Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Journal of Number Theory 114 (2005) 361–393
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Pesenti–Szpiro inequality for optimal elliptic curves☆

Mihran Papikian

Department of Mathematics, Stanford University, Stanford, CA 94305, USA

Received 1 March 2004; revised 9 September 2004
Available online 30 January 2005
Communicated by D. Goss

Abstract

We study Pesenti–Szpiro inequality in the case of elliptic curves over $\mathbb{F}_q(t)$ which occur as subvarieties of Jacobian varieties of Drinfeld modular curves. In general, we obtain an upper-bound on the degrees of minimal discriminants of such elliptic curves in terms of the degrees of their conductors and q. In the special case when the level is prime, we bound the degrees of discriminants only in terms of the degrees of conductors. As a preliminary step in the proof of this latter result we generalize a construction (due to Gekeler and Reversat) of 1-dimensional optimal quotients of Drinfeld Jacobians.

MSC: primary 11G05; secondary 14G22; 11G18

Keywords: Szpiro inequality; Drinfeld modular curves; Monodromy pairing

1. Introduction

1.1. Statement of results

The aim of this paper is twofold. The initial motivation comes from a question about a possible refinement of Pesenti–Szpiro inequality [23] when we restrict the attention

☆ Part of the work on this paper was completed while the author was supported by a Rackham Predoctoral Fellowship from the University of Michigan.
E-mail address: papikian@math.stanford.edu.

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2004.11.007

to a special class of arithmetically important elliptic curves. To give an answer to this question we first will generalize the construction of 1-dimensional quotients of the Jacobian varieties of Drinfeld modular curves given in [15]. This generalization seems to be interesting in its own right.

Let $\mathbb{F}_q$ be a finite field with q elements and let $F := \mathbb{F}_q(t)$. This latter field is the field of rational functions on $\mathbb{P}^1_{\mathbb{F}_q}$. Let E be a non-isotrivial elliptic curve over F. This means that the j-invariant of E is a non-constant rational function on $\mathbb{P}^1_{\mathbb{F}_q}$, and hence gives a finite map $j_E : \mathbb{P}^1_{\mathbb{F}_q} \to \mathbb{P}^1_{\mathbb{F}_q}$. We define the *non-separable degree of* j_E, $\deg_{ns}(j_E)$, to be the non-separable degree of this morphism. In particular, $\deg_{ns}(j_E)$ is equal to some power of the characteristic p of F. We will say that the j-invariant is *separable* if $\deg_{ns}(j_E) = 1$. Let $\mathcal{D}_E$ be the divisor of the minimal discriminant of E, and let $\mathfrak{n}_E$ be the divisor of its conductor. The main result of [23] in the case of $\mathbb{P}^1_{\mathbb{F}_q}$ can be stated as follows:

Theorem 1.1 (*Pesenti–Szpiro*). *With previous notation we have*

$$\deg \mathcal{D}_E \leqslant 6 \cdot \deg_{ns}(j_E) \cdot (\deg \mathfrak{n}_E - 2).$$

This theorem (which the authors prove for general global fields of positive characteristic) is the function field analogue of a famous conjecture of Szpiro which asserts a certain inequality between the discriminants and the conductors of elliptic curves over $\mathbb{Q}$. Due to its relation to the *ABC conjecture*, Szpiro's conjecture is extremely important for Diophantine problems and is wide open in general. The above theorem is not important for Diophantine questions over function fields, but the statement (and the techniques of its proof) are quite interesting from the geometric viewpoint. In this paper we will complement Theorem 1.1 with extra information concerning $\deg_{ns}(j_E)$ when the elliptic curves in question are subvarieties of certain modular Jacobians.

In general, there are elliptic curves over F with arbitrarily large $\deg_{ns}(j)$, and the inequality in Theorem 1.1 is false without $\deg_{ns}(j)$ in it. More precisely, $\deg \mathcal{D}_E$ cannot be uniformly bounded only in terms of some fixed power of $\deg \mathfrak{n}_E$. This easily can be seen by fixing a non-isotrivial elliptic curve E and considering its Frobenius conjugates $E^{(p^n)}$.

Let $A = \mathbb{F}_q[t]$ be the ring of polynomials with coefficients in $\mathbb{F}_q$. Let $\mathfrak{n}$ be an ideal in A. Consider the *Drinfeld modular curve* $X_0(\mathfrak{n})_F$ which is the compactified coarse moduli space of Drinfeld A-modules of rank 2 over F with an $\mathfrak{n}$-cyclic subgroup. It is known that $X_0(\mathfrak{n})_F$ is a smooth projective geometrically connected curve over F. Denote by $J_0(\mathfrak{n})$ the Jacobian variety of $X_0(\mathfrak{n})_F$. Let E be an elliptic curve over F which is F-isomorphic to a 1-dimensional subvariety of $J_0(\mathfrak{n})$. Such an elliptic curve necessarily has split multiplicative reduction over the place $\infty := 1/t$ of F and conductor $\mathfrak{n}_E = \mathfrak{m} \cdot \infty$ for some $\mathfrak{m}|\mathfrak{n}$. We will call such curves *optimal*. It was Barry Mazur who in private communication brought to my attention the question of refining Theorem 1.1 for the case of optimal curves. That such a refinement might be possible can be motivated by the observation that the analogous curves over $\mathbb{Q}$ (that is, those elliptic curves which occur as subvarieties of classical modular Jacobians $J_0(N)$) tend to have small numerical invariants, like regulators or Faltings' heights, compared to other curves in the same $\mathbb{Q}$-isogeny class; cf. [6]. Hence over function fields one might expect that $\deg_{ns}(j)$ of optimal curves tend to be "small". The main results of this paper are the following theorems.

Let E be an optimal elliptic curve over F with conductor $\mathfrak{n}_E = \mathfrak{n} \cdot \infty$.

Theorem 1.2. *If $\mathfrak{n}$ is prime then j_E is separable. In particular,*

$$\deg \mathcal{D}_E \leqslant 6 \cdot (\deg \mathfrak{n}_E - 2).$$

This theorem can be considered as the function field analogue of the main result in [19]. It is proved as Theorem 6.1.

Theorem 1.3. *There is a bound*

$$\deg_{ns}(j_E) < q^6(1+q)(1+q \deg \mathfrak{n})^2(\deg \mathfrak{n})^3.$$

In particular,

$$\deg \mathcal{D}_E < 13 \cdot q^9(\deg \mathfrak{n})^6.$$

This is proved as Corollary 6.7. (To see the last inequality note that $1+q \leqslant \frac{3}{2}q$ and $1+q \deg \mathfrak{n} \leqslant \frac{7}{6}q \deg \mathfrak{n}$ since $q \geqslant 2$ and, from the Grothendieck–Ogg–Shafarevich formula, $\deg \mathfrak{n} \geqslant 3$.) The following example shows that the j-invariants of optimal curves need not always be separable.

Example 1.4. Consider the Drinfeld modular curves which have genus 1, i.e., are elliptic curves. This happens essentially only twice and only when $q = 2$. The first case is when $\mathfrak{n} = t^3$:

$$X_0(\mathfrak{n}) = E: \ y^2 + txy = x^3 + t^2.$$

One computes that $j_E = t^4$ and hence $\deg_{ns}(j) = 4$.

The second case is when $\mathfrak{n} = t^2(t+1)$. Now

$$X_0(\mathfrak{n}) = E: \ y^2 + txy + ty = x^3$$

and $j_E = t^8/(t+1)^2$. Hence $\deg_{ns}(j) = 2$.

The upshot of Theorems 1.2 and 1.3 is that both Szpiro's conjecture over $\mathbb{Q}$ and the provable result over $\mathbb{F}_q(t)$ take essentially the same form when we restrict the attention to optimal curves. It is known [15] that every F-isogeny class of elliptic curves with split multiplicative reduction at ∞ contains an optimal curve (this is the analogue of the Shimura–Taniyama–Weil conjecture over $\mathbb{Q}$). Hence our theorems apply to a wide class of curves.

1.2. Outline of the proofs and organization of the paper

We want to show that $\deg_{ns}(j)$ of an optimal curve is "small" (desirably equal to 1). For any place $\mathfrak{p}$ of F, $\deg_{ns}(j) | (-\mathrm{ord}_{\mathfrak{p}}(j))$. On the other hand, if $\mathfrak{p}$ is a place of multiplicative reduction of E then it is known that $-\mathrm{ord}_{\mathfrak{p}}(j)$ is the order of the group $\Phi_{E,\mathfrak{p}}$ of connected components of the geometric fibre of the Néron model of E over $\mathbb{P}^1_{\mathbb{F}_q}$ at $\mathfrak{p}$. Thus, one can try to bound $\#\Phi_{E,\mathfrak{p}}$, or to show that it is coprime to the characteristic p in some favorable situations, to conclude that j_E is separable.

As we already mentioned, the place ∞ is always a place of split multiplicative reduction of our optimal curve E. To prove Theorem 1.3 we use a formula from [21] which relates $\#\Phi_{E,\infty}$ to the value of $L(\mathrm{Sym}^2 E, s)$ at $s = 2$; see Subsection 6.2. One needs a bound on this special value of the L-function to complete the proof. Such an estimate is carried out in Appendix A.

Now let $\mathfrak{p} \neq \infty$ be a prime which strictly divides $\mathfrak{n}$ (so that E has multiplicative reduction at $\mathfrak{p}$). In this case, to get a handle on $\#\Phi_{E,\mathfrak{p}}$ we study the map $\Phi_{J_0(\mathfrak{n}),\mathfrak{p}} \to \Phi_{E,\mathfrak{p}}$ induced from the quotient map $J_0(\mathfrak{n}) \to E$ with connected smooth kernel. Whether this homomorphism of component groups is surjective or not is a rather subtle issue, closely related to level-lowering questions. In general it will not be surjective, due to the existence of congruences between automorphic forms. Nevertheless, when $\mathfrak{n} = \mathfrak{p}$ one should expect, in analogy with the situation over $\mathbb{Q}$, that the map between the component groups is surjective. Over $\mathbb{Q}$ this is proved in [19], using the full force of Mazur's Eisenstein ideal theory and Ribet's level-lowering results. In absence of a comprehensive theory of the Eisenstein ideal over function fields we are able to prove only a partial result in this direction but which is, nevertheless, sufficient to deduce Theorem 1.2. We show that $\#\mathrm{coker}(\Phi_{J_0(\mathfrak{p}),\mathfrak{p}} \to \Phi_{E,\mathfrak{p}})$ is coprime to p; see Theorems 4.9 and 6.1. It is known that $\#\Phi_{J_0(\mathfrak{p}),\mathfrak{p}}$ is coprime to p, hence the same must be true for $\#\Phi_{E,\mathfrak{p}}$. Since $\deg_{ns}(j)$ is a p-power, we conclude that optimal curves of conductor $\mathfrak{p} \cdot \infty$ have separable j-invariants.

Theorem 4.9 mentioned above follows from a careful study of the polarization induced on E by the canonical principal polarization of $J_0(\mathfrak{p})$, and calculation of its degree. This involves a construction of the analytification E^{an} of E over the completion $F_{\mathfrak{p}}$ as a 1-dimensional quotient of $J_0(\mathfrak{p})^{an}$. This construction is the analogue over $\mathfrak{p}$ of a construction of Gekeler and Reversat [15] over ∞. The construction in [15] uses the theory of theta functions on Mumford curves, and some parts of it crucially depend on a good understanding of the discrete groups involved. Such information is available when one works over the completion of F at ∞. Over $F_{\mathfrak{p}}$ the analogous groups are quite mysterious. We use instead the analytic description of Grothendieck's monodromy pairing [16, Exp. IX] and the moduli interpretation of the reduction of Drinfeld curves.

We review the rigid-analytic uniformization of totally degenerate abelian varieties in Section 2, and the monodromy pairing in Section 3. The construction of E^{an} and the proof of Theorem 4.9 are carried out in Section 4. Finally, after some preliminary results in Section 5, we present the proofs of main theorems of this paper in Section 6.

1.3. The situation over general function fields

The conclusion of Theorem 1.2 is valid in few other cases, and this can be proven by the same method. Let F be the function field of a smooth, projective, and geometrically connected curve C over $\mathbb{F}_q$ of genus g. Fix a place ∞ on C of degree δ, and let $A = \mathrm{H}^0(C - \infty, \mathcal{O}_C)$. Let $\mathfrak{n}$ be an ideal of A, and let $\mathfrak{p}$ be a prime dividing $\mathfrak{n}$. Let E be an optimal elliptic curve over F of conductor $\mathfrak{n} \cdot \infty$. The j-invariant of E will be separable whenever $\#\Phi_{J,\mathfrak{p}}$ is coprime to p and $J_0(\mathfrak{n})$ has purely toric reduction over $A_{\mathfrak{p}}$. For $\mathfrak{n}$ square-free we list all the cases when these last two conditions hold:

- $g = 0, \ \mathfrak{n} = \mathfrak{p}, \ \delta \leqslant 3;$
- $g = 0, \ \deg(\mathfrak{n}/\mathfrak{p}) = 1, \ \delta \leqslant 2;$
- $g = 0, \ \deg(\mathfrak{n}/\mathfrak{p}) \leqslant 2, \ \delta = 1;$
- $g = 1, \ \mathfrak{n} = \mathfrak{p}, \ \delta = 1.$

Once $g \geqslant 2$ then the Drinfeld Jacobians do not have purely toric reduction away from ∞. This is related to the fact that $X_0(1)_F$ has genus larger than 0. In this paper we have restricted to a single case (namely $g = 0$, $\delta = 1$, $\mathfrak{n}$ is prime) to avoid discussing the small nuances for different cases listed above, and to simplify the notation. The full proof is given in [22].

Theorem 1.3 holds for an arbitrary base curve C and an arbitrary choice of ∞, except that the universal constant appearing in the theorem, besides q, also depends on g and δ. The only missing ingredient needed in the proof is a formula similar to (6.1) for general function fields. This will be published elsewhere; see also [22].

2. Review of rigid-analytic uniformization of abelian varieties

The proof of Theorem 1.2 will use rigid-analytic uniformizations of abelian varieties with purely toric reduction. For the convenience of the reader, in this section we recall how such uniformizations are constructed and we recall some of their functorial properties. We will follow [1].

Let R be a complete discrete valuation ring, K be its field of fractions, ϖ be a uniformizer of K, and k be the residue field. We denote by ord_K the canonical valuation on K normalized by $\mathrm{ord}_K(\varpi) = 1$, and by $|\cdot|$ the norm associated to this valuation. We also let $G = (\mathbb{G}_{m,K}^{\mathrm{an}})^g$ be a split rigid-analytic torus over K and Λ a free discrete subgroup of $G(K)$ of full rank g. In particular, for each open affinoid U in G, $U \cap \Lambda$ is finite (equivalently, under $-\log|\cdot| : G(K) \to \mathbb{R}^g$, Λ maps bijectively onto a lattice of rank g in $\mathbb{R}^g$).

