all finite extensions of K) because each $g_{Q,Q'}$ only has finitely many conjugates in $\mathrm{Gal}(K'/K)$.

Now, let $\mathcal{O}_1, \ldots, \mathcal{O}_{r_L}$ be the orbits of poles of ϕ and denote for any $i \in \{1, \ldots, r_L\}$ by $f_{i,L}$ a product of $f_{Q_i,Q'_j,L}$ where $Q_i \in \mathcal{O}_i$ and Q'_j runs through representatives of the orbits (except $\mathcal{O}_i$). Again, there is a finite number of possible choices, and we obtain a function $f_{i,L} \in L(C)$ having for only poles the orbit $\mathcal{O}_i$ and vanishing at all the other poles of ϕ.

We apply Corollary 3.2 to $f_{i,L}/\phi^k$ and $f_{i,L}$ (for any i) for some k such that $f_{i,L}/\phi^k$ does not have poles at $\mathcal{O}_i$, and take the maximum of the induced M_K-constants (Definition 1.1) for any L and $1 \leq i \leq r_L$. This gives an M_K-constant $\mathcal{C}_0$ independent of L such that $\forall i \in \{1, \dots, r_L\}$, $\forall w \in M_{\overline{K}}$ and $\forall P \in C(\overline{K})$,

$$\log \min\left(\left| \frac{f_{i,L}}{\phi^k}(P) \right|_w, |f_{i,L}(P)|_w \right) \leq c_{0,v} \quad (w \mid v \in M_K).$$

In particular, the result interesting us in this case is that $\forall i \in \{1, \dots, r_L\}$, $\forall w \in M_{\overline{K}}$ and $\forall P \in C(\overline{K})$,

$$|\phi(P)|_w \leq 1 \Rightarrow \log|f_{i,L}(P)|_w \leq c_{0,v}, \tag{4-3}$$

and we can assume $c_{0,v}$ is 0 for any finite place v by integrality of the $f_{i,L}$ over $\mathcal{O}_K[\phi]$.

Given our construction, we also fix n such that for every $i \in \{1, \dots, r_L\}$, the $\phi f_{i,L}^n$ have poles at $\mathcal{O}_i$ and vanish at all other poles of ϕ. We reapply Corollary 3.2 for every pair $(\phi f_{i,L}^n, \phi f_{j,L}^n)$ with $1 \leq i < j \leq r_L$, which again by taking the maximum of the induced M_K-constants for all the possible combinations (Definition 1.1) gives an M_K-constant $\mathcal{C}_1$ such that for every $v \in M_K$ and every $(P, w) \in C(\overline{K}) \times M_{\overline{K}}$ with $w \mid v$, the inequality

$$\log|(\phi \cdot f_{i,L}^n)(P)|_w \leq c_{1,v} \tag{4-4}$$

is true for all indices i except at most one (depending on the choice of P and w).

Let us now suppose that (L, S_L) is a pair satisfying the Runge condition and $P \in C(L)$ with $\phi(P) \in \mathcal{O}_{L,S_L}$. By integrality on $\mathcal{O}_K[\phi]$, for every $i \in \{1, \dots, r_L\}$, $|f_{i,L}(P)|_w \leq 1$ for every place $w \in M_L \backslash S_L$. For every place $w \in S_L$, there is at most one index i not satisfying (4-4) hence by the Runge condition and the pigeon-hole principle, there remains one index i (depending on P) such that $\forall w \in M_L$,

$$\log|\phi(P) f_{i,L}^n(P)|_w \leq c_{1,v}. \tag{4-5}$$

With (4-3) and (4-5), we have obtained all the auxiliary results we need to finish the proof. By the product formula,

$$\begin{aligned} 0 &= \sum_{w \in M_L} n_w \log|f_{i,L}(P)|_w \\ &= \sum_{\substack{w \in M_L \\ |\phi(P)|_w > 1}} n_w \log|f_{i,L}(P)|_w + \sum_{w \in M_L^\infty |\phi(P)|_w \leq 1} n_w \log|f_{i,L}(P)|_w + \sum_{\substack{w \in M_L \backslash M_L^\infty \\ |\phi(P)|_w \leq 1}} n_w \log|f_{i,L}(P)|_w. \end{aligned}$$

Here, the first sum on the right side will be linked to the height $h \circ \phi$ and the third sum is negative by integrality of the $f_{i,L}$, so we only have to bound the second sum. From (4-3) and (1-4), we obtain

$$\sum_{\substack{w \in M_L^\infty \\ |\phi(P)|_w \leq 1}} n_w \log|f_{i,L}(P)|_w \leq \sum_{\substack{w \in M_L^\infty \\ |\phi(P)|_w \leq 1}} n_w c_{0,v} \leq [L:K] \sum_{v \in M_K^\infty} n_v c_{0,v}.$$

On another side, by (4-5) (and (1-4) again), we have

$$n \cdot \sum_{\substack{w \in M_L \\ |\phi(P)|_w > 1}} n_w \log|f_{i,L}(P)|_w = \sum_{\substack{w \in M_L \\ |\phi(P)|_w > 1}} n_w \log|\phi f_{i,L}^n(P)|_w - \sum_{\substack{w \in M_L \\ |\phi(P)|_w > 1}} n_w \log|\phi(P)|_w$$

$$\leq \left([L:K] \sum_{v \in M_K} n_v c_{1,v} \right) - [L:\mathbb{Q}] h(\phi(P)).$$

Hence, we obtain

$$0 \leq [L:K] \sum_{v \in M_K} n_v c_{1,v} - [L:\mathbb{Q}] h(\phi(P)) + [L:K] n \sum_{v \in M_K^\infty} n_v c_{0,v},$$

which is equivalent to

$$h(\phi(P)) \leq \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v (c_{1,v} + n c_{0,v}).$$

We thus obtained a bound on $h(\phi(P))$ independent on the choice of (L, S_L) satisfying the Runge condition, and together with the bound on the degree $[L:\mathbb{Q}] \leq 2|S_L| < 2r_L \leq 2r$, we get the finiteness. □

5. The main result: tubular Runge's theorem

We will now present our version of Runge theorem with tubular neighborhoods, which generalizes Theorem 4(b) and (c) of [Levin 2008]. As its complete formulation is quite lengthy, we indicated the different hypotheses by the letter **H** and the results by the letter **R**. The key condition for integral points (generalizing the Runge condition of Proposition 4.1) is indicated by the letters TRC.

We recall that the crucial notion of tubular neighborhood is explained in Definitions 2.1 and 2.2, and we advise the reader to look at the simplified version of this theorem stated in the Introduction to get more insight if necessary.

Theorem 5.1 (tubular Runge's theorem). **(H0)** *Let K be a number field, S_0 a set of places of K containing M_K^∞ and $\mathcal{O}$ the integral closure of $\mathcal{O}_{K,S_0}$ in some finite Galois extension K' of K.*

(H1) *Let $\mathcal{X}$ be a normal projective scheme over $\mathcal{O}_{K,S_0}$ and $D_1, \dots, D_r$ be effective Cartier divisors on $\mathcal{X}_\mathcal{O} = \mathcal{X} \times_{\mathcal{O}_{K,S_0}} \mathcal{O}$ such that $D_\mathcal{O} = \bigcup_{i=1}^r D_i$ is the scalar extension to $\mathcal{O}$ of some Cartier divisor D on $\mathcal{X}$, and that* Gal(K'/K) *permutes the generic fibers $(D_i)_{K'}$. For every extension L/K, we denote by $\boldsymbol{r_L}$ the number of orbits of $(D_1)_{K'}, \dots, (D_r)_{K'}$ for the action of* Gal$(K'L/L)$.

(H2) *Let Y be a closed subscheme of $\mathcal{X}_K$ and $\mathcal{V}$ be a tubular neighborhood of Y in $\mathcal{X}_K$. Let $\boldsymbol{m_Y} \in \mathbb{N}$ be the minimal number such that the intersection of any $(m_Y + 1)$ of the divisors $(D_i)_{K'}$ amongst the r possible ones is included in $Y_{K'}$.*

*TRC The **tubular Runge condition** for a pair (L, S_L), where L/K is finite and S_L contains all the places above S_0, is*

$$\boldsymbol{m_Y |S_L| < r_L}.$$

Under these hypotheses and notations, the results are the following:

(**R1**) *If* $(D_1)_{K'}, \dots, (D_r)_{K'}$ *are ample divisors, the set*

$$\bigcup_{(L,S_L)} \{P \in (\mathcal{X}\backslash D)(\mathcal{O}_{L,S_L}) \mid P \notin \mathcal{V}\}, \tag{5-1}$$

where (L, S_L) *goes through all the pairs satisfying the tubular Runge condition, is* ***finite***.

(**R2**) *If* $(D_1)_{K'}, \dots, (D_r)_{K'}$ *are big divisors, there exists a proper closed subset* $Z_{K'}$ *of* $\mathcal{X}_{K'}$ *such that the set*

$$\left(\bigcup_{(L,S_L)} \{P \in (\mathcal{X}\backslash D)(\mathcal{O}_{L,S_L}) \mid P \notin \mathcal{V}\}\right)\backslash Z_{K'}(\overline{K}),$$

where (L, S_L) *goes through all the pairs satisfying the tubular Runge condition, is* ***finite***.

Remark 5.2 explains the hypotheses and results of this theorem, and Remark 5.3 compares it with other theorems.

Remark 5.2. (a) The need for the extensions of scalars to K' and $\mathcal{O}$ in (**H0**) and (**H1**) is the analogue of the fact that the poles of ϕ are not necessarily K-rational in the case of curves, hence the assumption that the $(D_i)_{K'}$ are all conjugates by $\mathrm{Gal}(K'/K)$ and the definition of r_L given in (**H1**). It will induce technical additions of the same flavor as the auxiliary functions $f_{Q,Q',L}$ in the proof of Proposition 4.1.

(b) The motivation for the tubular Runge condition is the following: imitating the principle of proof for curves (Remark 4.3(b)), if $P \in (\mathcal{X}\backslash D)(\mathcal{O}_{L,S_L})$, we can say that at the places w of $M_L\backslash S_L$, this point is "w-adically far" from D. Now, the divisors $(D_1)_{K'}, \dots, (D_r)_{K'}$ can intersect (which does not happen for distinct points on curves), so for $w \in S_L$, this point P can be "w-adically close" to many divisors at the same time. More precisely, it can be "w-adically close" to at most m such divisors, where $m = m_\varnothing$, i.e., the largest number such that there are m divisors among $D_1, \dots, D_r$ whose set-theoretic intersection is nonempty. This number is also defined in [Levin 2008] but we found that for our applications, it often makes the Runge condition too strict. Therefore, we allow the use of the closed subset Y in (**H2**), and if we assume that our point P is never too close to Y (i.e., $P \notin \mathcal{V}$), this m goes down to m_Y by definition. Thus, we only need to take out m_Y divisors for each place w in S_L, hence the tubular Runge condition $m_Y|S_L| < r_L$. Actually, one can even mix the Runge conditions, i.e., assume that P is close to Y exactly at s_1 places, and close to one of the divisors (but not from Y) at s_2 places: following along the lines of the proof below, we obtain finiteness given the Runge condition $s_1 m_\varnothing + s_2 m_Y < r_L$ (this is exactly what we do for Theorem 8.2(a)).

(c) The last main difference with the case of curves is the assumption of ample or big divisors, respectively in (**R1**) and (**R2**). In both cases, such an assumption is necessary twice. First, we need it to translate by Proposition 3.4 the integrality condition on schemes to an integrality expression on auxiliary functions (such as in Section 2 of [Levin 2008]) to use the machinery of M_K-constants and the key result (Proposition 3.1).

Then, we need it to ensure that after obtaining a bound on the heights associated to the divisors, it implies finiteness (implicit in Proposition 3.4, see also Remark 3.5(a)).

Remark 5.3. (a) This theorem has some resemblance to the CLZ theorem of [Corvaja et al. 2009] (where our closed subset Y would be the analogue of the $\mathcal{Y}$ in that article), let us point out the differences. In the CLZ theorem, there is no hypothesis of the set of places S_L, no additional hypothesis of integrality (appearing for us under the form of a tubular neighborhood), and the divisors are assumed to be normal crossing divisors, which is replaced in our case by the tubular Runge condition. As for the results themselves, the finiteness formulated by CLZ depends on the set S_L (that is, it is not clear how it would prove that (5-1) is finite). Finally, the techniques employed are greatly different: the CLZ theorem uses Schmidt's subspace theorem (which has not been made effective yet), whereas our method can be made effective if one knows the involved auxiliary functions. It might be possible (and worthy of interest) to build some bridges between the two results, and the techniques involved.

(b) Theorem 5.1 can be seen as a stratification of Runge-like results depending on the dimension of the intersection of the involved divisors: at one extreme, the intersection is empty, and we get back Theorem 4(b) and (c) of [Levin 2008]. At the other extreme, the intersection is a divisor (ample or big), and the finiteness is automatic by (Remark 2.3). Of course, this stratification is not relevant in the case of curves. In another perspective, for a fixed closed subset Y, Theorem 5.1 is more a concentration result of integral points than a finiteness result, as it means that even if we choose a tubular neighborhood $\mathcal{V}$ of Y as small as possible around Y, there is only a finite number of integral points in the set (5-1), i.e., these integral points (ignoring the hypothesis $P \notin \mathcal{V}$) must concentrate around Y (at least at one of the places $w \in M_L$). Specific examples are given in Sections 7 and 8.

Let us now prove Theorem 5.1, following the ideas outlined in Remark 5.2.

Proof of Theorem 5.1. (**R1**) Let us first build the embeddings we need. For every subextension K'' of K'/K, the action of $\mathrm{Gal}(K'/K'')$ on the divisors $(D_1)_{K'}, \dots, (D_r)_{K'}$ has orbits denoted by $O_{K'',1}, \dots, O_{K'',r_{K''}}$. Notice that any $m_Y + 1$ such orbits still have their global intersection included in Y.

For each such orbit, the sum of its divisors is ample by hypothesis and coming from an effective Cartier divisor on $\mathcal{X}_{K''}$, One can then choose by Proposition 3.4 an appropriate embedding $\psi_{K'',i} : \mathcal{X}_{K''} \to \mathbb{P}^{n_i}_{K''}$, whose coordinate functions (denoted by $\phi_{K'',i,j} = (x_j/x_0) \circ \psi_{K'',i} (1 \leq j \leq n_i)$) satisfy Proposition 3.4 on all points of $(\mathcal{X}_{\mathcal{O}} \backslash \overline{O_{K'',i}})$ (where $\overline{O_{K'',i}}$ denotes the Zariski closure of $O_{K'',i}$ in $\mathcal{X}_{\mathcal{O}}$). We will denote by $\mathcal{C}_0$ the maximum of the (induced) M_K-constants obtained from Proposition 3.4 for all possible K''/K and orbits $O_{K'',i} (1 \leq i \leq r_{K''})$. The important point is that for any extension L/K, any $v \in M_K \backslash S_0$, any place $w \in M_L$ above v and any $P \in (\mathcal{X} \backslash D)(\mathcal{O}_{L,w})$, choosing $L' = K' \cap L$, one has

$$\max_{\substack{1 \leq i \leq r_L \\ 1 \leq j \leq n_i}} \log |\phi_{L',i,j}(P)|_w \leq c_{0,v}. \tag{5-2}$$

This is the first step to obtain a bound on the height of one of the $\psi_{K'',i}(P)$. For fixed P, we only have to do so for one of the $i \in \{1, \dots, r_L\}$ as long as the bound is uniform in the choice of (L, S_L) (and P), to obtain finiteness as each $\psi_{K'',i}$ is an embedding. To this end, one only needs to bound the coordinate functions on the places w of S_L, which is what we will do now.

For a subextension K'' of K'/K again, by (**H2**) (see the definition of m_Y), taking any set $\mathcal{I}$ of m_Y+1 couples (i,j), $1 \le i \le r_{K''}$, $j \in \{1,\dots,n_i\}$ with m_Y+1 different indices i and considering the rational functions $\phi_{K'',i,j}$, $(i,j) \in \mathcal{I}$, whose common poles are included in Y by hypothesis, we can apply Proposition 3.1 to these functions and the tubular neighborhood $\mathcal{V} = (V_w)_{w \in M_{\overline{K}}}$. Naming as $\mathcal{C}_1$ the maximum of all the (induced) obtained M_K-constants (also for all the possible K''), we just proved that for every subextension K'' of K'/K, every place $w \in M_{\overline{K}}$ (above $v \in M_K$) and any $P \in \mathcal{X}(\overline{K}) \backslash V_w$, the inequality

$$\max_{1 \le j \le n_i} \log|\phi_{K'',i,j}(P)|_w \le c_{1,v} \tag{5-3}$$

is true except for at most m_Y different indices $i \in \{1,\dots,r_{K''}\}$.

Now, let us consider (L, S_L) a pair satisfying the tubular Runge condition $m_Y|S_L| < r_L$ and denote $L' = K' \cap L$ again. For $P \in (\mathcal{X}\backslash D)(\mathcal{O}_{L,S_L})$ not belonging to $\mathcal{V}$, by (5-2), (5-3) and the tubular Runge condition, there remains an index $i \in \{1,\dots,r_L\}$ (dependent on P) such that $\forall w \in M_L$,

$$\max_{1 \le j \le n_i} \log|\phi_{L',i,j}(P)|_w \le \max(c_{0,v}, c_{1,v}) \quad (w \mid v \in M_K).$$

This immediately gives a bound on the height of $\psi_{L',i}(P)$ independent of the choice of pair (L, S_L) (except the fact that $L' = K' \cap L$). As $\psi_{L',i}$ is an embedding and $[L:\mathbb{Q}] \le 2|S_L| < 2r$, by Northcott's property, P belongs to a finite family of points (depending on i but not on (L, S_L)), and taking the union of these families for $i \in \{1,\dots,r_L\}$, we have proven the finiteness of the set of points

$$\bigcup_{(L,S_L)} \{P \in (\mathcal{X}\backslash D)(\mathcal{O}_{L,S_L}) \mid P \notin \mathcal{V}\},$$

where (L, S_L) goes through all the pairs satisfying the tubular Runge condition.

(**R2**) The proof is the same as for (**R1**) except that we have to exclude a closed subset of $\mathcal{X}_{K'}$ for every big divisor involved, and their union will be denoted by $Z_{K'}$. The arguments above hold for every point $P \notin Z_{K'}(\overline{K})$ (both for the expression of integrality by auxiliary functions, and for the conclusion and finiteness outside of this closed subset), using again Propositions 3.4 and 3.1. □

6. Reminders on Siegel modular varieties

In this section, we recall the classical constructions and results for the Siegel modular varieties, parametrizing principally polarized abelian varieties with a level structure. Most of those results are extracted (or easily deduced) from these general references: Chapter V of [Cornell and Silverman 1986] for the basic notions on abelian varieties, [Debarre 1999] for the complex tori, their line bundles, theta functions and moduli spaces, Chapter II of [Mumford 2007] for the classical complex theta functions, [Mumford 1984] for their links with theta divisors, and Chapter V of [Faltings and Chai 1990] for abelian schemes and their moduli spaces.

Unless specified, all the vectors of $\mathbb{Z}^g$, $\mathbb{R}^g$ and $\mathbb{C}^g$ are assumed to be row vectors.

6A. *Abelian varieties and Siegel modular varieties.*

Definition 6.1 (abelian varieties and polarization). • An *abelian variety* A over a field k is a projective algebraic group over k. Each abelian variety $A_{/k}$ has a dual abelian variety denoted by $\hat{A} = \mathrm{Pic}^0(A/k)$ [Cornell and Silverman 1986, §V.9].

• A *principal polarization* is an isomorphism $\lambda : A \to \hat{A}$ such that there exists a line bundle L on $A_{\bar{k}}$ with $\dim H^0(A_{\bar{k}}, L) = 1$ and λ is the morphism

$$\lambda : A_{\bar{k}} \to \widehat{A_{\bar{k}}}$$
$$x \mapsto T_x^* L \otimes L^{-1}$$

[Cornell and Silverman 1986, §V.13].

• Given a pair (A, λ), for every $n \geq 1$ prime to $\mathrm{char}(k)$, we can define the *Weil pairing*

$$A[n] \times A[n] \to \mu_n(\bar{k}),$$

where $A[n]$ is the n-torsion of $A(\bar{k})$ and μ_n the group of n-th roots of unity in $\bar{k}$. It is alternating and nondegenerate [Cornell and Silverman 1986, §V.16].

• Given a pair (A, λ), for $n \geq 1$ prime to $\mathrm{char}(k)$, a *symplectic level n structure on* $A[n]$ is a basis α_n of $A[n]$ in which the matrix of the Weil pairing is

$$J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

• Two triples (A, λ, α_n) and $(A', \lambda', \alpha'_n)$ of principally polarized abelian varieties over K with level n-structures are *isomorphic* if there is an isomorphism of abelian varieties $\phi : A \to A'$ such that $\phi^* \lambda' = \lambda$ and $\phi^* \alpha'_n = \alpha_n$.

In the case of complex abelian varieties, the previous definitions can be made more explicit.

Definition 6.2 (complex abelian varieties and symplectic group). Let $g \geq 1$.

• The *half-superior Siegel space of order* g, denoted by $\mathcal{H}_g$, is the set of matrices

$$\mathcal{H}_g := \{\tau \in M_g(\mathbb{C}) \mid {}^t\tau = \tau \text{ and } \operatorname{Im} \tau > 0\}, \tag{6-1}$$

where $\operatorname{Im} \tau > 0$ means that this symmetric matrix of $M_g(\mathbb{R})$ is positive definite. This space is an open subset of $M_g(\mathbb{C})$.

• For any $\tau \in \mathcal{H}_g$, we define

$$\Lambda_\tau := \mathbb{Z}^g + \mathbb{Z}^g \tau \quad \text{and} \quad A_\tau := \mathbb{C}^g / \Lambda_\tau. \tag{6-2}$$

Let L_τ be the line bundle on A_τ made up as the quotient of $\mathbb{C}^g \times \mathbb{C}$ by the action of Λ_τ defined $\forall p, q \in \mathbb{Z}^g$, by

$$(p\tau + q) \cdot (z, t) = (z + p\tau + q, e^{-i\pi p \tau^t p - 2i\pi p^t z} t). \tag{6-3}$$

Then, L_τ is an ample line bundle on A_τ such that $\dim H^0(A_\tau, L_\tau) = 1$, hence A_τ is a complex abelian variety and L_τ induces a principal polarization denoted by λ_τ on A_τ (see for example [Debarre 1999, Theorem VI.1.3]). We also denote by $\pi_\tau : \mathbb{C}^g \to A_\tau$ the quotient morphism.

- For every $n \geq 1$, the Weil pairing $w_{\tau,n}$ associated to (A_τ, λ_τ) on $A_\tau[n]$ is defined by

$$\begin{aligned} w_{\tau,n} : A_\tau[n] \times A_\tau[n] &\to \mu_n(\mathbb{C}) \\ (\bar{x}, \bar{y}) &\mapsto e^{2i\pi n w_\tau(x,y)} \end{aligned}$$

where $x, y \in \mathbb{C}^g$ have images $\bar{x}$ and $\bar{y}$ by π_τ, and w_τ is the $\mathbb{R}$-bilinear form on $\mathbb{C}^g \times \mathbb{C}^g$ (so that $w_\tau(\Lambda_\tau \times \Lambda_\tau) = \mathbb{Z}$) defined by

$$w_\tau(x, y) := \mathrm{Re}(x) \cdot \mathrm{Im}(\tau)^{-1} \cdot {}^t\,\mathrm{Im}(y) - \mathrm{Re}(y) \cdot \mathrm{Im}(\tau)^{-1} \cdot {}^t\,\mathrm{Im}(x)$$

(also readily checked by making explicit the construction of the Weil pairing).

- Let $(e_1, \dots, e_g)$ be the canonical basis of $\mathbb{C}^g$. The family

$$(\pi_\tau(e_1/n), \dots, \pi_\tau(e_g/n), \pi_\tau(e_1 \cdot \tau/n), \dots, \pi_\tau(e_g \cdot \tau/n)) \tag{6-4}$$

is a symplectic level n structure on (A_τ, λ_τ), denoted by $\alpha_{\tau,n}$.

- Let $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in M_{2g}(\mathbb{Z})$. For any commutative ring A, the *symplectic group of order g over A*, denoted by $\mathrm{Sp}_{2g}(A)$, is the subgroup of $\mathrm{GL}_{2g}(A)$ defined by

$$\mathrm{Sp}_{2g}(A) := \{M \in \mathrm{GL}_{2g}(A) \mid {}^t M J M = J\}, \quad J := \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}. \tag{6-5}$$

For every $n \geq 1$, the *symplectic principal subgroup of degree g and level n*, denoted by $\Gamma_g(n)$, is the subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z})$ made up by the matrices congruent to I_{2g} modulo n. For every $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_{2g}(\mathbb{R})$ and every $\tau \in \mathcal{H}_g$, we define

$$j_\gamma(\tau) = C\tau + D \in \mathrm{GL}_g(\mathbb{C}) \quad \text{and} \quad \gamma \cdot \tau = (A\tau + B)(C\tau + D)^{-1}, \tag{6-6}$$

which defines a left action by biholomorphisms of $\mathrm{Sp}_{2g}(\mathbb{R})$ on $\mathcal{H}_g$, and $(\gamma, \tau) \mapsto j_\gamma(\tau)$ is a left cocycle for this action [Klingen 1990, Proposition I.1].

- For every $g \geq 2$, $n \geq 1$ and $k \geq 1$, a *Siegel modular form of degree g, level n and weight k* is an holomorphic function f on $\mathcal{H}_g$ such that $\forall \gamma \in \Gamma_g(n)$,

$$f(\gamma \cdot z) = \det(j_\gamma(z))^k f(z). \tag{6-7}$$

The reason for this description of the complex abelian varieties is that the (A_τ, λ_τ) defined above make up all the principally polarized complex abelian varieties up to isomorphism. The following results can be found in Chapter VI of [Debarre 1999] except the last point which is straightforward.

Definition-Proposition 6.3 (uniformization of complex abelian varieties). • Every principally polarized complex abelian variety of dimension g with symplectic structure of level n is isomorphic to some triple $(A_\tau, \lambda_\tau, \alpha_{\tau,n})$ where $\tau \in \mathcal{H}_g$.

• For every $n \geq 1$, two triples $(A_\tau, \lambda_\tau, \alpha_{\tau,n})$ and $(A_{\tau'}, \lambda_{\tau'}, \alpha_{\tau',n})$ are isomorphic if and only if there exists $\gamma \in \Gamma_g(n)$ such that $\gamma \cdot \tau = \tau'$, and then such an isomorphism is given by

$$\begin{aligned} A_\tau &\to A_{\tau'} \\ z \bmod \Lambda_\tau &\mapsto z \cdot j_\gamma(\tau)^{-1} \bmod \Lambda_{\tau'} \end{aligned}.$$

• The *Siegel modular variety of degree g and level n* is the quotient $A_g(n)_{\mathbb{C}} := \Gamma_g(n) \backslash \mathcal{H}_g$. From the previous result, it is the moduli space of principally polarized complex abelian varieties of dimension g with a symplectic level n structure. As a quotient, it also inherits a structure of normal analytic space (with finite quotient singularities) of dimension $g(g+1)/2$, because $\Gamma_g(n)$ acts properly discontinuously on $\mathcal{H}_g$.

• For every positive divisor m of n, the natural morphism $A_g(n)_{\mathbb{C}} \to A_g(m)_{\mathbb{C}}$ induced by the identity of $\mathcal{H}_g$ corresponds in terms of moduli to multiplying the symplectic basis $\alpha_{\tau,n}$ by n/m, thus obtaining $\alpha_{\tau,m}$.

• For every $g \geq 1$ and $n \geq 1$, the quotient of $\mathcal{H}_g \times \mathbb{C}$ by the action of $\Gamma_g(n)$ defined as

$$\gamma \cdot (\tau, t) = (\gamma \cdot \tau, t/\det(j_\gamma(z))) \tag{6-8}$$

is a variety over $\mathcal{H}_g$ denoted by L. For a large enough power of k (or if $n \geq 3$), $L^{\otimes k}$ is a line bundle over $A_g(n)_{\mathbb{C}}$, hence L is a $\mathbb{Q}$-line bundle over $A_g(n)_{\mathbb{C}}$ called *line bundle of modular forms of weight one* over $A_g(n)_{\mathbb{C}}$. By definition (6-7), for every $k \geq 1$, the global sections of $L^{\otimes k}$ are the Siegel modular forms of degree g, level n and weight k.

Let us now present the compactification of $A_g(n)_{\mathbb{C}}$ we will use, that is the Satake compactification (for a complete description of it, see Section 3 of [Namikawa 1980]).

Definition-Proposition 6.4 (Satake compactification). Let $g \geq 1$ and $n \geq 1$. The normal analytic space $A_g(n)_{\mathbb{C}}$ admits a compactification called *Satake compactification* and denoted by $A_g(n)^S_{\mathbb{C}}$, satisfying the following properties.

(a) $A_g(n)^S_{\mathbb{C}}$ is a compact normal analytic space (of dimension $g(g+1)/2$, with finite quotient singularities) containing $A_g(n)_{\mathbb{C}}$ as an open subset and the boundary $\partial A_g(n)_{\mathbb{C}} := A_g(n)^S_{\mathbb{C}} \backslash A_g(n)_{\mathbb{C}}$ is of codimension g (see [Satake and Cartan 1957] for details).

(b) As a normal analytic space, $A_g(n)^S_{\mathbb{C}}$ is a projective algebraic variety. More precisely, for $\mathrm{M}_g(n)$ the graded ring of Siegel modular forms of degree g and level n, $A_g(n)^S_{\mathbb{C}}$ is canonically isomorphic to $\mathrm{Proj}_{\mathbb{C}} \mathrm{M}_g(n)$ [Cartan 1957, Théorème fondamental].

In particular, one can naturally obtain $A_g(n)^S_{\mathbb{C}}$ by fixing for some large enough weight k a basis of modular forms of $\mathrm{M}_g(n)$ of weight k and evaluating them all on $A_g(n)_{\mathbb{C}}$ to embed it in a projective space, so that $A_g(n)^S_{\mathbb{C}}$ is the closure of the image of the embedding in this projective space.

(c) The $\mathbb{Q}$-line bundle L of modular forms of weight 1 on $A_g(n)_{\mathbb{C}}$ extends naturally to an ample $\mathbb{Q}$-line bundle on $A_g(n)^S_{\mathbb{C}}$ (which is also denoted L); this is a direct consequence of (b).

6B. *Further properties of Siegel modular varieties.* As we are interested in the reduction of abelian varieties on number fields, one needs to have a good model of $A_g(n)_{\mathbb{C}}$ over integer rings, as well as some knowledge of the geometry of $A_g(n)_{\mathbb{C}}$. The integral models below and their properties are given in Chapter V of [Faltings and Chai 1990].

Definition 6.5 (abelian schemes). (a) An *abelian scheme* $A \to S$ is a smooth proper group scheme whose fibers are geometrically connected. It also has a natural *dual* abelian scheme $\hat{A} = \mathrm{Pic}^0(A/S)$, and it is *principally polarized* if it is endowed with an isomorphism $\lambda : A \to \hat{A}$ such that at every geometric point $\bar{s}$ of S, the induced isomorphism $\lambda_{\bar{s}} : A_{\bar{s}} \to \hat{A}_{\bar{s}}$ is a principal polarization of $A_{\bar{s}}$.

(b) A *symplectic structure of level* $n \geq 1$ on a principally polarized abelian scheme (A, λ) over a $\mathbb{Z}[\zeta_n, 1/n]$-scheme S is the datum of an isomorphism of group schemes $A[n] \to (\mathbb{Z}/n\mathbb{Z})^{2g}$, which is symplectic with respect to λ and the canonical pairing on $(\mathbb{Z}/n\mathbb{Z})^{2g}$ given by the matrix J (as in (6-5)).

Definition-Proposition 6.6 (algebraic moduli spaces). For every integers $g \geq 1$ and $n \geq 1$:

(a) The Satake compactification $A_g(n)^S_{\mathbb{C}}$ has an integral model $\mathcal{A}_g(n)^S$ on $\mathbb{Z}[\zeta_n, 1/n]$ which contains as a dense open subscheme the (coarse, if $n \leq 2$) moduli space $\mathcal{A}_g(n)$ over $\mathbb{Z}[\zeta_n, 1/n]$ of principally polarized abelian schemes of dimension g with a symplectic structure of level n. This scheme $\mathcal{A}_g(n)^S$ is normal, proper and of finite type over $\mathbb{Z}[\zeta_n, 1/n]$ [Faltings and Chai 1990, Theorem V.2.5].

(b) For every divisor m of n, we have canonical degeneracy morphisms $\mathcal{A}_g(n)^S \to \mathcal{A}_g(m)^S$ extending the morphisms of Definition-Proposition 6.3.

Before tackling our own problem, let us give some context on the divisors on $A_g(n)^S_{\mathbb{C}}$ to give a taste of the difficulties to overcome.

