COUNTING POINTS ON SURFACES IN POLYNOMIAL TIME

NITIN SAXENA AND MADHAVAN VENKATESH

To the memory of Sebastiaan Johan Edixhoven.

Abstract. We present a randomised algorithm to compute the local zeta function of a smooth, projective surface of fixed degree over $\mathbb{Q}$, at any large prime p of good reduction. Specifically, the runtime of our algorithm is polynomial in $\log p$, resolving a conjecture of Couveignes-Edixhoven. The main ingredient is an analytic, mixed characteristic method to *identify* vanishing cycles uniformly, employing the convergence bound of the Puiseux series, and the Picard-Lefschetz formula for the monodromy action on it.

Contents

1. Introduction

1.1. **Main result.** Let $X \subset \mathbb{P}^N$ be a smooth, projective, geometrically integral (properties we abbreviate to *nice*) surface of (fixed) degree D over a finite field $\mathbb{F}_q$, described by a system of homogeneous polynomial equations $f_1, \dots, f_m$ each of degree $\leq d$. We assume X is obtained via good reduction of a nice surface $\mathcal{X}$ over a number field K at a prime $\mathfrak{p} \subset \mathcal{O}_K$. We further assume the coefficients of the equations defining $\mathcal{X}$ have Weil height bounded by $H \in \mathbb{R}_{>0}$. The zeta function of X is

$$Z(X/\mathbb{F}_q, T) := \exp\left(\sum_{j=1}^{\infty} \#X(\mathbb{F}_{q^j})\frac{T^j}{j}\right).$$

Fix a prime ℓ coprime to q. From the Weil conjectures for X, we know that

$$Z(X/\mathbb{F}_q, T) = \frac{P_1(X/\mathbb{F}_q, T)P_3(X/\mathbb{F}_q, T)}{(1-T)P_2(X/\mathbb{F}_q, T)(1-q^2T)},$$

where $P_i(X/\mathbb{F}_q, T) := \det\left(1 - TF_q^\star \mid \mathrm{H}^i(X, \mathbb{Q}_\ell)\right)$ is the (reversed) characteristic polynomial of the geometric Frobenius acting on the i^{th} $\ell-$adic étale cohomology group of X. In [CE11, Epilogue], the existence of an algorithm that computes the point count $\#X(\mathbb{F}_q)$ in time polynomial in $\log q$ is conjectured. We prove this conjecture by exhibiting an algorithm that computes the action of Frobenius on the étale cohomology groups with torsion coefficients $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$, for primes $\ell = O(\log q)$, from which the zeta function of X, and thereby its point-count can be recovered by a Chinese-remainder process. Our main result is the following.

Theorem 1.1. *There exists an algorithm, that, on input X as above, outputs $Z(X/\mathbb{F}_q, T)$ in time bounded by a polynomial in $\log q$.*

Remark. This theorem is restated in more detail as Theorem 4.2 in Section 4.2 and proved therein. We further note that we consider the degree D of the surface $\mathcal{X}$, the embedding dimension N and the number of equations m defining $\mathcal{X}$ to be *fixed*. The runtime of our algorithm is polynomial in $(\log q \cdot H)$, where q is the size of the finite field and H is a bound for the heights of the coefficients of the polynomials defining $\mathcal{X}$.

1.2. **Motivation.** Our work is fundamentally motivated by the following paraphrase of a question of Serre [Ser16, Preface].

Question (Serre)**.** *Is there an algorithm that, given a $\mathbb{Z}$ – scheme $\mathcal{X}$ of finite type, computes the point count of its reduction $\#X(\mathbb{F}_p)$ at any prime p in time polynomial in $\log p$?*

In particular, this work solves the above question in the case $\dim X = 2$, when X is nice, at large enough primes of good reduction. In their monograph on computing the coefficients of the Ramanujan τ – function, Couveignes and Edixhoven [CE11, Epilogue] propose the existence of a strategy to count points on surfaces over finite fields, using the theory of Lefschetz pencils and dévissage; techniques which were used in Deligne's celebrated proof [Del74] of the Weil conjectures. If realised, this would be an extension of polynomial-time counting methods from the dimension-one case of curves (and the conceptually similar case of abelian varieties) [Sch85, Pil90] to varieties of a higher dimension.