Let A be an abelian variety over K with split toric reduction over R. This means that the connected component of the identity in the reduction of the Néron model of A over R is a split torus over k.

2.1. Uniformization of degenerate abelian varieties

Given a locally finitely presented scheme X over R there are two ways to associate a rigid-analytic space to it; cf. [4, Section 5.3]. First, we could consider the generic fibre $X_K := X \times_R K$ of X, which is a locally finite type K-scheme, and take its analytification X_K^{an}. Second, we could consider the formal completion $\mathfrak{X}$ of X along its closed fibre (i.e., the formal completion of X with respect to an ideal of definition (ϖ) of R), and then take its rigidification $\mathfrak{X}^{\mathrm{rig}}$; see [2]. For example, if $\mathfrak{X} = \mathrm{Spf}(S)$, then $\mathfrak{X}^{\mathrm{rig}} = \mathrm{Sp}(S \otimes_R K)$. In general there will be a quasi-compact morphism

$$i_X : \mathfrak{X}^{\mathrm{rig}} \to (X \times_R K)^{\mathrm{an}}, \tag{2.1}$$

which is an isomorphism for proper X over R, and an open immersion when X is separated and admits a locally finite affine covering; see [4, Theorem 5.3.1].

Example 2.1. The most important example for us is when $X = \mathbb{G}_{m,R}$ is a split torus over R, so $(X \times_R K)^{\mathrm{an}} = \mathbb{G}_{m,K}^{\mathrm{an}}$ is the analytic one-dimensional torus over K and $\mathfrak{X} = \mathrm{Spf}(R\{T, T^{-1}\})$. Hence $\mathfrak{X}^{\mathrm{rig}} = \mathrm{Sp}(K\langle T, T^{-1}\rangle)$. In this case i_X is the open immersion of the "unit circle" into the "punctured plane".

We apply the previous construction with X taken to be the relative connected component of the identity $\mathcal{A}^0$ of the Néron model of A. Since $\mathcal{A}_K^0 = A$, on the right side of (2.1) we have the analytification A^{an} of A. On the other hand, $\mathcal{A}_k^0 \cong \mathbb{G}_{m,k}^g$ is a split torus. The rigidity of tori [9, Exp. IX, Theorem 3.6] implies that the formal completion of $\mathcal{A}^0$ along its closed fibre is uniquely isomorphic to a formal split torus $\widehat{\mathbb{G}}_m^g = (\mathrm{Spf}(R\{T, T^{-1}\}))^g$ respecting a choice of isomorphism $\mathcal{A}_k^0 \cong \mathbb{G}_{m,k}^g$. Thus, we get an open immersion of analytic groups $i_{\mathcal{A}^0} : (\mathrm{Sp}(K\langle T, T^{-1}\rangle))^g \hookrightarrow A^{\mathrm{an}}$. As in Example 2.1, we also have the analytic torus $G = (\mathbb{G}_{m,K}^{\mathrm{an}})^g$ associated to $(\widehat{\mathbb{G}}_m^g)^{\mathrm{rig}}$, and an open immersion $(\widehat{\mathbb{G}}_m^g)^{\mathrm{rig}} \hookrightarrow G$. The key fact is that $i_{\mathcal{A}^0}$ extends uniquely to a rigid-analytic group morphism $\pi : G \to A^{\mathrm{an}}$, whose kernel is a lattice $\Lambda \subset G(K)$ of rank g, and we have an isomorphism of analytic groups $G/\Lambda \cong A^{\mathrm{an}}$; see [1, Theorem 1.2].

2.2. Functorial properties of the uniformization

Let

$$G^{\vee} = \mathrm{Hom}_{\mathrm{an.grps}}(\Lambda, \mathbb{G}_{m,K}^{\mathrm{an}}) \quad \text{and} \quad \Lambda^{\vee} = \mathrm{Hom}_{\mathrm{an.grps}}(G, \mathbb{G}_{m,K}^{\mathrm{an}})$$

be the dual groups, which we call the *split dual torus* and the *dual lattice*. Since all characters of $\mathbb{G}_{m,K}^{\mathrm{an}}$ are algebraic, $\Lambda^{\vee}$ is a free $\mathbb{Z}$-module of rank equal to $\dim(G)$.

There is a canonical bilinear pairing

$$\Lambda^\vee \times G \to \mathbb{G}_{m,K}^{\mathrm{an}} \tag{2.2}$$

given by evaluation of characters in $\Lambda^\vee$ on the points of G. For any fixed $\lambda' \in \Lambda^\vee$, the above bilinear pairing gives by restriction a homomorphism $\Lambda \to K^\times$, $\lambda \mapsto \lambda'(\lambda)$, and hence a K-valued point in $G^\vee$. If we vary λ' over $\Lambda^\vee$, we obtain a canonical homomorphism $\Lambda^\vee \to G^\vee(K)$ which is easy to check is an injection. This latter homomorphism has the property that via canonical isomorphisms $G \cong (G^\vee)^\vee$ and $\Lambda \cong (\Lambda^\vee)^\vee$, for $\lambda' \in \Lambda^\vee$ and $\lambda \in \Lambda$ we have $\lambda'(\lambda) = \lambda(\lambda')$. It follows immediately that $\Lambda^\vee \hookrightarrow G^\vee$ is a lattice of rank g, and this homomorphism is the dual of $\Lambda \hookrightarrow G$. The quotient $G^\vee/\Lambda^\vee$ is a proper analytic group space which we denote by A'. Consider the trivial line bundle on $G \times_K G^\vee$ with an action of $\Lambda \times \Lambda^\vee$ defined by

$$\begin{aligned}(\lambda, \lambda') : G \times_K G^\vee \times \mathbb{A}^1 &\to G \times_K G^\vee \times \mathbb{A}^1\\ (x, x', a) &\mapsto (\lambda \cdot x, \lambda' \cdot x', \lambda'(x) \cdot \lambda'(\lambda) \cdot x'(\lambda) \cdot a).\end{aligned}$$

The quotient by this action yields a line bundle $\mathcal{P}$ on $A^{\mathrm{an}} \times_K A'$ which has the properties of a Poincaré bundle, and hence identifies $G^\vee/\Lambda^\vee$ with $(A^\vee)^{\mathrm{an}}$ [1, Theorem 2.1]. Here $A^\vee$ is the dual abelian variety of A. This isomorphism is functorial and compatible with base change.

Let $f : A \to B$ be a homomorphism of abelian varieties over K with split toric reduction, and let $f^\vee : B^\vee \to A^\vee$ be the dual homomorphism. Let f^{an} and $(f^\vee)^{\mathrm{an}}$ be the induced maps on the analytifications $A^{\mathrm{an}} \cong G_A/\Lambda_A$, $B^{\mathrm{an}} \cong G_B/\Lambda_B$. It is a theorem of van der Put [27, (3.3)] that given two split analytic tori G_1 and G_2 over K, and $\Lambda_1 \subset G_1(K)$, $\Lambda_2 \subset G_2(K)$ two full-rank lattices, there is an isomorphism

$$\mathrm{Hom}_{\mathrm{an.grps}}(G_1/\Lambda_1, G_2/\Lambda_2) \xleftarrow{\sim} \{\varphi : G_1 \to G_2 \mid \varphi(\Lambda_1) \subseteq \Lambda_2\}. \tag{2.3}$$

By this isomorphism f^{an} and $(f^\vee)^{\mathrm{an}}$ lift uniquely to morphisms between the analytic tori which map lattices to lattices, and we denote these lifts by $\widetilde{f^{\mathrm{an}}}$ and $\widetilde{(f^\vee)^{\mathrm{an}}}$. There is a commutative diagram

$$\begin{array}{ccc} \Lambda_A^\vee \times G_A & \longrightarrow & \mathbb{G}_{m,K}^{\mathrm{an}} \\ \widetilde{(f^\vee)^{\mathrm{an}}}\uparrow \quad \downarrow \widetilde{f^{\mathrm{an}}} & & \| \\ \Lambda_B^\vee \times G_B & \longrightarrow & \mathbb{G}_{m,K}^{\mathrm{an}}, \end{array} \tag{2.4}$$

where the horizontal maps are the canonical pairings in (2.2).

2.3. Weil pairing

We would like to use the analytic uniformization of A and its dual to make the Weil pairing

$$\bar{e}_{\ell^n} : A[\ell^n] \times A^\vee[\ell^n] \to \mu_{\ell^n} \tag{2.5}$$

explicit, where ℓ is a prime not equal to the characteristic p of the residue field k.

There is an exact sequence of finite étale groups, compatible with change in n

$$0 \to G[\ell^n] \to A^{\mathrm{an}}[\ell^n] \to \Lambda/\ell^n\Lambda \to 0. \tag{2.6}$$

Since on the level on ℓ^n-torsion we have a canonical isomorphism of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules $A^{\mathrm{an}}[\ell^n] \cong A[\ell^n]$, taking the projective limit over n we get an exact sequence of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$0 \to T_\ell(G) \to T_\ell(A) \to \Lambda \otimes \mathbb{Z}_\ell \to 0, \tag{2.7}$$

where $T_\ell(A)$ is the ℓ-adic Tate module of A. Taking projective limits in (2.5) gives the perfect ℓ-adic Weil pairing $(\cdot,\cdot)_\ell : T_\ell(A) \times T_\ell(A^\vee) \to T_\ell(\mathbb{G}_m)$. By the universal property of Néron models, $A(K) = \mathcal{A}(R) = \widehat{\mathcal{A}}(R)$. Since formation of Néron models commutes with étale base change and $T_\ell(\mathcal{A}_k^0) \to T_\ell(\mathcal{A}_k)$ is an isomorphism, the description of the uniformization of A in Subsection 2.1 makes it evident that the part of $T_\ell(A)$ fixed by the inertia subgroup of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ is exactly $T_\ell(G)$. Since A is also assumed to be purely toric, in terminology of [16, Exp. IX, Section 2] the finite part of $T_\ell(A)$ equals its toric subgroup. Thus, Grothendieck's *Orthogonality Theorem* [16, Exp. IX, Theorem 2.4] implies that under the Weil pairing $T_\ell(G)$ and $T_\ell(G^\vee)$ are exact annihilators of each other, so (2.5) and (2.6) induce a canonical pairing

$$\bar{e}_{\ell^n} : \Lambda/\ell^n\Lambda \times G^\vee[\ell^n] \to \mu_{\ell^n}. \tag{2.8}$$

For $x' \in G^\vee$, define $[x'] \stackrel{\mathrm{def}}{=} x' \bmod \Lambda^\vee$. As one easily checks, the restriction of the Poincaré bundle $\mathcal{P}$ to $A^{\mathrm{an}} \times \{[x']\}$ is obtained as the quotient of the trivial line bundle $G \times \mathbb{A}^1 = G \times \{[x']\} \times \mathbb{A}^1$ by the action of $\Lambda = \Lambda \times \{0\}$ via

$$(x, a) \mapsto (\lambda \cdot x, x'(\lambda) \cdot a). \tag{2.9}$$

Now suppose $[x'] \in G^\vee[\ell^n]$. Since $G^\vee[\ell^n] = \mathrm{Hom}_{\mathrm{an.grps}}(\Lambda/\ell^n\Lambda, \mathbb{G}_{m,K}^{\mathrm{an}})$, the action of $\ell^n\Lambda$ along $\mathbb{A}^1$ in (2.9) will be trivial. Thus, the line bundle descends to the trivial rigidified bundle on $G/\ell^n\Lambda$ with an action of $\Lambda/\ell^n\Lambda$ given by $(\underline{x}, a) \mapsto (\lambda \cdot \underline{x}, x'(\lambda) \cdot a)$. From the definition of the Weil pairing [20, p. 183] we conclude that $\bar{e}_{\ell^n}$ in (2.8) is given by evaluation. By taking projective limits, one obtains an analogous description of the ℓ-adic Weil pairing on $T_\ell(A) \times T_\ell(A^\vee)$.

3. Monodromy pairing

In this section we recall the description of Grothendieck's monodromy pairing in terms of analytic uniformization of abelian varieties. Using this description we give analytic proofs of the main properties of monodromy pairing. This pairing plays a key role in the construction of quotients of certain Jacobians in Section 4. We keep the notation of Section 2.

3.1. Analytic realization of monodromy pairing

We have a natural $\mathbb{Z}$-valued pairing between Λ and $\Lambda^\vee$ given by

$$\begin{aligned} \Lambda \times \Lambda^\vee &\to \mathbb{Z}, \\ \langle , \rangle : (\lambda, \lambda') &\mapsto \operatorname{ord}_K \lambda'(\lambda). \end{aligned} \tag{3.1}$$

(Note that $\lambda'(\lambda) \in \mathbb{G}_{m,K}^{\text{an}}(K) = K^\times$.) We call this pairing the *monodromy pairing*. (For the choice of terminology see Subsection 3.2.) It plays a role in the non-archimedean setting similar to that of a Riemann form in the theory of analytic uniformization of complex tori over $\mathbb{C}$. The following theorem summarizes the main properties of the monodromy pairing. We interchangeably denote this pairing on $\Lambda \times \Lambda^\vee$ either by $\langle , \rangle_A$ or u_A.

Theorem 3.1. (i) *For a local extension $R \to R'$ with ramification degree $e(R'/R)$, we have $u_{A',R'} = e(R'/R)u_{A,R}$ for $A' = A \times R'$.*

(ii) *The pairing u_A is non-degenerate.*

(iii) *The pairing u_A is bi-functorial in A; that is, if $f : A \to B$ is a morphism of abelian varieties over K, with B also split purely toric, and $f^\vee : B^\vee \to A^\vee$ is the dual morphism, then for $\alpha \in \Lambda_A$, $\beta \in \Lambda_B$, $\alpha' \in \Lambda_A^\vee$ and $\beta' \in \Lambda_B^\vee$ we have*

$$\langle \widetilde{f}(\alpha), \beta' \rangle_B = \langle \alpha, \widetilde{f^\vee}(\beta') \rangle_A.$$

(iv) *If $\theta : A \to A^\vee$ is a polarization then*

$$u_{A,\theta} : \Lambda \times \Lambda \xrightarrow{1\times\widetilde{\theta}} \Lambda \times \Lambda^\vee \xrightarrow{u_A} \mathbb{Z},$$

is bilinear, symmetric, and positive-definite.

(v) *There is a functorial exact sequence*

$$0 \longrightarrow \Lambda \xrightarrow{u_A} \operatorname{Hom}(\Lambda^\vee, \mathbb{Z}) \longrightarrow \Phi_A \longrightarrow 0,$$

where Φ_A is the component group of the reduction of the Néron model $\mathcal{A}$ of A. Moreover, Φ_A is a constant group scheme over k.

Proof. (i) By [3, Corollary 7.4/4], the formation of the identity component $\mathcal{A}^0$ of the Néron model of an abelian variety A over K with toric reduction is compatible with faithfully flat extension of discrete valuation rings R'/R. As this underlies the relation between formation of analytic uniformization of A over K and K', cf. Subsection 2.1, the claim follows from the identity $\mathrm{ord}_{K'} = e(R'/R)\mathrm{ord}_K$.