Definition 6.7 (rational Picard group). For every normal algebraic variety X over a field K, the *rational Picard group* of X is the $\mathbb{Q}$-vector space

$$\mathrm{Pic}(X)_{\mathbb{Q}} := \mathrm{Pic}(X) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Proposition 6.8 (rational Picard groups of Siegel modular varieties). *Let $g \geq 2$ and $n \geq 1$.*

(a) *Every Weil divisor on $A_g(n)_{\mathbb{C}}$ or $A_g(n)^S_{\mathbb{C}}$ is up to some multiple a Cartier divisor, hence their rational Picard group is also their Weil class divisor group tensored by $\mathbb{Q}$.*

(b) *For $g = 3$, the Picard rational groups of $A_3(n)^S_{\mathbb{C}}$ and $A_3(n)_{\mathbb{C}}$ are equal to $\mathbb{Q} \cdot L$ for every $n \geq 1$.*

(c) *For $g = 2$, one has $\mathrm{Pic}_{\mathbb{Q}}(A_2(1)^S_{\mathbb{C}}) = \mathbb{Q} \cdot L$.*

This result has the following immediate corollary, because L is ample on $A_g(n)^S_{\mathbb{C}}$ for every $g \geq 2$ and every $n \geq 1$ (Definition-Proposition 6.4(c)).

Corollary 6.9 (ample and big divisors on Siegel modular varieties). *A $\mathbb{Q}$-divisor on $A_g(n)_\mathbb{C}$ or $A_g(n)^S_\mathbb{C}$ with $g{=}3$ (or $g{=}2$ and $n{=}1$) is ample if and only if it is big if and only if it is equivalent to $a \cdot L$ with $a > 0$.*

Remark 6.10. We did not mention the case of modular curves (also difficult, but treated by different methods): the point here is that the cases $g \geq 3$ are surprisingly much more uniform because then $\operatorname{Pic}(A_g(n)^S_\mathbb{C}) = \operatorname{Pic}(A_g(1)^S_\mathbb{C})$. The reason is that some rigidity appears from $g \geq 3$ (essentially by the general arguments of [Borel 1981]), whereas for $g = 2$, the situation seems very complex already for the small levels (see for example $n = 3$ in [Hoffman and Weintraub 2001]).

This is why the ampleness (or bigness) is in general hard to figure out for given divisors of $A_2(n)$, $n > 1$. We consider specific divisors in the following (namely, divisors of zeroes of theta functions), whose ampleness will not be hard to prove.

Proof of Proposition 6.8.

(a) This is true for the $A_g(n)^S_\mathbb{C}$ by [Artal Bartolo et al. 2014] as they only have finite quotient singularities (this result actually seems to have been generally assumed a long time ago). Now, as $\partial A_g(n)^S_\mathbb{C}$ is of codimension at least 2, the two varieties $A_g(n)^S_\mathbb{C}$ and $A_g(n)_\mathbb{C}$ have the same Weil and Cartier divisors, hence the same rational Picard groups.

(b) This is a consequence of general results of [Borel 1981] further refined in [Weissauer 1992] (it can even be generalized to every $g \geq 3$).

(c) This comes from the computations of Section III.9 of [Mumford 1983] (for another compactification, called toroidal), from which we extract the result for $A_2(1)_\mathbb{C}$ by a classical restriction theorem [Hartshorne 1977, Proposition II.6.5] because the boundary for this compactification is irreducible of codimension 1. The result for $A_2(1)^S_\mathbb{C}$ is then the same because the boundary is of codimension 2. ☐

6C. ***Theta divisors on abelian varieties and moduli spaces.*** We will now define the useful notions for our integral points problem.

Definition 6.11 (theta divisor on an abelian variety). Let k be an algebraically closed field and A an abelian variety over k.

Let L be an ample symmetric line bundle on A inducing a principal polarization λ on A. A *theta function associated to* (A, L) is a nonzero global section $\vartheta_{A,L}$ of L. The *theta divisor associated to* (A, L), denoted by $\Theta_{A,L}$, is the divisor of zeroes of $\vartheta_{A,L}$, well-defined and independent of our choice because $\dim H^0(A, L) = \deg(\lambda)^2 = 1$.

The theta divisor is in fact determined by the polarization λ itself up to a finite ambiguity, as the result below makes precise.

Proposition 6.12. *Let k be an algebraically closed field and A an abelian variety over k.*

Two ample symmetric line bundles L and L' on A inducing a principal polarization induce the same one if and only if $L' \cong T_x^* L$ for some $x \in A[2]$, and then

$$\Theta_{A,L'} = \Theta_{A,L} + x.$$

Proof. This is a well-known result relying on the properties of the map

$$L \mapsto (\phi_L : x \mapsto T_x^* L \otimes L^{-1})$$

from $\mathrm{Pic}(A)$ to $\mathrm{Hom}(A, \hat{A})$ [Mumford 1970, Corollary 4 p. 60 and Theorem 1 p. 77], and of ample symmetric line bundles. □

When $\mathrm{char}(k) \neq 2$, adding to a principally polarized abelian variety (A, λ) of dimension g the datum α_2 of a symplectic structure of level 2, we can determine an unique ample symmetric line bundle L with the following process called the *Igusa correspondence*, devised in [Igusa 1967]. To any ample symmetric Weil divisor D defining a principal polarization, one can associate bijectively a quadratic form q_D from $A[2]$ to $\{\pm 1\}$ called *even*, which means that the sum of its values on $A[2]$ is 2^g [loc. cit., Theorem 2 and the previous arguments]. On the other hand, the datum α_2 also determines an even quadratic form q_{α_2}, by associating to a $x \in A[2]$ with coordinates $(a, b) \in (\mathbb{Z}/2\mathbb{Z})^{2g}$ in the basis α_2 of $A[2]$ the value

$$q_{\alpha_2}(x) = (-1)^{a^t b}. \tag{6-9}$$

We now only have to choose the unique ample symmetric divisor D such that $q_D = q_{\alpha_2}$ and the line bundle L associated to D.

By construction of this correspondence [loc. cit., p. 823], a point $x \in A[2]$ of coordinates $(a, b) \in (\mathbb{Z}/2\mathbb{Z})^{2g}$ in α_2 automatically belongs to $\Theta_{A,L}$ (with L associated to (A, λ, α_2)) if $a^t b = 1 \bmod 2$. A point of $A[2]$ with coordinates (a, b) such that $a^t b = 0 \bmod 2$ can also belong to $\Theta_{A,L}$ but with even multiplicity.

This allows us to get rid of the ambiguity of choice of an ample symmetric L in the following, as soon as we have a symplectic level 2 structure (or finer) (this result is a reformulation of Theorem 2 of [loc. cit.]).

Definition-Proposition 6.13 (theta divisor canonically associated to a symplectic even level structure). Let $n \geq 2$ even and k algebraically closed such that $\mathrm{char}(k)$ does not divide n.

For (A, λ, α_n) a principally polarized abelian variety of dimension g with symplectic structure of level n (Definition 6.2), there is up to isomorphism an unique ample symmetric line bundle L inducing λ and associated by the Igusa correspondence to the symplectic basis of $A[2]$ induced by α_n. The *theta divisor associated to* (A, λ, α_n), denoted by $\Theta_{A,\lambda,\alpha_n}$, is then the theta divisor associated to (A, L).

The Runge-type theorem we give in Section 7 (Theorem 7.12) focuses on principally polarized abelian surfaces (A, λ) on a number field K whose theta divisor does not contain any n-torsion point of A (except 2-torsion points, as we will see it is automatic). This will imply (Proposition 7.5) that A is not a product of elliptic curves, but this is not a sufficient condition, as pointed out for example in [Boxall and Grant 2000].

We will once again start with the complex case to figure out how such a condition can be formulated on the moduli spaces, using complex theta functions [Mumford 2007, Chapter II].

Definition-Proposition 6.14 (complex theta functions). Let $g \geq 1$.

The holomorphic function Θ on $\mathbb{C}^g \times \mathcal{H}_g$ is defined by the series (uniformly convergent on any compact subset)

$$\Theta(z,\tau) = \sum_{n \in \mathbb{Z}^g} e^{i\pi n \tau^t n + 2i\pi n^t z}. \tag{6-10}$$

For any $a, b \in \mathbb{R}^g$, we also define the holomorphic function $\Theta_{a,b}$ by

$$\Theta_{a,b}(z,\tau) = \sum_{n \in \mathbb{Z}^g} e^{i\pi (n+a)\tau^t (n+a) + 2i\pi (n+a)^t (z+b)}. \tag{6-11}$$

For a fixed $\tau \in \mathcal{H}_g$, one defines $\Theta_\tau : z \mapsto \Theta(z,\tau)$ and similarly for $\Theta_{a,b,\tau}$. These functions have the following properties.

(a) For every $a, b \in \mathbb{Z}^g$,

$$\Theta_{a,b,\tau}(z) = e^{i\pi a \tau^t a + 2i\pi a^t (z+b)} \Theta_\tau(z + a\tau + b). \tag{6-12}$$

(b) For every $p, q \in \mathbb{Z}^g$,

$$\Theta_{a,b,\tau}(z + p\tau + q) = e^{-i\pi p \tau^t p - 2i\pi p^t z + 2i\pi (a^t q - b^t p)} \Theta_{a,b,\tau}(z). \tag{6-13}$$

(c) Let us denote by ϑ and $\vartheta_{a,b}$ the *normalized theta-constants*, which are the holomorphic functions on $\mathcal{H}_g$ defined by

$$\vartheta(\tau) := \Theta(0,\tau) \quad \text{and} \quad \vartheta_{a,b}(\tau) := e^{-i\pi a^t b} \Theta_{a,b}(0,\tau). \tag{6-14}$$

These theta functions satisfy the following modularity property: with the notations of Definition 6.2 and $\forall \gamma \in \Gamma_g(2)$,

$$\vartheta_{a,b}(\gamma \cdot \tau) = \zeta_8(\gamma) e^{i\pi (a,b)^t V_\gamma} \sqrt{j_\gamma(\tau)}\, \vartheta_{(a,b)\gamma}(\tau), \tag{6-15}$$

where $\zeta_8(\gamma)$ (an 8-th root of unity) and $V_\gamma \in \mathbb{Z}^g$ only depend on γ and the determination of the square root of $j_\gamma(\tau)$.

In particular, for every even $n \geq 2$, if $(na, nb) \in \mathbb{Z}^{2g}$, the function $\vartheta_{a,b}^{8n}$ is a Siegel modular form of degree g, level n and weight $4n$, which only depends on $(a,b) \bmod \mathbb{Z}^{2g}$.

Proof. The convergence of these series as well as their functional equations (6-12) and (6-13) are classical and can be found in Section II.1 of [Mumford 2007].

The modularity property (6-15) (also classical) is a particular case of the computations of Section II.5 of [Mumford 2007] (we do not need here the general formula for $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$).

Finally, by natural computations of the series defining $\Theta_{a,b}$, one readily obtains that

$$\vartheta_{a+p,b+q} = e^{2i\pi (a^t q - b^t p)} \vartheta_{a,b}.$$

Therefore, if $(na, nb) \in \mathbb{Z}^{2g}$, the function $\vartheta_{a,b}^n$ only depends on $(a,b) \bmod \mathbb{Z}^{2g}$. Now, putting the modularity formula (6-15) to the power $8n$, one eliminates the eight root of unity and if $\gamma \in \Gamma_g(n)$, one has $(a,b)\gamma = (a,b) \bmod \mathbb{Z}^g$ hence $\vartheta_{a,b}^{8n}$ is a Siegel modular form of weight $4n$ for $\Gamma_g(n)$. □

There is of course an explicit link between the theta functions and the notion of theta divisor, which we explain now with the notations of Definition 6.2.

Proposition 6.15 (theta divisor and theta functions). *Let $\tau \in \mathcal{H}_g$.*

The line bundle L_τ is ample and symmetric on A_τ, and defines a principal polarization on A_τ. It is also the line bundle canonically associated to the 2-structure $\alpha_{\tau,2}$ and its polarization by the Igusa correspondence (Definition-Proposition 6.13).

Furthermore, the global sections of L_τ canonically identify to the multiples of Θ_τ, hence the theta divisor associated to $(A_\tau, \lambda_\tau, \alpha_{\tau,2})$ is exactly the divisor of zeroes of Θ_τ modulo Λ_τ.

Thus, for every $a, b \in \mathbb{R}^g$, the projection of $\pi_\tau(a\tau + b)$ belongs to $\Theta_{A_\tau,\lambda_\tau,\alpha_{\tau,2}}$ if and only if $\vartheta_{a,b}(\tau) = 0$.

Remark 6.16. The proof below that the L_τ is the line bundle associated to $(A_\tau, \lambda_\tau, \alpha_{\tau,2})$ is a bit technical, but one has to suspect that Igusa normalized its correspondence by (6-9) exactly to make it work.

Proof. One can easily see that L_τ is symmetric by writing $[-1]^* L_\tau$ as a quotient of $\mathbb{C}^g \times \mathbb{C}$ by an action of Λ_τ, then figuring out it is the same as (6-3). Then, by simple connectedness, the global sections of L_τ lift by the quotient morphism $\mathbb{C}^g \times \mathbb{C} \to L_\tau$ into functions $z \mapsto (z, f(z))$, and the holomorphic functions f thus obtained are exactly the functions satisfying functional equation (6-13) for $a = b = 0$ because of (6-3), hence the same functional equation as Θ_τ. This identification is also compatible with the associated divisors, hence Θ_{A_τ,L_τ} is the divisor of zeroes of Θ_τ modulo Λ_τ. For more details on the theta functions and line bundles, see [Debarre 1999, Chapters IV, V and Section VI.2].

We now have to check that the Igusa correspondence indeed associates L_τ to $(A_\tau, \lambda_\tau, \alpha_{\tau,2})$. With the notations of the construction of this correspondence [Igusa 1967, pp. 822, 823 and 833], one sees that the meromorphic function ψ_x on A_τ (depending on L_τ) associated to $x \in A_\tau[2]$ has divisor $[2]^* T_x^* \Theta_{A_\tau,L_\tau} - [2]^* \Theta_{A_\tau,L_\tau}$, hence it is (up to a constant) the meromorphic function induced on A_τ by

$$f_x(z) = \frac{\Theta_{a,b,\tau}(2z)}{\Theta_\tau(2z)},$$

where $x = a\tau + b \mod \Lambda_\tau$. Now, the quadratic form q associated to L_τ is defined by the identity

$$f_x(-z) = q(x) f_x(z)$$

for every $z \in \mathbb{C}^g$, but Θ_τ is even hence

$$f_x(-z) = e^{4i\pi a^t b} f_x(z)$$

by (6-12). Now, the coordinates of x in $\alpha_{\tau,2}$ are exactly $(2b, 2a) \mod \mathbb{Z}^{2g}$ by definition, hence $q = q_{\alpha_{\tau,2}}$.

Let us finally make the explicit link between zeroes of theta-constants and theta divisors; using the argument above, the divisor of zeroes of Θ_τ modulo Λ_τ is exactly Θ_{A_τ,L_τ}, hence $\Theta_{A_\tau,\lambda_\tau,\alpha_{\tau,2}}$ by what we just proved for the Igusa correspondence. This implies that for every $z \in \mathbb{C}^g$, $\Theta_\tau(z) = 0$ if and only if $\pi_\tau(z)$ belongs to $\Theta_{A_\tau,\lambda_\tau,\alpha_{\tau,2}}$, and as $\vartheta_{a,b}(\tau)$ is a nonzero multiple of $\Theta(a\tau + b, \tau)$, we finally have that $\vartheta_{a,b}(\tau) = 0$ if and only if $\pi_\tau(a\tau + b)$ belongs to $\Theta_{A_\tau,\lambda_\tau,\alpha_{\tau,2}}$. ∎

7. Applications of the main result on a family of Siegel modular varieties

We now have almost enough definitions to state the problem which we will consider for our Runge-type result (Theorem 7.12). We consider theta divisors on abelian surfaces, and their torsion points.

To make their indexation easier, we use the following notation.

Notation. Until the end of this article, the expression "a couple $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^4$ (resp. $\mathbb{Z}^4$, $\mathbb{Q}^4$)" is a shorthand to designate the row vector with four coefficients where $a \in (\mathbb{Z}/n\mathbb{Z})^2$ (resp. $\mathbb{Z}^2$, $\mathbb{Q}^2$) make up the first two coefficients and b the last two coefficients.

7A. ***The specific situation for theta divisors on abelian surfaces.*** As an introduction and a preliminary result, let us treat first the case of theta divisors on elliptic curves.

Lemma 7.1 (theta divisor on an elliptic curve). *Let E be an elliptic curve on an algebraically closed field k with $\operatorname{char}(k) \neq 2$ and L an ample symmetric line bundle defining the principal polarization on E.*

The effective divisor $\Theta_{E,L}$ is a 2-torsion point of E with multiplicity one. More precisely, if (e_1, e_2) is the basis of $E[2]$ associated by Igusa correspondence to L (Definition-Proposition 6.13),

$$\Theta_{E,L} = [e_1 + e_2]. \tag{7-1}$$

Remark 7.2. In the complex case, this can simply be obtained by proving that $\Theta_{1/2,1/2,\tau}$ is odd for every $\tau \in \mathcal{H}_1$ hence cancels at 0, and has no other zeroes (by a residue theorem for example), then using Proposition 6.15.

Proof. By the Riemann–Roch theorem on E, the divisor $\Theta_{E,L}$ is of degree 1 because $h^0(E, L) = 1$ (and effective). Now, as explained before when discussing the Igusa correspondence, for $a, b \in \mathbb{Z}$, $ae_1 + be_2$ automatically belongs to $\Theta_{E,L}$ if $ab = 1 \mod 2\mathbb{Z}$, hence $\Theta_{E,L} = [e_1 + e_2]$. □

This allows one to describe the theta divisor of a product of two elliptic curves.

Proposition 7.3 (theta divisor on a product of two elliptic curves). *Let k be an algebraically closed field with $\operatorname{char}(k) \neq 2$.*

Let (A, L) with $A = E_1 \times E_2$ a product of elliptic curves over k and L an ample symmetric line bundle on A inducing the product principal polarization on A. The divisor $\Theta_{A,L}$ is then of the shape

$$\Theta_{A,L} = \{x_1\} \times E_2 + E_1 \times \{x_2\}, \tag{7-2}$$

with $x_i \in E_i[2]$ for $i = 1, 2$. In particular, this divisor has a (unique) singular point of multiplicity two at (x_1, x_2), and:

(a) *There are exactly seven 2-torsion points of A belonging to $\Theta_{A,L}$: the six points given by the coordinates $(a, b) \in (\mathbb{Z}/2\mathbb{Z})^4$ such that $a^t b = 1$ in a basis giving $\Theta_{A,L}$ by the Igusa correspondence, and the seventh point (x_1, x_2).*

(b) *For every even $n \geq 2$ which is nonzero in k, the number of n-torsion (but not 2-torsion) points of A belonging to $\Theta_{A,L}$ is exactly $2(n^2 - 4)$.*

Proof. By construction of (A, L), a global section of (A, L) corresponds to a tensor product of global sections of E_1 and E_2 (with their principal polarizations), hence the shape of $\Theta_{A,L}$ is a consequence of Lemma 7.1.

We readily deduce (a) and (b) from this shape, using that the intersection of the two components of $\Theta_{A,L}$ is a 2-torsion point of even multiplicity for the quadratic form hence different from the six other ones. □

Regarding abelian surfaces which are not products of elliptic curves, we recall below a fundamental result (proven in [Oort and Ueno 1973]).

Proposition 7.4 (shapes of principally polarized abelian surfaces). *Let k be any field.*

A principally polarized abelian surface (A, λ) over k is, after a finite extension of scalars, either the product of two elliptic curves (with its natural product polarization), or the jacobian J of an hyperelliptic curve C of genus 2 (with its canonical principal polarization). In the second case, for the Albanese embedding $\phi_x : C \to J$ with base-point x and an ample symmetric line bundle L over K inducing λ, the divisor $\Theta_{J,L}$ is irreducible, and it is actually a translation of $\phi_x(C)$ by some point of $J(\bar{k})$.

Let us now fix an algebraically closed field k with $\mathrm{char}(k) \neq 2$.

Let C be an hyperelliptic curve of genus 2, and ι its hyperelliptic involution. This curve has exactly six Weierstrass points (the fixed points of ι, by definition), and we fix one of them, denoted by ∞. For the Albanese morphism ϕ_∞, the divisor $\phi_\infty(C)$ is stable by $[-1]$ because the divisor $[x] + [\iota(x)] - 2[\infty]$ is principal for every $x \in C$. As $\Theta_{J,L}$ is also symmetric and a translation of $\phi_\infty(C)$, we know that $\Theta_{J,L} = T_x^*(\phi_\infty(C))$ for some $x \in J[2]$.

This tells us that understanding the points of $\Theta_{J,L}$ amounts to understanding how the curve C behaves when embedded in its jacobian (in particular, how its points add). It is a difficult problem to know which torsion points of J belong to the theta divisor (see [Boxall and Grant 2000] for example), but we will only need to bound their quantity here, with the following result.

Proposition 7.5. *Let k an algebraically closed field with* $\mathrm{char}(k) \neq 2$.

Let C be an hyperelliptic curve of genus 2 over k with jacobian J, and ∞ a fixed Weierstrass point of C. We denote by $\tilde{C}$ the image of C in J by the associated embedding $\phi_\infty : x \mapsto \overline{[x] - [\infty]}$.

(a) *The set $\tilde{C}$ is stable by $[-1]$, and the application*

$$\mathrm{Sym}^2(\tilde{C}) \to J$$
$$\{P, Q\} \mapsto P + Q$$

is the blow-up of J at the origin, in particular it is injective outside the fiber above 0.

(b) *There are exactly six 2-torsion points of J belonging to $\tilde{C}$, and they are equivalently the images of the Weierstrass points and the points of coordinates $(a, b) \in ((\mathbb{Z}/2\mathbb{Z})^2)^2$ such that $a^t b = 1$ in a basis giving $\tilde{C}$ by the Igusa correspondence.*

(c) *For any $n \geq 2$ which is nonzero in k, the number of n-torsion points of J belonging to $\tilde{C}$ is bounded by $\sqrt{2}n^2 + \frac{1}{2}$.*

Remark 7.6. This proposition is not exactly a new result, and its principle can be found (with slightly different formulations) in Theorem 1.3 of [Boxall and Grant 2000] or in Lemma 5.1 of [Pazuki 2013]. The problem of counting (or bounding) torsion points on the theta divisor has interested many people, e.g., [Boxall and Grant 2000] and very recently [Auffarth et al. 2017] in general dimension. Notice that the results above give the expected bound in the case $g = 2$, but we do not know how much we can lower the bound $\sqrt{2}n^2$ in the case of jacobians.

Proof. (a) is a well-known consequence of the Riemann–Roch theorem in genus 2. (b) comes from the construction of the Igusa correspondence, and the definition of Weierstrass points as points P such that $2[P]$ is a canonical divisor. Now, for any $n \geq 2$, let us denote $\tilde{C}[n] := \tilde{C} \cap J[n]$. The summing map from $\tilde{C}[n]^2$ to $J[n]$ has a fiber of cardinal $|\tilde{C}[n]|$ above 0 and at most 2 above any other point of $J[n]$ by (a), hence the inequality of degree two

$$|\tilde{C}[n]|^2 \leq |\tilde{C}[n]| + 2(n^4 - 1),$$

from which we directly obtain (c). □

We can now define the divisors we will consider for our Runge-type theorem.

Definition-Proposition 7.7 (theta divisors on $A_2(n)^S_{\mathbb{C}}$). Let $n \in \mathbb{N}_{\geq 2}$ even.

(a) A couple $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^4$ is called *regular* if it is *not* of the shape $((n/2)a', (n/2)b')$ with $(a', b') \in ((\mathbb{Z}/2\mathbb{Z})^2)^2$ such that $a'^t b' = 1 \bmod 2$. There are exactly 6 couples (a, b) not satisfying this condition, which we call *singular*.

(b) If $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^4$ is regular, for every lift $(\tilde{a}, \tilde{b}) \in \mathbb{Z}^4$ of (a, b), the function $\vartheta^{8n}_{\tilde{a}/n, \tilde{b}/n}$ is a *nonzero* Siegel modular form of degree 2, weight $4n$ and level n, independent of the choice of lifts. The *theta divisor associated to* (a, b), denoted by $(D_{n,a,b})_{\mathbb{C}}$, is the Weil divisor of zeroes of this Siegel modular form on $A_2(n)^S_{\mathbb{C}}$.

Remark 7.8. The singular couples correspond to what are called *odd characteristics* by Igusa.

The proof below uses Fourier expansions to figure out which theta functions are nontrivial. One can also prove through Fourier expansions that the Weil divisors $(D_{n,a,b})_{\mathbb{C}}$ and $(D_{n,a',b'})_{\mathbb{C}}$ are distinct (unless $(a, b) = \pm(a', b')$ of course) and it is likely true that they are even set-theoretically pairwise distinct (i.e., even without counting the multiplicities). This is not very important for us since Proposition 7.3 and 7.5 are not modified if some of the divisors taken into account are equal.

Proof of Definition-Proposition 7.7. (a) By construction, for any even $n \geq 2$, the number of singular couples $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^4$ is the number of couples $(a', b') \in (\mathbb{Z}/2\mathbb{Z})^4$ such that $a'^t b' = 1 \bmod 2$, and we readily see there are exactly six of them, namely

$$(0101), (1010), (1101), (1110), (1011) \text{ and } (0111).$$

For (b) and (c), the modularity of the function comes from Definition-Proposition 6.14(c) hence we only have to prove that it is nonzero when (a, b) is regular. To do this, we will use the Fourier expansion of this modular form (for more details on Fourier expansions of Siegel modular forms, see chapter 4 of [Klingen 1990]), and simply prove that it has nonzero coefficients. This is also how we will prove the $\vartheta_{a,b}$ are distinct.

To shorten the notations, given $(a,b) \in (\mathbb{Z}/n\mathbb{Z})^4$, we consider instead $(\tilde{a}/n, \tilde{b}/n) \in \mathbb{Q}^4$ for some lift $(\tilde{a}, \tilde{b})$ of (a,b) in $\mathbb{Z}^4$) and by abuse of notation we denote it (a,b) for simplicity. Regularity of the couple translates into the fact that (a,b) is different from six possibles values modulo $\mathbb{Z}^4$, namely

$$\left(0,\tfrac{1}{2},0,\tfrac{1}{2}\right), \left(\tfrac{1}{2},0,\tfrac{1}{2},0\right), \left(\tfrac{1}{2},\tfrac{1}{2},0,\tfrac{1}{2}\right), \left(\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},0\right), \left(\tfrac{1}{2},0,\tfrac{1}{2},\tfrac{1}{2}\right), \left(0,\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2}\right)$$

by (a), which we will assume now. We also fix $n \in \mathbb{N}$ even such that $(na, nb) \in \mathbb{Z}^4$.

Recall that

$$\vartheta_{a,b}(\tau) = e^{i\pi a^t b} \sum_{k \in \mathbb{Z}^2} e^{i\pi (k+a)\tau^t (k+a) + 2i\pi k^t b} \tag{7-3}$$

by (6-12) and (6-14). Therefore, for any symmetric matrix $S \in M_2(\mathbb{Z})$ such that $S/(2n^2)$ is half-integral (i.e., with integer coefficients on the diagonal, and half-integers otherwise), we have $\forall \tau \in \mathcal{H}_2$,

$$\vartheta_{a,b}(\tau + S) = \vartheta_{a,b}(\tau),$$

because for every $k \in \mathbb{Z}^2$,

$$(k+a)S^t(k+a) \in 2\mathbb{Z}.$$

Hence, the function $\vartheta_{a,b}$ admits a Fourier expansion of the form

$$\vartheta_{a,b}(\tau) = \sum_T a_T e^{2i\pi \operatorname{Tr}(T\tau)},$$

where T runs through all the matrices of $S_2(\mathbb{Q})$ such that $(2n^2)T$ is half-integral. This Fourier expansion is unique, because for any $\tau \in \mathcal{H}_2$ and any T, we have

$$(2n^2)a_T = \int_{[0,1]^4} \vartheta_{a,b}(\tau + x) e^{-2i\pi \operatorname{Tr}(T(\tau+x))}\, dx.$$

In particular, the function $\vartheta_{a,b}$ is zero if and only if all its Fourier coefficients a_T are zero, hence we will directly compute those, which are almost directly given by (7-3). For $a = (a_1, a_2) \in \mathbb{Q}^2$ and $k = (k_1, k_2) \in \mathbb{Z}^2$, let us define

$$T_{a,k} = \begin{pmatrix} (k_1+a_1)^2 & (k_1+a_1)(k_2+a_2) \\ (k_1+a_1)(k_2+a_2) & (k_2+a_2)^2 \end{pmatrix},$$

so that

$$\vartheta_{a,b}(\tau) = e^{i\pi a^t b} \sum_{k \in \mathbb{Z}^2} e^{2i\pi k^t b} e^{i\pi \operatorname{Tr}(T_{a,k}\tau)} \tag{7-4}$$

by construction. It is not yet exactly the Fourier expansion, because we have to gather the $T_{a,k}$ giving the same matrix T (and this is where we will use regularity). Clearly,

$$T_{a,k} = T_{a',k'} \iff (k+a) = \pm(k'+a').$$

If $2a \notin \mathbb{Z}^2$, the function $k \mapsto T_{a,k}$ is injective, so (7-4) is the Fourier expansion of $\vartheta_{a,b}$, with clearly nonzero coefficients, hence $\vartheta_{a,b}$ is nonzero.

If $2a = A \in \mathbb{Z}^2$, for every $k, k' \in \mathbb{Z}^2$, we have $(k+a) = \pm(k'+a)$ if and only if $k = k'$ or $k + k' = A$, so the Fourier expansion of $\vartheta_{a,b}$ is

$$\vartheta_{a,b}(\tau) = \frac{e^{i\pi a^t b}}{2} \sum_{T} \sum_{\substack{k,k' \in \mathbb{Z}^2 \\ T_{k,a} = T_{k',a} = T}} (e^{2i\pi k^t b} + e^{2i\pi(-A-k)^t b}) e^{i\pi \operatorname{Tr}(T\tau)}. \tag{7-5}$$

Therefore, the coefficients of this Fourier expansion are all zero if and only if, for every $k \in \mathbb{Z}^2$,

$$e^{2i\pi(2k+A)^t b} = -1,$$

i.e., if and only if $b \in (1/2)\mathbb{Z}$ and $(-1)^{4a^t b} = -1$, and this is exactly singularity of the couple (a, b) which proves (b). $\square$

These divisors have the following properties.

Proposition 7.9 (properties of the $(D_{n,a,b})_{\mathbb{C}}$). *Let $n \in \mathbb{N}_{\geq 2}$ even.*

(a) *For every regular $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^4$, the divisor $(D_{n,a,b})_{\mathbb{C}}$ is ample.*

(b) *For $n = 2$, the ten divisors $(D_{2,a,b})_{\mathbb{C}}$ are set-theoretically pairwise disjoint outside the boundary $\partial A_2(2)_{\mathbb{C}} := A_2(2)^S_{\mathbb{C}} \backslash A_2(2)_{\mathbb{C}}$, and their union is exactly the set of moduli of products of elliptic curves (with any symplectic basis of the 2-torsion).*

(c) *For (A, λ, α_n) a principally polarized complex abelian surface with symplectic structure of level n:*
- *If (A, λ) is a product of elliptic curves, the moduli of (A, λ, α_n) belongs to exactly $n^2 - 3$ divisors $(D_{n,a,b})_{\mathbb{C}}$.*
- *Otherwise, the point (A, λ, α_n) belongs to at most $(\sqrt{2}/2)n^2 + 1/4$ divisors $(D_{n,a,b})_{\mathbb{C}}$.*

Proof. (a) The divisor $(D_{n,a,b})_{\mathbb{C}}$ is by definition the Weil divisor of zeroes of a Siegel modular form of order 2, weight $4n$ and level n, hence of a section of $L^{\otimes 4n}$ on $A_2(n)^S_{\mathbb{C}}$. As L is ample on $A_2(n)^S_{\mathbb{C}}$ (Definition-Proposition 6.4(c)), the divisor $(D_{n,a,b})_{\mathbb{C}}$ is ample.

Now, we know that every complex pair (A, λ) is isomorphic to some (A_τ, λ_τ) with $\tau \in \mathcal{H}_2$ (Definition-Proposition 6.3). If (A, λ) is a product of elliptic curves, the theta divisor of (A, λ, α_2) contains exactly seven 2-torsion points (Proposition 7.3), only one of comes from a regular pair, i.e., (A, λ, α_2) is contained in exactly one of the ten divisors. If (A, λ) is not a product of elliptic curves, it is a jacobian (Proposition 7.4) and the theta divisor of (A, λ, α_2) only contains the six points coming from singular pairs (Proposition 7.5) i.e., (A, λ, α_2) does not belong to any of the ten divisors, which proves (b).

To prove (c), we use the same propositions for general n, keeping in mind that we only count as one the divisors coming from opposite values of (a, b): for products of elliptic curves, this gives $2(n^2-4)/2+1$ divisors (the 1 coming from the even 2-torsion), and for jacobians, this gives $(\sqrt{2}/2)n^2+\frac{1}{4}$ (there are no nontrivial 2-torsion points to consider here). □

We will now give the natural divisors extending $(D_{n,a,b})_{\mathbb{C}}$ on the integral models $\mathcal{A}_2(n)$ (Definition-Proposition 6.6).