An important motivation for these algorithms is computational evidence for conjectures in the Langlands program [Gel84], a vast philosophy encompassing several areas of modern mathematics including number theory, representation theory and algebraic geometry. An object of study in part of the program, is the $L-$function of a variety $\mathcal{X}/\mathbb{Q}$, a conglomeration of the zeta functions at all the local factors. The Langlands-Rapoport conjecture [LR87], in particular, gives the mod $-\ p$ point-counts of Shimura varieties [1] a certain group-theoretic description.

Another angle of motivation is diophantine geometry, i.e., counting or classifying rational points on a variety $\mathcal{X}/\mathbb{Q}$. One approach towards this is computing the Brauer-Manin obstruction [CTS21] (essentially measuring the failure of local-global principles) for specific varieties. This is defined using the Brauer group $\mathrm{H}^2(\mathcal{X}, \mathbb{G}_m)$ of the variety in question, which is the étale cohomology in degree two, with coefficients in the multiplicative sheaf. With a view towards the diophantine setting, it would be prudent to have algorithms for the scenario over a finite field, with constant torsion-coefficients to begin with.

1.3. **Potential applications in computing.** A fundamental aspect of our work is the explicitisation of the étale cohomology of a surface, which should be viewed as an arithmetic or discrete analogue of the usual topological or Betti cohomology over the complex numbers. The latter notions do not translate easily to the setting over a finite field, and thus required the revolution of the Grothendieck school, thereby putting the Weil conjectures in proper context.

Our work lays the stepping stones toward solving a foundational problem for topological computation in the discrete setting, i.e., over finite fields. In particular, we, for the first time, make explicit (and give algorithms to compute) the étale cohomology groups with constant torsion coefficients $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$ of a nice surface X. This generalises to being able to compute with cohomology in degrees one and two, for varieties of higher dimension as well [RSV24, KV].

The progenitor of point-counting algorithms, Schoof's algorithm [Sch85] for elliptic curves, paved the way for elliptic curve cryptography, which is ubiquitous today. In particular, it is necessary to run a point-counting algorithm to select a curve suitable for cryptosystems. It is conceivable that our algorithms may come of use in efficiently designing cryptosystems around surfaces as well. Further, Brauer groups, mentioned earlier, arise naturally in the context of class field theory and homogeneous spaces, for which a general framework has been proposed with regard to applications to cryptography [Cou06].

1.4. **Prior work & special cases.** As mentioned earlier, the first advance in point-counting over finite fields came with Schoof's algorithm for elliptic curves. This was generalised to curves of higher genus and abelian varieties by Pila [Pil90]. The cohomology groups in higher degree, however, have only recently been shown to be computable [MO15, PTvL15].

In Roy-Saxena-Venkatesh [RSV24], a randomised algorithm was given to compute the factor $P_1(X/\mathbb{F}_q, T)$ for a nice variety X of fixed degree, in time polynomial in $\log q$. Levrat has sketched a strategy to compute the full zeta function for surfaces [Lev22, IV.3.5, VI.4] (see also [Lev23, §5]) based on the description of Couveignes-Edixhoven, but its runtime is exponential.

When the characteristic p of the base field is fixed, the point-counting problem is essentially solved by Lauder-Wan [LW06] for varieties and Harvey [Har15] for general arithmetic schemes

[1] algebraic varieties equipped with rich arithmetic data

by means of $p-$adic algorithms. As opposed to using étale cohomology, they feature $p-$adic trace formulas. These algorithms, however, have a runtime exponential in $\log p$.