(ii) Suppose $\mathrm{ord}\,\lambda'(\lambda) = 1$ for a fixed λ' and all $\lambda \in \Lambda$. Since λ' is a character of the torus G it is of the form $\lambda'(z) = z_1^{\alpha_1} \cdots z_g^{\alpha_g}$, $\underline{\alpha} \in \mathbb{Z}^g$; see [11, VI.5.2]. The assumption that Λ is a lattice of full rank implies that under the homomorphism $G(K) \to \mathbb{R}^g$ defined by $(z_1, \ldots, z_g) \mapsto (-\log|z_1|, \ldots, -\log|z_g|)$ the image of Λ contains a basis of $\mathbb{R}^g$. On the other hand, λ' becomes the linear form $\sum_{i=1}^{g} \alpha_i x_i$ on $\mathbb{R}^g$, and since this vanishes on the image of Λ we get $\alpha_i = 0$ for all i. Dualizing, we get that u_A is also non-degenerate in Λ.

(iii) This follows from (2.4).

(iv) This is the non-archimedean analogue of the existence of a Riemann form on G/Λ; see [1, Theorem 2.4].

(v) (cf. [13, Corollary 2.11].) Because $\Lambda \subset G(K)$ and the quotient map $G \to G/\Lambda$ is étale surjective, we have an exact sequence of discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$0 \to \Lambda \to G(K^{\mathrm{sep}}) \to (G/\Lambda)(K^{\mathrm{sep}}) \to 0.$$

Since $\mathrm{H}^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), \Lambda) = \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathbb{Z}^g) = 1$, taking the long exact sequence of cohomology gives $G(K)/\Lambda \xrightarrow{\sim} (G/\Lambda)(K)$. Let $\widehat{G}$ be the formal completion of $\mathcal{A}^0$ along its closed fibre. Clearly $\widehat{G}(R) \hookrightarrow \widehat{G}^{\mathrm{rig}}(K) \hookrightarrow G(K)$ is identified with $(R^\times)^g \hookrightarrow (K^\times)^g$ upon trivializing $\mathcal{A}_k^0 \cong \mathbb{G}_{m,k}^g$, so we see that $\widehat{G}(R) = \{z \in G(K) \mid \mathrm{ord}_K(\lambda'(z)) = 0 \text{ for all } \lambda' \in \Lambda^\vee\}$. We get a commutative exact diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \downarrow & & & & \\
 & & & & \widehat{G}(R) & & & & \\
 & & & & \downarrow & & & & \\
0 & \longrightarrow & \Lambda & \longrightarrow & G(K) & \longrightarrow & A^{\mathrm{an}}(K) & \longrightarrow & 0. \\
 & & \downarrow{\scriptstyle u_A} & & \downarrow & & & & \\
 & & \mathrm{Hom}(\Lambda^\vee, \mathbb{Z}) & = & \mathrm{Hom}(\Lambda^\vee, \mathbb{Z}) & & & & \\
 & & & & \downarrow & & & & \\
 & & & & 0 & & & &
\end{array}$$

An easy diagram chaise gives the exact sequence

$$0 \longrightarrow \Lambda \xrightarrow{u_A} \mathrm{Hom}(\Lambda^\vee, \mathbb{Z}) \longrightarrow A^{\mathrm{an}}(K)/\widehat{G}(R) \longrightarrow 0.$$

Since $A^{\mathrm{an}}(K) = A(K)$, and by the Néronian property $A(K) \cong \mathcal{A}(R)$, we get

$$A^{\mathrm{an}}(K)/\widehat{G}(R) \cong \mathcal{A}(R)/\mathcal{A}^0(R).$$

We have $\mathcal{A}(R')/\mathcal{A}^0(R') \cong \Phi_A(\bar{k})$ for an appropriately large finite étale local extension R' of R. On the other hand, the quotient $\mathrm{Hom}(\Lambda^\vee, \mathbb{Z})/u_A(\Lambda)$ is insensitive to such extensions and the preceding construction commutes with base change to R'. Hence Φ_A is a constant group scheme over k and $\mathrm{coker}(u_A) \cong \Phi_A$ functorially in A. □

3.2. Relation with the algebraic theory

Let $\widehat{G} = \widehat{\mathcal{A}}^0$ be the split formal torus over $\mathrm{Spf}(R)$ as in the proof of Theorem 3.1(v). Let M be the character group of the split torus $\mathcal{A}_k^0$ over k, so M is functorially isomorphic to $\Lambda^\vee$ since $M = \mathrm{Hom}(\widehat{G}_k, \mathbb{G}_{m,k})$ and $\Lambda^\vee = \mathrm{Hom}(G, \mathbb{G}_{m,K}^{\mathrm{an}}) \cong \mathrm{Hom}(\widehat{G}, \widehat{\mathbb{G}}_{m,R})$.

In [16, Exp. IX, Section 9] Grothendieck defines a pairing between M and $M^\vee = \mathrm{Hom}(\mathcal{A}_k^{\vee 0}, \mathbb{G}_{m,k})$ as $\mathrm{Gal}(\bar{k}/k)$-modules

$$\langle, \rangle : M \times_{\mathbb{Z}} M^\vee \to \mathbb{Z}, \tag{3.2}$$

which he calls the *monodromy pairing*. Canonically identifying M and $\Lambda^\vee$, we will treat his monodromy pairing as a pairing between the lattices Λ and $\Lambda^\vee$. Using (2.7), the extension of scalars of the monodromy pairing $\langle, \rangle_\ell$ to $\mathbb{Z}_\ell$ is defined as follows:

Let K^{ur} be the maximal unramified extension of K. Consider the natural homomorphism $t : I = \mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{ur}}) \to T_\ell(\mathbb{G}_{m,K})$ given by

$$i \in I \mapsto \varprojlim i(\varpi^{1/\ell^n})/\varpi^{1/\ell^n}, \tag{3.3}$$

where we take ϖ also to be the uniformizer of K^{ur}. For $x \in \Lambda \otimes \mathbb{Z}_\ell$ lifting to $x' \in T_\ell(A)$ and $y \in \Lambda^\vee \otimes \mathbb{Z}_\ell$ lifting to $y' \in T_\ell(A^\vee)$, define $\langle x, y \rangle_\ell$ by the condition

$$((i-1)x', y')_\ell = t(i)^{\langle x, y \rangle_\ell}, \tag{3.4}$$

where $(\cdot, \cdot)_\ell$ is the ℓ-adic Weil pairing. Observe that $(i-1)$ sends $T_\ell(A)$ into $T_\ell(G)$, since (2.7) is compatible with base change and Λ is a constant group over $\mathrm{Sp}(K)$. Hence the orthogonality theorem shows that $\langle x, y \rangle_\ell$ is independent of the choices of x' and y'. Moreover, Grothendieck proved that $\langle, \rangle_\ell$ restricts to a $\mathbb{Z}$-valued pairing between Λ and $\Lambda^\vee$ which is independent of ℓ. This defines (3.2).

On the other hand, in (3.1) we defined another natural $\mathbb{Z}$-valued pairing between Λ and $\Lambda^\vee$, which we again called monodromy pairing, given by the valuation $\mathrm{ord}_K \lambda'(\lambda)$. The next theorem, which is the non-archimedean analogue of Theorem 1 on p. 237 in [20], says that there is no ambiguity in our terminology. The theorem relates the Weil pairing on abelian varieties with analytic uniformization to a pairing given by the "Riemann form" (3.1).

Theorem 3.2. *The pairings between* Λ *and* $\Lambda^\vee$ *given by* (3.1) *and* (3.2) *coincide.*

Proof. Let $[\lambda] \in \Lambda/\ell^n\Lambda$ and $[\lambda'] \in \Lambda^\vee/\ell^n\Lambda^\vee$. Write $\lambda = \ell^n g$ for $g \in G(K')$ and likewise $\lambda' = \ell^n g'$ for $g' \in G^\vee(K')$, where K' is a sufficiently large finite separable extension of K. As we explained in Section 2.3,

$$\bar{e}_{\ell^n}((i-1)g, g') = \lambda'((i-1)g) = \frac{i(\lambda'(g))}{\lambda'(g)}.$$

Since $\lambda'(g)$ is ℓ^n-th root of $\lambda'(\lambda) \in K^\times$, by definition of $t(i)$ in (3.3) we get

$$\bar{e}_{\ell^n}((i-1)g, g') = t(i)^{\mathrm{ord}_K \lambda'(\lambda)}.$$

as desired. □

Remark 3.3. Theorems 3.1 and 3.2 give an analytic proof of all of the main properties of Grothendieck's monodromy pairing in the special case when $\mathcal{A}^0$ has purely toric reduction. Grothendieck's original proof of properties (i)–(iv) in Theorem 3.1 uses the well-known properties of the Weil pairing. Property (v) is comparatively harder to prove algebraically, it is Theorem 11.5 in [16, Exp. IX].

3.3. Optimal quotients

Let A and B be two abelian varieties over K with split toric reduction, and let their corresponding uniformizations be given by G_A/Λ_A and G_B/Λ_B respectively. Let $\phi : B \hookrightarrow A$ be a closed immersion. According to (2.3) ϕ lifts uniquely to a morphism of analytic tori $\widetilde{\phi}_G : G_B \to G_A$. Since by [5, Theorem 8.2] the induced map $\phi_k : \mathcal{B}_k^0 \to \mathcal{A}_k^0$ on the closed fibre tori is also a closed immersion, from the construction of the analytic uniformization in Subsection 2.1 it is clear that $\widetilde{\phi}_G$ is a closed immersion. Hence by applying $\mathrm{Hom}(-, \mathbb{G}_{m,K}^{\mathrm{an}})$ to $\widetilde{\phi}_G$ we get an exact sequence of free $\mathbb{Z}$-modules

$$\Lambda_{A^\vee} \xrightarrow{\widetilde{\phi}_\Lambda^\vee} \Lambda_{B^\vee} \to 0. \tag{3.5}$$

Definition 3.4. We will say that the abelian variety C is an *optimal quotient* of the abelian variety A if there is a faithfully flat morphism $\theta : A \to C$ whose functorial kernel is represented by an abelian subvariety of A (that is, $\ker\theta$ is connected and smooth).

Let $\theta: A \to C$ be as in the definition. From the dual exact sequence, cf. [20, Section 13], we have a closed immersion $\theta^\vee: C^\vee \hookrightarrow A^\vee$, and (3.5) gives a *surjective* homomorphism $\widetilde{\theta}_\Lambda: \Lambda_A \to \Lambda_C$.

Remark 3.5. It is well-known that over $\mathbb{C}$ the optimal quotients of abelian varieties $\theta: A \to C$ are characterized by the property that the induced homomorphism on the integral homology groups $\mathrm{H}^1(\theta, \mathbb{Z}): \mathrm{H}_1(A, \mathbb{Z}) \to \mathrm{H}_1(C, \mathbb{Z})$ is surjective. The condition on $\widetilde{\theta}_\Lambda$ being surjective is a non-archimedean analogue of this.

Consider the diagram induced by θ on the sequence in Theorem 3.1(v)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda_A & \xrightarrow{u_A} & \mathrm{Hom}(\Lambda_{A^\vee}, \mathbb{Z}) & \longrightarrow & \Phi_A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \widetilde{\theta}} & & \downarrow{\scriptstyle \mathrm{Hom}(\widetilde{\theta}^\vee, \mathbb{Z})} & & \downarrow{\scriptstyle \theta} & & \\ 0 & \longrightarrow & \Lambda_C & \xrightarrow{u_C} & \mathrm{Hom}(\Lambda_{C^\vee}, \mathbb{Z}) & \longrightarrow & \Phi_C & \longrightarrow & 0. \end{array}$$

Since the left vertical arrow is surjective, we get

$$\begin{aligned} \#\mathrm{coker}(\Phi_A \xrightarrow{\theta} \Phi_C) &= \#\mathrm{Ext}^1_{\mathbb{Z}}(\Lambda_{A^\vee}/\widetilde{\theta}^\vee(\Lambda_{C^\vee}), \mathbb{Z}) \\ &= \#(\Lambda_{A^\vee}/\widetilde{\theta}^\vee(\Lambda_{C^\vee}))_{\mathrm{tor}}. \end{aligned} \tag{3.6}$$

This allows to reduce the questions about homomorphisms between component groups to questions about homomorphisms between lattices which are easier to handle. We will apply this trick in the proof of Theorem 4.9 (which is the main technical entry in the proof of Theorem 1.2).

4. Analytic construction of elliptic curves

We keep the notation of Section 2. Let J be the Jacobian variety of some projective smooth geometrically connected curve X over K, and assume J has split purely toric reduction. Hence J has an analytic uniformization as in Subsection 2.1

$$0 \to \Lambda \to G \to J^{\mathrm{an}} \to 0, \tag{4.1}$$

where G is a split analytic torus over K and $\Lambda \subset G(K)$ is a lattice.

Let E be a one-dimensional optimal quotient of J; cf. Definition 3.4. By [3, 7.4/2] E has split multiplicative reduction over R. In this section we are primarily interested in studying the map $\Phi_J \to \Phi_E$ induced by $\pi : J \to E$. Even though π is an optimal quotient, the map on the component groups in general will not be surjective; see [3, Section 7.5]. Nevertheless, in some special cases one can say something about the cokernel of this map.

Later on we will restrict our attention to the case when J is the Jacobian of a Drinfeld modular curve $X_0(\mathfrak{n})$. Since the arguments we are about to present are more general (for example, they apply in the case of classical modular curves too, and other moduli problems), to clarify the main ideas we will make several assumptions about J and in Subsection 5.2 verify that these assumptions hold for Drinfeld Jacobians. Some of our arguments are motivated by the ideas of Gekeler and Reversat in [15,13].

For simplicity, in this section we write J to denote J^{an}. Given a $\mathbb{Z}$-module or a $\mathbb{Z}$-algebra M, we will denote $M \otimes_{\mathbb{Z}} \mathbb{Q}$ by $M_{\mathbb{Q}}$.

4.1. Assumptions

By (2.3) every endomorphism α of J lifts in a unique way to an endomorphism $\widetilde{\alpha}$ of G such that $\widetilde{\alpha}(\Lambda) \subseteq \Lambda$. We make the following assumptions:

A1. There is a commutative (necessarily finite) free $\mathbb{Z}$-subalgebra $\mathbb{T}$ in $\mathrm{End}_K(J)$ such that $\dim_{\mathbb{Q}} \mathbb{T}_{\mathbb{Q}} = \dim_{\mathbb{Q}} \Lambda_{\mathbb{Q}}$, and $\mathbb{T}_{\mathbb{Q}}$ acts faithfully on $\Lambda_{\mathbb{Q}}$. (To be accurate we should denote $\mathbb{T}$ acting on Λ as $\widetilde{\mathbb{T}} \subseteq \mathrm{End}_{\mathbb{Z}}(\Lambda)$, but no confusion seems to arise.)