Definition 7.10. Let $n \in \mathbb{N}_{\geq 2}$ even.

For every regular $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^4$, the divisor $(D_{n,a,b})_{\mathbb{C}}$ is the geometric fiber at $\mathbb{C}$ of an effective Weil divisor $D_{n,a,b}$ on $\mathcal{A}_2(n)$, such that the moduli of a triple (A, λ, α_n) (on a field k of characteristic prime to n) belongs to $D_{n,a,b}(k)$ if and only if the point of $A[n](\bar{k})$ of coordinates (a, b) for α_n belongs to the theta divisor $\Theta_{A,\lambda,\alpha_n}$ (Definition-Proposition 6.13).

Proof. This amounts to giving an algebraic construction of the $D_{n,a,b}$ satisfying the wanted properties. The following arguments are extracted from Remark I.5.2 of [Faltings and Chai 1990]. Let $\pi : A \to S$ an abelian scheme and $\mathcal{L}$ a symmetric invertible sheaf on A, relatively ample over S and inducing a principal polarization on A. If $s : S \to A$ is a section of A over S, the evaluation at s induces an $\mathcal{O}_S$-module isomorphism between $\pi_*\mathcal{L}$ and $s^*\mathcal{L}$. Now, if s is of n-torsion in A, for $e : S \to A$ the zero section, the sheaf $(s^*\mathcal{L})^{\otimes 2n}$ is isomorphic to $(e^*\mathcal{L})^{\otimes 2n}$, i.e., trivial. We denote by $\omega_{A/S}$ the invertible sheaf on S obtained as the determinant of the sheaf of invariant differential forms on A, and the computations of Theorem I.5.1 and Remark I.5.2 of [Faltings and Chai 1990] give $8\pi_*\mathcal{L} = -4\omega_{A/S}$ in $\mathrm{Pic}(A/S)$. Consequently, the evaluation at s defines (after a choice of trivialization of $(e^*\mathcal{L})^{\otimes 2n}$ and putting to the power $8n$) a section of $\omega_{A/S}^{\otimes 4n}$. Applying this result on the universal abelian scheme (stack if $n \leq 2$) $\mathcal{X}_2(n)$ on $\mathcal{A}_2(n)$, for every $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^4$, the section defined by the point of coordinate (a, b) for the n-structure on $\mathcal{X}_2(n)$ induces a global section $s_{a,b}$ of $\omega_{\mathcal{X}_2(n)/\mathcal{A}_2(n)}^{\otimes 4n}$, and we define $D_{n,a,b}$ as the Weil divisor of zeroes of this section. It remains to check that it satisfies the correct properties.

Let (A, λ, α_n) be a triple over a field k of characteristic prime to n, and L the ample line bundle associated to it by Definition-Proposition 6.13. By construction, its moduli belongs to $D_{n,a,b}$ if and only if the unique (up to constant) nonzero section vanishes at the point of $A[n]$ of coordinates (a, b) in α_n, hence if and only if this point belongs to $\Theta_{A,\lambda,\alpha_n}$.

Finally, we see that the process described above applied to the universal abelian variety $\mathcal{X}_2(n)_{\mathbb{C}}$ of $\mathcal{A}_2(n)_{\mathbb{C}}$ (by means of explicit description of the line bundles as quotients) gives (up to invertible holomorphic functions) the functions $\vartheta_{\tilde{a}/n,\tilde{b}/n}^{8n}$, which proves that $(D_{n,a,b})_{\mathbb{C}}$ is indeed the geometric fiber of $D_{n,a,b}$ (it is easier to see that their complex points are the same, by Proposition 7.9(c) and the above characterization applied to the field $\mathbb{C}$).

If one does not want to use stacks for $n = 2$, one can consider for $(a, b) \in (\mathbb{Z}/2\mathbb{Z})^4$ the divisor $D_{4,2a,2b}$ which is the pullback of $D_{2,a,b}$ by the degeneracy morphism $A_2(4) \to A_2(2)$. □

7B. *Tubular Runge theorems for abelian surfaces and their theta divisors.* We can now prove a family of tubular Runge theorems for the theta divisors $D_{n,a,b}$ (for even $n \geq 2$).

We will state the case $n = 2$ first because its moduli interpretation is easier but the proofs are the same, as we explain below.

In the following results, the *boundary* of $A_2(n)^S_{\mathbb{C}}$ is defined as $\partial A_2(n)^S_{\mathbb{C}} := A_2(n)^S_{\mathbb{C}} \backslash A_2(n)_{\mathbb{C}}$.

Theorem 7.11 (tubular Runge for products of elliptic curves on $\mathcal{A}_2(2)^S$). *Let U be an open neighborhood of $\partial A_2(2)^S_{\mathbb{C}}$ in $A_2(2)^S_{\mathbb{C}}$ for the natural complex topology.*

For any such U, we define $\mathcal{E}(U)$ the set of moduli P of triples (A, λ, α_2) in $\mathcal{A}_2(2)(\overline{\mathbb{Q}})$ such that (choosing L a number field of definition of the moduli):

- *The abelian surface A has potentially good reduction at every finite place $w \in M_L$ (**tubular condition for finite places**).*
- *For any embedding $\sigma : L \to \mathbb{C}$, the image P_σ of P in $\mathcal{A}_2(2)_{\mathbb{C}}$ is outside of U (**tubular condition for archimedean places**).*
- *The number s_L of nonintegrality places of P, i.e., places $w \in M_L$ such that*
  - *either w is above M_L^∞ or 2,*
  - *or the semistable reduction modulo w of (A, λ) is a product of elliptic curves*

  *satisfies the **tubular Runge condition***

$$s_L < 10.$$

*Then, for every choice of U, the set $\mathcal{E}(U)$ is **finite**.*

Theorem 7.12 (tubular Runge for theta divisors on $\mathcal{A}_2(n)^S$). *Let $n \geq 4$ even.*

Let U be an open neighborhood of $\partial A_2(n)^S_{\mathbb{C}}$ in $A_2(n)^S_{\mathbb{C}}$ for the natural complex topology.

For any such U, we define $\mathcal{E}(U)$ the set of moduli P of triples (A, λ, α_n) in $\mathcal{A}_2(n)(\overline{\mathbb{Q}})$ such that (choosing $L \supset \mathbb{Q}(\zeta_n)$ a number field of definition of the triple):

- *The abelian surface A has potentially good reduction at every place $w \in M_L^\infty$ (**tubular condition for finite places**).*
- *For any embedding $\sigma : L \to \mathbb{C}$, the image P_σ of P in $\mathcal{A}_2(n)_{\mathbb{C}}$ is outside of U (**tubular condition for archimedean places**).*
- *The number s_L of nonintegrality places of P, i.e., places $w \in M_L$ such that*
  - *either w is above M_L^∞ or a prime factor of n,*
  - *or the theta divisor of the semistable reduction modulo w of (A, λ, α_n) contains an n-torsion point which is not one of the six points coming from odd characteristics,*

  *satisfies the **tubular Runge condition***

$$(n^2 - 3)s_L < \frac{n^4}{2} + 2.$$

*Then, for every choice of U, the set of points $\mathcal{E}(U)$ is **finite**.*

Remark 7.13. We put an emphasis on the conditions given in the theorem to make it easier to identify how it is an application of our main result, Theorem 5.1. The tubular conditions (archimedean and finite) mean that our points P do not belong to some tubular neighborhood $\mathcal{V}$ of the boundary. We of course chose the boundary as our closed subset to exclude because of its modular interpretation for finite places. The places above M_L^∞ or a prime factor of n are automatically of nonintegrality for our divisors because the model $\mathcal{A}_2(n)$ is not defined at these places. Finally, the second possibility to be a place of nonintegrality straightforwardly comes from the moduli interpretation of the divisors $D_{n,a,b}$ (Definition 7.10). All this is detailed in the proof below.

To give an example of how we can obtain an explicit result in practice, we prove in Section 8 an explicit (and even theoretically better) version of Theorem 7.11.

It would be more satisfying (and easier to express) to give a tubular Runge theorem for which the divisors considered are exactly the irreducible components parametrizing the products of elliptic curves. Unfortunately, except for $n = 2$, there is a serious obstruction because those divisors are not ample, and there are even reasons to suspect they are not big. We have explained in Remark 6.10 why proving the ampleness for general divisors on $A_2(n)^S_{\mathbb{C}}$ is difficult.

It would also be morally satisfying to give a better interpretation of the moduli of the union of all the $D_{n,a,b}$ (for a fixed $n > 2$), i.e., not in terms of the theta divisor, but maybe of the structure of the abelian surface if possible (nontrivial endomorphisms? isogenous to products of elliptic curves?). As far as the author knows, the understanding of abelian surfaces admitting some nontrivial torsion points on their theta divisor is still very limited.

Finally, to give an idea of the margin the tubular Runge condition gives for $n > 2$ (in terms of the number of places which are not "taken" by the automatic bad places), we can easily see that the number of places of $\mathbb{Q}(\zeta_n)$ which are archimedean or above a prime factor of n is less than $n/2$. Hence, we can find examples of extensions L of $\mathbb{Q}(\zeta_n)$ of degree n such that some points defined on it still can satisfy the tubular Runge condition. This is also where using the full strength of tubular Runge theorem is crucial: for $n = 2$, one can compute that some points of the boundary are contained in 6 different divisors $D_{2,a,b}$, and for general even n, a similar analysis gives that the intersection number $m_\varnothing$ is quartic in n, which leaves a lot less margin for the places of nonintegrality (or even none at all).

Proof of Theorems 7.11 and 7.12. As announced, this result is an application of the tubular Runge theorem (Theorem 5.1) to $\mathcal{A}_2(n)^S_{\mathbb{Q}(\zeta_n)}$ (Definition-Proposition 6.6) and the divisors $D_{n,a,b}$ (Definition 7.10), whose properties will be used without specific mention. We reuse the notations of the hypotheses of Theorem 5.1 to explain carefully how it is applied.

(H0) The field of definition of $A_2(n)^S_{\mathbb{C}}$ is $\mathbb{Q}(\zeta_n)$, and the ring over which our model $\mathcal{A}_2(n)^S$ is built is $\mathbb{Z}[\zeta_n, 1/n]$, hence S_0 is made up with all the archimedean places and the places above prime factors of n. There is no need for a finite extension here as all the $D_{n,a,b}$ are divisors on $\mathcal{A}_2(n)^S$.

(H1) The model $\mathcal{A}_2(n)^S_{\mathbb{C}}$ is indeed normal projective, and we know that the $D_{n,a,b}$ are effective Weil divisors hence Cartier divisors up to multiplication by some constant by Proposition 6.8. For any finite extension L of $\mathbb{Q}(\zeta_n)$, the number of orbits r_L is the number of divisors $D_{n,a,b}$ (as they are divisors on the base model), i.e., $n^4/2+2$ (Proposition 7.9(c)).

(**H2**) The chosen closed subset Y of $\mathcal{A}_2(n)^S_{\mathbb{Q}}(\zeta_n)$ is the boundary, namely

$$\partial \mathcal{A}_2(n)^S_{\mathbb{Q}(\zeta_n)} = \mathcal{A}_2(n)^S_{\mathbb{Q}(\zeta_n)} \backslash \mathcal{A}_2(n)_{\mathbb{Q}(\zeta_n)}.$$

We have to prove that the tubular conditions given above correspond to a tubular neighborhood. To do this, let $\mathcal{Y}$ be the boundary $\mathcal{A}_2(n)^S \backslash \mathcal{A}_2(n)$ and $g_1, \ldots, g_s$ homogeneous generators of the ideal of definition of $\mathcal{Y}$ after having fixed a projective embedding of $\mathcal{A}_2(n)$. Let us find an $M_{\mathbb{Q}(\zeta_n)}$-constant such that $\mathcal{E}(U)$ is included in the tubular neighborhood of $\partial \mathcal{A}_2(n)^S_{\mathbb{Q}}(\zeta_n)$ in $A_2(n)^S_{\mathbb{Q}(\zeta_n)}$ associated to $\mathcal{C}$ and $g_1, \ldots, g_k$. For the places w not above M_L^∞ or a prime factor of n, the fact that $P = (A, \lambda, \alpha_n)$ does not reduce in Y modulo w is exactly equivalent to A having potentially good reduction at w hence we can choose $c_v = 0$ for the places v of $\mathbb{Q}(\zeta_n)$ not archimedean and not dividing n. For archimedean places, belonging to U for an embedding $\sigma : L \to \mathbb{C}$ implies that $g_1, \ldots, g_n$ are small, and we just have to choose c_v strictly larger than the maximum of the norms of the $g_i(U \cap V_j)$ (in the natural affine covering $(V_j)_j$ of the projective space), independent of the choice of $v \in M^\infty_{\mathbb{Q}(\zeta_n)}$. Finally, we have to consider the case of places above a prime factor of n. To do this, we only have to recall that having potentially good reduction can be given by integrality of some quotients of the Igusa invariants at finite places, and these invariants are modular forms on $\Gamma_2(1)$. We can add those who vanish on the boundary to the homogeneous generators $g_1, \ldots, g_n$ and consider $c_v = 0$ for these places as well. This is explicitly done in Section 8C for $A_2(2)$.

(**TRC**) As said before, there are $n^4/2+2$ divisors considered, and their generic fibers are ample by Proposition 7.9. Furthermore, by Propositions 7.3 and 7.5, outside the boundary, at most (n^2-3) can have nonempty common intersection, and this exact number is attained only for products of elliptic curves.

This gives the tubular Runge condition

$$(n^2-3)s_L < \frac{n^4}{2} + 2,$$

which concludes the proof.

For $n = 2$, the union of the ten $D_{2,a,b}$ is made up with the moduli of products of elliptic curves, and they are pairwise disjoint outside $\partial A_2(2)$ (Proposition 7.9(b)), hence the simply expressed condition $s_L < 10$ in this case. □

8. The explicit Runge result for level two

To finish this paper, we improve and make explicit the finiteness result of Theorem 7.11, as a proof of principle of the method.

Before stating Theorem 8.2, we need some notations. In level two, the auxiliary functions are deduced from the ten even theta constants of characteristic two, namely the functions $\Theta_{m/2}(\tau)$ (notation (6-11)), with the quadruples m going through

$$E = \{(0000), (0001), (0010), (0011), (0100), (0110), (1000), (1001), (1100), (1111)\} \tag{8-1}$$

(see Sections 6C and 7A for details). We recall [van der Geer 1982, Theorem 5.2] that these functions define an embedding

$$\begin{aligned} \psi : A_2(2) &\to \mathbb{P}^9 \\ \bar{\tau} &\mapsto (\Theta^4_{m/2}(\tau))_{m \in E} \end{aligned} \tag{8-2}$$

which induces an isomorphism between $A_2(2)^S_{\mathbb{C}}$ and the subvariety of $\mathbb{P}^9$ (with coordinates indexed by $m \in E$) defined by the linear equations

$$x_{1000} - x_{1100} + x_{1111} - x_{1001} = 0 \tag{8-3}$$

$$x_{0000} - x_{0001} - x_{0110} - x_{1100} = 0 \tag{8-4}$$

$$x_{0110} - x_{0010} - x_{1111} + x_{0011} = 0 \tag{8-5}$$

$$x_{0100} - x_{0000} + x_{1001} + x_{0011} = 0 \tag{8-6}$$

$$x_{0100} - x_{1000} + x_{0001} - x_{0010} = 0 \tag{8-7}$$

(which makes it a subvariety of $\mathbb{P}^4$) together with the quartic equation

$$\left(\sum_{m \in E} x_m^2 \right)^2 - 4 \sum_{m \in E} x_m^4 = 0. \tag{8-8}$$

Remark 8.1. For the attentive reader, the first linear equation has sign $(+1)$ in x_{1111} whereas it is (-1) in [van der Geer 1982], as there seems to be a typographic mistake there: we found the mistake during our computations in Sage in Section 8C and found the correct sign using Igusa's relations [1964, Lemma 1 combined with the proof of Theorem 1].

There is a natural definition for a tubular neighborhood of $Y = \partial A_2(2)$: for a finite place v, as in Theorem 7.11, we choose V_v as the set of triples $P = \overline{(A, \lambda, \alpha_2)}$ where A has potentially bad reduction modulo v. To complete it with archimedean places, we use the classical fundamental domain for the action of $\mathrm{Sp}_4(\mathbb{Z})$ on $\mathcal{H}_2$ denoted by $\mathcal{F}_2$ (see [Klingen 1990, §I.2], for details). Given some parameter $t \geq \sqrt{3}/2$, the neighborhood $V(t)$ of $\partial A_2(2)^S_{\mathbb{C}}$ in $A_2(2)^S_{\mathbb{C}}$ is made up with the points P whose lift τ in $\mathcal{F}_2$ (for the usual quotient morphism $\mathcal{H}_2 \to A_2(1)_{\mathbb{C}}$) satisfies $\mathrm{Im}(\tau_4) \geq t$, where τ_4 is the lower-right coefficient of τ. We choose $V(t)$ as the archimedean component of the tubular neighborhood for every archimedean place. The reader knowledgeable with the construction of Satake compactification will have already seen such neighborhoods of the boundary.

Notice that for a point $P = \overline{(A, \lambda, \alpha_2)} \in A_2(2)(K)$, the abelian surface A is only defined over a finite extension L of K, but for prime ideals $\mathfrak{P}_1$ and $\mathfrak{P}_2$ of $\mathcal{O}_L$ above the same prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$, the reductions of A modulo $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are of the same type because $P \in A_2(2)(K)$. This justifies what we mean by "semistable reduction of A modulo $\mathfrak{P}$" below.

Theorem 8.2. *Let K be a number field and $P = \overline{(A, \lambda, \alpha_2)} \in A_2(2)(K)$ where A has potentially good reduction at every finite place.*

Let s_P be the number of prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$ such that the semistable reduction of A modulo $\mathfrak{P}$ is a product of elliptic curves. We denote by $h_{\mathcal{F}}$ the stable Faltings height of A.

(a) *If $K = \mathbb{Q}$ or an imaginary quadratic field and*

$$|s_P| < 4$$

then

$$h(\psi(P)) \leq 10.75, \quad h_{\mathcal{F}}(A) \leq 828.$$

(b) *Let $t \geq \sqrt{3}/2$ be a real number. If for every embedding $\sigma : K \to \mathbb{C}$, the point $P_\sigma \in A_2(2)_{\mathbb{C}}$ does not belong to $V(t)$, and*

$$|s_P| + |M_K^\infty| < 10$$

then

$$h(\psi(P)) \leq 4\pi t + 8.44, \quad h_{\mathcal{F}}(A) \leq 2\pi t + 5 + 533 \log(\pi t + 5)$$

Remark 8.3. Previous versions gave a bound $h_{\mathcal{F}}(A) \leq 1070$. This was actually due to an error in comparing the height of $\psi(P)$ and the Faltings height, and this error worsened the bounds, hence the slightly better new bound.

The Runge condition for (b) is a straightforward application of our tubular Runge theorem. For (a), we did not assume anything on the point P at the (unique) archimedean place, which eliminates six divisors when applying Runge's method here, hence the different Runge condition here (see Remark 5.2(b)).

The principle of proof is very simple: we apply Runge's method to bound the height of $\psi(P)$ when P satisfies the conditions of Theorem 7.11, and using the link between this height and Faltings height given in [Pazuki 2012, Corollary 1.3], we know we will obtain a bound of the shape

$$h_{\mathcal{F}}(P) \leq f(t)$$

where f is an explicit function of t, for every point P satisfying the conditions of Theorem 7.11.

At the places of good reduction not dividing 2, the contribution to the height is easy to compute thanks to the theory of algebraic theta functions devised in [Mumford 1966; 1967]. The theory will be sketched in Section 8A, resulting in Proposition 8.4.

For the archimedean places, preexisting estimates due to Streng for Fourier expansions on each of the ten theta functions allow us to make explicit how only one of them can be too small compared to the others, when we are outside of $V(t)$. This is the topic of Section 8B.

For the places above 2, the theory of algebraic theta functions cannot be applied. To bypass the problem, we use Igusa invariants (which behave in a well-known fashion for reduction in any characteristic) and prove that the theta functions are algebraic and "almost integral" on the ring of these Igusa invariants, with explicit coefficients. Combining these two facts in Section 8C, we will obtain Proposition 8.7, a less-sharp avatar of Proposition 8.4, but explicit nonetheless.

Finally, we put together these estimates in Section 8D and obtain the stated bounds on $h \circ \psi$ and the Faltings height.

8A. ***Algebraic theta functions and the places of potentially good reduction outside of 2.*** The goal of this part is the following result.

Proposition 8.4. *Let K be a number field and $\mathfrak{P}$ a maximal ideal of $\mathcal{O}_K$, of residue field $k(\mathfrak{P})$ with characteristic different from 2. Let $P = \overline{(A, \lambda, \alpha_2)} \in A_2(2)(K)$. Then, $\psi(P) \in \mathbb{P}^9(K)$ and:*

(a) *If the semistable reduction of A modulo $\mathfrak{P}$ is a product of elliptic curves, the reduction of $\psi(P)$ modulo $\mathfrak{P}$ has exactly one zero coordinate, in other words every coordinate of $\psi(P)$ has the same $\mathfrak{P}$-adic norm except one which is strictly smaller.*

(b) *If the semistable reduction of A modulo $\mathfrak{P}$ is a jacobian of hyperelliptic curve, the reduction of $\psi(P)$ modulo $\mathfrak{P}$ has no zero coordinate, in other words every coordinate of $\psi(P)$ has the same $\mathfrak{P}$-adic norm.*

To link $\psi(P)$ with the intrinsic behavior of A, we use the theory of algebraic theta functions, devised in [Mumford 1966; 1967] (see also [David and Philippon 2002; Pazuki 2012]). As it is not very useful nor enlightening to go into detail or repeat known results, we only mention them briefly here. In the following, A is an abelian variety of dimension g over a field k and L an ample symmetric line bundle on A inducing a principal polarization λ. We also fix $n \geq 2$ even, assuming that all the points of $2n$-torsion of A are defined over k and $\mathrm{char}(k)$ does not divide n (in particular, we always assume $\mathrm{char}(k) \neq 2$). Let us denote formally the Heisenberg group $\mathcal{G}(\underline{n})$ as the set

$$\mathcal{G}(\underline{n}) := k^* \times (\mathbb{Z}/n\mathbb{Z})^g \times (\mathbb{Z}/n\mathbb{Z})^g$$

equipped with the group law

$$(\alpha, a, b) \cdot (\alpha', a', b') := (\alpha\alpha' e^{(2i\pi/n)a^t b'}, a + a', b + b')$$

(contrary to the convention of [Mumford 1966, p. 294], we identified the dual of $(\mathbb{Z}/n\mathbb{Z})^g$ with itself). Recall that $A[n]$ is exactly the group of elements of $A(\bar{k})$ such that $T_x^*(L^{\otimes n}) \cong L^{\otimes n}$; indeed, it is by definition the kernel of the morphism $\phi_{L^{\otimes n}} = n\phi_L$ from A to $\hat{A}$ (see the references mentioned in the proof of Proposition 6.12).

Proof. Given the datum of a *theta structure* on $L^{\otimes n}$, i.e., an isomorphism $\beta : \mathcal{G}(L^{\otimes n}) \cong \mathcal{G}(\underline{n})$ which is the identity on k^* (see [Mumford 1966, p. 289] for the definition of $\mathcal{G}(L^{\otimes n})$), one has a natural action of $\mathcal{G}(\underline{n})$ on $\Gamma(A, L^{\otimes n})$ (a consequence of Proposition 3 and Theorem 2 of [Mumford 1966]), hence for $n \geq 4$ the following projective embedding of A:

$$\begin{aligned} \psi_\beta : A &\to \mathbb{P}_k^{n^{2g}-1} \\ x &\mapsto (((1, a, b) \cdot (s_0^{\otimes n}))(x))_{a,b \in (\mathbb{Z}/n\mathbb{Z})^g}, \end{aligned} \tag{8-9}$$

where s_0 is a nonzero section of $\Gamma(A, L)$, hence unique up to multiplicative scalar (therefore ψ_β only depends on β). This embedding is not exactly the same as the one defined in [Mumford 1966, p. 298] (it has more coordinates), but the principle does not change at all. One calls *Mumford coordinates of* (A, L) *associated to* β the projective point $\psi_\beta(0) \in \mathbb{P}^{n^{2g}-1}(k)$.

Now, one has the following commutative diagram whose rows are canonical exact sequences [Mumford 1966, Corollary of Theorem 1],

$$\begin{array}{ccccccccc} 0 & \longrightarrow & k^* & \longrightarrow & \mathcal{G}(L^{\otimes n}) & \longrightarrow & A[n] & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow{\beta} & & \downarrow{\alpha_n} & & \\ 0 & \longrightarrow & k^* & \longrightarrow & \mathcal{G}(\underline{n}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^{2g} & \longrightarrow & 0, \end{array}$$

where α_n is a symplectic level n structure on $A[n]$ (Definition 6.1), called *the symplectic level n structure induced by* β. Moreover, for every $x \in A(k)$, the coordinates of $\psi_\beta(x)$ are (up to constant values for each coordinate, only depending on β) the $\vartheta_{A,L}([n]x + \alpha_n^{-1}(a, b))$ (see Definition 6.11). In particular, for any $a, b \in (\mathbb{Z}/n\mathbb{Z})^g$,

$$\psi_\beta(0)_{a,b} = 0 \Leftrightarrow \alpha_n^{-1}(a, b) \in \Theta_{A,L}. \tag{8-10}$$

Furthermore, for two theta structures β and β' on $[n]^*L$ inducing α_n, one sees that $\beta' \circ \beta^{-1}$ is of the shape $(\alpha, a, b) \mapsto (\alpha \cdot f(a, b), a, b)$, where f has values in n-th roots of unity, hence ψ_β and $\psi_{\beta'}$ only differ multiplicatively by n-th roots of unity.

Conversely, given the datum of a symplectic structure α_{2n} on $A[2n]$, there exists an unique *symmetric theta structure* on $[n]^*L$ which is *compatible* with some symmetric theta structure on $[2n]^*L$ inducing α_{2n} [Mumford 1966, p. 317 and Remark 3 p. 319]. We call it the *theta structure on* $[n]^*L$ *induced by* α_{2n}. Thus, we just proved that the datum of a symmetric theta structure on $[n]^*L$ is intermediary between a level $2n$ symplectic structure and a level n symplectic structure (the exact congruence group is easily identified as $\Gamma_g(n, 2n)$ with the notations of [Igusa 1966]).

Now, for a triple (A, L, α_{2n}) (notations of Section 6A), when A is a complex abelian variety, there exists $\tau \in \mathcal{H}_g$ such that this triple is isomorphic to $(A_\tau, L_\tau, \alpha_{\tau,2n})$ (Definition-Proposition 6.3). By definition of L_τ as a quotient (6-3), the sections of $L_\tau^{\otimes n}$ canonically identify to holomorphic functions ϑ on $\mathbb{C}^g$ such that, $\forall p, q \in \mathbb{Z}^g$ and $\forall z \in \mathbb{C}^g$,

$$\vartheta(z + p\tau + q) = e^{-i\pi n \tau^t n - 2i\pi n^t z}\vartheta(z), \tag{8-11}$$

and through this identification one sees (after some tedious computations) that the symmetric theta structure β_τ on $L_\tau^{\otimes n}$ induced by $\alpha_{\tau,2n}$ acts by

$$((\alpha, a, b) \cdot \vartheta)(z) = \alpha \exp\left(\frac{i\pi}{n}\tilde{a}\tau\tilde{a} + \frac{2i\pi}{n}\tilde{a}^t(z + \tilde{b})\right)\vartheta\left(z + \frac{\tilde{a}}{n}\tau + \frac{\tilde{b}}{n}\right),$$

where $\tilde{a}$ and $\tilde{b}$ are lifts of a and b in $\mathbb{Z}^g$ (the result does not depend on this choice by (8-11)). Therefore, by ψ_β and the theta functions with characteristic (formula (6-12)), the Mumford coordinates of (A, L, α_{2n})

(with the induced theta structure β on $L^{\otimes n}$) are *exactly* the projective coordinates

$$(\Theta^n_{\tilde{a}/n,\tilde{b}/n(\tau)}(\tau))_{a,b\in\frac{1}{n}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}} \in \mathbb{P}^{n^{2g}-1}(\mathbb{C}),$$

where the choices of lifts $\tilde{a}$ and $\tilde{b}$ for a and b still do not matter.

In particular, for every $\tau \in \mathcal{H}_2$, the point $\psi(\tau)$ can be intrinsically given as the squares of Mumford coordinates for β_τ, where the six odd characteristics (whose coordinates vanish everywhere) are taken out. The result only depends on the isomorphism class of $(A_\tau, L_\tau, \alpha_{\tau,2})$, as expected.

Finally, as demonstrated in paragraph 6 of [Mumford 1967] (especially the theorem on page 83), the theory of theta structures (and the associated Mumford coordinates) can be extended to abelian schemes (Definition 6.5) (still outside characteristics dividing $2n$), and the Mumford coordinates in this context lead to an embedding of the associated moduli space in a projective space as long as the *type* of the sheaf is a multiple of 8 (which for us amounts to $8 \mid n$). Here, fixing a principally polarized abelian variety A over a number field K and $\mathfrak{P}$ a prime ideal of $\mathcal{O}_K$ not above 2, this theory means that given a symmetric theta structure on (A, L) for $L^{\otimes n}$ where $8 \mid n$, if A has good reduction modulo $\mathfrak{P}$, this theta structure has a natural reduction to a theta structure on the reduction $(A_\mathfrak{P}, L_\mathfrak{P})$ for $L_\mathfrak{P}^{\otimes n}$, and this reduction is compatible with the reduction of Mumford coordinates modulo $\mathfrak{P}$. To link this with the reduction of coordinates of ψ, one just has to extend the number field K of definition of A so that all 8-torsion points of A are defined over K (in particular, the reduction of A modulo $\mathfrak{P}$ is semistable), and consider a symmetric theta structure on $L^{\otimes 8}$. The associated Mumford coordinates then reduce modulo $\mathfrak{P}$, and making use of (8-10) and Propositions 7.3 and 7.5 over the residue field, one of the Mumford coordinates coming from the 2-torsion does not vanish. We can now consider only the coordinates coming from the 2-torsion and it yields Proposition 8.4 (not forgetting the six ever-implicit odd characteristics). □

8B. ***Evaluating the theta functions at archimedean places.*** We denote by $\mathcal{H}_2$ the Siegel half-space of degree 2, and by $\mathcal{F}_2$ the usual fundamental domain of this half-space for the action of $\mathrm{Sp}_4(\mathbb{Z})$ (see [Klingen 1990, §I.2] for details). For $\tau \in \mathcal{H}_2$, we denote by y_4 the imaginary part of the lower-right coefficient of τ.

Proposition 8.5. *For every $\tau \in \mathcal{H}_2$ and a fixed real parameter $t \geq \sqrt{3}/2$, one has*:

(a) *Amongst the ten even characteristics m of E, at most six of them can satisfy*

$$|\Theta_{m/2}(\tau)| < 0.42 \max_{m'\in E} |\Theta_{m'/2}(\tau)|.$$

(b) *If the representative of the orbit of τ in the fundamental domain $\mathcal{F}_2$ satisfies $y_4 \leq t$, at most one of the ten even characteristics m of E can satisfy*

$$|\Theta_{m/2}(\tau)| < 0.747 e^{-\pi t} \max_{m'\in E} |\Theta_{m'/2}(\tau)|.$$

Proof. First, we can assume that $\tau \in \mathcal{F}_2$ as the inequalities (a) and (b) are invariant by the action of $\mathrm{Sp}_4(\mathbb{Z})$, given the complete transformation formula of these theta functions [Mumford 2007, §II.5]. Now, using the Fourier expansions of the ten theta constants (mentioned in the proof of Definition-Proposition 7.7) and isolating their respective dominant terms (such as in [Klingen 1990], proof of Proposition IV.2), we obtain explicit estimates. More precisely, Proposition 7.7 of [Streng 2010] states that, for every $\tau = \left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_4 \end{smallmatrix}\right) \in \mathcal{B}_2$ (which is a domain containing $\mathcal{F}_2$), one has

$$|\Theta_{m/2}(\tau) - 1| < 0.405, \quad m \in \{(0000)(0001),(0010),(0011)\}.$$

$$\left|\frac{\Theta_{m/2}(\tau)}{2e^{i\pi\tau_1/2}} - 1\right| < 0.348, \quad m \in \{(0100),(0110)\}.$$

$$\left|\frac{\Theta_{m/2}(\tau)}{2e^{i\pi\tau_4/2}} - 1\right| < 0.348, \quad m \in \{(1000),(1001)\}.$$

$$\left|\frac{\Theta_{m/2}(\tau)}{2(\varepsilon_m + e^{2i\pi\tau_2})e^{i\pi(\tau_1+\tau_4-2\tau_2)/2}} - 1\right| < 0.438, \quad m \in \{(1100),(1111)\},$$

with $\varepsilon_m = 1$ if $m = (1100)$ and -1 if $m = (1111)$.