1.5. **Obstructions in the prior techniques.** The main difficulty in counting points on surfaces in polynomial time so far, has been the lack of a concise representation of the étale cohomology groups $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$, particularly for $i = 2$, on which the induced Frobenius action may be computed. In the approach of Levrat [Lev23], one reduces the computation of the group $\mathrm{H}^2(X, \mathbb{Z}/\ell\mathbb{Z})$ to the computation of $\mathrm{H}^1(V, \mathbb{Z}/\ell\mathbb{Z})$, where V is a curve of genus polynomial in ℓ. While algorithms are known to compute the first cohomology of curves [HI98, Cou09], their runtime is exponential in its genus. Thus for a prime ℓ of size $O(\log q)$, which is required for the intended Chinese remainder process, the above strategy ends up giving an exponential-time algorithm.

In terms of *quantum* algorithms, it is conceivable that the approach of Levrat would yield a polynomial-time quantum algorithm for surfaces of fixed degree, by running Kedlaya's quantum algorithm [Ked06] to compute the zeta function of curves, which is poly-time in the genus. However, this does not address the explicitisation of the étale cohomology groups.

Another approach would be to work directly with the Brauer group of X, whose $\ell-$torsion the group $\mathrm{H}^2(X, \mu_\ell)$ captures. Elements in the Brauer group are, a priori, equivalence classes of Azumaya algebras; but it is not clear how one may obtain bounds to represent them, along with their group law and the equivalence relation they are subjected to.

1.6. **Proof ideas.** Our algorithm studies the étale cohomology of a surface by using the formalism of monodromy of vanishing cycles arising from a Lefschetz pencil. More specifically, we fibre the given surface $\mathcal{X}$ as a Lefschetz pencil of hyperplane sections, and then blow it up at the axis, yielding a morphism to $\mathbb{P}^1$. The cohomology of the blowup $\tilde{\mathcal{X}}$, is understood using the sequence (2.5) coming from the Galois cohomology of the tame fundamental group of the line with the critical locus (i.e., the finite set $Z \subset \mathbb{P}^1$ where the fibres are nodal) removed. A serious bottleneck is the consistent representation of the cospecialisation morphisms from the cohomology of the critical fibres at all singular points to the cohomology of the generic fibre. In particular, one needs to be able to compute the pairings of vanishing cycles $\langle \delta_{z_i}, \delta_{z_j} \rangle$ for $z_i, z_j \in Z$ arising in the Picard-Lefschetz formulas (2.4) for the monodromy action on the cohomology of the generic fibre.

Our solution is to first compute the $\ell-$division polynomial system (the zero dimensional ideal whose roots are the distinct $\ell-$torsion points) for the torsion in the Jacobian of the generic fibre, and view the choice of a cospecialisation morphism at a singular point z as picking a Puiseux series expansion around z. Working in characteristic zero, we identify the vanishing cycle δ_z at z using an auxiliary smooth point u_z within the radii of convergence of the Puiseux expansions around z combined with numerical/diophantine approximation methods in a technique we call 're-centering'. Specifically, we compute the vanishing cycle as an element in the cohomology of the fibre at u_z.

However, one still seeks a common, consistent representation for all the vanishing cycles at different singular points to compute the pairings between them. This is resolved by choosing the smooth points u_j for the distinct $z_j \in Z$ all congruent modulo $\mathfrak{p}$ to the same finite field element u. This enables us to recover all the vanishing cycles in the cohomology of the fibre at u via moving to positive characteristic. Below is a high-level overview of the algorithm.

- Fibre the surface as a Lefschetz pencil. Denote by $Z \subset \mathbb{P}^1$ the subset parametrising the critical fibres and $U = \mathbb{P}^1 \setminus Z$, the smooth ones.
- Compute the ℓ – division polynomial of the Jacobian of the generic fibre of the pencil as in Algorithm 2.
- For all but one singular $z \in Z$ express the elements of $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$ using the above ℓ – division polynomial system as Puiseux series around z, by making a choice of a cospecialisation. This is done in Algorithm 4.
- Compute the vanishing cycle as an element of $\mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ for smooth u_z chosen within the radii of convergence of the Puiseux expansions around z via specialisation (Algorithm 5) using convergence properties and the Picard-Lefschetz formulas, as in Algorithm 6.
- Assume for each $z \in Z$, the associated smooth point $u_z \equiv \mathsf{u} \mod \mathfrak{p}$ for an arbitrarily chosen smooth finite field value u. Then, the vanishing cycles at the distinct singular points are all identified in $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$ via reduction to positive characteristic, as in Algorithm 7.
- Specialise the sequence (2.5) to u, compute the cohomology groups and the action of Frobenius on them. This is done in Algorithms 8 and 9.