A2. The action of $\mathbb{T}$ on Λ is symmetric with respect to $u_{J,\theta}$ in the notation of Theorem 3.1, where θ is the canonical principal polarization of J.

Lemma 4.1. *Assumptions* 1 *and* 2 *imply that* $\Lambda_{\overline{\mathbb{Q}}}$ *has a basis consisting of simultaneous eigenvectors for the operators in* $\mathbb{T}$, *and* $\Lambda_{\mathbb{Q}}$ *is a free* $\mathbb{T}_{\mathbb{Q}}$*-module of rank one.*

Proof. Indeed, according to Theorem 3.1 $u_{J,\theta}$ is a positive definite symmetric bilinear form. The *spectral theorem* for commuting operators implies that $\mathbb{T}_{\mathbb{Q}}$ is semi-simple, so $\Lambda_{\overline{\mathbb{Q}}}$ has a basis of simultaneous eigenvectors. Now $\mathbb{T}_{\mathbb{Q}}$ is semi-simple and, by the first assumption, acts faithfully on $\Lambda_{\mathbb{Q}}$ which is of the same dimension over $\mathbb{Q}$ as $\mathbb{T}_{\mathbb{Q}}$. Hence $\Lambda_{\mathbb{Q}}$ is a free $\mathbb{T}_{\mathbb{Q}}$-module of rank one. □

Let E be an elliptic curve which is an optimal quotient of J. Assume that the kernel of the quotient map $\pi : J \to E$, as an abelian subvariety of J, is invariant under the action of $\mathbb{T}$. As we already mentioned, E has split multiplicative reduction over R. That is, E is a Tate curve, so it has no CM and hence the induced action of $\mathbb{T}$ on E must be via multiplication by integers. Considering the dual map to the optimal quotient π, one observes that J contains an abelian subvariety *isomorphic* to E. This determines a 1-dimensional subtorus of G in (4.1) and also a 1-dimensional subspace of $\Lambda_{\mathbb{Q}}$ on which $\mathbb{T}$ acts by multiplication by the same integers as on E. Conversely, given a 1-dimensional eigenspace of $\Lambda_{\mathbb{Q}}$ with integer eigenvalues, in the next subsection we will construct an optimal elliptic quotient of J on which $\mathbb{T}$ acts by multiplication by these eigenvalues.

4.2. Analytic construction of E

Suppose we are given a one-dimensional eigenspace of $\Lambda_{\mathbb{Q}}$ for the action of $\mathbb{T}$ and the eigenvalues are integers. Let $v \in \Lambda$ be a primitive eigenvector of this subspace; i.e., $\Lambda/v\mathbb{Z}$ is torsion free. This v is well-defined up to a sign. Starting with v, in this subsection we construct a 1-dimensional optimal quotient of J. Before we give the construction we need a more explicit description of the polarized monodromy pairing. This naturally leads to a question about describing the line bundles on a totally degenerate abelian variety in terms of its analytic uniformization. With the notation as in Section 2, we have the following analogue of the *Appell–Humbert theorem* over $\mathbb{C}$.

Proposition 4.2. *There is a functorial isomorphism of groups*

$$\mathrm{Pic}(A) \cong \mathrm{H}^1(\Lambda, \mathcal{O}(G)^\times),$$

where $\mathcal{O}(G)^\times = \{\beta \cdot z_1^{\alpha_1} \cdots z_g^{\alpha_g} \mid \beta \in K^\times \text{ and } \underline{\alpha} \in \mathbb{Z}^g\}$ *is the multiplicative group of nowhere-vanishing holomorphic functions on* G, *and* $\Lambda \subset G(K)$ *acts through its translation action on* G.

Proof. The proof is essentially the same as over $\mathbb{C}$ [20, Chapter 1], using the fact [11, VI.3.5] that the line bundles on G are trivial. □

Next, we can explicitly describe the cocycles in $\mathrm{H}^1(\Lambda, \mathcal{O}(G)^\times)$ in analogy with the lemma on p. 20 of [20].

Proposition 4.3. *Every element in* $\mathrm{H}^1(\Lambda, \mathcal{O}(G)^\times)$ *can be uniquely represented by* $Z_\lambda(z) = d(\lambda)H(\lambda)(z)$, *where*

$$H : \Lambda \to \Lambda^\vee = \{z_1^{\alpha_1} \cdots z_g^{\alpha_g} \mid \underline{\alpha} \in \mathbb{Z}^g\}$$

is a group homomorphism and $d : \Lambda \to K^\times$ *is a map satisfying*

$$d(\lambda_1\lambda_2)d(\lambda_1)^{-1}d(\lambda_2)^{-1} = H(\lambda_2)(\lambda_1).$$

Proof. See [11, VI.5.2]. The key for the second half of the proposition is that A has an admissible affinoid cover $\{U_i\}$ over which $G \to A$ is totally split (this uses that Λ is discrete in $G(K)$). □

To summarize, the analytification of every line bundle L on A corresponds to a cocycle Z_λ, and every such cocycle is given by a pair (H, d). Thus, every line bundle corresponds to a pair (H, d), and we will denote this line bundle by $L(H, d)$. One easily checks that $L(H_1, d_1) \cong L(H_2, d_2)$ if and only if $H_1 = H_2$ and $d_1(\lambda) = \lambda^{\underline{\alpha}} d_2(\lambda)$ for some $\underline{\alpha} \in \mathbb{Z}^g$.

Following [20, II.6], consider the functorial homomorphism $\varphi_L : A \to \mathrm{Pic}^0_{A/K} \cong A^\vee$ given by $x \mapsto T_x^* L \otimes L^{-1}$, where $T_x : a \mapsto a + x$. By (2.3), φ_L^{an} lifts uniquely to a homomorphism $\widetilde{\varphi}_L : G \to G^\vee$ such that $\widetilde{\varphi}_L(\Lambda) \subset \Lambda^\vee$.

Lemma 4.4. *If $L^{\mathrm{an}} \cong L(H, d)$ then $\widetilde{\varphi}_L$ restricted to Λ is equal to H. Moreover, if L is ample then H is injective.*

Proof. Let $z_0 \in G(K)$ be fixed. As in [20, p. 83] one easily verifies that

$$T^*_{\pi(z_0)} L(Z_\lambda(g)) \cong L(Z_\lambda(z_0 g)).$$

Since $Z_\lambda(z_0 g) = Z_\lambda(g) H(\lambda)(z_0)$, $\widetilde{\varphi}_L(z_0)$ as a K-point of $G^\vee = \mathrm{Hom}(\Lambda, \mathbb{G}^{\mathrm{an}}_{m,K})$ is given by $\widetilde{\varphi}_L(z_0)(\lambda) = H(\lambda)(z_0)$. Thus, for $z_0 = \lambda_0 \in \Lambda$, we get that $\widetilde{\varphi}_L$ restricted to Λ is given by $\widetilde{\varphi}_L(\lambda_0)(\lambda) = H(\lambda)(\lambda_0)$. On the other hand, from Proposition 4.3 it is clear that $H(\lambda)(\lambda_0) = H(\lambda_0)(\lambda)$. Hence $\widetilde{\varphi}_L(\lambda_0)(\lambda) = H(\lambda_0)(\lambda)$ as claimed.

If L is ample then φ_L is an isogeny, so $\widetilde{\varphi}_L$ obviously has torsion kernel. Since Λ is torsion free, $\widetilde{\varphi}_L|_\Lambda = H$ must be injective. □

Now let us return to the original situation of this section. By passing to a finite unramified extension of K we may assume that the canonical principal polarization $\theta : J \xrightarrow{\sim} J^\vee$ is equal to φ_L for some ample $L = L(H, d)$ on J. Using Lemma 4.4, the polarized monodromy pairing $u_{J,\theta}$ on $\Lambda \times \Lambda$ is given by

$$\langle , \rangle : \lambda_1, \lambda_2 \mapsto \mathrm{ord}\ H(\lambda_1)(\lambda_2). \tag{4.2}$$

Moreover, H induces an isomorphism $H : \Lambda \cong \Lambda^\vee = \mathrm{Hom}(G, \mathbb{G}^{\mathrm{an}}_{m,K})$ and the uniformization of J can be written as

$$0 \to \Lambda \to \mathrm{Hom}(\Lambda, \mathbb{G}^{\mathrm{an}}_{m,K}) \to J \to 0.$$

Proposition 4.5. *The action of the algebra $\mathbb{T}$ is symmetric with respect to the pairing $\Lambda \times \Lambda \to \mathbb{G}^{\mathrm{an}}_{m,K}$ defined by*

$$\lambda_1, \lambda_2 \mapsto H(\lambda_1)(\lambda_2),$$

i.e., if $T \in \mathbb{T}$ then $H(T\lambda_1)(\lambda_2) = H(\lambda_1)(T\lambda_2)$.

Proof. Indeed, using (4.2), Assumption 2 of Subsection 4.1 can be interpreted as

$$\mathrm{ord}\ H(T\lambda_1)(\lambda_2) = \mathrm{ord}\ H(\lambda_1)(T\lambda_2)$$

for all $\lambda_1, \lambda_2 \in \Lambda$. Moreover, regarding T as an endomorphism of G, $H(T\lambda_1)(-)$ and $H(\lambda_1)(T(-))$ are functions in $\mathrm{Hom}(G, \mathbb{G}^{\mathrm{an}}_{m,K})$. Now we can use the same argument as in the proof of Theorem 3.1(ii): a character of the torus G with values in $R^\times$ when restricted to a full-rank lattice in $G(K)$ must be trivial. Hence, $H(T\lambda_1)(-) = H(\lambda_1)(T(-))$. □

Proposition 4.6. *Define the subgroup*

$$\Gamma := \{H(\lambda)(v) \mid \lambda \in \Lambda\} \subseteq \mathbb{G}_{m,K}^{\mathrm{an}}(K) = K^\times.$$

There exists $w \in \Gamma$ *with* $\mathrm{ord}(w) = \min\{\mathrm{ord}\, H(\lambda)(v) > 0 \mid \lambda \in \Lambda\}$ *and a positive integer* d *such that* $\Gamma = \mu_d(K) \times w^{\mathbb{Z}}$ *inside* $K^\times$.

Proof. First observe that since the lattice Λ lies in $G(K)$, the group Γ is indeed a subgroup of $K^\times$. Next, by Lemma 4.1, $\Lambda_{\mathbb{Q}}$ is a free $\mathbb{T}_{\mathbb{Q}}$-module of rank 1. Thus the $\mathbb{Z}$-lattice Λ contains a sublattice Λ' of full rank which is cyclic under $\mathbb{T}$; i.e., $\Lambda' = \mathbb{T}\lambda'$ for some $\lambda' \in \Lambda$ and $[\Lambda : \Lambda']$ is finite. Let $\lambda \in \Lambda'$ be written additively

$$\lambda = \sum n_i T_i(\lambda'), \quad n_i \in \mathbb{Z}.$$

By Proposition 4.5,

$$H(\lambda)(v) = H(\lambda')\left(\sum n_i T_i(v)\right) = H(\lambda')(n_\lambda v) = H(\lambda')(v)^{n_\lambda}$$

for some $n_\lambda \in \mathbb{Z}$, since v is an eigenvector for the T_i with integral eigenvalues.

Hence $\{H(\lambda)(v) \mid \lambda \in \Lambda'\} = (w')^{\mathbb{Z}}$ with $w' = H(\lambda')(v)$. Using the facts that $|H(v)(v)| < 1$ and $[\Lambda : \Lambda']$ is finite, we conclude that there is $w \in \Gamma$ with $|w| < 1$ such that $w^{\mathbb{Z}}$ has finite index in Γ. Taking $|w|$ maximal, yields the claim. □

Note that Γ in Proposition 4.6 uniformizes the Tate curve $\mathrm{Tate}(w^d)$ over K with period w^d, since $\mathbb{G}_{m,K}^{\mathrm{an}}/\Gamma \cong \mathbb{G}_{m,K}^{\mathrm{an}}/w^{d\mathbb{Z}}$. Thus, using the eigenvector v we have constructed an elliptic curve $E_v \cong \mathrm{Tate}(w^d)$ together with a map $\pi : J \to E_v$ which is given by the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathrm{Hom}(\Lambda, \mathbb{G}_{m,K}^{\mathrm{an}}) & \longrightarrow & J & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \mathrm{ev} & & \downarrow \pi & & \\ 0 & \longrightarrow & \Gamma & \longrightarrow & \mathbb{G}_{m,K}^{\mathrm{an}} & \longrightarrow & E_v & \longrightarrow & 0, \end{array} \tag{4.3}$$

where the second row is the Tate uniformization of E_v and ev is the map "evaluation at v". The top row is $\mathbb{T}$-equivariant. Indeed, the action of $\mathbb{T}$ on $G \cong \mathrm{Hom}(\Lambda, \mathbb{G}_{m,K}^{\mathrm{an}})$ is induced from the action of $\mathbb{T}$ on J and $\Lambda \to \mathrm{Hom}(\Lambda, \mathbb{G}_{m,K}^{\mathrm{an}})$ is $\mathbb{T}$-equivariant by Proposition 4.5. Hence each operator T induces an endomorphism of E_v which agrees with the multiplication by the eigenvalue of T acting on v. On the other hand, if we define $G' := \mathrm{Hom}(\Lambda/v\mathbb{Z}, \mathbb{G}_{m,K}^{\mathrm{an}})$ and $\Lambda' = \Lambda \cap G'$ then the kernel of π is G'/Λ'. Since v is assumed to be primitive, $\Lambda/v\mathbb{Z}$ is a free $\mathbb{Z}$-module, and hence G' is a split subtorus of G. Moreover, Λ' is a full rank sublattice of G'. One way to see this is to observe that $v^{\perp} := \{v' \in \Lambda \mid \langle v, v'\rangle = 0\}$ maps injectively into Λ' with finite index. Since the quotient map $G' \to G'/\Lambda' = \ker(\pi)$ is étale surjective, $\ker(\pi)$ is connected and smooth, so, by the definition of optimality 3.4, E_v is optimal. Moreover, by GAGA, π is an algebraic homomorphism of abelian varieties.