Under the assumption that $y_4 \le t$ (which induces the same bound for $\operatorname{Im} \tau_1$ and $2 \operatorname{Im} \tau_2$), we obtain

$$0.595 < |\Theta_{m/2}(\tau)| < 1.405, \quad m \in \{(0000)(0001),(0010),(0011)\}.$$

$$1.304e^{-\pi t/2} < |\Theta_{m/2}(\tau)| < 0.692, \quad m \in \{(0100),(0110),(1000),(1001)\}.$$

$$1.05e^{-\pi t} < |\Theta_{m/2}(\tau)| < 0.855, \quad m = (1100).$$

$$|\Theta_{m/2}(\tau)| < 0.855, \quad m = (1111)$$

Thus, we get (a) with $\frac{0.595}{1.405} > 0.42$, and (b) with $\frac{1.05}{1.405}e^{-\pi t} > 0.747e^{-\pi t}$. □

8C. ***Computations with Igusa invariants for the places above 2 case.*** In this case, as emphasized before, it is not possible to use Proposition 8.4, as the algebraic theory of theta functions does not work.

We have substituted it in the following way.

Definition 8.6 (auxiliary polynomials). For every $i \in \{1, \dots, 10\}$, let Σ_i be the i-th symmetric polynomial in the ten modular forms $\Theta^8_{m/2}$, $m \in E$ (notation (8-1)). This is a modular form of level $4i$ for the whole modular group $\mathrm{Sp}_4(\mathbb{Z})$.

Indeed, each $\Theta^8_{m/2}$ is a modular form for the congruence subgroup $\Gamma_2(2)$ of weight 4, and they are permuted by the modular action of $\Gamma_2(1)$ [Mumford 2007, §II.5]. The important point is that the Σ_i are then polynomials in the four Igusa modular forms ψ_4, ψ_6, χ_{10} and χ_{12} [Igusa 1967, pp. 848–849]. We can now explain the principle of this paragraph: these four modular forms are linked explicitly with the Igusa invariants (for a given jacobian of an hyperelliptic curve C over a number field K), and the semistable reduction of the jacobian at some place $v \mid 2$ is determined by the integrality (or not) of some quotients of these invariants, hence rational fractions of the modular forms. Now, with the explicit expressions of the Σ_i in terms of ψ_4, ψ_6, χ_{10} and χ_{12}, we can bound these Σ_i by one of the Igusa invariants, and as every $\Theta^8_{m/2}$ is a root of the polynomial

$$P(X) = X^{10} - \Sigma_1 X^9 + \Sigma_2 X^8 - \Sigma_3 X^7 + \Sigma_4 X^6 - \Sigma_5 X^5 + \Sigma_6 X^4 - \Sigma_7 X^4 + \Sigma_8 X^2 - \Sigma_9 X + \Sigma_{10},$$

we can infer an explicit bound above on the $\Theta_{m/2}^8/\lambda$, with a well-chosen normalizing factor λ such that these quotients belong to K. Actually, we will even give an approximate shape of the Newton polygon of the polynomial $\lambda^{10} P(X/\lambda)$, implying that its slopes (except maybe the first one) are bounded above and below, thus giving us a lower bound for each of the $|\Theta_{m/2}|_v / \max_{m' \in E} |\Theta_{m'/2}|_v$, except maybe for one m. The explicit result is the following.

Proposition 8.7. *Let K be a number field, (A, L) a principally polarized jacobian of dimension 2 over K and $\tau \in \mathcal{H}_2$ such that $(A_\tau, L_\tau) \cong (A, L)$.*

Let $\mathfrak{P}$ be a prime ideal of K above 2 such that A has potentially good reduction at $\mathfrak{P}$, and the reduced (principally polarized abelian surface) is denoted by $(A_{\mathfrak{P}}, L_{\mathfrak{P}})$. By abuse of notation, we forget the normalizing factor ensuring that the coordinates $\Theta_{m/2}(\tau)^8$ belong to K.

(a) *If $(A_{\mathfrak{P}}, L_{\mathfrak{P}})$ is the jacobian of a smooth hyperelliptic curve, all the $m \in E$ satisfy*

$$\frac{|\Theta_{m/2}(\tau)^8|_{\mathfrak{P}}}{\max_{m' \in E} |\Theta_{m'/2}(\tau)^8|_{\mathfrak{P}}} \geq |2|_{\mathfrak{P}}^{12}.$$

(b) *If $(A_{\mathfrak{P}}, L_{\mathfrak{P}})$ is a product of elliptic curves, all the $m \in E$ except at most one satisfy*

$$\frac{|\Theta_{m/2}(\tau)^8|_{\mathfrak{P}}}{\max_{m' \in E} |\Theta_{m'/2}(\tau)^8|_{\mathfrak{P}}} \geq |2|_{\mathfrak{P}}^{21}.$$

Proof. The most technical part is computing the Σ_i as polynomials in the four Igusa modular forms. To do this, we worked with Sage in the formal algebra generated by some sums of $\Theta_{m/2}^4$ with explicit relations (namely, $y_0, \ldots, y_4$ in the notations of [Igusa 1964, pp. 396–397]). The total computation time, done on a laptop PC, was approximately twelve hours (including the verification of the results). The algorithms and details of their construction is available on a Sage worksheet (in Jupyter format).[1] An approach based on Fourier expansions might be more efficient, but as there is no clear closed formula for the involved modular forms, we privileged computations in this formal algebra. For easier reading, we slightly modified the Igusa modular forms into h_4, h_6, h_{10}, h_{12} defined as

$$\begin{cases} h_4 = 2 \cdot \psi_4 = \frac{1}{2} \displaystyle\sum_{m \in E} \Theta_{m/2}^8 \\ h_6 = 2^2 \cdot \psi_6 = \displaystyle\sum_{\substack{\{m_1, m_2, m_3\} \subset E \\ \text{syzygous}}} \pm (\Theta_{m_1/2} \Theta_{m_2/2} \Theta_{m_3/2})^4 \\ h_{10} = 2^{15} \cdot \chi_{10} = 2 \displaystyle\prod_{m \in E} \Theta_{m/2}^2 \\ h_{12} = 2^{16} \cdot 3 \cdot \chi_{12} = \frac{1}{2} \displaystyle\sum_{\substack{C \subset E \\ C \text{ Göpel}}} \prod_{m \in E \setminus C} \Theta_{m/2}^4 \end{cases} \tag{8-12}$$

([Igusa 1967, p. 848] for details on these definitions, notably syzygous triples and Göpel quadruples). The third expression is not explicitly a polynomial in $y_0, \ldots, y_4$, but there is such an expression, given

[1] This worksheet can be found at http://msp.org/ant/2019/13-1/ant-v13-n1-x01-Igusainvariants.ipynb.

on page 397 of [Igusa 1964]. We also used to great benefit (both for understanding and computations) Section I.7.1 of [Streng 2010].

Now, the computations in Sage gave us the following formulas (the first and last one being trivial given (8-12), were not computed by the algorithm)

$$\Sigma_1 = 2h_4 \tag{8-13}$$

$$\Sigma_2 = \frac{3}{2}h_4^2 \tag{8-14}$$

$$\Sigma_3 = \frac{29}{2\cdot 3^3}h_4^3 - \frac{1}{2\cdot 3^3}h_6^2 + \frac{1}{2\cdot 3}h_{12} \tag{8-15}$$

$$\Sigma_4 = \frac{43}{2^4\cdot 3^3}h_4^4 - \frac{1}{2\cdot 3^3}h_4h_6^2 + \frac{23}{2\cdot 3}h_4h_{12} + \frac{2}{3}h_6h_{10} \tag{8-16}$$

$$\Sigma_5 = \frac{1}{2^2\cdot 3^3}h_4^5 - \frac{1}{2^3\cdot 3^3}h_4^2h_6^2 + \frac{25}{2^3\cdot 3}h_4^2h_{12} - \frac{1}{2\cdot 3}h_4h_6h_{10} + \frac{123}{2^2}h_{10}^2 \tag{8-17}$$

$$\begin{aligned}\Sigma_6 = {} & \frac{1}{2^2\cdot 3^6}h_4^6 - \frac{1}{2^2\cdot 3^6}h_4^3h_6^2 + \frac{7}{2\cdot 3^3}h_4^3h_{12} - \frac{1}{2^2\cdot 3}h_4^2h_6h_{10} \\ & + \frac{47}{2\cdot 3}h_4h_{10}^2 + \frac{1}{2^4\cdot 3^6}h_6^4 - \frac{5}{2^3\cdot 3^3}h_6^2h_{12} + \frac{43}{2^4\cdot 3}h_{12}^2\end{aligned} \tag{8-18}$$

$$\begin{aligned}\Sigma_7 = {} & \frac{1}{2\cdot 3^4}h_4^2h_{12} - \frac{1}{2\cdot 3^4}h_4^3h_6h_{10} + \frac{41}{2^3 3^2}h_4^2h_{10}^2 - \frac{1}{2^2\cdot 3^4}h_4h_6^2h_{12} \\ & + \frac{11}{2^2\cdot 3^2}h_4h_{12}^2 + \frac{1}{2^2\cdot 3^4}h_6^3h_{10} - \frac{19}{2^2\cdot 3^2}h_6h_{10}h_{12}\end{aligned} \tag{8-19}$$

$$\Sigma_8 = \frac{1}{2^2\cdot 3^3}h_4^3h_{10}^2 + \frac{1}{2^2\cdot 3^2}h_4^2h_{12}^2 - \frac{1}{2\cdot 3^2}h_4h_6h_{10}h_{12} + \frac{5}{2^3\cdot 3^3}h_6^2h_{10}^2 - \frac{11}{2^3}h_{10}^2h_{12} \tag{8-20}$$

$$\Sigma_9 = \frac{-5}{2^2\cdot 3^2}h_4h_{10}^2h_{12} + \frac{7}{2^2\cdot 3^3}h_6h_{10}^3 + \frac{1}{3^3}h_{12}^3 \tag{8-21}$$

$$\Sigma_{10} = \frac{1}{2^4}h_{10}^4. \tag{8-22}$$

Remark 8.8. The denominators are always products of powers of 2 and 3. This was predicted by Ichikawa [2009], as all Fourier expansions of $\Theta_{m/2}$ (therefore of the Σ_i) have integral coefficients. Surprisingly, the result of [Ichikawa 2009] would actually be false for a $\mathbb{Z}[1/3]$-algebra instead of a $\mathbb{Z}[1/6]$-algebra, as the expression of Σ_3 (converted as a polynomial in ψ_4, ψ_6, χ_{12}) shows, but this does not provide a counterexample for a $\mathbb{Z}[1/2]$-algebra.

Now, let C be a hyperelliptic curve of genus 2 on a number field K and $\mathfrak{P}$ a prime ideal of $\mathcal{O}_K$ above 2. We will denote by $|\cdot|$ the norm associated to $\mathfrak{P}$ to lighten the notation. Let A be the jacobian of C and J_2, J_4, J_6, J_8, J_{10} the homogeneous Igusa invariants of the curve C, defined as in [Igusa 1960, pp. 621–622] up to a choice of hyperelliptic equation for C. We fix $\tau \in \mathcal{H}_2$ such that A_τ is isomorphic to A, which will be implicit in the following (i.e., h_4 denotes $h_4(\tau)$ for example). By [Igusa 1967, p. 848] applied with our normalization, there is an hyperelliptic equation for C (and we fix it) such that

$$J_2 = \frac{1}{2}\frac{h_{12}}{h_{10}} \tag{8-23}$$

$$J_4 = \frac{1}{2^5\cdot 3}\left(\frac{h_{12}^2}{h_{10}^2} - 2h_4\right) \tag{8-24}$$

$$J_6 = \frac{1}{2^7\cdot 3^3}\left(\frac{h_{12}^3}{h_{10}^3} - 6\frac{h_4 h_{12}}{h_{10}} + 4h_6\right) \tag{8-25}$$

$$J_8 = \frac{1}{2^{12}\cdot 3^3}\left(\frac{h_{12}^4}{h_{10}^4} - 12\frac{h_4 h_{12}^2}{h_{10}^2} + 16\frac{h_6 h_{12}}{h_{10}} - 12h_4^2\right) \tag{8-26}$$

$$J_{10} = \frac{1}{2^{13}}h_{10}. \tag{8-27}$$

Let us now figure out the Newton polygons allowing us to bound our theta constants.

(a) If A has potentially good reduction at $\mathfrak{P}$, and this reduction is also a jacobian, by Proposition 3 of [Igusa 1960], the quotients J_2^5/J_{10}, J_4^5/J_{10}^2, J_6^5/J_{10}^3 and J_8^5/J_{10}^4 are all integral at $\mathfrak{P}$. Translating it into quotients of modular forms, this gives

$$\left|\frac{J_2^5}{J_{10}}\right| = |2|^8\left|\frac{h_{12}^5}{h_{10}^6}\right| \le 1$$

$$\left|\frac{J_4^5}{J_{10}^2}\right| = |2|^3\left|\frac{h_{12}^2}{h_{10}^{12/5}} - 2\frac{h_4}{h_{10}^{2/5}}\right|^5 \le 1$$

$$\left|\frac{J_6^5}{J_{10}^3}\right| = |2|^4\left|\frac{h_{12}^3}{h_{10}^{18/5}} - 6\frac{h_4 h_{12}}{h_{10}^{8/5}} + 4\frac{h_6}{h_{10}^{3/5}}\right|^5 \le 1$$

$$\left|\frac{J_8^5}{J_{10}^4}\right| = |2|^{-8}\left|\frac{h_{12}^4}{h_{10}^{24/5}} - 12\frac{h_4 h_{12}^2}{h_{10}^{14/5}} + 16\frac{h_6 h_{12}}{h_{10}^{9/5}} - 12\frac{h_4^2}{h_{10}^{4/5}}\right|^5 \le 1.$$

By successive bounds on the three first lines, we obtain

$$\left|\frac{h_4}{h_{10}^{2/5}}\right| \le |2|^{-21/5}, \qquad \left|\frac{h_6}{h_{10}^{3/5}}\right| \le |2|^{-34/5}, \qquad \left|\frac{h_{12}}{h_{10}^{6/5}}\right| \le |2|^{-8/5}. \tag{8-28}$$

Using the expressions of the Σ_i ((8-13)–(8-22)), we compute that for every $i \in \{1,\dots,10\}$, one has $\left|\Sigma_i/h_{10}^{2i/5}\right| \le |2|^{\lambda_i}$ with the following values of λ_i:

i	10	9	8	7	6	5	4	3	2	1
λ_i	$-\frac{20}{5}$	$-\frac{44}{5}$	$-\frac{83}{5}$	$-\frac{112}{5}$	$-\frac{156}{5}$	$-\frac{125}{5}$	$-\frac{104}{5}$	$-\frac{73}{5}$	$-\frac{47}{5}$	$-\frac{16}{5}$

and for $i = 10$, it is an equality. Therefore, the highest slope of the Newton polygon is at most $\frac{26}{5}\cdot v_{\mathfrak{P}}(2)$, whereas the lowest one is at least $-\frac{34}{5}\cdot v_{\mathfrak{P}}(2)$, which gives part (a) of Proposition 8.7 by the theory of Newton polygons.

(b) If A has potentially good reduction at $\mathfrak{P}$ and the semistable reduction is a product of elliptic curves, defining

$$I_4 = J_2^3 - 25J_4 = \frac{h_4}{2} \tag{8-29}$$

$$I_{12} = -8J_4^3 + 9J_2J_4J_6 - 27J_6^2 - J_2^2J_8 = \frac{1}{2^{10}\cdot 3^3}(2h_4^3 - h_6^2), \tag{8-30}$$

$$P_{48} = 2^{12}\cdot 3^3 h_{10}^4 J_8 = h_{12}^4 - 12h_4h_{12}^2h_{10}^2 + 16h_6h_{12}h_{10}^3 - 12h_4^2h_{10}^4 \tag{8-31}$$

(which as modular forms are of respective weights 4, 12 and 48), by Theorem 1 (parts (V_*) and (V)) of [Liu 1993], we obtain in the same fashion that

$$\left|\frac{h_4}{P_{48}^{1/12}}\right| \le |2|^{-13/3}, \qquad \left|\frac{h_6}{P_{48}^{1/8}}\right| \le |2|^{-3}, \qquad \left|\frac{h_{10}}{P_{48}^{5/24}}\right| \le |2|^{-4/3}. \tag{8-32}$$

Using the Newton polygon for the polynomial of (8-31) defining P_{48}, one deduces quickly that

$$\left|\frac{h_{12}}{P_{48}^{1/4}}\right| \le |2|^{-7/2}. \tag{8-33}$$

As before, with the explicit expression of the Σ_i, one obtains that the $|\Sigma_i/P_{48}^{i/12}|$ are bounded by $|2|^{\lambda_i}$ with the following values of λ:

i	10	9	8	7	6	5	4	3	2	1
λ_i	$-\frac{28}{3}$	$-\frac{71}{6}$	$\frac{-53}{3}$	$\frac{-55}{3}$	$\frac{-84}{3}$	$\frac{-71}{3}$	$\frac{-64}{3}$	-14	$\frac{-29}{3}$	$\frac{-10}{3}$

(8-34)

This implies directly that the highest slope of the Newton polygon is at most $\frac{16}{3}\cdot v_{\mathfrak{P}}(2)$. Now, for the lowest slope, there is no immediate bound which was expected; in this situation, $\Sigma_{10} = 2^{-4}h_{10}^4$ can be relatively very small compared to $P_{48}^{5/6}$.

As P_{48} is in the ideal generated by h_{10}, h_{12} (in other words, is cuspidal) and dominates all modular forms h_4, h_6, h_{10}, h_{12}, one of h_{10} and h_{12} has to be relatively large enough compared to P_{48}. In practice, we get (with (8-32), (8-33) and (8-31))

$$\left|\frac{h_{12}}{P_{48}^{1/4}}\right| \ge 1 \quad \text{or} \quad \left|\frac{h_{10}}{P_{48}^{5/24}}\right| \ge |2|^{13/6}.$$

Now, if h_{10} is relatively very small (for example, $|h_{10}/P_{48}^{5/24}| \le |2|^{19/6}|h_{12}/P_{48}^{1/4}|$), we immediately get $|h_{12}/P_{48}^{1/4}| = 1$ and $|\Sigma_9/P_{48}^{3/4}| = 1$. Computing again with these estimates for h_{10} and h_{12}, we obtain that the $|\Sigma_i/P_{48}^{i/12}|$ are bounded by $|2|^{\lambda_i}$ with the following slightly improved values of λ,

i	9	8	7	6	5	4	3	2	1
λ_i	0	$-\frac{32}{3}$	$-\frac{51}{3}$	$\frac{-84}{3}$	$\frac{-71}{3}$	$\frac{-64}{3}$	-14	$\frac{-29}{3}$	$\frac{-10}{3}$

The value at $i = 9$ is exact, hence the second lowest slope is then at least $-\frac{32}{3}\cdot v_{\mathfrak{P}}(2)$.

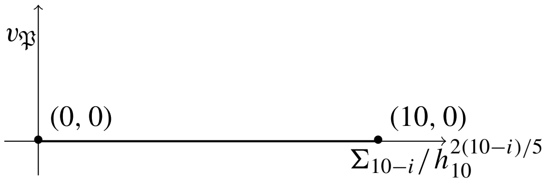


Figure 4. When the reduction of A is a jacobian.

If it is not so small, we have a bound on $v_{\mathfrak{P}}(\Sigma_{10}/P_{48}^{6/5})$, hence the Newton polygon itself is bounded (and looks like the first situation). In practice, one finds that the lowest slope is at least $-\frac{47}{3}\cdot v_{\mathfrak{P}}(2)$, hence all others slopes are at least this value, and this concludes the proof of Proposition 8.7(b). □

Remark 8.9. In characteristics $\neq 2, 3$, Theorem 1 of [Liu 1993] and its precise computations on pages 4 and 5 give the following exact shapes of Newton polygons (notice the different normalization factors).

In particular, when A reduces to a jacobian, the theta coordinates all have the same $\mathfrak{P}$-adic norm and when A reduces to a product of elliptic curves, exactly one of them has smaller norm; in other words, we reproved Proposition 8.4, and the Newton polygons have a very characteristic shape.

The idea behind the computations above is that in cases (a) and (b) (with other normalization factors), the Newton polygons have a shape close to these ones, therefore estimates can be made. It would be interesting to see what the exact shape of the Newton polygons is, to maybe obtain sharper results.

8D. ***Wrapping up the estimates and end of the proof.*** We can now prove the explicit refined version of Theorem 7.11, namely Theorem 8.2.

Proof of Theorem 8.2. In case (a), one can avoid the tubular assumption for the archimedean place of K; indeed, amongst the ten theta coordinates, there remain 4 which are large enough with no further assumption. As $|s_P| < 4$, there remains one theta coordinate which is never too small (at any place). In practice, normalizing the projective point $\psi(P)$ by this coordinate, one obtains with Propositions 8.5(a) (archimedean places) 8.4 (finite places not above 2) and 8.7 (finite places above 2)

$$h(\psi(P)) \leq -4\log(0.42) + \frac{21/2}{[K:\mathbb{Q}]}\sum_{v\,|\,2} n_v \log(2) \leq 10.75$$

after approximation.

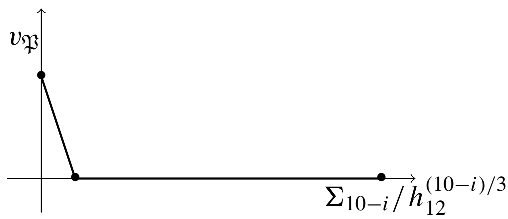


Figure 5. When the reduction of A is a product of elliptic curves.

In case (b), one has to use the tubular neighborhood implicitly given by the parameter t, namely Proposition 8.5(b) for archimedean places, again with Propositions 8.4 and 8.7 for the finite places, hence we get

$$h(\psi(P)) \leq 4\log(e^{\pi t}/0.747) + \frac{21/2}{[K:\mathbb{Q}]}\sum_{v\,|\,2} n_v \log(2) \leq 4\pi t + 8.44$$

after approximation.

Finally, we deduce from there the bounds on the stable Faltings height by Corollary 1.3 of [Pazuki 2012] (with its notations, $h_\Theta(A, L) = h(\psi(P))/4$). □

It would be interesting to give an analogous result for Theorem 7.12, and the estimates for archimedean and finite places not above 2 should not give any particular problem. For finite places above 2, the method outlined above can only be applied if, taking the symmetric polynomials $\Sigma_1, \dots, \Sigma_{f(n)}$ in well-chosen powers $\Theta_{\tilde{a}/n,\tilde{b}/n}(\tau)$ for $\tilde{a}, \tilde{b} \in \mathbb{Z}^g$, we can figure out by other arguments the largest rank k_0 for which Σ_{k_0} is cuspidal but not in the ideal generated by h_{10}. Doing so, we could roughly get back the pictured shape of the Newton polygon when h_{10} is relatively very small (because then Σ_k is relatively very small for $k > k_0$ by construction). Notice that for this process, one needs some way to theoretically bound the denominators appearing in the expressions of the Σ_i in h_4, h_6, h_{10}, h_{12}, but if this works, the method can again be applied.

Acknowledgements

I am very grateful to Fabien Pazuki and Qing Liu for having kindly answered my questions and given me useful bibliographic recommendations on the subject of Igusa invariants. I also wish to thank Josha Box for pointing out two small errors in Section 8 which have been corrected in the present version. A good portion of the time writing this paper was spent as AGPR at the ENS de Lyon, and I want to thank this institution and my former colleagues for the friendly and productive research environment. Finally, I gratefully thank the anonymous referee for his careful reading and many useful remarks and advice for citations improving the paper.

References

[Artal Bartolo et al. 2014] E. Artal Bartolo, J. Martín-Morales, and J. Ortigas-Galindo, "Cartier and Weil divisors on varieties with quotient singularities", *Internat. J. Math.* **25**:11 (2014), 1450100, 20. MR Zbl

[Atiyah and Macdonald 1969] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, MA, 1969. MR Zbl

[Auffarth et al. 2017] R. Auffarth, G. P. Pirola, and R. S. Manni, "Torsion points on theta divisors", *Proc. Amer. Math. Soc.* **145**:1 (2017), 89–99. MR Zbl

[Bilu 1995] Y. Bilu, "Effective analysis of integral points on algebraic curves", *Israel J. Math.* **90**:1-3 (1995), 235–252. MR Zbl

[Bilu and Parent 2011] Y. Bilu and P. Parent, "Runge's method and modular curves", *Int. Math. Res. Not.* **2011**:9 (2011), 1997–2027. MR Zbl

[Bombieri 1983] E. Bombieri, "On Weil's "théorème de décomposition"", *Amer. J. Math.* **105**:2 (1983), 295–308. MR Zbl

[Bombieri and Gubler 2006] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs **4**, Cambridge University Press, 2006. MR Zbl

[Borel 1981] A. Borel, "Stable real cohomology of arithmetic groups II", pp. 21–55 in *Manifolds and Lie groups* (Notre Dame, In, 1980), edited by J. Hano et al., Progr. Math. **14**, Birkhäuser, Boston, 1981. MR Zbl

[Boxall and Grant 2000] J. Boxall and D. Grant, "Examples of torsion points on genus two curves", *Trans. Amer. Math. Soc.* **352**:10 (2000), 4533–4555. MR Zbl

[Cartan 1957] H. Cartan, "Plongements projectifs", *Séminaire Henri Cartan* **10**:2 (1957), 1–19.

[Cornell and Silverman 1986] G. Cornell and J. H. Silverman (editors), *Arithmetic geometry*, Springer, 1986. MR Zbl

[Corvaja et al. 2009] P. Corvaja, A. Levin, and U. Zannier, "Integral points on threefolds and other varieties", *Tohoku Math. J.* (2) **61**:4 (2009), 589–601. MR Zbl

[David and Philippon 2002] S. David and P. Philippon, "Minorations des hauteurs normalisées des sous-variétés de variétés abeliennes, II", *Comment. Math. Helv.* **77**:4 (2002), 639–700. MR Zbl

[Debarre 1999] O. Debarre, *Tores et variétés abéliennes complexes*, Cours Spécialisés [Specialized Courses] **6**, Société Mathématique de France, Paris; EDP Sciences, Les Ulis, 1999. MR Zbl

[Faltings and Chai 1990] G. Faltings and C.-L. Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)] **22**, Springer, 1990. MR Zbl

[van der Geer 1982] G. van der Geer, "On the geometry of a Siegel modular threefold", *Math. Ann.* **260**:3 (1982), 317–350. MR Zbl

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math. **52**, Springer, 1977. MR Zbl

[Hoffman and Weintraub 2001] J. W. Hoffman and S. H. Weintraub, "The Siegel modular variety of degree two and level three", *Trans. Amer. Math. Soc.* **353**:8 (2001), 3267–3305. MR Zbl

[Ichikawa 2009] T. Ichikawa, "Siegel modular forms of degree 2 over rings", *J. Number Theory* **129**:4 (2009), 818–823. MR Zbl

[Igusa 1960] J.-i. Igusa, "Arithmetic variety of moduli for genus two", *Ann. of Math.* (2) **72** (1960), 612–649. MR Zbl

[Igusa 1964] J.-i. Igusa, "On Siegel modular forms genus two, II", *Amer. J. Math.* **86** (1964), 392–412. MR Zbl

[Igusa 1966] J.-i. Igusa, "On the graded ring of theta-constants, II", *Amer. J. Math.* **88** (1966), 221–236. MR Zbl

[Igusa 1967] J.-i. Igusa, "Modular forms and projective invariants", *Amer. J. Math.* **89** (1967), 817–855. MR Zbl

[Klingen 1990] H. Klingen, *Introductory lectures on Siegel modular forms*, Cambridge Studies in Advanced Mathematics **20**, Cambridge University Press, 1990. MR Zbl

[Le Fourn 2015] S. Le Fourn, *Points entiers et rationnels sur des courbes et variétés modulaires de dimension supérieure*, Ph.D. thesis, Université de Bordeaux, 2015.

[Le Fourn 2016] S. Le Fourn, "Surjectivity of Galois representations associated with quadratic $\mathbb{Q}$-curves", *Math. Ann.* **365**:1-2 (2016), 173–214. MR Zbl

[Le Fourn 2017] S. Le Fourn, "Sur la méthode de Runge et les points entiers de certaines variétés modulaires de Siegel", *C. R. Math. Acad. Sci. Paris* **355**:8 (2017), 847–852. MR Zbl

[Levin 2008] A. Levin, "Variations on a theme of Runge: effective determination of integral points on certain varieties", *J. Théor. Nombres Bordeaux* **20**:2 (2008), 385–417. MR Zbl

[Liu 1993] Q. Liu, "Courbes stables de genre 2 et leur schéma de modules", *Math. Ann.* **295**:2 (1993), 201–222. MR Zbl

[Mazur 1977] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186. MR Zbl

[Merel 1996] L. Merel, "Bornes pour la torsion des courbes elliptiques sur les corps de nombres", *Invent. Math.* **124**:1-3 (1996), 437–449. MR Zbl

[Mumford 1966] D. Mumford, "On the equations defining abelian varieties, I", *Invent. Math.* **1** (1966), 287–354. MR Zbl

[Mumford 1967] D. Mumford, "On the equations defining abelian varieties, II", *Invent. Math.* **3** (1967), 75–135. MR

[Mumford 1970] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics **5**, Oxford University Press, London, 1970. MR Zbl

[Mumford 1983] D. Mumford, "Towards an enumerative geometry of the moduli space of curves", pp. 271–328 in *Arithmetic and geometry*, vol. II, edited by M. Artin and J. Tate, Progr. Math. **36**, Birkhäuser, Boston, 1983. MR Zbl

[Mumford 1984] D. Mumford, *Tata lectures on theta, II*, Progress in Mathematics **43**, Birkhäuser, Boston, 1984. MR Zbl

[Mumford 2007] D. Mumford, *Tata lectures on theta, I*, Birkhäuser, Boston, 2007. MR Zbl

[Namikawa 1980] Y. Namikawa, *Toroidal compactification of Siegel spaces*, Lecture Notes in Mathematics **812**, Springer, 1980. MR Zbl

[Oort and Ueno 1973] F. Oort and K. Ueno, "Principally polarized abelian varieties of dimension two or three are Jacobian varieties", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **20** (1973), 377–381. MR Zbl

[Pazuki 2012] F. Pazuki, "Theta height and Faltings height", *Bull. Soc. Math. France* **140**:1 (2012), 19–49. MR Zbl

[Pazuki 2013] F. Pazuki, "Minoration de la hauteur de Néron–Tate sur les surfaces abéliennes", *Manuscripta Math.* **142**:1-2 (2013), 61–99. MR Zbl

[Runge 1887] C. Runge, "Ueber ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen", *J. Reine Angew. Math.* **100** (1887), 425–435. MR Zbl

[Satake and Cartan 1957] I. Satake and H. Cartan, "Démonstration du théorème fondamental", *Séminaire Henri Cartan* **10**:2 (1957), 1–12.

[Schoof 2008] R. Schoof, *Catalan's conjecture*, Springer, 2008. MR Zbl

[Silverman 1987] J. H. Silverman, "Arithmetic distance functions and height functions in Diophantine geometry", *Math. Ann.* **279**:2 (1987), 193–216. MR Zbl

[Streng 2010] M. Streng, *Complex multiplication of abelian surfaces*, Ph.D. thesis, University of Leiden, 2010, Available at https://openaccess.leidenuniv.nl/handle/1887/15572.

[Vojta 1987] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics **1239**, Springer, 1987. MR Zbl

[Weissauer 1992] R. Weissauer, "The Picard group of Siegel modular threefolds", *J. Reine Angew. Math.* **430** (1992), 179–211. MR Zbl

Communicated by Jonathan Pila
Received 2018-01-08 Revised 2018-08-30 Accepted 2018-10-08

samuel.le-fourn@warwick.ac.uk University of Warwick, Coventry, CV5 6EF, United Kingdom

ALGEBRA AND NUMBER THEORY 13:1 (2019)
dx.doi.org/10.2140/ant.2019.13.211

Algebraic cycles on genus-2 modular fourfolds

Donu Arapura

To the memory of my father

This paper studies universal families of stable genus-2 curves with level structure. Among other things, it is shown that the (1, 1)-part is spanned by divisor classes, and that there are no cycles of type (2, 2) in the third cohomology of the first direct image of $\mathbb{C}$ under projection to the moduli space of curves. Using this, it shown that the Hodge and Tate conjectures hold for these varieties.

One of the goals of this article is to extend some results from Shioda's study [1972] of elliptic modular surfaces to families of genus-2 curves. We recall that elliptic modular surfaces $f : \bar{C}_{1,1}[n] \to \overline{M}_{1,1}[n]$ are the universal families of elliptic curves over modular curves. Among other things, Shioda showed that $\bar{C}_{1,1}[n]$ has maximal Picard number in the sense that $H^{1,1}(\bar{C}_{1,1}[n])$ is spanned by divisors. He also showed that the Mordell–Weil rank is zero. A related property, observed later by Viehweg and Zuo [2004], is that a certain Arakelov inequality becomes equality. As they observe, this is equivalent to the map

$$f_*\omega_{\bar{C}_{1,1}[n]/\overline{M}_{1,1}[n]} \to \Omega^1_{\overline{M}_{1,1}[n]}(\log D) \otimes R^1 f_*\mathcal{O}_{\bar{C}_{1,1}[n]}$$

induced by the Kodaira–Spencer class being an isomorphism. The divisor D is the discriminant of f.