1.7. **Leitfaden.** Section 2 delineates the cohomological preliminaries that form the fundamental basis of our algorithms. Section 3 develops subroutines including Weil pairings and Puiseux expansions for vanishing cycles, which are used in our main algorithms of Section 4. Complexity analyses of all algorithms are provided in Section 5. The appendices in order include material on recovering the zeta function, background on height theory, a recap of certain results of Igusa, and a known algorithm for computing equations of Jacobians due to Anderson.

2. Cohomological preliminaries

The aim of this section is to compile standard background material on the cohomology of the various varieties that will be required for the algorithm. We present cohomology computations when explicitly known, and point to the existence of algorithms in the curve case: smooth, nodal, and for a smooth curve over the rational function field.

2.1. **Cohomology of a surface.** In this subsection, we briefly recall cohomology computations for surfaces. A standard reference is [Mil80, V.3]. Let k be a field and let X be a surface over the algebraic closure $\overline{k}$. Following [RSV24, Algorithm 3], one may fibre X as a Lefschetz pencil $\pi : \tilde{X} \to \mathbb{P}^1$ of hyperplane sections over the projective line, where $\tilde{X}$ is the surface obtained by blowing up X at the axis Υ of the pencil. Denote $Z \subset \mathbb{P}^1$ the finite critical locus, whose corresponding fibres have exactly one node (with $\#Z = r$) and let $U = \mathbb{P}^1 \setminus Z$ be the locus of smooth fibres. Write $\mathcal{F} := R^1\pi_\star\mu_\ell$ for the constructible derived push-forward sheaf on $\mathbb{P}^1$. We note that the restriction $\mathcal{F}|_U$ is a locally constant sheaf (or local system) on U. Let $\overline{\eta} \to \mathbb{P}^1$ be a geometric generic point and let g denote the genus of the generic fibre $X_{\overline{\eta}}$, viewed as a curve over the function field of the projective line. Firstly, one recalls [Mil98, Lemma 33.2]

$$\mathrm{H}^i(\tilde{X}, \mathbb{Q}_\ell) \simeq \begin{cases} \mathrm{H}^i(X, \mathbb{Q}_\ell), \ i \neq 2; \\ \mathrm{H}^2(X, \mathbb{Q}_\ell) \oplus \mathrm{H}^0(\Upsilon \cap X, \mathbb{Q}_\ell)(-1), \ i = 2 \end{cases} \tag{2.1}$$

so it suffices to compute the zeta function of $\tilde{X}$ (see Appendix A). In Algorithm 1, we detail a method to compute equations for the blowup.

Algorithm 1 `Blowup of a surface at a point`

```
• Input: A nice surface $X \subset \mathbb{P}^N$ presented as homogeneous forms $f_1, \dots, f_m$ and a point $P \in X$. Assume without loss, $P = [0 : 0 : \dots : 1]$.
• Output: A surface $\tilde{X}$ that is the blowup of $X$ at $P$ and a morphism $\pi : \tilde{X} \to X$
Consider the projection $\varphi_P : \mathbb{P}^N \setminus P \to \mathbb{P}^{N-1}$ from $P$.
The blowup $\tilde{X}$ of $X$ at $P$ is given by the closure in $X \times \mathbb{P}^{N-1}$ of the graph of $\varphi_P$ restricted to $X \setminus P$.
Use the Segre embedding to obtain equations for $\tilde{X}$.
The morphism $\pi : \tilde{X} \to X$ is obtained by projection to the first factor.
```