4.3. *Calculation of* $\deg(\pi \circ \pi^{\vee})$

Let $E := E_v$ be as in Subsection 4.2, with v being its corresponding primitive eigenvector in Λ (which is unique up to a sign). Consider the dual $\pi^{\vee} : E^{\vee} \hookrightarrow J^{\vee}$ to the optimal quotient map π in (4.3). Since Jacobians of curves are canonically self-dual, the image of $\pi^{\vee}$ is a copy of E embedded in J. The composite $\pi \circ \pi^{\vee}$ is a polarization of E, and is necessarily a multiplication by some positive integer n as an element of $\mathrm{End}(E)$. In this subsection we compute $n = \deg(\pi \circ \pi^{\vee})^{1/2}$ in two different ways. Comparison of these two expressions easily implies the main theorem of this section (Theorem 4.9). Denote

$$d := \#\Gamma_{\mathrm{tor}}, \text{ as given in Proposition 4.6},$$

$$v^{\perp} := \{v' \in \Lambda \mid \langle v, v'\rangle = 0\},$$

$$m := \min\{|\langle v, v'\rangle| \mid v' \notin v^{\perp}\},$$

$$r := [\Lambda : \mathbb{Z}v \oplus v^{\perp}] = \frac{\langle v, v\rangle}{m}.$$

This last equality is an elementary fact concerning symmetric bilinear positive-definite $\mathbb{Z}$-valued pairings on free $\mathbb{Z}$-modules.

Proposition 4.7. *We have* $n \cdot \#\Phi_E = d^2 \langle v, v\rangle$.

Proof. The subvariety $\pi^{\vee} : E \hookrightarrow J$ corresponds to the subtorus $\mathrm{Hom}(\Lambda/v^{\perp}, \mathbb{G}_{m,K}^{\mathrm{an}})$ of $\mathrm{Hom}(\Lambda, \mathbb{G}_{m,K}^{\mathrm{an}})$. Hence via $\pi^{\vee}$,

$$0 \to \Delta \to \mathrm{Hom}(\Lambda/v^{\perp}, \mathbb{G}_{m,K}^{\mathrm{an}}) \to E \to 0,$$

where $\Delta = \Lambda \cap \mathrm{Hom}(\Lambda/v^\perp, \mathbb{G}_{m,K}^{\mathrm{an}}) = \{\lambda \in \Lambda \mid H(\lambda)|_{v^\perp} = 1\}$. Therefore by (4.3), the map $\pi \circ \pi^\vee : E \to E$ is given by the right column in

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Delta & \longrightarrow & \mathrm{Hom}(\Lambda/v^\perp, \mathbb{G}_{m,K}^{\mathrm{an}}) & \longrightarrow & E & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \mathrm{ev} & & \downarrow \pi\circ\pi^\vee = \cdot n & & \\ 0 & \longrightarrow & \Gamma & \longrightarrow & \mathbb{G}_{m,K}^{\mathrm{an}} & \longrightarrow & E & \longrightarrow & 0, \end{array}$$

where ev is the map induced from the evaluation at v. Now $\mathrm{ev}|_\Delta$ is injective. Indeed, if $H(\lambda)$ is in the kernel then $H(\lambda) = 1$ on $\mathbb{Z}v \oplus v^\perp$, and the latter is a lattice of full rank in G, so $H(\lambda) = 1$. Since H is an isomorphism, $H(\lambda) = 1$ implies $\lambda = 1$.

Next, if $\lambda \in \Delta$ then $H(\lambda)|_{v^\perp} = 1$, so $\langle \lambda, v^\perp \rangle = 0$. Hence $\lambda \in \mathbb{Z}v$ since v is a primitive vector. We also have $H(v)|_{v^\perp} = \Gamma_{\mathrm{tor}} = \mu_d(K)$ is cyclic of order d, so by writing $\lambda = \ell \cdot v$ we see that $H(\lambda)|_{v^\perp} = 1$ if and only if $d|\ell$. Thus

$$\mathrm{ev}(\Delta) = \{H(\lambda)(v) \mid \lambda \in \Lambda,\ H(\lambda)|_{v^\perp} = 1\} = H(v)(v)^{d\mathbb{Z}}.$$

Using that v is primitive, it is easy to see from the proof of Proposition 4.6 that, up to an element in Γ_{tor}, $H(v)(v) = w^r$. Finally, $\mathrm{ev}(\Delta) = w^{rd\mathbb{Z}}$ inside of $\Gamma = \mu_d(K) \times w^{\mathbb{Z}}$. Thus $\Gamma/\Delta \cong \mu_d(K) \times \mathbb{Z}/rd\mathbb{Z}$.

Clearly $\ker(\mathrm{ev}) = \mathrm{Hom}(\Lambda/\mathbb{Z}v \oplus v^\perp, \mathbb{G}_{m,K}^{\mathrm{an}}) = \mu_r$ as a finite flat group scheme, and ev is surjective. Thus, working rigid analytically, the snake lemma yields an exact sequence of finite flat group schemes

$$0 \to \mu_r \to E[n] \to \mu_d \times \mathbb{Z}/dr\mathbb{Z} \to 0.$$

This immediately implies $n = d \cdot r$. Next, by Proposition 4.6, $m = \mathrm{ord}(w)$. On the other hand, E is a Tate curve with period w^d. Hence $\#\Phi_E = \mathrm{ord}(w^d) = dm$, as follows from Theorems IV.9.4 and V.3.1 in [25]. Since $r \cdot m = \langle v, v \rangle$, the proposition follows. □

Now we compute n in a different way. Let $c = \mathrm{coker}(\pi_* : \Phi_J \to \Phi_E)$.

Proposition 4.8. *We have* $n \cdot \#\Phi_E = c^2 \langle v, v \rangle$.

Proof. Let Λ_E be the lattice associated with E. We choose a generator ρ of this infinite cyclic group. The natural map $\pi^* : \Lambda_E \to \Lambda$ induced by $\pi^\vee$ sends this generator to a multiple of the primitive vector v in Λ. According to (3.6), $\pi^*(\rho) = c \cdot v$. There is a second natural map $\pi_* : \Lambda \to \Lambda_E$ induced by π, and the endomorphism $\pi_* \circ \pi^*$ of Λ_E is multiplication by n. Using the bifunctoriality of the monodromy pairing

(Theorem 3.1(iii)) and its relation with component groups (Theorem 3.1(v)), we have

$$n \cdot \#\Phi_E = n\langle \rho, \rho\rangle_E = \langle n\cdot\rho, \rho\rangle_E = \langle \pi_*\pi^*\rho, \rho\rangle_E$$
$$= \langle \pi^*\rho, \pi^*\rho\rangle_J = \langle c\cdot v, c\cdot v\rangle_J = c^2\langle v, v\rangle_J. \qquad \square$$

Theorem 4.9. *If* $\mathrm{char}(K) = p > 0$ *then* $\mathrm{coker}(\pi_* : \Phi_J \to \Phi_E)$ *has vanishing p-torsion. In particular,* $\#\Phi_E[p^\infty] \leqslant \#\Phi_J[p^\infty]$.

Proof. Combining Propositions 4.7 and 4.8, we can conclude that $\#\mathrm{coker}(\pi_*)$ is equal to the order of a finite subgroup of the group of roots of unity in $K^\times$. If $\mathrm{char}(K) = p$ this latter group is trivial, and hence the cokernel is of order coprime to p. $\square$

5. Drinfeld modular curves

In the next section we will apply the construction of Section 4 to the Jacobians of Drinfeld modular curves of prime level. From this, more precisely from Theorem 4.9, Theorem 1.2 will easily follow. To apply Theorem 4.9 we first need to check that the assumptions A1 and A2 of Subsection 4.1 hold for Drinfeld Jacobians. It is the purpose of this section to verify the assumptions in this case.

Notation: Let $F = \mathbb{F}_q(t)$ be the field of rational functions on $\mathbb{P}^1_{\mathbb{F}_q}$. Let ∞ be a rational closed point on $\mathbb{P}^1_{\mathbb{F}_q}$. Let $A = \mathrm{H}^0(\mathbb{P}^1_{\mathbb{F}_q} - \infty, \mathcal{O}_{\mathbb{P}^1})$. Without loss of generality we can take $\infty = 1/t$ and $A = \mathbb{F}_q[t]$. For a prime ideal $\mathfrak{p}$ of the Dedekind domain A we denote the completion of A at $\mathfrak{p}$ by $A_\mathfrak{p}$, and the residue field $A/\mathfrak{p}$ by $\mathbb{F}_\mathfrak{p}$. We also let $p = \mathrm{char}(F)$.

5.1. Preliminaries

Let S be a scheme over A with the canonical ring homomorphism $\gamma : A \to \mathrm{H}^0(S, \mathcal{O}_S)$ and choose $r \in \mathbb{N}$. A pair $D = (\mathcal{G}, \phi)$ consisting of an $\mathbb{F}_q$-vector space scheme $\mathcal{G}$ over S and an $\mathbb{F}_q$-algebra homomorphism

$$\phi : A \to \mathrm{End}_S(\mathcal{G}), \quad a \mapsto \phi_a$$

from A into the ring of $\mathbb{F}_q$-linear S-endomorphisms of $\mathcal{G}$ is called a *Drinfeld module of rank r over S* if the following conditions are satisfied. The group scheme $\mathcal{G}$ is Zariski-locally isomorphic to the additive group scheme $\mathbb{G}_{a,S}$ over S, for each non-zero $a \in A$, ϕ_a is finite flat of degree $|a|_\infty^r$, and the induced action on the tangent space at the identity is via the structure map γ.

An $\mathfrak{n}$-*cyclic subgroup* $Z_\mathfrak{n} = (\mathcal{Z}, \psi)$ of $D = (\mathcal{G}, \phi)$ is a finite flat S-subgroup scheme $\mathcal{Z}$ of $\mathcal{G}$ and a homomorphism of A-modules $\psi : A/\mathfrak{n} \to \mathcal{G}(S)$ such that there is an equality of relative effective Cartier divisors in $\mathcal{G}$, $\sum_{m\in A/\mathfrak{n}} \psi(m) = \mathcal{Z}$.

The functor which associates to an A-scheme S the set of isomorphism classes of pairs $(D, Z_{\mathfrak{n}})$, where D is a Drinfeld module of rank 2 over S and $Z_{\mathfrak{n}}$ is an $\mathfrak{n}$-cyclic subgroup of D, is not representable but possesses a coarse moduli scheme $M_0(\mathfrak{n})$ that is affine of finite type over A and is A-flat with pure relative dimension 1. By adding extra level structure, $M_0(\mathfrak{n})$ can be obtained as a quotient of some fine moduli scheme by the action of a finite group. For example, if $\mathfrak{n}$ is divisible by at least two distinct primes then $M_0(\mathfrak{n})$ is the quotient of the fine moduli scheme $M^2(\mathfrak{n})$ of rank-2 Drinfeld modules with full level $\mathfrak{n}$-structure by the action of the subgroup of upper triangular matrices in the finite group $\mathrm{GL}_2(A/\mathfrak{n})$. Let $X_0(\mathfrak{n})$ be the canonical compactification of $M_0(\mathfrak{n})$ over $\mathrm{Spec}(A)$; see [10, Section 9]. Using the properties of fine moduli schemes proved in [10, Section 5] and also Theorems 1 and 2 in loc. cit., one gets the following:

Theorem 5.1. (a) $X_0(\mathfrak{n})$ *is a proper, normal, A-flat, and irreducible scheme of pure relative dimension* 1 *over* $\mathrm{Spec}(A)$.

(b) $X_0(\mathfrak{n}) \to \mathrm{Spec}\, A\left[\frac{1}{\mathfrak{n}}\right]$ *is smooth.*

(c) $X_0(\mathfrak{n})_F$ *is a smooth proper geometrically connected curve over F.*

Let $\mathfrak{p}$ be a prime ideal not dividing $\mathfrak{n}$. Consider the algebraic correspondence $T_{\mathfrak{p}} = \beta_* \circ \alpha^*$ on $M_0(\mathfrak{n})$ arising from the following diagram of morphisms

$$\begin{array}{ccccc} & & M_0(\mathfrak{p}\mathfrak{n}) & & \\ & \overset{\alpha}{\swarrow} & & \overset{\beta}{\searrow} & \\ M_0(\mathfrak{n}) & & & & M_0(\mathfrak{n}), \end{array}$$

where α, β are induced by the maps defined in terms of the moduli problem

$$\alpha : (D, Z_{\mathfrak{p}} Z_{\mathfrak{n}}) \mapsto (D, Z_{\mathfrak{n}})$$

$$\beta : (D, Z_{\mathfrak{p}} Z_{\mathfrak{n}}) \mapsto (D/Z_{\mathfrak{p}}, Z_{\mathfrak{p}} Z_{\mathfrak{n}}/Z_{\mathfrak{p}})$$

and thus are quasi-finite. Using the valuative criterion of properness, one shows that α and β are proper, and hence are also finite. These morphisms uniquely extend to the canonical compactifications $X_0(\mathfrak{p}\mathfrak{n})$ and $X_0(\mathfrak{n})$ due to the following general fact (taking S below to be $\mathrm{Spec}(A)$),

Lemma 5.2. *Let S be a locally noetherian scheme and C, C' two separated S-schemes of finite type. Assume that C is integral and normal, and that C' is integral and proper. Let U and U' be respective open subschemes with $C' - U'$ quasi-finite over S and U dense in C. A proper S-map $f : U \to U'$ uniquely extends to an S-map $C \to C'$.*

Proof. This proof was communicated to me by Brian Conrad. We only give a sketch.

Let $\Gamma \hookrightarrow C \times_S C'$ be the closure of the graph of *f*. For the existence of an extension $\bar{f}$ of f it is enough to show that the projection $\pi_1 : \Gamma \to C$ is an isomorphism. (The uniqueness follows from U being dense in C.) Let Γ_f be the closed subscheme in $U \times_S U'$ which is the graph of *f*. Using the fact that f is proper one shows that this subscheme is still closed in $C \times_S U'$. Hence $\Gamma \cap (C \times_S U') = \Gamma \cap (U \times_S U')$. In particular, $\Gamma \cap \big((C - U) \times_S C'\big)$ is contained in $(C - U) \times_S (C' - U')$. Since this latter scheme is quasi-finite over $C - U$, the projection π_1 will also be quasi-finite. From Zariski's Main Theorem, cf. [3, Theorem 2.3/2'], we conclude that π_1 is an open immersion (here we use the assumption that C is normal). Next, since we assumed C' is proper, $C \times_S C'$ is proper over C. This implies that the image of Γ is closed in C, so π_1 must be an isomorphism. □

Hence we get an algebraic correspondence $T_\mathfrak{p}$ on $X_0(\mathfrak{n})$, which we call the *Hecke correspondence*. This correspondence induces an endomorphism of the Jacobian variety $J_0(\mathfrak{n})$ of $X_0(\mathfrak{n})_F$, which we denote by the same symbol $T_\mathfrak{p}$. The *Hecke algebra* $\mathbb{T}$ is the commutative subalgebra of $\mathrm{End}_F(J_0(\mathfrak{n}))$ generated by all $T_\mathfrak{p}$, $\mathfrak{p} \nmid \mathfrak{n}$, over $\mathbb{Z}$.