In this paper, we study universal curves $f' : \bar{C}_2[\Gamma] \to \overline{M}_2[\Gamma]$ over the moduli space of stable genus-2 curves with generalized level structure. The level Γ is a finite-index subgroup of the mapping class group Γ_2. The classical level n-structures correspond to the case where Γ is the preimage $\widetilde{\Gamma}(n)$ of the principal congruence subgroup $\Gamma(n) \subset \mathrm{Sp}_4(\mathbb{Z})$. We fix a suitable nonsingular birational model $f : X \to Y$ for f'. Let $D \subset Y$ be the discriminant, and $U = Y - D$. We show that, as before, for a classical level, the Mordell–Weil rank of $\mathrm{Pic}^0(X) \to Y$ is zero and $H^{1,1}(X)$ is spanned by divisors. These results are deduced from Raghunathan's vanishing theorem [1967]. We also prove an analogue of Viehweg–Zuo that the map

$$\Omega^1_Y(\log D) \otimes f_*\omega_{X/Y} \to \Omega^2_Y(\log D) \otimes R^1 f_*\mathcal{O}_X$$

is an isomorphism. We will see that this implies that there are no cycles of type (2, 2) in the mixed Hodge structure $H^3(U, R^1 f_*\mathbb{C})$. As an application, we deduce that the Hodge conjecture holds for X. We also show that the Tate conjecture holds for X for a classical level using, in addition, Faltings' p-adic Hodge theorem [1988] and Weissauer's work [1988] on Siegel modular threefolds.

Partially supported by a grant from the Simons foundation.
MSC2010: 14C25.
Keywords: Hodge conjecture, Tate conjecture, moduli of curves.

If X is a complex variety, then unless indicated otherwise, sheaves should be understood as sheaves on the associated analytic space X^{an}.

1. Hodge theory of semistable maps

We start with some generalities. By a log pair $\mathcal{X} = (X, E)$, we mean a smooth variety X together with a divisor with simple normal crossings E. We usually denote log pairs by the symbols $\mathcal{X}, \mathcal{Y}, \ldots$ with corresponding varieties $X, Y, \ldots$. Given $\mathcal{X}$, set

$$\Omega^1_{\mathcal{X}} = \Omega^1_X(\log E) \quad \text{and} \quad T_{\mathcal{X}} = (\Omega^1_{\mathcal{X}})^\vee.$$

Recall that a semistable map $f : (X, E) \to (Y, D)$ of log pairs is a morphism $f : X \to Y$ such that $f^{-1}D = E$ and étale locally it is given by

$$\begin{aligned} y_1 &= x_1 \cdots x_{r_1}, \\ &\vdots \\ y_k &= x_{r_{k-1}+1} \cdots x_{r_k}, \\ y_{k+1} &= x_{r_k+1}, \\ &\vdots \end{aligned}$$

where $y_1 \cdots y_k = 0$ and $x_1 \cdots x_{r_k} = 0$ are local equations for D and E respectively. We will say f is log étale if it is semistable of relative dimension zero. (This is a bit more restrictive than the usual definition).

Fix a projective semistable map $f : (X, E) \to (Y, D)$. The map restricts to a smooth projective map f^o from $\widetilde{U} = X - E$ to $U = Y - D$. Let

$$\Omega^i_{\mathcal{X}/\mathcal{Y}} = \Omega^i_{X/Y}(\log E).$$

The sheaf $\mathcal{L}^m = R^m f^o_* \mathbb{Q}$ is a local system, which is part of a variation of Hodge structure. Let $V^m = R^m f_* \Omega^\bullet_{\mathcal{X}/\mathcal{Y}}$ with filtration F induced by the stupid filtration $R^m f_* \Omega^{\geq p}_{\mathcal{X}/\mathcal{Y}}$. It carries an integrable logarithmic connection

$$\nabla : V^m \to \Omega^1_{\mathcal{Y}} \otimes V^m$$

such that $\ker \nabla|_U = \mathbb{C}_U \otimes \mathcal{L}^m$. Griffiths transversality

$$\nabla(F^p) \subseteq \Omega^1_{\mathcal{Y}} \otimes F^{p-1}$$

holds. The relative de Rham to Hodge spectral sequence

$$E_1 = R^j f_* \Omega^i_{\mathcal{X}/\mathcal{Y}} \Rightarrow R^{i+j} f_* \Omega^\bullet_{\mathcal{X}/\mathcal{Y}}$$

degenerates at E_1 by [Illusie 1990, Corollaire 2.6; Fujisawa 1999, Theorem 6.10]. Therefore

$$\mathrm{Gr}^p_F V^m \cong R^{m-p} f_* \Omega^p_{\mathcal{X}/\mathcal{Y}}.$$

The Kodaira–Spencer class

$$\kappa : \mathcal{O}_Y \to \Omega^1_{\mathcal{Y}} \otimes R^1 f_* T_{\mathcal{X}/\mathcal{Y}} \tag{1}$$

is given as the transpose of the map

$$T_{\mathcal{Y}} \to R^1 f_* T_{\mathcal{X}/\mathcal{Y}}$$

induced by the sequence

$$0 \to T_{\mathcal{X}/\mathcal{Y}} \to T_{\mathcal{X}} \to f^* T_{\mathcal{Y}} \to 0.$$

Proposition 1.1. *The associated graded*

$$\mathrm{Gr}(\nabla) : R^{m-p} f_* \Omega^p_{\mathcal{X}/\mathcal{Y}} \to \Omega^1_{\mathcal{Y}} \otimes R^{m-p+1} f_* \Omega^{p-1}_{\mathcal{X}/\mathcal{Y}}$$

coincides with cup product and contraction with κ.

Proof. In the nonlog setting, this is stated in [Katz 1970, Theorem 3.5], and the argument indicated there extends to the general case. □

By [Arapura 2005], we can give $H^i(U, R^j f_* \mathbb{Q})$ a mixed Hodge structure by identifying it with the associated graded of $H^{i+j}(\widetilde{U}, \mathbb{Q})$ with respect to the Leray filtration. It can also be defined intrinsically using mixed Hodge module theory, but the first description is more convenient for us. We will need a more precise description of the Hodge filtration. We define a complex

$$K_{\mathcal{X}/\mathcal{Y}}(m, p) = [R^{m-p} f_* \Omega^p_{\mathcal{X}/\mathcal{Y}} \xrightarrow{\kappa} \Omega^1_{\mathcal{Y}} \otimes R^{m-p+1} f_* \Omega^{p-1}_{\mathcal{X}/\mathcal{Y}} \xrightarrow{\kappa} \Omega^2_{\mathcal{Y}} \otimes R^{m-p+2} f_* \Omega^{p-2}_{\mathcal{X}/\mathcal{Y}} \cdots].$$

Proposition 1.2. $$\mathrm{Gr}^p_F H^i(U, R^j f_* \mathbb{C}) \cong H^i(K_{\mathcal{X}/\mathcal{Y}}(j, p)).$$

Proof. (Compare with [Zucker 1979, 2.16].) Define a filtration

$$L^i \Omega^\bullet_{\mathcal{X}} = \mathrm{im}\, f^* \Omega^i_{\mathcal{Y}} \otimes \Omega^\bullet_{\mathcal{X}}.$$

Then

$$\mathrm{Gr}^i_L \Omega^\bullet_{\mathcal{X}} = f^* \Omega^i_{\mathcal{Y}} \otimes \Omega^\bullet_{\mathcal{X}/\mathcal{Y}}[-i]$$

from which we deduce that

$$\mathrm{Gr}^i_L Rf_* \Omega^\bullet_{\mathcal{X}} \cong \Omega^i_{\mathcal{Y}} \otimes Rf_* \Omega^\bullet_{\mathcal{X}/\mathcal{Y}}[-i]. \tag{2}$$

Therefore, we obtain a spectral sequence

$${}_L E_1^{i,j} = \mathcal{H}^{i+j}(\mathrm{Gr}^i_L Rf_* \Omega^\bullet_{\mathcal{X}}) \cong \Omega^i_{\mathcal{Y}} \otimes R^j f_* \Omega^\bullet_{\mathcal{X}/\mathcal{Y}} = \Omega^i_{\mathcal{Y}} \otimes V^j \Rightarrow R^{i+j} f_* \Omega^\bullet_{\mathcal{X}}$$

Recall that to L we can associate a new filtration $\mathrm{Dec}(L)$ [Deligne 1971] such that

$${}_{\mathrm{Dec}(L)} E_0^{i,j} \cong {}_L E_1^{2i+j,-i}.$$

Therefore we obtain a quasiisomorphism

$$\mathrm{Gr}^i_{\mathrm{Dec}(L)} Rf_* \Omega^\bullet_{\mathcal{X}} \xrightarrow{\sim} \Omega^\bullet_{\mathcal{Y}} \otimes V^{-i}[i]. \tag{3}$$

This becomes a map of filtered complexes with respect to the filtration induced by Hodge filtration $F^p = \Omega^{\geq p}_{\mathcal{X}}$. On the right of (3), it becomes

$$F^p \Omega^\bullet_{\mathcal{Y}} \otimes V^{-i} = F^p V^{-i} \to \Omega^1_{\mathcal{Y}} \otimes F^{p-1} V^{-i} \to \cdots.$$

The relative de Rham to Hodge spectral sequence

$$ {}_F E_1 = R^j f_* \Omega^i_{\mathcal{X}} \Rightarrow R^{i+j} f_* \Omega^\bullet_{\mathcal{X}/\mathcal{Y}} $$

degenerates at E_1 [Illusie 1990, Corollaire 2.6; Fujisawa 1999, Theorem 6.10]. Therefore by [Deligne 1971, 1.3.15], we can conclude that (3) is a filtered quasiisomorphism.

The spectral sequence associated to the filtration induced by $\mathrm{Dec}(L)$ on $R\Gamma(Rf_*\Omega^\bullet_{\mathcal{X}})$

$$ {}_{\mathrm{Dec}(L)} E_1^{i,j} = H^{2i+j}(Y, \Omega^\bullet_{\mathcal{Y}} \otimes V^{-i}) = H^{2i+j}(U, R^{-i} f_* \mathbb{C}) $$

coincides with Leray after reindexing. Therefore this degenerates at the first page by [Deligne 1968]. The above arguments plus [Deligne 1971, 1.3.17] show that F-filtration on the $H^{2i+j}(Y, \Omega^\bullet_{\mathcal{Y}} \otimes V^{-i})$ coincides with the filtration on ${}_{\mathrm{Dec}(L)}E_\infty$, which is the Hodge filtration on $H^{2i+j}(U, R^{-i} f_* \mathbb{C})$. The proposition follows immediately from this. □

One limitation of the notion of semistability is that it is not stable under base change. In order to handle this, we need to work in the broader setting of log schemes [Kato 1989]. We recall that a log scheme consists of a scheme X and a sheaf of monoids M on $X_{\text{ét}}$ together with a multiplicative homomorphism $\alpha : M \to \mathcal{O}_X$ such that α induces an isomorphism $\alpha^{-1}(\mathcal{O}_X^*) \cong \mathcal{O}_X^*$. A log pair (X, E) gives rise to a log scheme where M is the sheaf of functions invertible outside of E. If $f : (X, E) \to (Y, D)$ is semistable, and $\pi : (Y', D') \to (Y, D)$ is log étale in our sense, then $X' = X \times_Y Y'$ can be given the log structure pulled back from Y'. Then $X' \to Y'$ becomes a morphism $\mathcal{X}' \to \mathcal{Y}'$ of log schemes, which is log smooth and exact. Logarithmic differentials can be defined for log schemes [Kato 1989], so the complexes $K_{\mathcal{X}'/\mathcal{Y}'}(m, p)$ can be constructed exactly as above. Since π is log étale, we easily obtain:

Lemma 1.3. *With the above notation,* $\pi^* K_{\mathcal{X}/\mathcal{Y}}(m, p) \cong K_{\mathcal{X}'/\mathcal{Y}'}(m, p)$.

Let us spell things out for curves. Suppose that $f : \mathcal{X} \to \mathcal{Y}$ is semistable with relative dimension 1. From

$$ 0 \to \Omega^1_{\mathcal{Y}} \to \Omega^1_{\mathcal{X}} \to \Omega^1_{\mathcal{X}/\mathcal{Y}} \to 0 $$

we get an isomorphism

$$ \Omega^1_{\mathcal{X}/\mathcal{Y}} = \det \Omega^1_{\mathcal{X}} \otimes (\det \Omega^1_{\mathcal{Y}})^{-1} \cong \omega_{X/Y}. $$

The complex $K_{\mathcal{X}/\mathcal{Y}}(1, i)$ satisfies

$$ K_{\mathcal{X}/\mathcal{Y}}(1, i) = [\Omega^{i-1}_{\mathcal{Y}} \otimes f_* \omega_{X/Y} \to \Omega^i_{\mathcal{Y}} \otimes R^1 f_* \mathcal{O}_X], $$

where the first term sits in degree $i - 1$. We note that this complex, which we now denote by $K_{X/Y}(1, i)$, can be defined when X/Y is a semistable curve in the usual sense (a proper flat map of relative dimension 1 with reduced connected nodal geometric fibres). In general, any such curve carries a natural log structure [Kato 2000], and the differential of this complex can be interpreted as a cup product with the associated Kodaira–Spencer class. Consequently, given a map $\pi : X' \to X$ of curves over Y, we get an induced map of complexes $\pi^* : K_{X/Y}(1, i) \to K_{X'/Y'}(1, i)$. Finally, we note that these constructions can be extended to Deligne–Mumford stacks, such as the moduli stack of stable curves $\overline{\mathbb{M}}_g$, without difficulty.

2. Consequences of Raghunathan's vanishing

Let M_g be the moduli space of smooth projective curves of genus g, let $M_{g,n}$ be the moduli space of smooth genus-g curves with n marked points, and let A_2 be the moduli space of principally polarized g-dimensional abelian varieties. The symbols $\mathbb{M}_g$, $\mathbb{A}_g$ etc. will be reserved for the corresponding moduli stacks. We note that $\dim M_2 = 3$. The Torelli map $\tau : M_2 \to A_2$ is injective and the image of M_2 is the complement of the divisor parametrizing products of two elliptic curves. As an analytic space, M_2^{an} is a quotient of the Teichmüller space T_2 by the mapping class group Γ_2. Given a finite-index subgroup $\Gamma \subset \Gamma_2$, let $M_2[\Gamma] = T_2/\Gamma$. We view this as the moduli space of curves with generalized level structure. When $\Gamma = \widetilde{\Gamma}(n)$ is the preimage of the principal congruence subgroup $\Gamma(n) \subseteq \mathrm{Sp}_4(\mathbb{Z})$ under the canonical map $\Gamma_2 \to \mathrm{Sp}_4(\mathbb{Z})$, the space $M_2[n] := M_2[\widetilde{\Gamma}(n)]$ is the moduli space of curves with classical (or abelian or Jacobi) level n-structure. It is smooth and fine as soon as $n \geq 3$, and defined over the cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$. More generally $M_2[\Gamma]$ is smooth, and defined over a number field, as soon as $\Gamma \subseteq \widetilde{\Gamma}(n)$ with $n \geq 3$. We refer to Γ as *fine*, when the last condition holds. Torelli extends to a map $M_2[n] \to A_2[n]$ to the moduli space of abelian varieties with level n-structure.

Let $\overline{M}_2$ denote the Deligne–Mumford compactification of M_2. The boundary divisor Δ consists of a union of two components $\Delta_0 \cup \Delta_1$. The generic point of Δ_0 corresponds to an irreducible curve with a single node, and the generic point of Δ_1 corresponds to a union of two elliptic curves meeting transversally. Let $\pi : \overline{M}_2[\Gamma] \to \overline{M}_2$ denote the normalization of $\overline{M}_2$ in the function field of $M_2[\Gamma]$. When $\Gamma = \widetilde{\Gamma}(n)$, we denote this by $\overline{M}_2[n]$. On the other side $A_2[n]$ has a unique smooth toroidal compactification, first constructed by Igusa, and τ extends to an isomorphism between $\overline{M}_2[n]$ and the Igusa compactification [Namikawa 1980, §9]. The space $\overline{M}_2[\Gamma]$ is smooth, when $\Gamma = \widetilde{\Gamma}(n)$, $n \geq 3$, and in some other cases [Pikaart and de Jong 1995]. Suppose that $n \geq 3$. The boundary $D = \overline{M}_2[n] - M_2[n]$ is a divisor with normal crossings. Let $D_i = \pi^{-1}\Delta_i$. Since D_1 parametrizes unordered pairs of (generalized) elliptic curves with level structure, its irreducible components are isomorphic to symmetric products $\overline{M}_{1,1}[n] \times \overline{M}_{1,1}[n]/S_2$ of the modular curve of full level n. Let $\overline{C}_{1,m}[n]/\overline{M}_{1,m}[n]$ denote the pullback of the universal elliptic curve under the canonical map $\overline{M}_{1,m}[n] \to \overline{\mathbb{M}}_{1,m}$. The components of D_0 are birational to the elliptic modular surfaces $\overline{C}_{1,1}[n]$ [Oda and Schwermer 1990, §1.4].

Given a fine level structure Γ, let $\overline{C}_2[\Gamma] \to \overline{M}_2[\Gamma]$ be the pullback of the universal curve from $\overline{\mathbb{M}}_2$. The space $\overline{C}_2[\Gamma]$ will be singular [Boggi and Pikaart 2000, Proposition 1.4], so we will replace it with a suitable birational model $f : X \to Y$ whose construction we now explain. If $\Gamma = \widetilde{\Gamma}[n]$, we set $Y = \overline{M}_2[n]$. As noted above, Y is smooth. For other Γ's, we choose a desingularization $Y \to \overline{M}_2[\Gamma]$ which is an isomorphism over $M_2[\Gamma]$ and such that boundary divisor D has simple normal crossings. We have a morphism $Y \to \overline{\mathbb{M}}_2$ to the moduli stack, which is log étale. It follows in particular that $\Omega^1_{\overline{\mathbb{M}}_2}(\log \Delta)$ pulls back to $\Omega^1_Y(\log D)$. The space Y will carry a stable curve $X' \to Y$ obtained by pulling back the universal family over $\overline{\mathbb{M}}_2$. The space X' will be singular, however:

Lemma 2.1. (a) *X' will have rational singularities.*

(b) *There exists a desingularization $\pi : X \to X'$ such that $X \to Y$ is semistable.*

(c) *The map $\pi : X \to X'$ can be chosen so as to have the following additional property. After extending scalars to $\overline{\mathbb{Q}}$, let E be a component of an exceptional divisor of π. Then*:

(i) *If $\pi(E)$ is a point, E is a rational variety.*

(ii) *If $\pi(E) = C$ is a curve, there is a map $E \to C$ such that the pullback under a finite map $\widetilde{C} \to C$ is birational to $\mathbb{P}^2 \times \widetilde{C}$.*

(iii) *If $\pi(E)$ is a surface, there is a map $E \to D_i$, for some i, such that the pullback of E to an étale cover $\widetilde{D}_i \to D_i$ is birational to $\mathbb{P}^1 \times \widetilde{D}_i$.*

(iv) *If* $\dim \pi(E) = 3$, *then $E \to \pi(E)$ is birational.*

(d) $K_{X/Y}(1,i) \cong K_{X'/Y}(1,i)$.

Proof. The singularities of X' are analytically of the form $xy = t_1^a t_2^b t_3^c$. These are toroidal singularities, in the sense that is local analytically, or étale locally, isomorphic to a toric variety. (This is a bit weaker than the notion of toroidal embedding in [Kempf et al. 1973], but it is sufficient for our needs.) Such singularities are well known to be rational; see [Kempf et al. 1973; Viehweg 1977]. Item (b) follows from [de Jong 1996, Proposition 3.6].

To prove (c), we need to recall some details of the construction of X from [de Jong 1996]. First, as explained in the proof of [loc. cit., Lemma 3.2], one blows up a codimension-2 component $T \subset X'_{\text{sing}}$. The locus T is an étale cover of some component D_i. Furthermore, from the description in [loc. cit.] we can see that T is compatible with the toroidal structure. Consequently, we can find a toric variety V with torus fixed point 0, and an étale local isomorphism between X' and $V \times T$, over the generic point of T, which takes T to $\{0\} \times T$. This shows that, over the generic point, the exceptional divisor E to T is étale locally a product of T with a toric curve. So we get case (iii). Note that this step is repeated until the X'_{sing} has codimension at least 3. One does further blow ups to obtain X. An examination of the proof of [loc. cit., Proposition 3.6] shows that the required blow ups are also compatible with the toroidal structure in the previous sense. If the centre of the blow up is a point, then the exceptional divisor is toric and we have case (i). If the centre is a smooth curve C, we obtain case (ii). The last item (iv) is automatic for blow ups.

By the remarks at the end of the last section, there is a commutative diagram marked with solid arrows

$$\begin{array}{ccc} \Omega_{\mathcal{Y}}^{i-1} \otimes f_*\omega_{X/Y} & \longrightarrow & \Omega_{\mathcal{Y}}^{i} \otimes R^1 f_*\mathcal{O}_X \\ \pi^* \uparrow \downarrow \pi_* & & \pi^* \uparrow \downarrow \pi_* \\ \Omega_{\mathcal{Y}}^{i-1} \otimes f_*\omega_{X'/Y} & \longrightarrow & \Omega_{\mathcal{Y}}^{i} \otimes R^1 f_*\mathcal{O}_{X'} \end{array}$$

Since X' has rational singularities, the dotted arrows labelled with π_* are isomorphisms, and these are left inverse to the arrows labelled with π^*. Therefore π^* are also isomorphisms, and this proves (d). □

We refer to $f : X \to Y$ constructed in Lemma 2.1 as *a good model* of $\overline{C}_2[\Gamma] \to \overline{M}_2[\Gamma]$. We let $U = Y - D$, $E = f^{-1}D$, and $\widetilde{U} = X - E$ as above.

Corollary 2.2. *After extending scalars to $\overline{\mathbb{Q}}$, let E_1 be an irreducible component of E for a classical fine level $\widetilde{\Gamma}(n)$. Then there exists a dominant rational map $\widetilde{E}_1 \dashrightarrow E_1$, where $\widetilde{E}_1$ is one of*

(1) $\overline{C}_{1,1}[n] \times \overline{M}_{1,1}[n]$,

(2) $\overline{C}_{1,2}[n]$,

(3) $\overline{C}_{1,1}[m] \times \mathbb{P}^1$ *for some* $n \mid m$,

(4) $\overline{M}_{1,1}[m] \times \overline{M}_{1,1}[m] \times \mathbb{P}^1$ *for some* $n \mid m$,

(5) *a product of* $\mathbb{P}^2$ *with a curve,*

(6) $\mathbb{P}^3$.

Proof. The preimage of D_1 in $\overline{C}_2[n]$ parametrizes a union of pairs of (generalized) elliptic curves with level structure together with a point on the union. It follows that a component of E dominating D_1 is dominated by $\overline{C}_{1,1}[n] \times \overline{M}_{1,1}[n]$. The preimage of D_0 in $\overline{C}_2[n]$ is a family of nodal curves over D_0; its normalization is $\overline{C}_{1,2}[n]$. Therefore a component of E dominating D_0 is birational to $\overline{C}_{1,2}[n]$. Case (3) follows from Lemma 2.1(ciii) once we observe that an étale cover of $\overline{C}_{1,1}[n]$ is dominated by $\overline{C}_{1,1}[m]$ for some $n \mid m$. This is because we have a surjection of étale fundamental groups

$$\pi_1^{\text{ét}}(M_{1,1}[n]) \cong \pi_1^{\text{ét}}(C_{1,1}[n]) \to \pi_1^{\text{ét}}(\overline{C}_{1,1}[n])$$

[Cox and Zucker 1979, Theorem 1.36], and $\{M_{1,1}[m]\}_{n \mid m}$ is cofinal in the set of étale covers of $M_{1,1}[n]$. Case (4) is similar. The remaining cases follow immediately from the lemma. □

Proposition 2.3. *When $\Gamma = \widetilde{\Gamma}(n)$, with $n \geq 3$, $H^1(U, R^1 f_*\mathbb{C}) = 0$.*

Proof. As explained above, $Y = \overline{M}_2[n] = \bar{A}_2[n]$ and $U = A_2[n] - D_1^o$, where $D_1^o = D_1 - D_0$. Let $g : \mathrm{Pic}^0(X/Y) \to Y$ denote the relative Picard scheme. Then $R^1 f_*\mathbb{C} = R^1 g_*\mathbb{C}|_U$. We have an exact sequence

$$H^1(A_2[n], R^1 g_*\mathbb{C}) \to H^1(U, R^1 f_*\mathbb{C}) \to H^0(D_1^o, R^1 g_*\mathbb{C}).$$

The group on the left vanishes by Raghunathan [1967, p. 423, Corollary 1]. The local system $R^1 g_*\mathbb{C}|_{D_1^o}$ decomposes into a sum of two copies of the standard representation of the congruence group $\Gamma(n) \subset \mathrm{SL}_2(\mathbb{Z})$. Therefore it has no invariants. Consequently, $H^1(U, R^1 f_*\mathbb{C}) = 0$ as claimed. □

Lemma 2.4. *Let η denote the generic point of Y. Then we have an exact sequence*

$$0 \to \mathrm{Pic}(U) \xrightarrow{s} \mathrm{Pic}(\widetilde{U}) \xrightarrow{r} \mathrm{Pic}(X_\eta) \to 0,$$

where r and s are the natural maps.

Proof. Consider the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbb{C}(U)^* & \longrightarrow & \mathbb{C}(U)^* \oplus \mathbb{C}(\widetilde{U})^* & \longrightarrow & \mathbb{C}(\widetilde{U})^* & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{div}} & & \downarrow{\scriptstyle \mathrm{div}+\mathrm{div}} & & \downarrow{\scriptstyle \mathrm{div}} & & \\
0 & \longrightarrow & \mathrm{Div}(U) & \xrightarrow{s'} & \mathrm{Div}(\widetilde{U}) & \xrightarrow{r'} & \mathrm{Div}(X_\eta) & \longrightarrow & 0
\end{array}$$

The map r' is surjective because any codimension-1 point of X_η is the restriction of its scheme-theoretic closure. A straightforward argument also shows that s' is injective and $\ker r' = \operatorname{im} s'$. The lemma now follows from the snake lemma. □

Lemma 2.5. *The first Chern class map induces injections*

$$\operatorname{Pic}(\widetilde{U})/\operatorname{Pic}^0(X)\otimes\mathbb{Q} \hookrightarrow H^2(\widetilde{U},\mathbb{Q}), \tag{4}$$
$$\operatorname{Pic}(U)/\operatorname{Pic}^0(Y)\otimes\mathbb{Q} \hookrightarrow H^2(U,\mathbb{Q}). \tag{5}$$

Proof. To prove (4), we observe that there is a commutative diagram with exact lines

$$\begin{array}{ccccc}
 & & & & \operatorname{Pic}(\widetilde{U})/\operatorname{Pic}^0(X)\otimes\mathbb{Q} \\
 & & & \nearrow & \downarrow \\
 & & \operatorname{Pic}(\widetilde{U})\otimes\mathbb{Q} & \xrightarrow{c_1} & H^2(\widetilde{U},\mathbb{Q}) \\
 & \nearrow & \uparrow & & \uparrow \\
\operatorname{Pic}^0(X)\otimes\mathbb{Q} & \longrightarrow & \operatorname{Pic}(X)\otimes\mathbb{Q} & \xrightarrow{c_1} & H^2(X,\mathbb{Q}) \\
 & & \uparrow & & \uparrow \\
 & & \bigoplus\mathbb{Q}E_i & & \bigoplus\mathbb{Q}[E_i]
\end{array}$$

The existence and injectivity of the dotted arrow follows from this diagram. Existence and injectivity of the map of (5) is proved similarly. □

We refer to the group of $\mathbb{C}(Y)$ rational points of $\operatorname{Pic}^0(X_\eta)$ as the Mordell–Weil group of X/Y.

Theorem 2.6. *Let $f : X \to Y$ be a good model of $\overline{C}_2[n] \to \overline{M}_2[n]$, where $n \geq 3$:*

(a) *The space $H^{1,1}(X)$ is spanned by divisors.*

(b) *The rank of the Mordell–Weil group of X/Y is zero.*

Proof. We have an sequence

$$\bigoplus\mathbb{Q}[E_i] \to H^2(X) \to \operatorname{Gr}_2^W H^2(\widetilde{U}) \to 0$$

of mixed Hodge structures. So for (a), it suffices to show that the $(1, 1)$-part of rightmost Hodge structure is spanned by divisors. The Leray spectral sequence together with Proposition 2.3 gives an exact sequence

$$0 \to H^2(U, f_*\mathbb{Q}) \to H^2(\widetilde{U}) \to H^0(U, R^2 f_*\mathbb{Q}) \to 0$$

of mixed Hodge structures. Therefore, we get an exact sequence

$$0 \to \operatorname{Gr}_2^W H^2(U, f_*\mathbb{Q}) \to \operatorname{Gr}_2^W H^2(\widetilde{U}) \to \operatorname{Gr}_2^W H^0(U, R^2 f_*\mathbb{Q}) \to 0.$$

The space on the right is 1-dimensional and spanned by the class of any horizontal divisor. We can identify

$$\mathrm{Gr}_2^W H^2(U, f_*\mathbb{Q}) = \mathrm{Gr}_2^W H^2(U, \mathbb{Q})$$

with a quotient of $H^2(Y)$. Weissauer [1988, p. 101] showed that $H^{1,1}(Y)$ is spanned by divisors. This proves (a).

By Lemma 2.4, we have isomorphisms

$$\mathrm{Pic}(X_\eta)\otimes\mathbb{Q} \cong \frac{\mathrm{Pic}(\widetilde{U})}{\mathrm{Pic}(U)}\otimes\mathbb{Q} \cong \frac{\mathrm{Pic}(\widetilde{U})/\mathrm{Pic}^0(X)}{\mathrm{Pic}(U)/\mathrm{Pic}^0(Y)}\otimes\mathbb{Q}$$

and, by Lemma 2.5, the last group embeds into $H^2(\widetilde{U}, \mathbb{Q})/H^2(U, \mathbb{Q})$. Therefore, $\mathrm{Pic}^0(X_\eta)\otimes\mathbb{Q}$ embeds into

$$\frac{\ker[H^2(\widetilde{U}, \mathbb{Q}) \to H^2(X_t, \mathbb{Q})]}{H^2(U, \mathbb{Q})} \cong H^1(U, R^1 f_*\mathbb{Q}) = 0,$$

where $t \in U$. For the first isomorphism, we use the fact the Leray spectral sequence over U degenerates by [Deligne 1968]; the second is Proposition 2.3. □

3. Key vanishing

Let us fix a fine level structure $\Gamma \subseteq \Gamma_2$. We do not assume that it is classical. Choose a good model $f : X \to Y$ for $\bar{C}_2[\Gamma] \to \bar{M}_2[\Gamma]$, with $U, E, \widetilde{U}$ as above. Our goal in this section is to establish the vanishing of $\mathrm{Gr}_F^2 H^3(U, R^1 f_*\mathbb{C})$. This is the key fact which, when combined with Lemma 4.3 proved later on, will allow us to prove the Hodge conjecture for X.

Theorem 3.1. *$K_{X/Y}(1, 2)$ is quasiisomorphic to* 0.

Proof. The moduli stack $\bar{\mathbb{M}}_2$ is smooth and proper, the boundary divisor has normal crossings, and the universal curve is semistable. So we can define an analogue of $K(1, 2)$ on it. Since the canonical map $Y \to \bar{\mathbb{M}}_2$ is log étale, $K_{X/Y}(1, 2)$ is the pullback of the corresponding complex on the moduli stack. So we replace Y by $\bar{\mathbb{M}}_2$ and X by the universal curve $\bar{\mathbb{M}}_{2,1}$.

Set

$$H = f_*\omega_{X/Y}.$$

By duality, we have an isomorphism

$$H \cong R^1 f_*\mathcal{O}_X^\vee.$$

Thus the Kodaira–Spencer map

$$H \to \Omega^1_{\mathcal{Y}} \otimes H^\vee$$

induces an adjoint map

$$(H)^{\otimes 2} \to \Omega^1_{\mathcal{Y}}.$$

This factors through the symmetric power to yield a map

$$S^2 H \to \Omega^1_{\mathcal{Y}}. \tag{6}$$

After identifying $\overline{\mathbb{M}}_2 \cong \overline{\mathbb{A}}_2$, and $\mathrm{Pic}^0(X/Y)$ with the universal semiabelian variety, we see that (6) is an isomorphism by [Faltings and Chai 1990, Chapter IV, Theorem 5.7].