5.2. Verification of the assumptions

Now assume $\mathfrak{n}$ is prime. A Drinfeld module $(\mathcal{G}, \phi)$ over an extension of $\mathbb{F}_\mathfrak{n}$ is called *supersingular* if its $\mathfrak{n}$-torsion is connected, or equivalently, $\phi_f(\overline{\mathbb{F}}_\mathfrak{n}) = 0$ for any non-trivial divisor f of a power of $\mathfrak{n}$. Any supersingular Drinfeld module in characteristic $\mathfrak{n}$ of rank 2 is defined over the quadratic extension $\mathbb{F}_\mathfrak{n}^{(2)}$ of $\mathbb{F}_\mathfrak{n}$, and there are only finitely many isomorphism classes of super-singular Drinfeld modules over $\overline{\mathbb{F}}_\mathfrak{n}$. The special fibre $X_0(\mathfrak{n})_{\overline{\mathbb{F}}_\mathfrak{n}}$ is reduced and is a union of two copies of $X_0(1)_{\overline{\mathbb{F}}_\mathfrak{n}} = \mathbb{P}^1_{\overline{\mathbb{F}}_\mathfrak{n}}$, intersecting transversally at the points representing the isomorphism classes of super-singular Drinfeld modules; see [12, Section 5].

Let $\mathcal{J}$ be the Néron model of $J_0(\mathfrak{n})$ over the base curve $\mathbb{P}^1_{\mathbb{F}_q}$. Since $X_0(\mathfrak{n})$ has a degenerate $\mathbb{F}_\mathfrak{n}$-fibre, by Example 9.2/8 in [3], $\mathcal{J}^0_{\mathbb{F}_\mathfrak{n}}$ is a torus which splits over $\mathbb{F}_\mathfrak{n}^{(2)}$. Let $M = \mathrm{Hom}_{\overline{\mathbb{F}}_\mathfrak{n}}(\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{n}}, \mathbb{G}_{m,\overline{\mathbb{F}}_\mathfrak{n}})$ be the character group of $\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{n}}$. By the Néron mapping property the endomorphisms of $J_0(\mathfrak{n})$ act on $\mathcal{J}^0_{\overline{\mathbb{F}}_\mathfrak{n}}$, and this action is faithful since the reduction is toric. Thus, the Hecke algebra $\mathbb{T}$ acts faithfully on M.

Let R be the unramified quadratic extension of $A_\mathfrak{n}$. Let K be the fraction field of R. As we discussed in Subsections 2.1 and 3.2, $J := J_0(\mathfrak{n})_K$ will have an analytic uniformization $J^{\mathrm{an}} \cong G/\Lambda$, where $G \cong (\mathbb{G}^{\mathrm{an}}_{m,K})^g$ is a split torus of dimension g(= genus of $X_0(\mathfrak{n})_F$) and $\Lambda \subset G(K)$ is a lattice, and $\Lambda^\vee$ and M are isomorphic $\mathbb{T}$-modules. Hence, using the canonical principal polarization of J, we also have $\Lambda \cong M$ as $\mathbb{T}$-modules.

Theorem 5.3. *If we take J and $\mathbb{T}$ in Subsection 4.1 to be $J_0(\mathfrak{n})_K$ and the Hecke algebra respectively then the assumptions* A1 *and* A2 *are satisfied.*

Proof. We have already explained why $\Lambda_\mathbb{Q}$ is a faithful $\mathbb{T}_\mathbb{Q}$-module. Moreover, it is well-known that $\dim_\mathbb{Q} \mathbb{T}_\mathbb{Q} = g = \dim_\mathbb{Q} \Lambda_\mathbb{Q}$; see, for example, [26, Proposition 4.2]. Hence the assumption A1 holds.

Next, we need to show that the action $\mathbb{T}$ on Λ is symmetric with respect to the θ-polarized monodromy pairing $u_{J,\theta}$ on $\Lambda \times \Lambda$. Theorem 3.2 reduces this to checking that the action of $\mathbb{T}$ on the Tate module $T_\ell(J)$, $\ell \neq p$, is symmetric with respect to the θ-polarized ℓ-adic Weil pairing. This last property is an easy consequence of *Eichler–Shimura congruence relations*: In $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(J_{\mathbb{F}_\mathfrak{p}})$ we have

$$T_\mathfrak{p} = \mathrm{Frob}_\mathfrak{p} + \mathrm{Frob}_\mathfrak{p}^\vee,$$

where $\mathrm{Frob}_\mathfrak{p}^\vee$ denotes the dual morphism of $\mathrm{Frob}_\mathfrak{p}$, identified with an endomorphism of $J_{\mathbb{F}_\mathfrak{p}}$ via the canonical principal θ-polarization. □

6. Proofs of the main results

In this section we prove the results stated in the introduction. We keep the notation of previous sections. Let E be an elliptic curve of conductor $\mathfrak{n}_E = \mathfrak{n} \cdot \infty$, and assume it is an optimal quotient of the Drinfeld Jacobian $J_0(\mathfrak{n})$. Let $\mathcal{E}$ be the Néron model of E over $\mathbb{P}^1_{\mathbb{F}_q}$.

6.1. Separable j-invariants

Theorem 6.1. *If $\mathfrak{n}$ is prime then the order of the group of connected components $\Phi_{E,\mathfrak{n}} := \mathcal{E}_{\overline{\mathbb{F}}_\mathfrak{n}}/\mathcal{E}^0_{\overline{\mathbb{F}}_\mathfrak{n}}$ is coprime to p, and the j-invariant of E is separable.*

Proof. It is enough to prove the theorem after a base change to a finite local étale extension of $A_\mathfrak{n}$ over which the reduction of $J_0(\mathfrak{n})$ is split toric. Indeed, the formation of the Néron models commutes with such a base change (in particular, the component groups are preserved) and the non-separable degree of the j-invariant is also preserved.

By Raynaud's theorem on the specialization of the Picard functor, and the structure of $X_0(\mathfrak{n})_{\mathbb{F}_\mathfrak{n}}$, one knows that the component group $\Phi_{J_0(\mathfrak{n}),\mathfrak{n}}$ is cyclic and of order coprime to p; [12, (5.9)]. Hence the first part of the theorem follows from Theorems 4.9 and 5.3. On the other hand, $\#\Phi_{E,\mathfrak{n}} = -\mathrm{ord}_\mathfrak{n}(j_E)$. As this is prime to p, $j_E \in F$ cannot be a p-th power. Thus, $\deg_{\mathrm{ns}}(j_E) = 1$. □

6.2. Place at infinity

Now we explore what can be said about $\deg_{\mathrm{ns}}(j)$ for optimal curves when we use the place ∞. It is known that $X_0(\mathfrak{n})_{F_\infty}$ is a Mumford curve [10, Proposition 6.6], so its Jacobian always has split purely toric reduction over this place. Nevertheless, as the next example shows, there is no hope of proving the separability of j-invariants by using a possible analogue of Theorem 6.1 for ∞.

Example 6.2. Let $A = \mathbb{F}_2[t]$, $\mathfrak{n} = t^4+t^3+1$. Note that $\mathfrak{n}$ is a prime. Gekeler calculated in [13] that $E:\ y^2+txy+y = x^3+x^2$ is an optimal curve of conductor $\mathfrak{n}_E = \mathfrak{n}\cdot\infty$ and $j = t^{12}/\mathfrak{n}$. Thus $\deg_{\mathrm{ns}}(j) = 1$ and $\Phi_{E,\mathfrak{n}} = 1$, but $\Phi_{E,\infty} \cong \mathbb{Z}/8\mathbb{Z}$.

Instead we take a different approach. We will use a result proved in [21] which relates the degree of optimal modular parametrization to special values of certain L-functions. Consider the composite of the canonical embedding $X_0(\mathfrak{n}) \hookrightarrow J_0(\mathfrak{n})$, given by sending the cusp at ∞ to 0, with the optimal quotient map $J_0(\mathfrak{n}) \to E$. We obtain a non-constant morphism of algebraic curves $\wp : X_0(\mathfrak{n}) \to E$, which we call the *optimal modular parametrization* of E. (The "cusp ∞" which we use for the embedding $X_0(\mathfrak{n}) \hookrightarrow J_0(\mathfrak{n})$ is a canonical rational point on $X_0(\mathfrak{n})$ naturally arising from the compactification of the moduli scheme $M_0(\mathfrak{n})$, and it is not related in any way to the place ∞.) We have the following formula [21, (27)]

$$\deg \wp = \frac{q^{\deg \mathfrak{n}-1}}{\#\Phi_{E,\infty}} L(\mathrm{Sym}^2 E, 2), \tag{6.1}$$

where $L(\mathrm{Sym}^2 E, s)$ is the L-function of the symmetric square of the ℓ-adic representation $\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{GL}(V_\ell(E)^\vee)$. Using this formula, we will get an upper bound on $\#\Phi_{E,\infty}$ in terms of the conductor, and hence also an upper bound on $\deg_{\mathrm{ns}}(j)$, since E is split multiplicative over ∞.

Remark 6.3. In [21] an assumption is made that elliptic curves in question are semistable. As one easily verifies, this assumption is not used in derivation of [21, (27)]. The assumption is used in giving asymptotic bounds on $L(\mathrm{Sym}^2 E, 2)$, since the bounds are deduced from convexity estimates which require the knowledge of the functional equation of $L(\mathrm{Sym}^2 E, s)$. Such a functional equation is not hard to deduce when the level is square-free, cf. loc. cit., but in general this is quite non-trivial. As we will need an upper bound on $|L(\mathrm{Sym}^2 E, 2)|$ and we do not want to impose any restrictive assumptions on $\mathfrak{n}$, we prove such a bound in Appendix A by appealing to Grothendieck's theory of L-functions.

Theorem 6.4. *If E is an optimal elliptic curve of conductor $\mathfrak{n}\cdot\infty$, then*

$$\frac{\mathcal{N}(\mathfrak{n})}{(1+q)(1+q\deg \mathfrak{n})^2} \leqslant \deg \wp \leqslant q^6 (\deg \mathfrak{n})^3 \mathcal{N}(\mathfrak{n}),$$

where $\mathcal{N}(\mathfrak{n}) = q^{\deg \mathfrak{n}}$.

Proof. The 2-dimensional ℓ-adic representation of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ attached to E is irreducible, almost everywhere unramified and pure of weight 1. Hence from Corollary A.5 we deduce

$$|L(\mathrm{Sym}^2 E, 2)| \leqslant q^7 \cdot (\deg \mathfrak{n})^3.$$

The upper bound on the degree of $\wp$ follows from this, (6.1), and the trivial observation $\#\Phi_{E,\infty} \geqslant 1$.

Let $S = \mathrm{Spec}(A[\mathfrak{n}^{-1}])$. Consider the Néron model $\mathcal{E}$ of E over S. Since E has good reduction over S, $\mathcal{E}$ is an abelian scheme. By Theorem 5.1, $X := X_0(\mathfrak{n})_F$ is geometrically connected and is the generic fibre of a smooth proper curve $\mathcal{X}$ over S, so all fibers of $\mathcal{X}$ over S are geometrically connected. By the Néron mapping property, the finite surjective morphism $\wp : X \to E$ extends to a morphism $\wp_{/S} : \mathcal{X} \to \mathcal{E}$ of relative smooth curves over S. This must be surjective (by S-flatness and properness) and hence is finite. Let $\mathfrak{p}$ be a closed point of S and consider the fibre map $\wp_{/\mathfrak{p}} : \mathcal{X}_{\mathbb{F}_\mathfrak{p}} \to \mathcal{E}_{\mathbb{F}_\mathfrak{p}}$. This is a finite flat map from a smooth geometrically connected proper curve over $\mathbb{F}_\mathfrak{p}$ to an elliptic curve, and moreover $\deg \wp_{/\mathfrak{p}} = \deg \wp$. Indeed, since $\wp_{/S}$ is finite flat and $\mathcal{E}$ is connected, the induced finite flat maps on *all* fibers have the same degree. Denote $\mathcal{X}_\mathfrak{p} := \mathcal{X}_{\mathbb{F}_\mathfrak{p}}$ and $\mathcal{E}_\mathfrak{p} := \mathcal{E}_{\mathbb{F}_\mathfrak{p}}$. It is clear that for any extension $\mathbb{F}_\mathfrak{p}^{(m)}$ of degree m of $\mathbb{F}_\mathfrak{p}$ we have

$$\#\mathcal{X}_\mathfrak{p}(\mathbb{F}_\mathfrak{p}^{(m)})/(\deg \wp) \leqslant \#\mathcal{E}_\mathfrak{p}(\mathbb{F}_\mathfrak{p}^{(m)}).$$

Modular curves are known to have "lots" of rational points over residue fields, cf. [14]. The reason is that, using the moduli interpretation, one can check that $\mathcal{X}_\mathfrak{p}$ has rational points over $\mathbb{F}_\mathfrak{p}^{(2)}$ corresponding to the super-singular Drinfeld modules and the cusps. The number of rational super-singular points over $\mathbb{F}_\mathfrak{p}^{(2)}$ is larger than $\mathcal{N}(\mathfrak{n})/(q+1)$; see [14, Sections 7 and 9]. On the other hand, by Hasse–Weil

$$\#\mathcal{E}_\mathfrak{p}(\mathbb{F}_\mathfrak{p}^{(2)}) \leqslant (1+\mathcal{N}(\mathfrak{p}))^2.$$

Thus,

$$\deg \wp \geqslant \mathcal{N}(\mathfrak{n})/(q+1)(1+\mathcal{N}(\mathfrak{p}))^2.$$

I claim that we can choose $\mathfrak{p}$ satisfying $\mathcal{N}(\mathfrak{p}) \leqslant q \cdot (\deg \mathfrak{n})$. In fact, a moment of thought shows that the "worst" that can happen is $\mathfrak{n} = \prod_{\deg v \leqslant s} v$, where the product is over primes of degree less than or equal to some number s. If b_d is the number of places on $\mathbb{P}^1_{\mathbb{F}_q}$ of degree d, then $\deg \mathfrak{n} = \sum_{d \leqslant s} d b_d$. On the other hand, it is clear that $\sum_{d|s} d b_d = \#\mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_{q^s})$. Hence we have $\deg \mathfrak{n} \geqslant \#\mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_{q^s}) \geqslant q^s + 1$. Since for $\mathfrak{p}$ of degree $s+1$ we have $\mathcal{N}(\mathfrak{p}) = q^{s+1}$, the claim follows. Choosing $\mathfrak{p}$ with $\mathcal{N}(\mathfrak{p}) \leqslant q \cdot (\deg \mathfrak{n})$, we obtain the desired lower bound on the degree of optimal modular parametrization. □

Remark 6.5. It is clear from the proof that in many cases the lower bound in the theorem can be improved to $\deg \wp \geqslant \mathcal{N}(\mathfrak{n})/(q+1)^3$. For example, if E has a place of good reduction which is rational, such an improvement holds.

Remark 6.6. The upper bound in the theorem is the analogue over function fields of a conjecture over $\mathbb{Q}$ known as the *degree conjecture*. The degree conjecture states that for an optimal elliptic curve E over $\mathbb{Q}$ of conductor N (optimal for the parametrization by the classical modular curve $\wp : X_0(N) \to E$), and for any $\varepsilon > 0$ there is a universal constant $c(\varepsilon)$ depending only on ε such that $\deg \wp \leqslant c(\varepsilon)N^{2+\varepsilon}$. The degree conjecture for semi-stable curves is known to imply the celebrated *ABC conjecture* [18].