With the above notation $K(1, 2)$ can be written as

$$\Omega^1_{\mathcal{Y}} \otimes H \to \Omega^2_{\mathcal{Y}} \otimes H^\vee.$$

We need to show that the map in this complex is an isomorphism. It is enough to prove that the map is surjective, because both sides are locally free of the same rank. To do this, it suffices to prove that the adjoint map

$$\kappa' : \Omega^1_{\mathcal{Y}} \otimes (H)^{\otimes 2} \to \Omega^2_{\mathcal{Y}}$$

is surjective. Let κ'' denote the restriction of κ' to $\Omega^1_{\mathcal{Y}} \otimes S^2 H$. We can see that we have a commutative diagram

$$\begin{array}{ccc} \Omega^1_{\mathcal{Y}} \otimes S^2 H & \xrightarrow{\kappa''} & \Omega^2_{\mathcal{Y}} \\ \big\downarrow \cong & & \big\downarrow = \\ \Omega^1_{\mathcal{Y}} \otimes \Omega^1_{\mathcal{Y}} & \xrightarrow{\wedge} & \Omega^2_{\mathcal{Y}} \end{array}$$

This implies that κ'', and therefore κ', is surjective. □

From Proposition 1.2, we obtain:

Corollary 3.2.
$$\mathrm{Gr}^2_F H^*(U, R^1 f_*\mathbb{C}) = 0.$$

Remark 3.3. The referee has pointed out that for a classical level, a short alternative proof of the corollary can be deduced using Faltings' BGG resolution as follows. It suffices to prove $\mathrm{Gr}^2_F H^*(A_2[\Gamma], R^1 f'_*\mathbb{C}) = 0$, where f' is the universal abelian variety, because the restriction map to $\mathrm{Gr}^2_F H^*(U, R^1 f_*\mathbb{C})$ can be seen to be surjective. By [Faltings and Chai 1990, Chapter VI, Theorem 5.5] (see also [Petersen 2015, Theorem 2.4] for a more explicit statement) $\mathrm{Gr}^a_F H^*(A_2[\Gamma], R^1 f_*\mathbb{C})$ is zero unless $a \in \{0, 1, 3, 4\}$.

4. Hodge and Tate

Given a smooth projective variety X defined over $\mathbb{C}$, a Hodge cycle of degree $2p$ is an element of $\mathrm{Hom}_{\mathrm{HS}}(\mathbb{Q}(-p), H^{2p}(X, \mathbb{Q}))$, and given a smooth projective variety X defined over a finitely generated field K, an ℓ-adic Tate cycle of degree $2p$ is an element of $\sum H^{2p}_{\text{ét}}(X \otimes \overline{K}, \mathbb{Q}_\ell(p))^{\mathrm{Gal}(\overline{K}/L)}$ as L/K runs over finite extensions. The image of the cycle maps from $CH^p(X) \otimes \mathbb{Q}$ or $CH^p(X \otimes \overline{K}) \otimes \mathbb{Q}_\ell$ lands in these spaces. We say that the Hodge or Tate conjecture holds for X (in a given degree) if the space of Hodge or Tate cycles (of the given degree) are spanned by algebraic cycles. Here is the main result of the paper:

Theorem 4.1. *Let $f : X \to Y$ be a good model of $\overline{C}_2[\Gamma] \to \overline{M}_2[\Gamma]$, where $\Gamma \subseteq \Gamma_2$ is a fine level:*

(A) *The Hodge conjecture holds for X.*

(B) *When $\Gamma = \widetilde{\Gamma}(n)$ is a classical level, the Tate conjecture holds for X.*

We deduce this with the help of the following lemmas.

Lemma 4.2. *Let X_1 and X_2 be smooth projective varieties defined over a finitely generated field*:

(1) *If X_1 and X_2 are birational, then the Tate conjecture holds in degree 2 for X_1 if and only if it holds for X_2.*

(2) *If the Tate conjecture holds in degree 2 for X_1 and there is a dominant rational map $X_1 \dashrightarrow X_2$, then the Tate conjecture holds in degree 2 for X_2; if the Tate conjecture holds in degree $2d$ for X_1 and there is a surjective regular map $X_1 \dashrightarrow X_2$, then the Tate conjecture holds in degree $2d$ for X_2.*

(3) *If the Tate conjecture holds in degree 2 for X_i, then the Tate conjecture holds in degree 2 for $X_1 \times X_2$.*

Proof. See [Tate 1994, Theorem 5.2]. □

Lemma 4.3. *Let $f : (X, E) \to (Y, D)$ be a semistable map of smooth projective varieties with* $\dim Y = 3$ *and* $\dim X = 4$. *Suppose that*

$$\mathrm{Gr}_F^2 H^3(U, R^1 f_*\mathbb{C}) = 0,$$

where $U = Y - D$. Then the Hodge conjecture holds for X.

Proof. Also let $\widetilde{U} = X - E$. Since X is a fourfold, it is enough to prove that Hodge cycles in $H^4(X)$ are algebraic. The other cases follow from the Lefschetz (1, 1) and hard Lefschetz theorems. Using the main theorems of [Deligne 1968; Arapura 2005], and the semisimplicity of the category of polarizable Hodge structures, we have a noncanonical isomorphism of Hodge structures

$$\mathrm{Gr}_4^W H^4(\widetilde{U}) \cong \underbrace{\mathrm{Gr}_4^W H^4(U, f_*\mathbb{Q})}_{I} \oplus \underbrace{\mathrm{Gr}_4^W H^3(U, R^1 f_*\mathbb{Q})}_{II} \oplus \underbrace{\mathrm{Gr}_4^W H^2(U, R^2 f_*\mathbb{Q})}_{III}. \tag{7}$$

The first summand I can be identified with

$$\mathrm{im}[H^4(Y) \to H^4(U)] \cong \frac{H^4(Y)}{\sum \mathrm{im}\, H^2(D_i)(-1)} \cong L\left(\frac{H^2(Y)}{\sum L^{-1}\, \mathrm{im}\, H^2(D_i)(-1)}\right),$$

where L is the Lefschetz operator with respect to an ample divisor on Y. The Lefschetz (1, 1) theorem shows that the Hodge cycles in I are algebraic.

We have an isomorphism $\mathbb{Q}_U \cong R^2 f_*^o\mathbb{Q}$, under which $1 \in H^0(U, \mathbb{Q})$ maps to the class of a multisection $[\sigma] \in H^0(U, R^2 f_*^o\mathbb{Q})$. Thus the summand III can be identified with

$$[\sigma] \cup \mathrm{im}[H^2(Y) \to H^2(U)] \cong \frac{[\sigma] \cup H^2(Y)}{\sum [\sigma] \cup [D_i]}.$$

It follows again, by the Lefschetz (1, 1) theorem, that any Hodge cycle in the summand III is algebraic. This is also vacuously true for II because, by assumption, there are no Hodge cycles in $\mathrm{Gr}_4^W H^3(U, R^1 f_*\mathbb{Q})$.

From the sequence

$$\bigoplus H^2(E_i)(-1) \to H^4(X) \to \mathrm{Gr}_4^W H^4(\widetilde{U}) \to 0$$

we deduce that

$$H^4(X) \cong \bigoplus \operatorname{im} H^2(E_i)(-1) \oplus \operatorname{Gr}_4^W H^4(\widetilde{U}) \quad \text{(noncanonically).}$$

Therefore all the Hodge cycles in $H^4(X)$ are algebraic. □

Lemma 4.4. *Let $f : (X, E) \to (Y, D)$ be a semistable map of smooth projective varieties defined over a finitely generated subfield $K \subset \mathbb{C}$ with $\dim Y = 3$ and $\dim X = 4$. Let $U = Y - D$. Suppose that*

$$\operatorname{Gr}_F^2 H^3(U, R^1 f_* \mathbb{C}) = 0,$$

that $H^{1,1}(Y)$ is spanned by algebraic cycles, and that the Tate conjecture holds in degree 2 for the components E_i of E. Then the Tate conjecture holds for X in degree 4.

Proof. By the Hodge index theorem

$$\langle \alpha, \beta \rangle = \pm \operatorname{tr}(\alpha \cup \beta)$$

gives a positive definite pairing on the primitive part of $H^4(X)$, and this can be extended to the whole of H^4 by hard Lefschetz. Let

$$\begin{aligned} S_B &= \sum \operatorname{im} H^2(E_i(\mathbb{C}), \mathbb{C})(1) \subseteq H^4(X(\mathbb{C}), \mathbb{C})(2), \\ S_{\mathrm{Hdg}} &= \sum \operatorname{im} H^1(E_i, \Omega^1_{E_i}) \subseteq H^2(X, \Omega^2_X), \\ S_\ell &= \sum \operatorname{im} H^2_{\text{ét}}(E_i \otimes \overline{K}, \mathbb{Q}_\ell(1)) \subseteq H^4_{\text{ét}}(X \otimes \overline{K}, \mathbb{Q}_\ell(2)), \end{aligned}$$

where the images above are with respect to the Gysin maps. Set

$$\begin{aligned} V_B &= H^4(X(\mathbb{C}), \mathbb{C})(2)/S_B, \\ V_{\mathrm{Hdg}} &= H^2(X, \Omega^2_X)/S_{\mathrm{Hdg}}, \\ V_\ell &= H^4_{\text{ét}}(X \otimes \overline{K}, \mathbb{Q}_\ell(2))/S_\ell. \end{aligned}$$

Observe that V_B is a Hodge structure and V_ℓ is a Galois module. Let us say that a class in any one of these spaces is algebraic if it lifts to an algebraic cycle in $H^4(X)$ or $H^2(X, \Omega^2_X)$. Let us write

$$\operatorname{Tate}(-) = \sum_{[L:K]<\infty} (-)^{\operatorname{Gal}(\overline{K}/L)},$$

where $(-)$ can stand for V_ℓ or any other Galois module. Clearly

$$\dim(\text{space of algebraic classes in } V_\ell) \le \dim \operatorname{Tate}(V_\ell). \tag{8}$$

We also claim that

$$\dim \operatorname{Tate}(V_\ell) \le \dim V_{\mathrm{Hdg}}. \tag{9}$$

This will follow from the Hodge–Tate decomposition. After passing to a finite extension, we can assume that all elements of $\operatorname{Tate}(H^4(X, \mathbb{Q}_\ell(2)))$ and $\operatorname{Tate}(V_\ell)$ are fixed by $\operatorname{Gal}(\overline{K}/K)$. Let K_ℓ denote the completion of K at a prime lying over ℓ, and let $\mathbb{C}_\ell = \widehat{\overline{K}}_\ell$. By [Faltings 1988] there is a Hodge–Tate decomposition, i.e., a functorial isomorphism of $\mathrm{Gal}(\overline{K}_\ell/K_\ell)$-modules

$$H^4_{\text{ét}}(X \otimes \overline{K}, \mathbb{Q}_\ell(2)) \otimes_{\mathbb{Q}_\ell} \mathbb{C}_\ell \cong \bigoplus_{a+b=4} H^a(X, \Omega^b_X) \otimes_K \mathbb{C}_\ell(2-b).$$

This is compatible with products, Poincaré/Serre duality, and cycle maps. Since we can decompose $H^4_{\text{ét}}(X \otimes \overline{K}, \mathbb{Q}_\ell(2)) = S_\ell \oplus S_\ell^\perp$ as an orthogonal direct sum, and this is a decomposition of $\mathrm{Gal}(\overline{K}/K)$-modules, an element of $\gamma \in \mathrm{Tate}(V_\ell)$ can be lifted to $\gamma_1 \in \mathrm{Tate}(H^4_{\text{ét}}(X \otimes \overline{K}, \mathbb{Q}_\ell(2)))$. This gives a $\mathrm{Gal}(\overline{K}_\ell/K_\ell)$-invariant element of $H^4_{\text{ét}}(X \otimes \overline{K}, \mathbb{Q}_\ell(2)) \otimes \mathbb{C}_\ell$, and thus an element of $\gamma_2 \in H^2(X, \Omega^2_X) \otimes K_\ell$. Let $\gamma_3 \in V_{\mathrm{Hdg}} \otimes K_\ell$ denote the image. One can check that $\gamma \mapsto \gamma_3$ is a well-defined injection of $\mathrm{Tate}(V_\ell) \otimes K_\ell \to V_{\mathrm{Hdg}} \otimes K_\ell$. This proves that (9) holds.

As in the proof of Lemma 4.3, we can split $V_B(-2)$ as

$$V_B(-2) = I \oplus II \oplus III,$$

where the summands are defined as in (7). Arguing as above, but with the stronger assumption that $H^{1,1}(Y)$ is algebraic, we can see that the (not necessarily rational) $(2,2)$-classes in I and III are algebraic, and that II has no such classes. Therefore V_{Hdg} is spanned by algebraic classes. Combined with inequalities (8) and (9), we find that every element of $\mathrm{Tate}(V_\ell)$ is an algebraic class. Therefore given a Tate cycle $\gamma \in \mathrm{Tate}(H^4_{\text{ét}}(X \otimes \overline{K}, \mathbb{Q}_\ell(2)))$, there is an algebraic cycle γ' so that $\gamma - \gamma' \in S_\ell$. This means that $\gamma - \gamma'$ is the sum of images of Tate cycles in $H^2(E_i)$. By assumption, this is again algebraic. □

Lemma 4.5. *Let X be a smooth projective variety defined over a finitely generated subfield $K \subset \mathbb{C}$. If $H^{1,1}(X)$ is spanned by divisors, the Tate conjecture holds for X in degree* 2.

Proof. This is similar to the previous proof. We have inequalities

$$\operatorname{rank} \mathrm{NS}(X) \le \dim \mathrm{Tate}(H^2_{\text{ét}}(X \otimes \overline{K}, \mathbb{Q}_\ell(1))) \le h^{1,1}(X),$$

where the second follows from Hodge–Tate. Since $H^{1,1}(X)$ is spanned by divisors, we must have equality above. □

Proof of Theorem 4.1. The statement (A) about the Hodge conjecture follows immediately from Corollary 3.2 and Lemma 4.3.

We now turn to part (B) on the Tate conjecture. We break the analysis into cases. Tate in degree 2 follows from Theorem 2.6 and Lemma 4.5. Hard Lefschetz then implies Tate in degree 6. In degree 4, by Lemmas 4.2 and 4.4, it is enough to verify that $H^{1,1}(Y)$ is spanned by divisors and that the Tate conjecture holds in degree 2 for varieties rationally dominating components of the divisor E. The first condition for Y is due to [Weissauer 1988, p. 101]. By Corollary 2.2, irreducible components of E are dominated by $\overline{C}_{1,1}[n] \times \overline{M}_{1,1}[n]$, $\overline{C}_{1,2}[n]$, $\overline{C}_{1,1}[m] \times \mathbb{P}^1$, $\overline{M}_{1,1}[m] \times \overline{M}_{1,1}[m]$, $\mathbb{P}^2$ times a curve, or $\mathbb{P}^3$. The Tate conjecture in degree 2 is trivially true for the last two cases. The Tate conjecture in degree 2 for the other cases follows from [Gordon 1993, Theorem 5] and Lemma 4.2. □

Part (B) of the previous theorem can be extended slightly. Suppose that $\Gamma \subseteq \Gamma_2$ is the preimage of a finite-index subgroup of $\mathrm{Sp}_4(\mathbb{Z})$ such that $\overline{M}_2[\Gamma]$ is smooth. With this assumption, we may choose a good model $X \to Y$ of $\overline{C}_2[\Gamma] \to \overline{M}_2[\Gamma]$, with $Y = \overline{M}_2[\Gamma]$.

Corollary 4.6. *The Tate conjecture holds for X as above.*

Proof. We first note that Γ contains some $\widetilde{\Gamma}(n)$, because the congruence subgroup problem has a positive solution for $\mathrm{Sp}_4(\mathbb{Z})$ [Bass et al. 1967]. Therefore the good model $X[n]$ for $\widetilde{\Gamma}(n)$ surjects onto X. Since we know that Tate holds for $X[n]$, it holds for X by Lemma 4.2. □

Acknowledgement

My thanks to the referee for Remark 3.3 and other comments.

References

[Arapura 2005] D. Arapura, "The Leray spectral sequence is motivic", *Invent. Math.* **160**:3 (2005), 567–589. MR Zbl

[Bass et al. 1967] H. Bass, J. Milnor, and J.-P. Serre, "Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$", *Inst. Hautes Études Sci. Publ. Math.* **33** (1967), 59–137. MR Zbl

[Boggi and Pikaart 2000] M. Boggi and M. Pikaart, "Galois covers of moduli of curves", *Compositio Math.* **120**:2 (2000), 171–191. MR Zbl

[Cox and Zucker 1979] D. A. Cox and S. Zucker, "Intersection numbers of sections of elliptic surfaces", *Invent. Math.* **53**:1 (1979), 1–44. MR Zbl

[Deligne 1968] P. Deligne, "Théorème de Lefschetz et critères de dégénérescence de suites spectrales", *Inst. Hautes Études Sci. Publ. Math.* **35** (1968), 259–278. MR Zbl

[Deligne 1971] P. Deligne, "Théorie de Hodge, II", *Inst. Hautes Études Sci. Publ. Math.* **40** (1971), 5–57. MR Zbl

[Faltings 1988] G. Faltings, "p-adic Hodge theory", *J. Amer. Math. Soc.* **1**:1 (1988), 255–299. MR Zbl

[Faltings and Chai 1990] G. Faltings and C.-L. Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik (3) **22**, Springer, 1990. MR Zbl

[Fujisawa 1999] T. Fujisawa, "Limits of Hodge structures in several variables", *Compositio Math.* **115**:2 (1999), 129–183. MR Zbl

[Gordon 1993] B. B. Gordon, "Algebraic cycles and the Hodge structure of a Kuga fiber variety", *Trans. Amer. Math. Soc.* **336**:2 (1993), 933–947. MR Zbl

[Illusie 1990] L. Illusie, "Réduction semi-stable et décomposition de complexes de de Rham à coefficients", *Duke Math. J.* **60**:1 (1990), 139–185. MR Zbl

[de Jong 1996] A. J. de Jong, "Smoothness, semi-stability and alterations", *Inst. Hautes Études Sci. Publ. Math.* **83** (1996), 51–93. MR Zbl

[Kato 1989] K. Kato, "Logarithmic structures of Fontaine–Illusie", pp. 191–224 in *Algebraic analysis, geometry, and number theory* (Baltimore, 1988), edited by J.-I. Igusa, Johns Hopkins Univ. Press, Baltimore, 1989. MR Zbl

[Kato 2000] F. Kato, "Log smooth deformation and moduli of log smooth curves", *Int. J. Math.* **11**:2 (2000), 215–232. MR Zbl

[Katz 1970] N. M. Katz, "Nilpotent connections and the monodromy theorem: applications of a result of Turrittin", *Inst. Hautes Études Sci. Publ. Math.* **39** (1970), 175–232. MR Zbl

[Kempf et al. 1973] G. Kempf, F. F. Knudsen, D. Mumford, and B. Saint-Donat, *Toroidal embeddings, I*, Lecture Notes in Math. **339**, Springer, 1973. MR Zbl

[Namikawa 1980] Y. Namikawa, *Toroidal compactification of Siegel spaces*, Lecture Notes in Math. **812**, Springer, 1980. MR Zbl

[Oda and Schwermer 1990] T. Oda and J. Schwermer, "Mixed Hodge structures and automorphic forms for Siegel modular varieties of degree two", *Math. Ann.* **286**:1-3 (1990), 481–509. MR Zbl

[Petersen 2015] D. Petersen, "Cohomology of local systems on the moduli of principally polarized abelian surfaces", *Pacific J. Math.* **275**:1 (2015), 39–61. MR Zbl

[Pikaart and de Jong 1995] M. Pikaart and A. J. de Jong, "Moduli of curves with non-abelian level structure", pp. 483–509 in *The moduli space of curves* (Texel Island, Netherlands, 1994), edited by R. Dijkgraaf et al., Progr. Math. **129**, Birkhäuser, Boston, 1995. MR Zbl

[Raghunathan 1967] M. S. Raghunathan, "Cohomology of arithmetic subgroups of algebraic groups, I", *Ann. of Math.* (2) **86** (1967), 409–424. MR Zbl

[Shioda 1972] T. Shioda, "On elliptic modular surfaces", *J. Math. Soc. Japan* **24**:1 (1972), 20–59. MR Zbl

[Tate 1994] J. Tate, "Conjectures on algebraic cycles in l-adic cohomology", pp. 71–83 in *Motives* (Seattle, 1991), edited by U. Jannsen et al., Proc. Sympos. Pure Math. **55**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Viehweg 1977] E. Viehweg, "Rational singularities of higher dimensional schemes", *Proc. Amer. Math. Soc.* **63**:1 (1977), 6–8. MR Zbl

[Viehweg and Zuo 2004] E. Viehweg and K. Zuo, "A characterization of certain Shimura curves in the moduli stack of abelian varieties", *J. Differential Geom.* **66**:2 (2004), 233–287. MR Zbl

[Weissauer 1988] R. Weissauer, "Differentialformen zu Untergruppen der Siegelschen Modulgruppe zweiten Grades", *J. Reine Angew. Math.* **391** (1988), 100–156. MR Zbl

[Zucker 1979] S. Zucker, "Hodge theory with degenerating coefficients: L_2 cohomology in the Poincaré metric", *Ann. of Math.* (2) **109**:3 (1979), 415–476. MR Zbl

Communicated by Vasudevan Srinivas
Received 2018-02-28 Revised 2018-11-11 Accepted 2018-11-30

arapura@math.purdue.edu *Department of Mathematics, Purdue University, West Lafayette, IN, United States*

ALGEBRA AND NUMBER THEORY 13:1 (2019)
dx.doi.org/10.2140/ant.2019.13.227

Average nonvanishing of Dirichlet L-functions at the central point

Kyle Pratt

The generalized Riemann hypothesis implies that at least 50% of the central values $L\left(\frac{1}{2}, \chi\right)$ are nonvanishing as χ ranges over primitive characters modulo q. We show that one may unconditionally go beyond GRH, in the sense that if one averages over primitive characters modulo q and averages q over an interval, then at least 50.073% of the central values are nonvanishing. The proof utilizes the mollification method with a three-piece mollifier, and relies on estimates for sums of Kloosterman sums due to Deshouillers and Iwaniec.

1. Introduction

It is widely believed that no primitive Dirichlet L-function $L(s, \chi)$ vanishes at the central point $s = \frac{1}{2}$. Most of the progress towards this conjecture has been made by working with various families of Dirichlet L-functions. Balasubramanian and Murty [1992] showed that, in the family of primitive characters modulo q, a positive proportion of the L-functions do not vanish at the central point. Iwaniec and Sarnak [1999] later improved this lower bound, showing that at least $\frac{1}{3}$ of the L-functions in this family do not vanish at the central point. Bui [2012] improved this further to 34.11%, and Khan and Ngo [2016] showed at least $\frac{3}{8}$ of the central values are nonvanishing[1] for prime moduli. Soundararajan [2000] worked with a family of quadratic Dirichlet characters, and showed that $\frac{7}{8}$ of the family do not vanish at $s = \frac{1}{2}$. These proofs all proceed through the mollification method, which we discuss in Section 2 below.

If one assumes the generalized Riemann hypothesis, one can show that at least half of the primitive characters $\chi \pmod q$ satisfy $L\left(\frac{1}{2}, \chi\right) \neq 0$ [Balasubramanian and Murty 1992; Sica 1998; Miller and Takloo-Bighash 2006, Exercise 18.2.8]. One uses the explicit formula, rather than mollification, and the proportion $\frac{1}{2}$ arises from the choice of a test function with certain positivity properties.

It seems plausible that one may obtain a larger proportion of nonvanishing by also averaging over moduli q. Indeed, Iwaniec and Sarnak [1999] already claimed that by averaging over moduli one can prove at least half of the central values are nonzero. This is striking, in that it is as strong, on average, as the proportion obtained via GRH.

MSC2010: primary 11M06; secondary 11M26.
Keywords: Dirichlet L-function, nonvanishing, central point, mollifier, sums of Kloosterman sums.

[1] A clear preference for "non-vanishing" or "nonvanishing" has not yet materialized in the literature. We exclusively use the latter term throughout this work.

A natural question is whether, by averaging over moduli, one can breach the 50% barrier, thereby going beyond the immediate reach of GRH. We answer this question in the affirmative.

Let $\sum_{\chi(q)}^{*}$ denote a sum over the primitive characters modulo q, and define $\varphi^*(q)$ to be the number of primitive characters modulo q.

Theorem 1.1. *Let Ψ be a fixed, nonnegative smooth function, compactly supported in $\left[\frac{1}{2}, 2\right]$, which satisfies*

$$\int_{\mathbb{R}} \Psi(x)\,dx > 0.$$

Then for Q sufficiently large we have

$$\sum_{q} \Psi\left(\frac{q}{Q}\right)\frac{q}{\varphi(q)} \sideset{}{^*}\sum_{\substack{\chi(q) \\ L(\frac{1}{2},\chi)\neq 0}} 1 \geq 0.50073 \sum_{q} \Psi\left(\frac{q}{Q}\right)\frac{q}{\varphi(q)}\varphi^*(q).$$

Thus, roughly speaking, a randomly chosen central value $L\left(\frac{1}{2}, \chi\right)$ is more likely nonzero than zero. We remark also that the appearance of the arithmetic weight $q/\varphi(q)$ is technically convenient, but not essential.

2. Mollification and a sketch for Theorem 1.1

The proof of Theorem 1.1 relies on the powerful technique of mollification. For each character χ we associate a function $\psi(\chi)$, called a mollifier, that serves to dampen the large values of $L\left(\frac{1}{2}, \chi\right)$. By the Cauchy–Schwarz inequality we have

$$\frac{\left|\sum_{q\asymp Q}\sum_{\chi(q)}^{*} L\left(\frac{1}{2}, \chi\right)\psi(\chi)\right|^2}{\sum_{q\asymp Q}\sum_{\chi(q)}^{*}\left|L\left(\frac{1}{2}, \chi\right)\psi(\chi)\right|^2} \leq \sum_{q\asymp Q} \sideset{}{^*}\sum_{\substack{\chi(q) \\ L(\frac{1}{2},\chi)\neq 0}} 1. \tag{2-1}$$

The better the mollification by ψ, the larger proportion of nonvanishing one can deduce.

It is natural to choose $\psi(\chi)$ such that

$$\psi(\chi) \approx \frac{1}{L\left(\frac{1}{2}, \chi\right)}.$$

Since $L\left(\frac{1}{2}, \chi\right)$ can be written as a Dirichlet series

$$L\left(\tfrac{1}{2}, \chi\right) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^{1/2}}, \tag{2-2}$$

this suggests the choice

$$\psi(\chi) \approx \sum_{\ell\leq y} \frac{\mu(\ell)\chi(\ell)}{\ell^{1/2}}. \tag{2-3}$$

We have introduced a truncation y in anticipation of the need to control various error terms that will arise. We write $y = Q^{\theta}$, where $\theta > 0$ is a real number. At least heuristically, larger values of θ yield better mollification by (2-3). Iwaniec and Sarnak [1999] made this choice (2-3) (up to some smoothing), and found that the proportion of nonvanishing attained was

$$\frac{\theta}{1+\theta}. \tag{2-4}$$

When $\theta = 1$ we see (2-4) is exactly $\frac{1}{2}$, so we need $\theta > 1$ in order to conclude Theorem 1.1. This seems beyond the range of present technology. Without averaging over moduli we may take $\theta = \frac{1}{2} - \varepsilon$, and the asymptotic large sieve of Conrey, Iwaniec, and Soundararajan [Conrey et al. 2011] allows one to take $\theta = 1 - \varepsilon$ if one averages over moduli. This just falls short of our goal.

Thus, a better mollifier than (2-3) is required. Part of the problem is that (2-2) is an inefficient representation of $L(\frac{1}{2}, \chi)$. A better representation of $L(\frac{1}{2}, \chi)$ may be obtained through the approximate functional equation, which states

$$L\left(\tfrac{1}{2}, \chi\right) \approx \sum_{n \le q^{1/2}} \frac{\chi(n)}{n^{1/2}} + \epsilon(\chi) \sum_{n \le q^{1/2}} \frac{\overline{\chi}(n)}{n^{1/2}}. \tag{2-5}$$

Here $\epsilon(\chi)$ is the root number, which is a complex number of modulus 1 defined by

$$\epsilon(\chi) = \frac{1}{q^{1/2}} \sum_{h \pmod q} \chi(h) e\left(\frac{h}{q}\right). \tag{2-6}$$

Inspired by (2-5), Michel and VanderKam [2000] chose a mollifier

$$\psi(\chi) \approx \sum_{\ell \le y} \frac{\mu(\ell)\chi(\ell)}{\ell^{1/2}} + \bar{\epsilon}(\chi) \sum_{\ell \le y} \frac{\mu(\ell)\overline{\chi}(\ell)}{\ell^{1/2}}. \tag{2-7}$$

We note that Soundararajan [1995] earlier used a mollifier of this shape in the context of the Riemann zeta function.

For $y = Q^\theta$, Michel and VanderKam found that (2-7) gives a nonvanishing proportion of

$$\frac{2\theta}{1+2\theta}. \tag{2-8}$$

Thus, we need $\theta = \frac{1}{2} + \varepsilon$ in order for (2-8) to imply a proportion of nonvanishing greater than $\frac{1}{2}$. However, the more complicated nature of the mollifier (2-7) means that, without averaging over moduli, only the choice $\theta = \frac{3}{10} - \varepsilon$ is acceptable [Khan and Ngo 2016].

As we allow ourselves to average over moduli, however, one might hope to obtain (2-8) for $\theta = \frac{1}{2} + \varepsilon$. Again we fall just short of our goal. Using a powerful result of Deshouillers and Iwaniec on cancellation in sums of Kloosterman sums (see Lemma 5.1 below) we shall show that $\theta = \frac{1}{2} - \varepsilon$ is acceptable, but increasing θ any further seems very difficult. It follows that we need any extra amount of mollification in order to obtain a proportion of nonvanishing strictly greater than $\frac{1}{2}$.

The solution is to attach yet another piece to the mollifier $\psi(\chi)$, but here we wish for the mollifier to have a very different shape from (2-7). Such a mollifier was utilized by Bui [2012], who showed that

$$\psi_{\mathrm{B}}(\chi) \approx \frac{1}{\log q} \sum\sum_{bc \le y} \frac{\Lambda(b)\mu(c)\overline{\chi}(b)\chi(c)}{(bc)^{1/2}} \tag{2-9}$$

is a mollifier for $L\left(\frac{1}{2}, \chi\right)$. It turns out that adding (2-9) to (2-7) gives a sufficient mollifier to conclude Theorem 1.1.

One may roughly motivate a mollifier of the shape (2-9) as follows. Working formally,

$$\begin{aligned}
\frac{1}{L\left(\frac{1}{2}, \chi\right)} = \frac{L\left(\frac{1}{2}, \overline{\chi}\right)}{L\left(\frac{1}{2}, \chi\right)L\left(\frac{1}{2}, \overline{\chi}\right)} &= \sum\sum\sum_{r,s,v} \frac{\overline{\chi}(r)\mu(s)\overline{\chi}(s)\mu(v)\chi(v)}{(rsv)^{1/2}} \\
&\approx \sum\sum\sum_{r,s,v} \frac{\log r}{\log q} \frac{\overline{\chi}(r)\mu(s)\overline{\chi}(s)\mu(v)\chi(v)}{(rsv)^{1/2}} \\
&= \frac{1}{\log q} \sum\sum_{u,v} \frac{(\mu \star \log)(u)\overline{\chi}(u)\mu(v)\chi(v)}{(uv)^{1/2}}.
\end{aligned}$$

One might wonder what percentage of nonvanishing one can obtain using only a mollifier of the shape (2-9). The analysis for Bui's mollifier is more complicated, and it does not seem possible to write down simple expressions like (2-4) or (2-8) that give a percentage of nonvanishing for (2-9) in terms of θ. If one assumes, perhaps optimistically, that averaging over moduli allows one to take any $\theta < 1$ in (2-9), then some numerical computation indicates that the nonvanishing percentage does not exceed 27%, say.

We remark that, in the course of the proof, the main terms are easily extracted and we have no need here for the averaging over moduli. We require the averaging over moduli in order to estimate some of the error terms.

The structure of the remainder of the paper is as follows. In Section 3 we reduce the proof of Theorem 1.1 to two technical results, Lemmas 3.3 and 3.4, which give asymptotic evaluations of certain mollified sums. In Section 4 we extract the main term of Lemma 3.3, and in Section 5 we use estimates on sums of Kloosterman sums to complete the proof of this lemma. Section 6 similarly proves the main term of Lemma 3.4, but this derivation is longer than that given in Section 4 because the main terms are more complicated. In the final section, Section 7, we bound the error term in Lemma 3.4, again using results on sums of Kloosterman sums.

3. Proof of Theorem 1.1: first steps

Let us fix some notation and conventions that shall hold for the remainder of the paper.

The notation $a \equiv b(q)$ means $a \equiv b \pmod q$, and when $a(q)$ occurs beneath a sum it indicates a summation over residue classes modulo q.

We denote by ϵ an arbitrarily small positive quantity that may vary from one line to the next, or even within the same line. Thus, we may write $X^{2\epsilon} \le X^{\epsilon}$ with no reservations.