Corollary 6.7. *We have a bound*

$$\deg_{\mathrm{ns}}(j_E) \leqslant q^6(1+q)(1+q \deg \mathfrak{n})^2(\deg \mathfrak{n})^3.$$

Proof. Indeed, from (6.1) and the upper bound on the absolute value of $L(\mathrm{Sym}^2 E, 2)$ in the proof of Theorem 6.4 we have

$$(\deg \wp) \cdot \#\Phi_{E,\infty} \leqslant q^6(\deg \mathfrak{n})^3 \mathcal{N}(\mathfrak{n}).$$

Using this inequality and the lower bound on $\deg \wp$ from Theorem 6.4, we get

$$\#\Phi_{E,\infty} \leqslant q^6(1+q)(1+q \deg \mathfrak{n})^2(\deg \mathfrak{n})^3.$$

Since $\#\Phi_{E,\infty} = -\mathrm{ord}_\infty(j_E)$, and $\deg_{\mathrm{ns}}(j_E)$ divides $-\mathrm{ord}_\infty(j_E)$ the claim follows. □

Acknowledgments

I would like to express my gratitude to my thesis advisor Brian Conrad, whose guidance and support were crucial for the successful completion of this project. I also thank Barry Mazur for suggesting the problem considered in this paper.

Appendix A. Bounding special values of L-functions

Let C be a smooth, proper, geometrically irreducible curve over a finite field $\mathbb{F}_q$ of characteristic p and let F be the field of rational functions on C. Choose a separable closure F^{sep} of F and let $G = \mathrm{Gal}(F^{\mathrm{sep}}/F)$ be the absolute Galois group of F.

Fix a prime $\ell \neq p$. By an *ℓ-adic representation* ρ of G we shall understand a finite-dimensional representation of G over $\overline{\mathbb{Q}}_\ell$ which is continuous in the ℓ-adic topology (with G given its usual profinite topology), and is unramified outside a finite set of places. We say that ρ is *self-dual* if it is isomorphic to its contragredient representation $\widehat{\rho}$. This is equivalent to the existence of a non-degenerate G-equivariant bilinear pairing on the underlying space.

Let $\rho : G \to \mathrm{GL}(V)$ be a 2-dimensional irreducible ℓ-adic representation of G, where V is a 2-dimensional vector space over some finite extension of $\mathbb{Q}_\ell$. Denote by $\mathrm{Sym}^n \rho$ the irreducible $(n+1)$-dimensional ℓ-adic representation of G obtained from the action of G on the symmetric tensors of $V^{\otimes n}$ via ρ. Let $L(\mathrm{Sym}^n\,\rho, s)$ be Grothendieck's L-function for $\mathrm{Sym}^n\,\rho$. The purpose of this appendix is to estimate the absolute values of $L(\mathrm{Sym}^n\,\rho, s)$ in the vertical strip $0 \leqslant \mathrm{Re}(s) \leqslant 1$ in terms of the norm of the conductor of ρ, assuming ρ is self-dual.

A.1. Preliminaries

The principal reference for this subsection is [7].

By a *quasi-character* χ of a group H we mean a homomorphism $\chi : H \to \mathbb{C}^\times$. A *character* is a unitary quasi-character. If H is a topological group we will understand that (quasi-)characters are required to be continuous (with $\mathbb{C}^\times$ given its usual topology).

Let K be a (complete) non-archimedean local field; an example of such is the completion F_v of our function field F at any place v. Let $\mathcal{O}$ be the ring of integers in K, ϖ be a uniformizer, $\mathfrak{p} = \varpi\mathcal{O}$ be the maximal ideal of $\mathcal{O}$, $k = \mathcal{O}/\mathfrak{p}$ be the residue field, $q = \#k$, $p = \mathrm{char}(k)$. We denote by $|\cdot|$ the norm on K associated to the valuation ord_K normalized by $\mathrm{ord}_K(\varpi) = 1$.

The topological groups K and $K^\times$ have a basis of neighborhoods of the identity consisting of compact open subgroups. It is a well-known fact that sufficiently small neighborhoods of the identity in $\mathbb{C}^\times$ do not contain any non-trivial subgroups. Thus, any quasi-character of K or $K^\times$ must contain an open subgroup in its kernel. Given a non-trivial additive quasi-character ψ of K, there is a unique integer m such that ψ is trivial on $\mathfrak{p}^{-m}$ but not on $\mathfrak{p}^{-m-1}$. We call $\mathfrak{n}(\psi) := \mathfrak{p}^{-m}$ the *conductor* of ψ. Similarly, if χ is a multiplicative quasi-character of $K^\times$ which is non-trivial on $\mathcal{O}^\times$ then there is a largest ideal $\mathfrak{p}^n$ $(n \geqslant 1)$ such that χ is trivial on the open subgroup $1 + \mathfrak{p}^n$ of the units $\mathcal{O}^\times$. We call $\mathfrak{n}(\chi) := \mathfrak{p}^n$ the *conductor* of χ; if χ is trivial on $\mathcal{O}^\times$ we define the conductor of χ to be $\mathfrak{n}(\chi) = \mathcal{O}$. We say that an additive or multiplicative character is *unramified* if its conductor is $\mathcal{O}$.

Recall that $\mathrm{Gal}(\bar{k}/k)$ is isomorphic to $\widehat{\mathbb{Z}}$ and is topologically generated by the automorphism $\varphi : x \mapsto x^q$. The (absolute) *Weil group* W_K is the dense subgroup of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ consisting of all elements whose image in $\mathrm{Gal}(\bar{k}/k)$ is a power of φ. The *inertia* subgroup of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ is the subgroup I of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ whose image in $\mathrm{Gal}(\bar{k}/k)$ is trivial. To topologize W_K we require I to be an open subgroup and to have induced on itself the usual profinite topology. Any element Φ of W_K whose image in $\mathrm{Gal}(\bar{k}/k)$ is φ^{-1} is called a *geometric Frobenius*.

Local class field theory provides an isomorphism of topological groups $\mathrm{rec} : W_K^{\mathrm{ab}} \xrightarrow{\sim} K^\times$ which we normalize by sending a geometric Frobenius to a uniformizer of K. Let ω_1 be the quasi-character $\omega_1(x) = |x|$ of $K^\times$. Note that $\omega_1 \circ \mathrm{rec}$ is unramified and with the previous normalization we have $\omega_1(\mathrm{rec}(\Phi)) = q^{-1}$. For $g \in W_K$ we shall write $\omega_1(g)$ rather than $\omega_1(\mathrm{rec}(g))$ from now on.

Recall that a *Weil–Deligne representation* σ' of W_K consists of a pair (σ, N), where $\sigma : W_K \to \mathrm{GL}_n(\mathbb{C})$ is a complex semi-simple n-dimensional representation, and N is a nilpotent matrix in $M_n(\mathbb{C})$ satisfying $\sigma(g)N\sigma(g)^{-1} = \omega_1(g)N$, $g \in W_K$. Weil–Deligne representations naturally arise from the ℓ-adic representations of W_K. If we fix an isomorphism $\imath : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$, then there is a simple recipe for converting an ℓ-adic representation σ'_ℓ of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ into a Weil–Deligne representation. The construction is due to Grothendieck and Deligne. The essential point is that there is a canonical way to associate to σ'_ℓ a pair (σ_ℓ, N_ℓ) consisting of a homomorphism $\sigma_\ell: W_K \to \mathrm{GL}(V_\ell)$ trivial on an open subgroup of I and a nilpotent endomorphism N_ℓ of V_ℓ such that $\sigma_\ell(g)N_\ell\sigma_\ell(g)^{-1} = \omega_1(g)N_\ell$; see [7, Section 8].

Example A.1. An important example of a Weil–Deligne representation is the *special representation* $\mathrm{sp}(n)$ defined as follows. Fix a basis $\{e_0, e_1, \dots, e_{n-1}\}$ for $\mathbb{C}^n$. Define (σ, N) by $\sigma(g)e_i = \omega_1^i(g)e_i$, $Ne_{n-1} = 0$, and $Ne_i = e_{i+1}$ $(0 \leqslant i < n-1)$.

The *conductor* $\mathfrak{n}(\sigma')$ of σ' is an ideal $\varpi^{a(\sigma')}\mathcal{O}$, for some non-negative integer $a(\sigma')$. This integer is naturally a sum of two terms, $a(\sigma') = a(\sigma) + b(\sigma')$, and as the notation indicates, the first term depends only on σ. Writing V for the space of σ', we have $b(\sigma') = \dim V^I/V_N^I$, where $V_N^I = V^I \cap \ker N$. To define $a(\sigma)$, choose a finite Galois extension M of K^{ur} such that σ is trivial on the subgroup $\mathrm{Gal}(K^{\mathrm{sep}}/M)$ of I, and put G_j, $j \geqslant 0$, for the higher ramification groups of $\mathrm{Gal}(M/K^{\mathrm{ur}})$. If we denote $g_j := \#G_j$, $j \geqslant 0$, then $a(\sigma) = \sum_{j=1}^{\infty}(g_j/g_0)\dim(V/V^{G_j})$. This definition is independent of the choice of M. We say that σ' is *unramified* if σ is unramified and $N = 0$. These conditions are equivalent to the vanishing of $a(\sigma')$.

Let V be the vector space of the Weil–Deligne representation $\sigma' = (\sigma, N)$. We will denote by $\mathrm{Sym}^n\,\sigma'$ the Weil–Deligne representation of W_K on the subspace of $V^{\otimes n}$ spanned by symmetric tensors. Recall that $(\sigma, N) \otimes (\tau, M) = (\sigma \otimes \tau, N \otimes 1 + 1 \otimes M)$ by definition.

Lemma A.2. *If* $\dim \sigma' = 2$ *then* $a(\mathrm{Sym}^n\,\sigma') \leqslant n \cdot a(\sigma')$.

Proof. First of all, let χ be a quasi-character of W_K and let $\tau' = \chi \otimes \mathrm{sp}(n)$. We have

$$a(\tau') = \begin{cases} n \cdot a(\chi) & \text{if } \chi \text{ is ramified,} \\ n-1 & \text{otherwise.} \end{cases}$$

Indeed, if W is the space of χ, so that $V = W \otimes \mathbb{C}^n$ is the space of τ', then $V^I = W^I \otimes \mathbb{C}^n$ and $V_N^I = W^I \otimes e_{n-1}$. If χ is ramified then $W^I = \{0\}$; if χ is unramified then $W^I = W$. It follows that $b(\tau')$ is equal to 0 or $n-1$ when χ is ramified or unramified, respectively. On the other hand, τ is the direct sum of the representations $\chi \otimes \omega_1^j$ for $0 \leqslant j \leqslant n-1$. Since ω_1 is unramified we have $a(\chi \otimes \omega_1^j) = a(\chi)$. Therefore $a(\tau) = n \cdot a(\chi)$.

Another remark we make is that for a quasi-character χ we have $a(\chi^m) \leqslant a(\chi)$ for any positive integer m, as is clear from the definition.

Now let σ' be a 2-dimensional Weil–Deligne representation. There are three cases to consider. If σ' is decomposable then $\sigma' = \chi_1 \oplus \chi_2$ for two quasi-characters of W_K (and $N = 0$) and $\mathrm{Sym}^n\,\sigma' \cong \chi_1^n \oplus \chi_1^{n-1}\chi_2 \oplus \cdots \oplus \chi_2^n$. Hence

$$a(\mathrm{Sym}^n\,\sigma') = a(\chi_1^n) + a(\chi_1^{n-1}\chi_2) + \cdots + a(\chi_2^n)$$

$$\leqslant a(\chi_1) + (n-2)\max(a(\chi_1), a(\chi_2)) + a(\chi_2)$$
$$\leqslant n(a(\chi_1) + a(\chi_2)) = n \cdot a(\sigma').$$

If σ' is reducible but indecomposable then $\sigma' = \chi \otimes \mathrm{sp}(2)$ for some quasi-character χ and $\mathrm{Sym}^n \sigma' \cong \chi^n \otimes \mathrm{sp}(n+1)$. First suppose χ is unramified. From what we proved, $a(\sigma') = 1$ and $a(\mathrm{Sym}^n \sigma') = n$, so $a(\mathrm{Sym}^n \sigma') \leqslant n \cdot a(\sigma')$ as required. If χ is ramified and χ^n is unramified, then $a(\sigma') = 2a(\chi) \geqslant 2$. Hence $a(\mathrm{Sym}^n \sigma') = n-1 \leqslant 2n \leqslant n \cdot a(\sigma')$. If both χ and χ^n are ramified then (since $a(\chi^n) \leqslant a(\chi)$) we have

$$a(\mathrm{Sym}^n \sigma') = (n+1)a(\chi^n) \leqslant (n+1)a(\chi) \leqslant 2n \cdot a(\chi) = n \cdot a(\sigma').$$

Finally, if σ' is irreducible then $\sigma' = (\sigma, 0)$ and

$$a(\sigma') = a(\sigma) = \sum_{j=1}^{\infty} \frac{g_j}{g_0} \dim(V/V^{G_j}).$$

Obviously

$$\dim(\mathrm{Sym}^n V/(\mathrm{Sym}^n V)^{G_j}) \leqslant n \cdot \dim(V/V^{G_j}),$$

and again $a(\mathrm{Sym}^n \sigma') \leqslant n \cdot a(\sigma')$. $\square$

Now we state a fact concerning epsilon-factors for σ'. Epsilon-factors are characterized axiomatically, one of the axioms being induction. This permits reduction to the case of dimension 1 for computations, where the corresponding factors were explicitly defined by Tate in his thesis. The first point to make about the epsilon-factor $\varepsilon(\sigma', \psi, dx) \in \mathbb{C}^\times$ of a representation $\sigma' = (\sigma, N)$ is that it also depends on a choice of a non-trivial additive character $\psi : K \to \mathbb{C}^\times$, and a Haar measure dx on K. For a non-trivial additive ψ denote by dx_ψ the unique Haar measure on K that is self-dual with respect to ψ.

Proposition A.3. *For $s \in \mathbb{C}$, the ε-factor $\varepsilon(\sigma' \otimes \omega_1^s, \psi, dx_\psi)$ is a non-zero monomial in $\mathbb{C}[q^{-s}]$ which is equal to 1 when σ' and ψ are unramified. If we assume σ' is isomorphic to its contragredient $\widehat{\sigma'}$ then*

$$|\varepsilon(\sigma' \otimes \omega_1^s, \psi, dx_\psi)| = q^{(a(\sigma') - \dim(\sigma')\mathrm{ord}_K \mathfrak{n}(\psi)) \cdot (\frac{1}{2} - \mathrm{Re}(s))},$$

where the absolute value is the absolute value on $\mathbb{C}$.

Proof. This follows from the Deligne–Langlands "Formulaire" in [7, Sections 4–5]. $\square$

A.2. Upper bound

We return to our initial goal of estimating the absolute values of $L(\mathrm{Sym}^n \rho, s)$ in the critical strip, where ρ is an irreducible 2-dimensional self-dual ℓ-adic representation of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$. Even though these L-functions are known to be polynomials in q^{-s}, analytic methods (which do not use this extra information) give very good bounds on the special values.

Theorem A.4. *Let ρ be an irreducible 2-dimensional self-dual ℓ-adic representation of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ with determinant quasi-character $\det(\rho)$ of finite order. Let $\mathfrak{n} := \mathfrak{n}(\rho)$ be the global conductor of ρ, viewed as an effective divisor on C. Denote $\mathcal{N}(\mathfrak{n}) = q^{\deg \mathfrak{n}}$. Let g be the genus of the base curve C. If $\deg \mathfrak{n} > 0$ then*

$$|L(\mathrm{Sym}^n \rho, s)| \leqslant q^{(4g+2)(n+1)+\frac{n}{2}} \mathcal{N}(\mathfrak{n})^{\frac{n}{2}(1-\mathrm{Re}(s))} (\deg \mathfrak{n})^{n+1}$$

for $0 \leqslant \mathrm{Re}(s) \leqslant 1$. In particular,

$$|L(\mathrm{Sym}^n \rho, 1)| \leqslant q^{(4g+2)(n+1)+\frac{n}{2}} (\deg \mathfrak{n})^{n+1}.$$

(*If* $\deg \mathfrak{n} = 0$ *then, as will be clear from the proof,* $|L(\mathrm{Sym}^n \rho, s)| \leqslant q^{(4g+2)(n+1)+\frac{n}{2}}$.)

Proof. Drinfeld's proof of the Langlands conjecture for GL(2) over function fields implies that ρ is pure of weight 0; i.e., for any place v where ρ is unramified, the images of the geometric Frobenius eigenvalues $\alpha_{1,v}$ and $\alpha_{2,v}$ under any embedding of $\overline{\mathbb{Q}}_\ell$ into $\mathbb{C}$ are of absolute value 1. The local factors of $L(\mathrm{Sym}^n \rho, s)$ at the places where ρ is unramified are easy to describe: with $\alpha_{1,v}$ and $\alpha_{2,v}$ as above we have

$$L_v(\mathrm{Sym}^n \rho, s) = \Big[(1-\alpha_{1,v}^n q_v^{-s})(1-\alpha_{1,v}^{n-1}\alpha_{2,v} q_v^{-s}) \cdots (1-\alpha_{2,v}^n q_v^{-s})\Big]^{-1},$$

where $q_v = q^{\deg v}$. Thus, for $\mathrm{Re}(s) = 1+\varepsilon$, with $\varepsilon > 0$,

$$|L_v(\mathrm{Sym}^n \rho, s)| \leqslant \zeta_{F_v}(1+\varepsilon)^{n+1},$$

where $\zeta_{F_v}(s) = (1-q_v^{-s})^{-1}$. The product $\zeta_F(s) = \prod_v \zeta_{F_v}(s)$ is the zeta function of C. The same estimate is also valid at the ramified places by [8, Lemma 1.8.1] (in fact the estimates at the ramified places are even somewhat better). Putting the local factors together we get that on the line $\mathrm{Re}(s) = 1+\varepsilon$

$$|L(\mathrm{Sym}^n \rho, s)| \leqslant \zeta_F(1+\varepsilon)^{n+1}.$$

From Grothendieck's theory of L-functions of ℓ-adic representations, $L(\mathrm{Sym}^n \rho, s)$ is an entire function [7, Section 10]; in fact it is a polynomial in q^{-s}, since we assumed ρ

is irreducible. Moreover, as we also assumed ρ to be self-dual, Grothendieck's functional equation for $L(\mathrm{Sym}^n\,\rho, s)$ takes the form

$$L(\mathrm{Sym}^n\,\rho, s) = \varepsilon(\mathrm{Sym}^n\,\rho, s) L(\mathrm{Sym}^n\,\rho, 1-s),$$

where $\varepsilon(\mathrm{Sym}^n\,\rho, s)$ is a monomial in $\mathbb{C}[q^{-s}]$. By restricting ρ to each $W_{F_v} \hookrightarrow \mathrm{Gal}(F^{\mathrm{sep}}/F)$, we obtain an ℓ-adic representation ρ_v of the local Weil group (and as was discussed in Subsection A.1, ρ_v can be thought of as a Weil–Deligne representation). We have $\mathfrak{n}(\rho) = \prod_v \mathfrak{n}(\rho_v)$, and by [17, Theorem 0.4] the global ε-factor can be decomposed as

$$\varepsilon(\mathrm{Sym}^n\,\rho, s) = \prod_v \varepsilon(\mathrm{Sym}^n\,\rho_v \otimes \omega_{1,v}^s, \psi_v, dx_{\psi_v}),$$

where $\psi = \prod_v \psi_v$ is a non-trivial character of $\mathbb{A}_F/F$. As the notation indicates $\varepsilon(\mathrm{Sym}^n\,\rho, s)$ is independent of the choice of the character ψ. As ρ and ψ are almost everywhere unramified, almost all $\varepsilon(\mathrm{Sym}^n\,\rho_v \otimes \omega_{1,v}^s, \psi_v, dx_{\psi_v})$ are equal to 1. Using Proposition A.3,

$$\begin{aligned}|\varepsilon(\mathrm{Sym}^n\,\rho, s)| &= \prod_v |\varepsilon(\mathrm{Sym}^n\,\rho_v \otimes \omega_{1,v}^s, \psi_v, dx_{\psi_v})| \\ &= q^{(\sum_v \deg(v)\cdot a((\mathrm{Sym}^n\,\rho)_v) - \dim(\mathrm{Sym}^n\,\rho)\sum_v \deg(v)\cdot \mathrm{ord}_v \mathfrak{n}(\psi_v))\cdot(\frac{1}{2}-\mathrm{Re}(s))}.\end{aligned}$$

It is well-known that $\sum_v \deg(v)\cdot \mathrm{ord}_v \mathfrak{n}(\psi_v) = 2-2g$. Thus, for $\mathrm{Re}(s) = 1+\varepsilon$,

$$|\varepsilon(\mathrm{Sym}^n\,\rho, s)| = q^{-(\sum_v \deg(v)\cdot a((\mathrm{Sym}^n\,\rho)_v) - (n+1)(2-2g))\cdot(\frac{1}{2}+\varepsilon)}.$$

Thus, by Lemma A.2

$$\begin{aligned}|\varepsilon(\mathrm{Sym}^n\,\rho, s)| &\geqslant q^{(n+1)(2-2g)(\frac{1}{2}+\varepsilon)} q^{-(n\sum_v \deg(v)\cdot a(\rho_v))(\frac{1}{2}+\varepsilon)} \\ &= q^{(n+1)(2-2g)(\frac{1}{2}+\varepsilon)} \mathcal{N}(\mathfrak{n})^{-n(\frac{1}{2}+\varepsilon)}.\end{aligned}$$

Going back to the L-function and combining the estimates, for $\mathrm{Re}(s) = 1+\varepsilon$ we have

$$|L(\mathrm{Sym}^n\,\rho, 1-s)| \leqslant q^{(n+1)(2g-2)(\frac{1}{2}+\varepsilon)} \mathcal{N}(\mathfrak{n})^{n(\frac{1}{2}+\varepsilon)} \zeta_F(1+\varepsilon)^{n+1}.$$

Since $L(\mathrm{Sym}^n\,\rho, s)$ is entire and bounded in vertical strips we can apply Rademacher's version of Phragmén–Lindelöf theorem, [24, Theorem 2], to conclude that in this vertical strip

$$|L(\mathrm{Sym}^n\,\rho, s)| \leqslant \left(q^{(g-1)(n+1)} \mathcal{N}(\mathfrak{n})^{\frac{n}{2}}\right)^{(1+\varepsilon-\mathrm{Re}(s))} \zeta_F(1+\varepsilon)^{n+1}.$$

Now assume $\deg \mathfrak{n} > 0$. Choosing $\varepsilon = (\deg \mathfrak{n})^{-1}$ the bound becomes

$$|L(\mathrm{Sym}^n \rho, s)| \leqslant q^{2g(n+1)+\frac{n}{2}} \cdot \mathcal{N}(\mathfrak{n})^{\frac{n}{2}(1-\mathrm{Re}(s))} \cdot \zeta_F(1+(\deg \mathfrak{n})^{-1})^{n+1}. \tag{A.1}$$

Recall that

$$\zeta_F(s) = \frac{P(s)}{(1-q^{-s})(1-q\cdot q^{-s})},$$

where $P(s) = \prod_{i=1}^{2g}(1-a_i q^{-s})$, with $|a_i| = \sqrt{q}$. As one easily checks

$$\zeta_F(1+\varepsilon) \leqslant 2\left(1+\frac{1}{\sqrt{q}}\right)^{2g} \frac{1}{(1-q^{-1})} \cdot \varepsilon^{-1}.$$

Combining this with (A.1), we finally get

$$|L(s, \mathrm{Sym}^n \rho)| \leqslant c \cdot \mathcal{N}(\mathfrak{n})^{\frac{n}{2}(1-\mathrm{Re}(s))} \cdot (\deg \mathfrak{n})^{n+1},$$

where c can be taken to be $q^{(4g+2)(n+1)+\frac{n}{2}}$. □

In Theorem A.4 we assumed that ρ is pure of weight 0 (see the beginning of the proof). This is not a restrictive assumption. Indeed, let G^0 be the kernel of the natural homomorphism $G = \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and let ω_1 be the quasi-character of G which is trivial on G^0 and takes value q^{-1} on the elements which map to the geometric Frobenius in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. If we are given an irreducible 2-dimensional ℓ-adic representation of G then from Lafforgue's proof of Deligne's conjecture [8, 1.2.10] ρ is pure of some integral weight w, i.e., for every place v where ρ is unramified, each eigenvalue α of $\rho(\Phi_v)$ satisfies $|\alpha_v| = q_v^{w/2}$. Now $\omega_1^{w/2} \otimes \rho$ is still irreducible but has weight 0. Since $L(\mathrm{Sym}^n(\omega_1^{w/2} \otimes \rho), s) = L(\mathrm{Sym}^n \rho, s + \frac{wn}{2})$, we can apply our theorem to this representation to deduce.

Corollary A.5. *Suppose ρ is an irreducible 2-dimensional ℓ-adic representation of G which is pure of weight w. If $\deg \mathfrak{n} > 0$ then*

$$\left|L\left(\mathrm{Sym}^n \rho, 1+\frac{nw}{2}\right)\right| \leqslant q^{(4g+2)(n+1)+\frac{n}{2}} (\deg \mathfrak{n})^{n+1},$$

and $|L(\mathrm{Sym}^n \rho, 1+\frac{nw}{2})| \leqslant q^{(4g+2)(n+1)+\frac{n}{2}}$ if ρ is everywhere unramified.

References

[1] S. Bosch, W. Lütkebohmert, Degenerating abelian varieties, Topology 30 (1991) 653–698.

[2] S. Bosch, W. Lütkebohmert, Formal and rigid geometry I, Math. Ann. 295 (1993) 291–317.
[3] S. Bosch, W. Lütkebohmert, M. Raynaud, Néron Models, Springer, Berlin, 1990.
[4] B. Conrad, Irreducible components of rigid spaces, Ann. Inst. Fourier 49 (1999) 473–541.
[5] B. Conrad, W. Stein, Component groups of purely toric quotients, Math. Res. Lett. 8 (2001) 745–766.
[6] J. Cremona, The analytic order of Ш for modular elliptic curves, J. Théor. Nombres Bordeaux 5 (1993) 179–184.
[7] P. Deligne, Les constantes des équations fonctionnelles des fonctions L, in: Modular Functions of One Variable II, Lecture Notes in Mathematics, vol. 349, Springer, Berlin, 1973, pp. 501–598.
[8] P. Deligne, La conjecture de Weil, II, Publ. Math. IHES 52 (1980) 137–252.
[9] M. Demazure, A. Grothendieck, Schémas en groupes, SGA 3, Lecture Notes in Mathematics, vols. 151–153, Springer, Berlin, 1970.
[10] V. Drinfeld, Elliptic modules, Math. Sbornik. 94 (1974) 594–627.
[11] J. Fresnel, M. van der Put, Géométrie Analytique Rigide et Applications, Birkhäuser, Basel, 1981.
[12] E.-U. Gekeler, Über Drinfeld'sche Modulkurven vom Hecke-Typ, Compositio Math. 57 (1986) 219–236.
[13] E.-U. Gekeler, Analytic construction of Weil curves over function fields, J. Théor. Nombres Bordeaux 7 (1995) 27–49.
[14] E.-U. Gekeler, Invariants of some algebraic curves related to Drinfeld modular curves, J. Number Theory 90 (2001) 166–183.
[15] E.-U. Gekeler, M. Reversat, Jacobians of Drinfeld modular curves, J. Reine Angew. Math. 476 (1996) 27–93.
[16] A. Grothendieck, M. Raynaud, D. Rim, Groupes de monodromie en géométrie algébrique, SGA 7-I, Lecture Notes in Mathematics, vol. 288, Springer, Berlin, 1972.
[17] G. Laumon, Les constantes des équations fonctionnelles des fonctions L sur un corps global de caractéristique positive, C. R. Acad. Sci. Paris Sér. I Math. 298 (1984) 181–184.
[18] L. Mai, M. Ram Murty, The Phragmén–Lindelöf theorem and modular elliptic curves, Contemp. Math. 166 (1994) 335–340.
[19] J.-F. Mestre, J. Oesterlé, Courbes de Weil semi-stables de discriminant une puissance m-ième, J. Reine Angew. Math. 400 (1989) 173–184.
[20] D. Mumford, Abelian Varieties, Oxford University Press, Oxford, 1970.
[21] M. Papikian, On the degree of modular parametrizations over function fields, J. Number Theory 97 (2002) 317–349.
[22] M. Papikian, Optimal elliptic curves, discriminants, and the degree conjecture over function fields, Ph.D. Thesis, University of Michigan, 2003.
[23] J. Pesenti, L. Szpiro, Inégalite du discriminant pour les pinceaux elliptiques à réductions quelconques, Compositio Math. 120 (2000) 83–117.
[24] H. Rademacher, On the Phragmén–Lindelöf theorem and some applications, Math. Z. 72 (1959) 192–204.
[25] J. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate Text in Mathematics, vol. 151, Springer, Berlin, 1994.
[26] A. Tamagawa, The Eisenstein quotient of the Jacobian variety of a Drinfeld modular curve, Publ. RIMS 31 (1995) 204–246.
[27] M. van der Put, A note on p-adic uniformization, Proc. Nederl. Akad. Wetensch. 90 (1987) 313–318.