We need to treat separately the even primitive characters and odd primitive characters. We focus exclusively on the even primitive characters, since the case of odd characters is nearly identical. We write $\sum_{\chi(q)}^{+}$ for a sum over even primitive characters modulo q, and we write $\varphi^{+}(q)$ for the number of such characters. Observe that $\varphi^{+}(q) = \frac{1}{2}\varphi^{*}(q) + O(1)$.

We shall encounter the Ramanujan sum $c_q(n)$ (see the proof of Proposition 5.2), defined by

$$c_q(n) = \sum_{\substack{a(q)\\(a,q)=1}} e\left(\frac{an}{q}\right).$$

We shall only need to know that $c_q(1) = \mu(q)$ and $|c_q(n)| \le (q,n)$, where (q,n) is the greatest common divisor of q and n.

We now fix a smooth function Ψ as in the statement of Theorem 1.1, and allow all implied constants to depend on Ψ. We let Q be a large real number, and set $y_i = Q^{\theta_i}$ for $i \in \{1,2,3\}$, where $0 < \theta_i < \frac{1}{2}$ are fixed real numbers. We further define $L = \log Q$. The notation $o(1)$ denotes a quantity that goes to zero as Q goes to infinity.

Let us now begin the proof of Theorem 1.1 in earnest. As discussed in Section 2, we choose our mollifier $\psi(\chi)$ to have the form

$$\psi(\chi) = \psi_{\mathrm{IS}}(\chi) + \psi_{\mathrm{B}}(\chi) + \psi_{\mathrm{MV}}(\chi), \tag{3-1}$$

where

$$\begin{aligned} \psi_{\mathrm{IS}}(\chi) &= \sum_{\ell \le y_1} \frac{\mu(\ell)}{\ell^{1/2}} P_1\left(\frac{\log(y_1/\ell)}{\log y_1}\right), \\ \psi_{\mathrm{B}}(\chi) &= \frac{1}{L} \sum\sum_{bc \le y_2} \frac{\Lambda(b)\mu(c)\overline{\chi}(b)\chi(c)}{(bc)^{1/2}} P_2\left(\frac{\log(y_2/bc)}{\log y_2}\right), \\ \psi_{\mathrm{MV}}(\chi) &= \epsilon(\overline{\chi}) \sum_{\ell \le y_3} \frac{\mu(\ell)\overline{\chi}(\ell)}{\ell^{1/2}} P_3\left(\frac{\log(y_3/\ell)}{\log y_3}\right). \end{aligned} \tag{3-2}$$

The smoothing polynomials P_i are real and satisfy $P_i(0) = 0$. For notational convenience we write

$$P_i\left(\frac{\log(y_i/x)}{\log y_i}\right) = P_i[x].$$

There is some ambiguity in this notation because of the y_i-dependence in the polynomials, and this needs to be remembered in calculations.

Now define sums S_1 and S_2 by

$$\begin{aligned} S_1 &= \sum_q \Psi\left(\frac{q}{Q}\right) \frac{q}{\varphi(q)} \sum_{\chi(q)}^{+} L\left(\tfrac{1}{2},\chi\right)\psi(\chi), \\ S_2 &= \sum_q \Psi\left(\frac{q}{Q}\right) \frac{q}{\varphi(q)} \sum_{\chi(q)}^{+} \left|L\left(\tfrac{1}{2},\chi\right)\psi(\chi)\right|^2. \end{aligned} \tag{3-3}$$

We apply Cauchy–Schwarz as in (2-1) and get

$$\sum_q \Psi\left(\frac{q}{Q}\right)\frac{q}{\varphi(q)} \sideset{}{^+}\sum_{\substack{\chi(q)\\ L(\frac{1}{2},\chi)\neq 0}} 1 \geq \frac{S_1^2}{S_2}. \tag{3-4}$$

The proof of Theorem 1.1 therefore reduces to estimating S_1 and S_2. We obtain asymptotic formulas for these two sums.

Lemma 3.1. *Suppose* $0 < \theta_1, \theta_2 < 1$ *and* $0 < \theta_3 < \frac{1}{2}$. *Then*

$$S_1 = \left(P_1(1) + P_3(1) + \frac{\theta_2}{2}\widetilde{P}_2(1) + o(1)\right)\sum_q \Psi\left(\frac{q}{Q}\right)\frac{q}{\varphi(q)}\varphi^+(q),$$

where

$$\widetilde{P}_2(x) = \int_0^x P_2(u)\,du.$$

Lemma 3.2. *Let* $0 < \theta_1, \theta_2, \theta_3 < \frac{1}{2}$ *with* $\theta_2 < \theta_1, \theta_3$. *Then*

$$S_2 = \left(2P_1(1)P_3(1) + P_3(1)^2 + \frac{1}{\theta_3}\int_0^1 P_3'(x)^2\,dx + \kappa + \lambda + o(1)\right)\sum_q \Psi\left(\frac{q}{Q}\right)\frac{q}{\varphi(q)}\varphi^+(q),$$

where

$$\kappa = 3\theta_2 P_3(1)\widetilde{P}_2(1) - 2\theta_2\int_0^1 P_2(x)P_3(x)\,dx$$

and

$$\begin{aligned}\lambda = P_1(1)^2 + \frac{1}{\theta_1}\int_0^1 P_1'(x)^2\,dx - \theta_2 P_1(1)\widetilde{P}_2(1) + 2\theta_2\int_0^1 P_1\left(1 - \frac{\theta_2(1-x)}{\theta_1}\right)P_2(x)\,dx \\ + \frac{\theta_2}{\theta_1}\int_0^1 P_1'\left(1 - \frac{\theta_2(1-x)}{\theta_1}\right)P_2(x)\,dx + \theta_2^2\int_0^1 (1-x)P_2(x)^2\,dx \\ + \frac{\theta_2}{2}\int_0^1 (1-x)^2 P_2'(x)^2\,dx - \frac{\theta_2^2}{4}\widetilde{P}_2(1)^2 + \frac{\theta_2}{4}\int_0^1 P_2(x)^2\,dx.\end{aligned}$$

Proof of Theorem 1.1. Lemmas 3.1 and 3.2 give the evaluations of S_1 and S_2 for even characters. The identical formulas hold for odd characters. Theorem 1.1 then follows from (3-4) upon choosing $\theta_1 = \theta_3 = \frac{1}{2}$, $\theta_2 = 0.163$, and

$$\begin{aligned}P_1(x) &= 4.86x + 0.29x^2 - 0.96x^3 + 0.974x^4 - 0.17x^5,\\ P_2(x) &= -3.11x - 0.3x^2 + 0.87x^3 - 0.18x^4 - 0.53x^5,\\ P_3(x) &= 4.86x + 0.06x^2.\end{aligned}$$

These choices actually yield a proportion[2]

$$\geq 0.50073004\ldots,$$

which allows us to state Theorem 1.1 with a clean inequality. □

[2] A Mathematica file with this computation is included with this paper on arXiv at https://arxiv.org/e-print/1804.01445v1.

We note without further comment the curiosity in the proof of Theorem 1.1 that the largest permissible value of θ_2 is not optimal.

We can dispense with S_1 quickly.

Proof of Lemma 3.1. Apply [Bui 2012, Theorem 2.1] and the argument of [Michel and VanderKam 2000, §3], using the facts $L = \log q + O(1)$ and $y_i = q^{\theta_i + o(1)}$. □

The analysis of S_2 is much more involved, and we devote the remainder of the paper to this task. We first observe that (3-1) yields

$$|\psi(\chi)|^2 = |\psi_{\mathrm{IS}}(\chi) + \psi_{\mathrm{B}}(\chi)|^2 + 2\,\mathrm{Re}\{\psi_{\mathrm{IS}}(\chi)\psi_{\mathrm{MV}}(\overline{\chi}) + \psi_{\mathrm{B}}(\chi)\psi_{\mathrm{MV}}(\overline{\chi})\} + |\psi_{\mathrm{MV}}(\chi)|^2.$$

By [Bui 2012, Theorem 2.2] we have

$$\sideset{}{^+}\sum_{\chi(q)} \bigl|L\bigl(\tfrac{1}{2}, \chi\bigr)\bigr|^2 |\psi_{\mathrm{IS}}(\chi) + \psi_{\mathrm{B}}(\chi)|^2 = \lambda\varphi^+(q) + O(qL^{-1+\epsilon}),$$

where λ is as in Lemma 3.2. We also have

$$\begin{aligned}\frac{1}{\varphi^+(q)} \sideset{}{^+}\sum_{\chi(q)} \bigl|L\bigl(\tfrac{1}{2}, \chi\bigr)\bigr|^2 |\psi_{\mathrm{MV}}(\chi)|^2 &= \frac{1}{\varphi^+(q)} \sideset{}{^+}\sum_{\chi(q)} \bigl|L\bigl(\tfrac{1}{2}, \chi\bigr)\bigr|^2 \biggl|\sum_{\ell \le y_3} \frac{\mu(\ell)\chi(\ell)P_3[\ell]}{\ell^{1/2}}\biggr|^2 \\ &= P_3(1)^2 + \frac{1}{\theta_3}\int_0^1 P_3'(x)^2\,dx + O(L^{-1+\epsilon}),\end{aligned}$$

by the analysis of the Iwaniec–Sarnak mollifier [Bui 2012, §2.3].

Therefore, in order to prove Lemma 3.2 it suffices to prove the following two results.

Lemma 3.3. *For* $0 < \theta_1, \theta_3 < \frac{1}{2}$ *we have*

$$\sum_q \Psi\Bigl(\frac{q}{Q}\Bigr)\frac{q}{\varphi(q)} \sideset{}{^+}\sum_{\chi(q)} \bigl|L\bigl(\tfrac{1}{2}, \chi\bigr)\bigr|^2 \psi_{\mathrm{IS}}(\chi)\psi_{\mathrm{MV}}(\overline{\chi}) = (P_1(1)P_3(1) + o(1)) \sum_q \Psi\Bigl(\frac{q}{Q}\Bigr)\frac{q}{\varphi(q)}\varphi^+(q).$$

Lemma 3.4. *Let* $0 < \theta_2 < \theta_3 < \frac{1}{2}$. *Then*

$$\begin{aligned}&\sum_q \Psi\Bigl(\frac{q}{Q}\Bigr)\frac{q}{\varphi(q)} \sideset{}{^+}\sum_{\chi(q)} \bigl|L\bigl(\tfrac{1}{2}, \chi\bigr)\bigr|^2 \psi_{\mathrm{B}}(\chi)\psi_{\mathrm{MV}}(\overline{\chi}) \\ &\qquad = \biggl(\frac{3\theta_2}{2}P_3(1)\widetilde{P}_2(1) - \theta_2\int_0^1 P_2(x)P_3(x)\,dx + o(1)\biggr) \sum_q \Psi\Bigl(\frac{q}{Q}\Bigr)\frac{q}{\varphi(q)}\varphi^+(q).\end{aligned}$$

4. Lemma 3.3: main term

The goal of this section is to extract the main term in Lemma 3.3. The main term analysis is given in [Michel and VanderKam 2000, §6], but as the ideas also appear in the proof of Lemma 3.4 we give details here.

We begin with two lemmas.

Lemma 4.1. *Let χ be a primitive even character modulo q. Let $G(s)$ be an even polynomial satisfying $G(0)=1$, and which vanishes to second order at $\frac{1}{2}$. Then we have*

$$\left|L\left(\tfrac{1}{2},\chi\right)\right|^2 = 2\sum_{m,n}\sum \frac{\chi(m)\overline{\chi}(n)}{(mn)^{1/2}} V\left(\frac{mn}{q}\right),$$

where

$$V(x) = \frac{1}{2\pi i}\int_{(1)} \frac{\Gamma^2\left(\frac{1}{2}s+\frac{1}{4}\right)}{\Gamma^2\left(\frac{1}{4}\right)} \frac{G(s)}{s} \pi^{-s} x^{-s}\, ds. \tag{4-1}$$

Proof. See [Iwaniec and Sarnak 1999, (2.5)]. The result follows along the lines of [Iwaniec and Kowalski 2004, Theorem 5.3]. □

We remark that V satisfies $V(x) \ll_A (1+x)^{-A}$, as can be seen by moving the contour of integration to the right. We also note that the choice of $G(s)$ in Lemma 4.1 is almost completely free. In particular, we may choose G to vanish at whichever finite set of points is convenient for us (see (4-6) below for an application).

Lemma 4.2. *Let $(mn,q)=1$. Then*

$$\sum_{\chi(q)}^{+} \chi(m)\overline{\chi}(n) = \frac{1}{2}\sum_{\substack{vw=q\\ w\mid m\pm n}}\sum \mu(v)\varphi(w).$$

Proof. See [Bui and Milinovich 2011, Lemma 4.1], for instance. □

We do not need the averaging over q in order to extract the main term of Lemma 3.3. We insert the definitions of the mollifiers $\psi_{\mathrm{IS}}(\chi)$ and $\psi_{\mathrm{MV}}(\overline{\chi})$, then apply Lemma 4.1, and interchange orders of summation. We obtain

$$\sum_{\chi(q)}^{+} \left|L\left(\tfrac{1}{2},\chi\right)\right|^2 \psi_{\mathrm{IS}}(\chi)\psi_{\mathrm{MV}}(\overline{\chi}) = 2\sum_{\substack{\ell_1\le y_1\\ \ell_3\le y_3\\ (\ell_1\ell_3,q)=1}}\sum \frac{\mu(\ell_1)\mu(\ell_3)P_1[\ell_1]P_3[\ell_3]}{(\ell_1\ell_3)^{1/2}} \sum_{(mn,q)=1}\sum \frac{1}{(mn)^{1/2}} V\left(\frac{mn}{q}\right) \sum_{\chi(q)}^{+} \epsilon(\chi)\chi(m\ell_1\ell_3)\overline{\chi}(n). \tag{4-2}$$

Opening $\epsilon(\chi)$ using (2-6) and applying Lemma 4.2, we find after some work [Iwaniec and Sarnak 1999, (3.4) and (3.7)] that

$$\sum_{\chi(q)}^{+} \epsilon(\chi)\chi(m\ell_1\ell_3)\overline{\chi}(n) = \frac{1}{q^{1/2}} \sum_{\substack{vw=q\\ (v,w)=1}}\sum \mu^2(v)\varphi(w)\cos\frac{2\pi n\overline{m\ell_1\ell_3 v}}{w}. \tag{4-3}$$

The main term comes from $m\ell_1\ell_3=1$. With this constraint in place we apply character orthogonality in reverse, obtaining that the main term $M_{\mathrm{IS,MV}}$ of Lemma 3.3 is

$$M_{\mathrm{IS,MV}} = 2P_1(1)P_3(1)\sum_{\chi(q)}^{+} \epsilon(\chi)\sum_n \frac{\overline{\chi}(n)}{n^{1/2}} V\left(\frac{n}{q}\right).$$

We have the following proposition.

Proposition 4.3. *Let χ be a primitive even character modulo q, and let $T > 0$ be a real number. Let V be defined as in (4-1). Then*

$$\sum_n \frac{\bar{\chi}(n)}{n^{1/2}} V\left(\frac{Tn}{q}\right) = L\left(\tfrac{1}{2}, \bar{\chi}\right) - \epsilon(\bar{\chi}) \sum_n \frac{\chi(n)}{n^{1/2}} F\left(\frac{n}{T}\right),$$

where

$$F(x) = \frac{1}{2\pi i} \int_{(1)} \frac{\Gamma\left(\frac{1}{2}s + \frac{1}{4}\right)\Gamma\left(-\frac{1}{2}s + \frac{1}{4}\right)}{\Gamma^2\left(\frac{1}{4}\right)} \frac{G(s)}{s} x^{-s}\, ds. \tag{4-4}$$

Before proving Proposition 4.3, let us see how to use it to finish the evaluation of $M_{\mathrm{IS,MV}}$. Proposition 4.3 gives

$$M_{\mathrm{IS,MV}} = 2P_1(1)P_3(1) \sum_{\chi(q)}^{+} \epsilon(\chi) L\left(\tfrac{1}{2}, \bar{\chi}\right) - 2P_1(1)P_3(1) \sum_{\chi(q)}^{+} \sum_n \frac{\chi(n)}{n^{1/2}} F(n),$$

and by the first moment analysis (see [Michel and VanderKam 2000, §3] and also Section 6 below) we have

$$2P_1(1)P_3(1) \sum_{\chi(q)}^{+} \epsilon(\chi) L\left(\tfrac{1}{2}, \bar{\chi}\right) = (1 + o(1)) 2P_1(1)P_3(1)\varphi^{+}(q). \tag{4-5}$$

For the other piece, we apply Lemma 4.2 to obtain

$$-2P_1(1)P_3(1) \sum_{\chi(q)}^{+} \sum_n \frac{\chi(n)}{n^{1/2}} F(n) = -P_1(1)P_3(1) \sum_{w \mid q} \varphi(w)\mu(q/w) \sum_{\substack{n \equiv \pm 1 (w) \\ (n,q)=1}} \frac{1}{n^{1/2}} F(n).$$

We choose G to vanish at all the poles of

$$\Gamma\left(\tfrac{1}{2}s + \tfrac{1}{4}\right)\Gamma\left(-\tfrac{1}{2}s + \tfrac{1}{4}\right)$$

in the disc $|s| \le A$, where $A > 0$ is large but fixed. By moving the contour of integration to the right we see

$$F(x) \ll \frac{1}{(1+x)^{100}}, \tag{4-6}$$

say, and therefore, the contribution from $n > q^{1/10}$ is negligible. By trivial estimation the contribution from $w \le q^{1/4}$ is also negligible. For $w > q^{1/4}$ and $n \le q^{1/10}$, we can only have $n \equiv \pm 1 \pmod{w}$ if $n = 1$. Adding back in the terms with $n \le q^{1/4}$, the contribution from these terms is therefore

$$-(1 + o(1)) 2P_1(1)P_3(1)F(1)\varphi^{+}(q). \tag{4-7}$$

Since the integrand in $F(1)$ is odd, we may evaluate $F(1)$ through a residue at $s = 0$. We shift the line of integration in (4-4) to $\operatorname{Re} s = -1$, picking up a contribution from the simple pole at $s = 0$. In the integral on the line $\operatorname{Re} s = -1$ we change variables $s \to -s$. This yields the relation $F(1) = 1 - F(1)$, whence $F(1) = \frac{1}{2}$. Combining (4-5) and (4-7), we obtain

$$M_{\mathrm{IS,MV}} = (1 + o(1)) P_1(1)P_3(1)\varphi^{+}(q),$$

as desired. This yields the main term of Lemma 3.3.

Proof of Proposition 4.3. We write V using its definition and interchange orders of summation and integration to get

$$\sum_n \frac{\overline{\chi}(n)}{n^{1/2}} V\left(\frac{Tn}{q}\right) = \frac{1}{2\pi i}\int_{(1)} \frac{\Gamma^2\left(\frac{1}{2}s+\frac{1}{4}\right)}{\Gamma^2\left(\frac{1}{4}\right)} \frac{G(s)}{s} \left(\frac{q}{\pi}\right)^s T^{-s} L\left(\tfrac{1}{2}+s, \overline{\chi}\right) ds.$$

We move the line of integration to $\operatorname{Re} s = -1$, picking up a contribution of $L\left(\frac{1}{2}, \overline{\chi}\right)$ from the pole at $s = 0$. Observe that we do not get any contribution from the double pole of $\Gamma^2\left(\frac{1}{2}s+\frac{1}{4}\right)$ at $s = -\frac{1}{2}$ because of our assumption that G vanishes at $s = \pm\frac{1}{2}$ to second order.

Now, for the integral on the line $\operatorname{Re} s = -1$, we apply the functional equation for $L\left(\frac{1}{2}+s, \overline{\chi}\right)$ and then change variables $s \to -s$ to obtain

$$-\epsilon(\overline{\chi}) \frac{1}{2\pi i}\int_{(1)} \frac{\Gamma\left(\frac{1}{2}s+\frac{1}{4}\right)\Gamma\left(-\frac{1}{2}s+\frac{1}{4}\right)}{\Gamma^2\left(\frac{1}{4}\right)} \frac{G(s)}{s} T^s L\left(\tfrac{1}{2}+s, \chi\right) ds.$$

The desired result follows by expanding $L\left(\frac{1}{2}+s, \chi\right)$ in its Dirichlet series and interchanging the order of summation and integration. □

5. Lemma 3.3: error term

Here we show that the remainder of the terms in (4-2) (those with $m\ell_1\ell_3 \neq 1$) contribute only to the error term of Lemma 3.3. Here we must avail ourselves of the averaging over q.

Inserting (4-3) into (4-2) and averaging over moduli, we wish to show that

$$\mathscr{E}_1 = \sum\sum_{(v,w)=1} \mu^2(v) \frac{v}{\varphi(v)} \frac{w^{1/2}}{v^{1/2}} \Psi\left(\frac{vw}{Q}\right) \sum\sum_{\substack{\ell_1 \le y_1 \\ \ell_3 \le y_3 \\ (\ell_1\ell_3, vw)=1}} \frac{\mu(\ell_1)\mu(\ell_3)P_1[\ell_1]P_3[\ell_3]}{(\ell_1\ell_3)^{1/2}}$$
$$\times \sum\sum_{(mn,vw)=1} \frac{1}{(mn)^{1/2}} Z\left(\frac{mn}{vw}\right) \cos \frac{2\pi n \overline{m\ell_1\ell_3 v}}{w} \ll Q^{2-\epsilon+o(1)}, \quad (5\text{-}1)$$

where $m\ell_1\ell_3 \neq 1$, but we do not indicate this in the notation. The function Z is actually just V in (4-1), but we do not wish to confuse the function V with the scale V that shall appear shortly.

Observe that the arithmetic weight $q/\varphi(q)$ has become $(v/\varphi(v))(w/\varphi(w))$ by multiplicativity, and that this factor of $\varphi(w)$ has canceled with $\varphi(w)$ in (4-3), making the sum on w smooth.

The main tool we use to bound $\mathscr{E}_1'$ is the following result, due to Deshouillers and Iwaniec, on cancellation in sums of Kloosterman sums.

Lemma 5.1. *Let C, D, N, R, S be positive numbers, and let $b_{n,r,s}$ be a complex sequence supported in $(0, N] \times (R, 2R] \times (S, 2S] \cap \mathbb{N}^3$. Let $g_0(\xi, \eta)$ be a smooth function having compact support in $\mathbb{R}^+ \times \mathbb{R}^+$,* *and let* $g(c,d)=g_0(c/C,d/D)$. *Then*

$$\sum_{c}\sum_{d}\sum_{n}\sum_{r}\sum_{s}{}_{(rd,sc)=1} b_{n,r,s}\, g(c,d)\, e\Big(n\frac{\overline{rd}}{sc}\Big) \ll_{\epsilon,g_0} (CDNRS)^{\epsilon} K(C,D,N,R,S)\|b_{N,R,S}\|_2,$$

where

$$\|b_{N,R,S}\|_2=\Big(\sum_{n}\sum_{r}\sum_{s}|b_{n,r,s}|^2\Big)^{1/2}$$

and

$$K(C,D,N,R,S)^2=CS(RS+N)(C+RD)+C^2DS\sqrt{(RS+N)R}+D^2NRS^{-1}.$$

Proof. This is essentially [Bombieri et al. 1986, Lemma 1], which is an easy consequence of [Deshouillers and Iwaniec 1982, Theorem 12]. □

We need to massage (5-1) before it is in a form where an application of Lemma 5.1 is appropriate. Let us briefly describe our plan of attack. We apply partitions of unity to localize the variables and then separate variables with integral transforms. By using the orthogonality of multiplicative characters we will be able to assume that v is quite small, which is advantageous when it comes time to remove coprimality conditions involving v. We next reduce to the case in which n is somewhat small. This is due to the fact that the sum on n is essentially a Ramanujan sum, and Ramanujan sums experience better than square-root cancellation on average. We next use Möbius inversion to remove the coprimality condition between n and w. This application of Möbius inversion introduces a new variable, call it f, and another application of character orthogonality allows us to assume f is small. We then remove the coprimality conditions on m. We finally apply Lemma 5.1 to get the desired cancellation, and it is crucial here that f and v are no larger than Q^{ϵ}.

Let us turn to the details in earnest. We apply smooth partitions of unity (see [Blomer et al. 2017, Lemma 1.6], for instance) in all variables, so that $\mathscr{E}_1$ can be written

$$\sum\cdots\sum_{M,N,L_1,L_3,V,W} \mathscr{E}_1(M,N,L_1,L_3,V,W), \tag{5-2}$$

where

$$\mathscr{E}_1(M,N,L_1,L_3,V,W)=\sum\sum_{(v,w)=1}\mu^2(v)\frac{v}{\varphi(v)}\frac{w^{1/2}}{v^{1/2}}\Psi\Big(\frac{vw}{Q}\Big)G\Big(\frac{v}{V}\Big)G\Big(\frac{w}{W}\Big)$$
$$\times\sum\sum_{\substack{\ell_1\le y_1\\ \ell_3\le y_3\\ (\ell_1\ell_3,vw)=1}}\frac{\mu(\ell_1)\mu(\ell_3)P_1[\ell_1]P_3[\ell_3]}{(\ell_1\ell_3)^{1/2}}G\Big(\frac{\ell_1}{L_1}\Big)G\Big(\frac{\ell_3}{L_3}\Big)$$
$$\times\sum\sum_{(mn,vw)=1}\frac{1}{(mn)^{1/2}}Z\Big(\frac{mn}{vw}\Big)G\Big(\frac{m}{M}\Big)G\Big(\frac{n}{N}\Big)\cos\frac{2\pi nm\overline{\ell_1\ell_3 v}}{w}.$$

Here G is a smooth, nonnegative function supported in $\left[\frac{1}{2}, 2\right]$, and the numbers M, N, L_i, V, W in (5-2) range over powers of two. We may assume

$$M, N, L_1, L_3, V, W \gg 1, \qquad VW \asymp Q, \qquad L_i \ll y.$$

Furthermore, by the rapid decay of Z we may assume $MN \le Q^{1+\epsilon}$. Thus, the number of summands $\mathscr{E}_1(M, \dots, W)$ in (5-2) is $\ll Q^{o(1)}$.

Up to changing the definition of G, we may rewrite $\mathscr{E}_1(M, \dots, W)$ as

$$\begin{aligned}\mathscr{E}_1(M, N, L_1, L_3, V, W) = \frac{W^{1/2}}{(MNL_1L_3V)^{1/2}} &\sum\sum_{(v,w)=1} \alpha(v) G\left(\frac{v}{V}\right) G\left(\frac{w}{W}\right) \Psi\left(\frac{vw}{Q}\right) \\ &\times \sum\sum_{\substack{\ell_i \le y_i \\ (\ell_i, vw)=1}} \beta(\ell_1)\gamma(\ell_3) G\left(\frac{\ell_1}{L_1}\right) G\left(\frac{\ell_3}{L_3}\right) \\ &\times \sum\sum_{(mn,vw)=1} Z\left(\frac{mn}{vw}\right) G\left(\frac{m}{M}\right) G\left(\frac{n}{N}\right) \cos \frac{2\pi n\overline{m\ell_1\ell_3 v}}{w},\end{aligned}$$

where α, β, γ are sequences satisfying $|\alpha(v)|, |\beta(\ell_1)|, |\gamma(\ell_3)| \ll Q^{o(1)}$.

We separate the variables in Z by writing Z using its definition as an integral (4-1) and moving the line of integration to $\operatorname{Re} s = L^{-1}$. By the rapid decay of the Γ function in vertical strips we may restrict to $|\operatorname{Im} s| \le Q^{\epsilon}$. We similarly separate the variables in Ψ using the inverse Mellin transform. Therefore, up to changing the definition of some of the functions G, it suffices to prove that

$$\begin{aligned}\mathscr{E}_1'(M, N, L_1, L_3, V, W) = \frac{W^{1/2}}{(MNL_1L_3V)^{1/2}} &\sum\sum_{(v,w)=1} \alpha(v) G\left(\frac{v}{V}\right) G\left(\frac{w}{W}\right) \\ &\times \sum\sum_{\substack{\ell_i \le y_i \\ (\ell_i, vw)=1}} \beta(\ell_1)\gamma(\ell_3) G\left(\frac{\ell_3}{L_3}\right) G\left(\frac{\ell_3}{L_3}\right) \\ &\times \sum\sum_{(mn,vw)=1} G\left(\frac{m}{M}\right) G\left(\frac{n}{N}\right) e\left(\frac{n\overline{m\ell_1\ell_3 v}}{w}\right) \ll Q^{2-\epsilon+o(1)}. \end{aligned} \tag{5-3}$$

Our smooth functions G all satisfy $G^{(j)}(x) \ll_j Q^{j\epsilon}$ for $j \ge 0$. To save on space we write the left side of (5-3) as simply $\mathscr{E}_1'$.

Observe that the trivial bound for $\mathscr{E}_1'$ is

$$\mathscr{E}_1' \ll V^{1/2} W^{3/2} (MN)^{1/2} (L_1L_3)^{1/2} Q^{o(1)} \ll \frac{Q^{2+\epsilon}(y_1y_3)^{1/2}}{V}. \tag{5-4}$$

This bound is worst when V is small. Since y_i will be taken close to $Q^{1/2}$, we therefore need to save $\approx Q^{1/2}$ in order to obtain (5-1). The trivial bound does show, however, that the contribution from $V > Q^{1/2+2\epsilon}$ is acceptably small, and we may therefore assume that $V \le Q^{1/2+2\epsilon}$. Note this implies $W \gg Q^{1/2-\epsilon}$.

We now reduce to the case $V \ll Q^\epsilon$. We accomplish this by reintroducing multiplicative characters. The orthogonality of multiplicative characters yields

$$e\left(\frac{nm\overline{\ell_1\ell_3 v}}{w}\right) = \frac{1}{\varphi(w)} \sum_{\chi(w)} \tau(\overline{\chi})\chi(n)\overline{\chi}(m\ell_1\ell_3 v). \tag{5-5}$$

Using the Gauss sum bound $|\tau(\overline{\chi})| \ll w^{1/2}$ we then arrange $\mathscr{E}_1'$ as

$$\mathscr{E}_1' \ll \frac{W}{(MNL_1L_3V)^{1/2}} \sum_{w\asymp W} \frac{1}{\varphi(w)} \sum_{v\asymp V} \left| \sum_{(mn,v)=1}\sum \chi(n)\overline{\chi}(m) \right| \left| \sum_{(\ell_1\ell_3,v)=1}\sum \overline{\chi}(\ell_1\ell_3) \right|,$$

where we have suppressed some things in the notation for brevity. By Cauchy–Schwarz and character orthogonality we obtain

$$\sum_{\chi(w)} \left| \sum_{m,n}\sum \right| \left| \sum_{\ell_1,\ell_3}\sum \right| \ll Q^{o(1)}(MNL_1L_3)^{1/2}(MN+W)^{1/2}(L_1L_3+W)^{1/2},$$

which yields a bound of

$$Q^{-o(1)}\mathscr{E}_1' \ll \frac{Q(MN)^{1/2}(y_1y_3)^{1/2}}{V^{1/2}} + \frac{Q^{3/2}(MN)^{1/2}}{V} + \frac{Q^{3/2}(y_1y_3)^{1/2}}{V} + \frac{Q^2}{V^{3/2}}. \tag{5-6}$$

We observe that (5-6) is acceptable for $V \geq Q^{3\epsilon}$, say. We may therefore assume $V \leq Q^\epsilon$.

We next show that $\mathscr{E}_1'$ is small provided N is somewhat large.

Proposition 5.2. *Assume the hypotheses of Lemma 3.3. If $N \geq MQ^{-2\epsilon}$ and $m\ell_1\ell_3 \neq 1$, then $\mathscr{E}_1' \ll Q^{2-\epsilon+o(1)}$.*

Proof. We make use only of cancellation in the sum on n, say

$$\Sigma_N = \sum_{(n,vw)=1} G\left(\frac{n}{N}\right) e\left(\frac{nm\overline{\ell_1\ell_3 v}}{w}\right).$$

We use Möbius inversion to detect the condition $(n,v)=1$, and then break n into primitive residue classes modulo w. Thus,

$$\Sigma_N = \sum_{d|v}\mu(d) \sum_{(a,w)=1} e\left(\frac{adm\overline{\ell_1\ell_3 v}}{w}\right) \sum_{n\equiv a(w)} G\left(\frac{dn}{N}\right).$$

We apply Poisson summation to each sum on n, and obtain

$$\Sigma_N = \sum_{d|v}\mu(d) \sum_{(a,w)=1} e\left(\frac{adm\overline{\ell_1\ell_3 v}}{w}\right) \frac{N}{dw} \sum_{|h|\leq W^{1+\epsilon}d/N} e\left(\frac{ah}{w}\right)\widehat{G}\left(\frac{hN}{dw}\right) + O_\epsilon(Q^{-100}),$$

say. The contribution of the error term is, of course, negligible. The contribution of the zero frequency $h=0$ to Σ_N is

$$\widehat{G}(0)\frac{N}{w}\sum_{d|v}\frac{\mu(d)}{d} \sum_{(a,w)=1} e\left(\frac{adm\overline{\ell_1\ell_3 v}}{w}\right) = \widehat{G}(0)\mu(w)\frac{N}{w}\frac{\varphi(v)}{v},$$

and upon summing this contribution over the remaining variables, the zero frequency contributes

$$\ll V^{1/2}W^{1/2}(MN)^{1/2}(y_1y_3)^{1/2}Q^{o(1)} \ll Q^{3/2}$$

to $\mathscr{E}_1'$, and this contribution is sufficiently small.

It takes just a bit more work to bound the contribution of the nonzero frequencies $|h| > 0$. We rearrange the sum as

$$\sum_{d|v} \mu(d)\frac{N}{dw} \sum_{|h|\le W^{1+\epsilon}d/N} \widehat{G}\Big(\frac{hN}{dw}\Big) \sum_{(a,w)=1} e\Big(\frac{adm\overline{\ell_1\ell_3 v}}{w} + \frac{ah}{w}\Big).$$

By a change of variables the inner sum is equal to the Ramanujan sum $c_w(hm\ell_1\ell_3 v + d)$. Note that $hm\ell_1\ell_3 v + d \neq 0$ because $m\ell_1\ell_3 \neq 1$. The nonzero frequencies therefore contribute to $\mathscr{E}_1'$ an amount

$$\ll Q^{\epsilon}\frac{(VWL_1L_3M)^{1/2}}{N^{1/2}} \sup_{0<|k|\ll Q^{O(1)}} \sum_{w\asymp W} |c_w(k)|.$$

Since $|c_w(k)| \le (k, w)$ the sum on w is $\ll W^{1+o(1)}$. It follows that

$$\mathscr{E}_1' \ll Q^{3/2} + Q^{3/2+\epsilon}(y_1y_3)^{1/2}\frac{M^{1/2}}{N^{1/2}}.$$

Since $y_i = Q^{\theta_i}$ and $\theta_i < \frac{1}{2} - 3\epsilon$, say, this bound for $\mathscr{E}_1'$ is acceptable provided $N \ge MQ^{-2\epsilon}$. □

By Proposition 5.2 we may assume $N \le MQ^{-2\epsilon}$. Since $MN \le Q^{1+\epsilon}$, the condition $N \le MQ^{-2\epsilon}$ implies $N \le Q^{1/2}$.

We now pause to make a comment on the condition $m\ell_1\ell_3 \neq 1$, which we have assumed throughout this section but not indicated in the notation for $\mathscr{E}_1'$. Observe that this condition is automatic if $ML_1L_3 > 2019$ (say). If $ML_1L_3 \ll 1$, then we may use the trivial bound (5-4) along with the bound $N \le Q^{1/2} \le Q^{1-\epsilon}$ to obtain

$$\mathscr{E}_1' \ll Q^{2-\epsilon}.$$

We may therefore assume $ML_1L_2 \gg 1$, so that the condition $m\ell_1\ell_3 \neq 1$ is satisfied.

We now remove the coprimality condition $(n, w) = 1$. By Möbius inversion we have

$$\mathbf{1}_{(n,w)=1} = \sum_{\substack{f|n\\ f|w}} \mu(f).$$

We move the sum on f to be the outermost sum, and note $f \ll N$. We then change variables $n \to nf$ and $w \to wf$. If a_*, say, is any lift of the multiplicative inverse of $m\ell_1\ell_3 v$ modulo wf, then $a_* \equiv \overline{m\ell_1\ell_3 v} \pmod{w}$, and therefore,

$$\frac{nf\overline{m\ell_1\ell_3 v}}{wf} \equiv \frac{n\overline{m\ell_1\ell_3 v}}{w} \pmod{1}.$$

It follows that

$$\mathscr{E}_1' = \frac{W^{1/2}}{(MNL_1L_3V)^{1/2}} \sum_{f \ll N} \mu(f) \sum\sum_{(v,wf)=1} \alpha(v) G\Big(\frac{v}{V}\Big) G\Big(\frac{wf}{W}\Big) \times \sum\sum_{\substack{\ell_i \le y_i \\ (\ell_i, fvw)=1}} \beta(\ell_1)\gamma(\ell_3) G\Big(\frac{\ell_1}{L_1}\Big) G\Big(\frac{\ell_3}{L_3}\Big) \sum\sum_{\substack{(m,fvw)=1 \\ (n,v)=1}} G\Big(\frac{m}{M}\Big) G\Big(\frac{nf}{N}\Big) e\Big(\frac{nm\overline{\ell_1\ell_3 v}}{w}\Big).$$

We next reduce the size of f by a similar argument to the one that let us impose the condition $V \le Q^\epsilon$. We obtain by transitioning to multiplicative characters (recall (5-5)) that the sum over $v, w, m, n, \ell_1, \ell_3$ is bounded by

$$\ll \frac{W^{1/2+o(1)}V^{1/2}}{f^{1/2}} \sum_{w \asymp W/f} \frac{1}{w^{1/2}} \Big(\frac{(MN)^{1/2}}{f^{1/2}} + w^{1/2}\Big)((L_1L_3)^{1/2} + w^{1/2}) \ll \frac{Q^{2+\epsilon}}{f^{3/2}},$$

and therefore, the contribution from $f > Q^{4\epsilon}$ is negligible.

Now the only barrier to applying Lemma 5.1 is the conditions $(m, f) = 1$ and $(m, v) = 1$. We remove both of these conditions with Möbius inversion, obtaining

$$\sum_{f \ll \min(N, Q^\epsilon)} \mu(f) \sum_{h|f} \mu(h) \sum_{t \ll V} \mu(t) \frac{W^{1/2}}{(MNL_1L_3V)^{1/2}} \sum\sum_{\substack{(v,wf)=1 \\ (w,ht)=1}} \alpha(v) G\Big(\frac{vt}{V}\Big) G\Big(\frac{wf}{W}\Big) \times \sum\sum_{\substack{\ell_i \le y_i \\ (\ell_i, fvw)=1}} \beta(\ell_1)\gamma(\ell_3) G\Big(\frac{\ell_1}{L_1}\Big) G\Big(\frac{\ell_3}{L_3}\Big) \sum\sum_{\substack{(m,w)=1 \\ (n,v)=1}} G\Big(\frac{mht}{M}\Big) G\Big(\frac{nf}{N}\Big) e\Big(\frac{nm\overline{ht^2\ell_1\ell_3 v}}{w}\Big).$$

We set

$$b_{n,ht^2k} = \mathbf{1}_{(n,v)=1} G\Big(\frac{nf}{N}\Big) \sum_{\substack{\ell_1 \\ \ell_1\ell_3 v = k \\ (\ell_1\ell_3, v)=1}} \sum_{\ell_3} \sum_{v} \beta(\ell_1)\gamma(\ell_3)\alpha(v) G\Big(\frac{vt}{V}\Big) G\Big(\frac{\ell_1}{L_1}\Big) G\Big(\frac{\ell_3}{L_3}\Big)$$

if $(k, f) = 1$, and for integers r not divisible by ht^2 we set $b_{n,r} = 0$. It follows that if $b_{n,r} \ne 0$, then $n \asymp N/f$ and $r \asymp htL_1L_3V$ with $r \equiv 0(ht^2)$. The sum over n, r, m, w is therefore a sum of the form to which Lemma 5.1 may be applied. We note that

$$\|b_{N,R}\|_2 \ll \frac{Q^{o(1)}}{(ft)^{1/2}} (NL_1L_3V)^{1/2},$$

and therefore, by Lemma 5.1 we have

$$\mathscr{E}_1' \ll Q^\epsilon \sum_{f \ll Q^\epsilon} \frac{1}{f^{1/2}} \sum_{h|f} \sum_{t \ll Q^\epsilon} \frac{1}{t^{1/2}} \frac{W^{1/2}}{M^{1/2}}$$
$$\times \left\{ \frac{W^{1/2}}{f^{1/2}}((htL_1L_3V)^{1/2} + \frac{N^{1/2}}{f^{1/2}})(\frac{W^{1/2}}{f^{1/2}} + (ML_1L_3V)^{1/2}) \right.$$
$$\left. + \frac{W}{f}\frac{M^{1/2}}{(ht)^{1/2}}((htL_1L_3V)^{1/2} + (htL_1L_3NV)^{1/4}) + \frac{M}{ht}(htL_1L_3NV)^{1/2} \right\}$$
$$\ll Q^\epsilon \left(\frac{W^{3/2}(y_1y_3)^{1/2}}{M^{1/2}} + Wy_1y_3 + W^{3/2}\frac{N^{1/2}}{M^{1/2}} + W(y_1y_3)^{1/2}N^{1/2} + W^{3/2}(y_1y_3)^{1/2} \right.$$
$$\left. + W^{3/2}(y_1y_3)^{1/4}N^{1/4} + W^{1/2}Q^{1/2}(y_1y_3)^{1/2} \right) \ll Q^{2-\epsilon},$$

upon recalling the bounds $W \ll Q$ and $y_i \le Q^{\theta_i}$ with $\theta_i < \frac{1}{2}$, and $N \le Q^{1-\epsilon}$. This completes the proof of Lemma 3.3.

6. Lemma 3.4: main term

In this section we obtain the main term of Lemma 3.4. We allow ourselves to recycle some notation from Sections 4 and 5.

Recall that we wish to asymptotically evaluate

$$\sum_{\chi(q)}^{+} \left|L\left(\tfrac{1}{2}, \chi\right)\right|^2 \psi_{\mathrm{B}}(\chi)\psi_{\mathrm{MV}}(\overline{\chi}).$$

We begin precisely as in Section 4. Inserting the definitions of $\psi_{\mathrm{B}}(\chi)$ and $\psi_{\mathrm{MV}}(\overline{\chi})$, we must asymptotically evaluate

$$\frac{2}{L} \sum\sum_{\substack{bc \le y_2 \\ (bc,q)=1}} \frac{\Lambda(b)\mu(c)P_2[bc]}{(bc)^{1/2}} \sum_{\substack{\ell \le y_3 \\ (\ell,q)=1}} \frac{\mu(\ell)P_3[\ell]}{\ell^{1/2}} \sum\sum_{(mn,q)=1} \frac{1}{(mn)^{1/2}} V\left(\frac{mn}{q}\right) \sum_{\chi(q)}^{+} \epsilon(\chi)\chi(c\ell m)\overline{\chi}(bn). \quad (6\text{-}1)$$

The main term of Lemma 3.3 arose from $m\ell_1\ell_3 = 1$. In the present case, the main term contains more than just $c\ell m = 1$; the main term arises from those $c\ell m$ which divide b. The support of the von Mangoldt function constrains b to be a prime power, so the condition $c\ell m \mid b$ is straightforward, but tedious, to handle.

There are three different cases to consider. The first case is $c\ell m = 1$. In the second case we have $c\ell m = p$ and $b = p$. Both of these cases contribute to the main term. The third case is everything else ($b = p^j$ with $j \ge 2$ and $c\ell m \mid b$ with $c\ell m \ge p$), and this case contributes only to the error term.

***First case*: $c\ell m = 1$.** If $c\ell m$ is equal to 1, then certainly $c\ell m$ divides b for every b. The contribution from $c\ell m = 1$ is equal to

$$M = \frac{2P_3(1)}{L} \sum_{\chi(q)}^{+} \epsilon(\chi) \sum_{b \le y_2} \frac{\Lambda(b)\overline{\chi}(b)P_2[b]}{b^{1/2}} \sum_n \frac{\overline{\chi}(n)}{n^{1/2}} V\left(\frac{n}{q}\right).$$

By an application of Proposition 4.3,

$$M = M_1 + M_2, \tag{6-2}$$

where

$$M_1 = \frac{2P_3(1)}{L} \sum_{\substack{b \le y_2 \\ (b,q)=1}} \frac{\Lambda(b)P_2[b]}{b^{1/2}} \sum_{\chi(q)}^{+} \epsilon(\chi)\overline{\chi}(b) L\left(\tfrac{1}{2}, \overline{\chi}\right),$$

$$M_2 = -\frac{2P_3(1)}{L} \sum_{\substack{b \le y_2 \\ (bn,q)=1}}\sum \frac{\Lambda(b)P_2[b]}{(bn)^{1/2}} F(n) \sum_{\chi(q)}^{+} \chi(n)\overline{\chi}(b),$$

and F is the rapidly decaying function given by (4-4). A main term arises from M_1, and M_2 contributes only to the error term.

Let us first investigate M_2. By Lemma 4.2 we have

$$M_2 = -\frac{P_3(1)}{L} \sum_{w|q} \varphi(w)\mu(q/w) \sum_{\substack{b \le y_2 \\ b \equiv \pm n (w) \\ (bn,q)=1}}\sum \frac{\Lambda(b)P_2[b]}{(bn)^{1/2}} F(n).$$

By the rapid decay of F (recall (4-6)) we may restrict n to $n \le q^{1/10}$. The contribution from $w \le q^{1/2+\epsilon}$ is then trivially $\ll q^{1-\epsilon}$, since $y_2 \ll q^{1/2-\epsilon}$. For the remaining terms, the congruence condition $b \equiv \pm n(w)$ becomes $b = n$, and thus,

$$M_2 \ll q^{1-\epsilon} + \frac{1}{L} \sum_{\substack{w|q \\ w > q^{1/2+\epsilon}}} \varphi(w) \sum_{b \le q^{1/10}} \frac{\Lambda(b)P_2[b]}{b} F(b) \ll qL^{-1}.$$

Let us turn to M_1. We use the following lemma to represent the central value $L\left(\frac{1}{2}, \overline{\chi}\right)$.

Lemma 6.1. *Let $\overline{\chi}$ be a primitive even character modulo q. Then*

$$L\left(\tfrac{1}{2}, \overline{\chi}\right) = \sum_n \frac{\overline{\chi}(n)}{n^{1/2}} V_1\left(\frac{n}{q^{1/2}}\right) + \epsilon(\overline{\chi}) \sum_n \frac{\chi(n)}{n^{1/2}} V_1\left(\frac{n}{q^{1/2}}\right),$$

where

$$V_1(x) = \frac{1}{2\pi i} \int_{(1)} \frac{\Gamma\left(\frac{1}{2}s + \frac{1}{4}\right)}{\Gamma\left(\frac{1}{4}\right)} \frac{G_1(s)}{s} \pi^{-s/2} x^{-s}\, ds$$

and $G_1(s)$ is an even polynomial satisfying $G_1(0) = 1$.

Proof. See [Iwaniec and Sarnak 1999, (2.2)]. □

Applying Lemma 6.1, the main term M_1 naturally splits as $M_1 = M_{1,1} + M_{1,2}$, where

$$M_{1,1} = \frac{2P_3(1)}{L} \sum\sum_{\substack{b \le y_2 \\ (bn,q)=1}} \frac{\Lambda(b)P_2[b]}{(bn)^{1/2}} V_1\left(\frac{n}{q^{1/2}}\right) \sum_{\chi(q)}^{+} \epsilon(\chi)\overline{\chi}(bn),$$

$$M_{1,2} = \frac{2P_3(1)}{L} \sum\sum_{\substack{b \le y_2 \\ (bn,q)=1}} \frac{\Lambda(b)P_2[b]}{(bn)^{1/2}} V_1\left(\frac{n}{q^{1/2}}\right) \sum_{\chi(q)}^{+} \chi(n)\overline{\chi}(b).$$

Applying character orthogonality to $M_{1,1}$ we arrive at

$$M_{1,1} = \frac{2P_3(1)}{Lq^{1/2}} \sum\sum_{\substack{vw=q \\ (v,w)=1}} \mu^2(v)\varphi(w) \sum\sum_{\substack{b \le y_2 \\ (bn,q)=1}} \frac{\Lambda(b)P_2[b]}{(bn)^{1/2}} V_1\left(\frac{n}{q^{1/2}}\right) \cos\frac{2\pi bn\bar{v}}{w},$$

and a trivial estimation shows

$$M_{1,1} \ll q^{1-\epsilon}.$$

Let us lastly examine $M_{1,2}$, from which a main term arises. By character orthogonality we have

$$M_{1,2} = \frac{P_3(1)}{L} \sum_{w|q} \varphi(w)\mu(q/w) \sum\sum_{\substack{b \le y_2 \\ b \equiv \pm n(w) \\ (b,q)=1}} \frac{\Lambda(b)P_2[b]}{(bn)^{1/2}} V_1\left(\frac{n}{q^{1/2}}\right).$$

By trivial estimation, the contribution from $w \le q^{1/2+\epsilon}$ is

$$\ll \sum_{\substack{w|q \\ w \le q^{1/2+\epsilon}}} \varphi(w) \sum_{b \le y_2} \frac{1}{b^{1/2}} \sum_{\substack{n \le q^{1/2+\epsilon} \\ n \equiv \pm b(w)}} \frac{1}{n^{1/2}} \ll y_2^{1/2} \sum_{\substack{w|q \\ w \le q^{1/2+\epsilon}}} \varphi(w)\left(\frac{q^{1/4+\epsilon}}{w} + O(1)\right) \ll q^{3/4+\epsilon}.$$

By the rapid decay of V_1, for $w > q^{1/2+\epsilon}$ the congruence $b \equiv \pm n(w)$ becomes $b = n$. Adding back in the terms $w \le q^{1/2+\epsilon}$, we have

$$M_{1,2} = \frac{2P_3(1)}{L}\varphi^+(q) \sum_{\substack{b \le y_2 \\ (b,q)=1}} \frac{\Lambda(b)P_2[b]}{b} V_1\left(\frac{b}{q^{1/2}}\right) + O(q^{1-\epsilon}).$$

For $x \ll 1$ we see by a contour shift that

$$V_1(x) = 1 + O(x^{1/3}),$$

and we have $bq^{-1/2} \ll q^{-\epsilon}$. It follows that

$$M_{1,2} = O(q^{1-\epsilon}) + \frac{2P_3(1)}{L}\varphi^+(q) \sum_{\substack{b \le y_2 \\ (b,q)=1}} \frac{\Lambda(b)P_2[b]}{b}.$$

We have

$$\sum_{(b,q)>1} \frac{\Lambda(b)}{b} \ll 1 + \sum_{p|q} \frac{\log p}{p} \ll \log\log q,$$

and therefore, we may remove the condition $(b, q) = 1$ at the cost of an error $O(qL^{-1+\epsilon})$. From the estimate

$$\sum_{n\le x} \frac{\Lambda(n)}{n} = \log x + O(1),$$

summation by parts, and elementary manipulations, we obtain

$$\sum_{b\le y_2} \frac{\Lambda(b)P_2[b]}{b} = (\log y_2)\int_0^1 P_2(u)\,du + O(1).$$

Therefore, the contribution to the main term of Lemma 3.4 from $c\ell m = 1$ is

$$(2\theta_2 P_3(1)\widetilde{P}_2(1) + o(1))\varphi^+(q). \tag{6-3}$$

***Second case*: $c\ell m = p$, $b = p$.** Another main term which contributes to Lemma 3.4 comes from $c\ell m = p$ and $b = p$. There are three subcases: $(c, \ell, m) = (p, 1, 1)$, $(1, p, 1)$, or $(1, 1, p)$. These three cases give (compare with (6-1))

$$N_1 = -\frac{2P_3(1)}{L}\sum_{\substack{p\le y_2^{1/2}\\(p,q)=1}} \frac{(\log p)P_2(\log(y_2^{1/2}/p)/\log(y_2^{1/2}))}{p}\sideset{}{^+}\sum_{\chi(q)}\epsilon(\chi)\sum_n \frac{\overline{\chi}(n)}{n^{1/2}}V\left(\frac{n}{q}\right),$$

$$N_2 = -\frac{2}{L}\sum_{\substack{p\le y_2\\(p,q)=1}} \frac{(\log p)P_2[p]P_3[p]}{p}\sideset{}{^+}\sum_{\chi(q)}\epsilon(\chi)\sum_n \frac{\overline{\chi}(n)}{n^{1/2}}V\left(\frac{n}{q}\right),$$

$$N_3 = \frac{2P_3(1)}{L}\sum_{\substack{p\le y_2\\(p,q)=1}} \frac{(\log p)P_2[p]}{p}\sideset{}{^+}\sum_{\chi(q)}\epsilon(\chi)\sum_n \frac{\overline{\chi}(n)}{n^{1/2}}V\left(\frac{pn}{q}\right).$$

The first two are somewhat easier to handle than the last one. We apply Proposition 4.3 and then argue as in Section 4 and the $c\ell m = 1$ case to obtain

$$\sideset{}{^+}\sum_{\chi(q)}\epsilon(\chi)\sum_n \frac{\overline{\chi}(n)}{n^{1/2}}V\left(\frac{n}{q}\right) = \tfrac{1}{2}\varphi^+(q) + O(q^{1-\epsilon}).$$

It follows that

$$\begin{aligned} N_1 &= -\left(\frac{\theta_2}{2}P_3(1)\widetilde{P}_2(1) + o(1)\right)\varphi^+(q),\\ N_2 &= -\left(\theta_2\int_0^1 P_2(u)P_3(u)\,du + o(1)\right)\varphi^+(q). \end{aligned} \tag{6-4}$$

Combining (6-3) and (6-4) gives the main term of Lemma 3.4.

The final term N_3 is more difficult because the inner sum now depends on p. However, M_3 contributes only to the error term. By Proposition 4.3 with $T = p$,

$$\sum_n \frac{\overline{\chi}(n)}{n^{1/2}}V\left(\frac{pn}{q}\right) = L\left(\tfrac{1}{2}, \overline{\chi}\right) - \sum_n \frac{\chi(n)}{n^{1/2}}F\left(\frac{n}{p}\right). \tag{6-5}$$

The first term on the right side of (6-5) contributes to N_3 an amount

$$(2\theta_2 P_3(1)\widetilde{P}_2(1)+o(1))\varphi^+(q). \tag{6-6}$$

For the second term on the right side of (6-5) we use character orthogonality and get

$$-\frac{2P_3(1)}{L}\sum_{\substack{p\le y_2\\(p,q)=1}}\frac{(\log p)P_2[p]}{p}\frac{1}{2}\sum_{w\mid q}\varphi(w)\mu(q/w)\sum_{n\equiv\pm 1(w)}\frac{1}{n^{1/2}}F\left(\frac{n}{p}\right).$$

By the rapid decay of F the contribution from $n>p^{11/10}$, say, is $O(qL^{-1})$. We next estimate trivially the contribution from $w\le q^{3/5}$, say. We have the bound

$$\sum_{\substack{n\equiv\pm 1(w)\\ n\le p^{11/10}}}\frac{1}{n^{1/2}}F\left(\frac{n}{p}\right)\ll q^{\epsilon}\left(\frac{p^{11/20}}{w}+1\right),$$

and this contributes to N_3 an amount

$$\ll q^{3/5+\epsilon}+q^{\epsilon}\sum_{p\le y_2}p^{-9/20}\ll q^{3/5+\epsilon},$$

since $y_2\ll q^{1/2}$. For $w>q^{3/5}$ and $n\le p^{11/10}$ the congruence $n\equiv\pm 1(w)$ becomes $n=1$. By a contour shift we have

$$F\left(\frac{1}{p}\right)=1+O(p^{-1/2}).$$

Thus, the second term on the right side of (6-5) contributes to N_3 an amount

$$-(2\theta_2 P_3(1)\widetilde{P}_2(1)+o(1))\varphi^+(q), \tag{6-7}$$

and (6-6) and (6-7) together imply N_3 is negligible.

Third case*: *everything else. This case is the contribution from $b=p^j$ with $j\ge 2$ and $c\ell m\mid b$ with $c\ell m\ge p$. This case contributes an error of size $O(qL^{-1+\epsilon})$, essentially because the sum

$$\sum_{\substack{p^k\\ k\ge 2}}\frac{\log(p^k)}{p^k}$$

converges. There are four different subcases to consider, since the Möbius functions attached to c and ℓ imply $c,\ell\in\{1,p\}$. The same techniques we have already employed allow one to bound the resulting sums, so we leave the details for the interested reader. This completes the proof of Lemma 3.4.

7. Lemma 3.4: error term

After the results of the previous section, it remains to finish the proof of Lemma 3.4 by showing the error term of (6-1) is negligible. The argument is very similar to that given in Section 5, and, indeed, the arguments are identical after a point.

The error term has the form

$$\mathscr{E}_2=\sum\sum_{(v,w)=1}\mu^2(v)\frac{v}{\varphi(v)}\frac{w^{1/2}}{v^{1/2}}\Psi\left(\frac{vw}{Q}\right)\sum_{\substack{\ell\le y_3\\(\ell,vw)=1}}\frac{\mu(\ell)P_3[\ell]}{\ell^{1/2}}$$

$$\times\sum\sum_{\substack{bc\le y_2\\(bc,vw)=1}}\frac{\Lambda(b)\mu(c)P_2[bc]}{(bc)^{1/2}}\sum\sum_{(mn,vw)=1}\frac{1}{(mn)^{1/2}}V\left(\frac{mn}{vw}\right)\cos\frac{2\pi bn\overline{c\ell mv}}{w},$$

where we also have the condition $c\ell m\nmid b$, which we do not indicate in the notation. This condition is awkward, but turns out to be harmless.

We note that we may separate the variables b and c from one another in $P_2[bc]$ by linearity, the additivity of the logarithm, and the binomial theorem. Thus, it suffices to study $\mathscr{E}_1$ with $P_2[bc]$ replaced by $(\log b)^{j_1}(\log c)^{j_2}$, for j_i some fixed nonnegative integers. Arguing as in the reduction to (5-3), we may bound $\mathscr{E}_2$ by $\ll Q^{o(1)}$ instances of $\mathscr{E}_2'=\mathscr{E}_2'(B,C,L,M,N,V,W)$, where

$$\mathscr{E}_2'=\frac{W^{1/2}}{(BCLMNV)^{1/2}}\sum\sum_{(v,w)=1}\alpha(v)G\left(\frac{v}{V}\right)G\left(\frac{w}{W}\right)\sum_{\substack{\ell\le y_3\\(\ell,vw)=1}}\beta(\ell)G\left(\frac{\ell}{L}\right)\sum\sum_{\substack{bc\le y_2\\(bc,vw)=1}}\gamma(b)\delta(c)G\left(\frac{b}{B}\right)G\left(\frac{c}{C}\right)$$

$$\times\sum\sum_{(mn,vw)=1}G\left(\frac{m}{M}\right)G\left(\frac{n}{N}\right)e\left(\frac{bn\overline{c\ell mv}}{w}\right),\qquad(7\text{-}1)$$

the function G is smooth as before, and $\alpha,\beta,\gamma,\delta$ are sequences f satisfying $|f(z)|\ll Q^{o(1)}$. We also have the conditions

$$VW\asymp Q,\qquad MN\le Q^{1+\epsilon},\qquad BC\ll y_2,\qquad L\ll y_3,\qquad B,C,L,M,N,V,W\gg 1.$$

By the argument that gave (5-6) we may also assume $V\le Q^{\epsilon}$. Lastly, we may remove the condition $bc\le y_2$ by Mellin inversion, at the cost of changing γ and δ by b^{it_0} and c^{it_0}, respectively, where $t_0\in\mathbb{R}$ is arbitrary (see [Duke et al. 1997, Lemma 9], for instance).

Recall the condition $c\ell m\nmid b$. This condition is unnecessary if $CLM>2019\,B$, so it is only in the case $CLM\ll B$ where we need to deal with it. However, the case $CLM\ll B$ is exceptional, since B is bounded by $y_2\ll Q^{1/2}$, but generically we would expect CLM to be much larger than $Q^{1/2}$.

Indeed, we now show that when $CLM\ll B$ it suffices to get cancellation from the n variable alone. The proof is essentially Proposition 5.2, so we just remark upon the differences. By Möbius inversion and Poisson summation we have

$$\sum_{(n,vw)=1}G\left(\frac{n}{N}\right)e\left(\frac{bn\overline{c\ell mv}}{w}\right)=\mu(w)\frac{N}{w}\frac{\varphi(v)}{v}$$

$$+\sum_{d|v}\mu(d)\frac{N}{dw}\sum_{|h|\le W^{1+\epsilon}d/N}\widehat{G}\left(\frac{hN}{dw}\right)\sum_{(a,w)=1}e\left(\frac{abd\overline{c\ell mv}}{w}+\frac{ah}{w}\right)$$

$$+O(Q^{-100}).$$

The first and third terms contribute acceptable amounts, so consider the second term. The sum over a is the Ramanujan sum $c_w(hc\ell mv + bd)$, and since $c\ell m$ does not divide b the argument of the Ramanujan sum is nonzero. Following the proof of Proposition 5.2, we therefore obtain a bound of

$$\mathscr{E}_2' \ll \frac{Q^{3/2+\epsilon}(BCLM)^{1/2}}{N^{1/2}}. \tag{7-2}$$

By the reasoning immediately after Proposition 5.2, the bound (7-2) allows us to assume $N \le MQ^{-2\epsilon}$, so that $N \le Q^{1/2}$, regardless of whether $CLM \ll B$. In the case $CLM \ll B$, the bound (7-2) becomes

$$\mathscr{E}_2' \ll \frac{Q^{3/2+\epsilon}B}{N^{1/2}} \ll Q^{3/2+\epsilon}B \ll Q^{3/2+\theta_2+\epsilon} \ll Q^{2-\epsilon},$$

which of course is acceptable.

At this point we can follow the rest of the proof in Section 5. We change variables $bn \to n$, and the rest follows mutatis mutandis (it is important that with $N \ll Q^{1/2}$ we have $BN \ll Q^{1-\epsilon}$). This completes the proof of Lemma 3.4.

Acknowledgments

The author thanks Kevin Ford and George Shakan for helpful comments on earlier drafts of this work. The author also thanks the anonymous referee for helpful comments. The author was supported in this work by NSF grant DMS-1501982, and is grateful to Kevin Ford for financial support.

References

[Balasubramanian and Murty 1992] R. Balasubramanian and V. K. Murty, "Zeros of Dirichlet L-functions", *Ann. Sci. École Norm. Sup.* (4) **25**:5 (1992), 567–615. MR Zbl

[Blomer et al. 2017] V. Blomer, E. Fouvry, E. Kowalski, P. Michel, and D. Milićević, "On moments of twisted L-functions", *Amer. J. Math.* **139**:3 (2017), 707–768. MR Zbl

[Bombieri et al. 1986] E. Bombieri, J. B. Friedlander, and H. Iwaniec, "Primes in arithmetic progressions to large moduli", *Acta Math.* **156**:3–4 (1986), 203–251. MR Zbl

[Bui 2012] H. M. Bui, "Non-vanishing of Dirichlet L-functions at the central point", *Int. J. Number Theory* **8**:8 (2012), 1855–1881. MR Zbl

[Bui and Milinovich 2011] H. M. Bui and M. B. Milinovich, "Central values of derivatives of Dirichlet L-functions", *Int. J. Number Theory* **7**:2 (2011), 371–388. MR Zbl

[Conrey et al. 2011] B. Conrey, H. Iwaniec, and K. Soundararajan, "Asymptotic large sieve", preprint, 2011. arXiv

[Deshouillers and Iwaniec 1982] J.-M. Deshouillers and H. Iwaniec, "Kloosterman sums and Fourier coefficients of cusp forms", *Invent. Math.* **70**:2 (1982), 219–288. MR Zbl

[Duke et al. 1997] W. Duke, J. Friedlander, and H. Iwaniec, "Bilinear forms with Kloosterman fractions", *Invent. Math.* **128**:1 (1997), 23–43. MR Zbl

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004. MR Zbl

[Iwaniec and Sarnak 1999] H. Iwaniec and P. Sarnak, "Dirichlet L-functions at the central point", pp. 941–952 in *Number theory in progress* (Zakopane, Poland, 1977), vol. 2: Elementary and analytic number theory, edited by K. Győry et al., de Gruyter, Berlin, 1999. MR Zbl

[Khan and Ngo 2016] R. Khan and H. T. Ngo, "Nonvanishing of Dirichlet L-functions", *Algebra Number Theory* **10**:10 (2016), 2081–2091. MR Zbl

[Michel and VanderKam 2000] P. Michel and J. VanderKam, "Non-vanishing of high derivatives of Dirichlet L-functions at the central point", *J. Number Theory* **81**:1 (2000), 130–148. MR Zbl

[Miller and Takloo-Bighash 2006] S. J. Miller and R. Takloo-Bighash, *An invitation to modern number theory*, Princeton University, 2006. MR Zbl

[Sica 1998] F. Sica, *The order of vanishing of L-functions at the center of the critical strip*, Ph.D. thesis, McGill University, 1998, Available at https://search.proquest.com/docview/304479758. MR

[Soundararajan 1995] K. Soundararajan, "Mean-values of the Riemann zeta-function", *Mathematika* **42**:1 (1995), 158–174. MR Zbl

[Soundararajan 2000] K. Soundararajan, "Nonvanishing of quadratic Dirichlet L-functions at $s = \frac{1}{2}$", *Ann. of Math.* (2) **152**:2 (2000), 447–488. MR Zbl

Communicated by Philippe Michel
Received 2018-04-04 Revised 2018-07-23 Accepted 2018-09-23

kpratt4@illinois.edu *Department of Mathematics, University of Illinois at Urbana–Champaign, Urbana, IL, United States*

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in *ANT* are usually in English, but articles written in other languages are welcome.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 13 No. 1 2019