Henceforth, without loss of generality, we may assume X may be fibred as $\pi : X \to \mathbb{P}^1$ as a Lefschetz pencil of hyperplane sections. From the Léray spectral sequence

$$\mathrm{H}^i(\mathbb{P}^1, R^j\pi_\star\mu_\ell) \Rightarrow \mathrm{H}^{i+j}(X, \mu_\ell),$$

one has

$$\mathrm{H}^i(X, \mu_\ell) \simeq \begin{cases} \mu_\ell, \ i = 0; \\ \mathrm{H}^0(\mathbb{P}^1, \mathcal{F}), i = 1; \\ \mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) \oplus \langle \gamma_E \rangle \oplus \langle \gamma_F \rangle, \ i = 2; \\ \mathrm{H}^2(\mathbb{P}^1, \mathcal{F}), \ i = 3; \\ \mu_\ell^\vee, \ i = 4; \\ 0, \ i > 4. \end{cases} \tag{2.2}$$

Here γ_E and γ_F are certain cycle classes on X (viewed in H^2 via the cycle class map) corresponding to the class of a section of π and the class of a smooth fibre of π respectively. One needs to work more to make the above groups explicit.

Recall the theory of *vanishing cycles* on a surface [RSV24, 3.1, 3.2]. For each $z \in Z$, one obtains a mod $-\ \ell$ vanishing cycle δ_z at z as the generator of the kernel of the map $\mathrm{Pic}^0(X_z)[\ell] \to \mathrm{Pic}^0(\widetilde{X}_z)[\ell]$ induced by the normalisation $\widetilde{X}_z \to X_z$. Using a *cospecialisation map*[2]

$$\phi_{z_j} : \mathcal{F}_{z_j} \hookrightarrow \mathcal{F}_{\overline{\eta}} \tag{2.3}$$

for each $z_j \in Z$, one obtains the subspace generated by all the vanishing cycles δ_{z_j} in $\mathcal{F}_{\overline{\eta}}$. The geometric étale fundamental group $\pi_1(U, \overline{\eta})$ acts on $\mathcal{F}_{\overline{\eta}}$, factoring through the tame quotient

[2] which depends on the choice of an embedding of the strict henselisation $\widehat{\mathcal{O}}_{\mathbb{P}^1,z} \hookrightarrow k(\overline{\eta})$, see Section 3.2

$\pi_1^{\mathrm{t}}(U,\overline{\eta})$, via the Picard-Lefschetz formulas. In particular, $\pi_1^{\mathrm{t}}(U,\overline{\eta})$ is generated topologically by $\# Z = r$ elements σ_j satisfying the relation $\prod_j \sigma_j = 1$. We have for $\gamma \in \mathcal{F}_{\overline{\eta}}$

$$\sigma_j(\gamma) = \gamma - \epsilon_j \cdot \langle \gamma, \delta_{z_j} \rangle \cdot \delta_{z_j}, \tag{2.4}$$

where $\langle \cdot, \cdot \rangle$ denotes the Weil pairing on $\mathrm{Pic}^0(X_{\overline{\eta}})[\ell]$ and for a uniformising parameter θ_j at z_j, one has $\sigma_j(\theta_j^{1/\ell}) = \epsilon_j \cdot \theta_j^{1/\ell}$. Further, σ_j is understood as the canonical topological generator for the tame inertia $I_{z_j}^{\mathrm{t}}$ at z_j (after having made consistent choices for primitive roots of unity).

One sees immediately that the monodromy [3] is symplectic, i.e., the representation

$$\rho : \pi_1^{\mathrm{t}}(U,\overline{\eta}) \longrightarrow \mathrm{GL}(2g, \mathbb{F}_\ell)$$

has image in $\mathrm{Sp}(2g,\mathbb{F}_\ell)$, the group of symplectic transformations of the vector space $\mathbb{F}_\ell^{2g}$.

Next, one recalls the following complex, [Mil80, Theorem 3.23] coming from the Galois cohomology of $\pi_1^{\mathrm{t}}(U,\overline{\eta})$

$$\mathcal{F}_{\overline{\eta}} \xrightarrow{\alpha} (\mathbb{Z}/\ell\mathbb{Z})^r \xrightarrow{\beta} \mathcal{F}_{\overline{\eta}} \tag{2.5}$$

with, for any $\gamma \in \mathcal{F}_{\overline{\eta}}$

$$\alpha(\gamma) = (\langle \gamma, \delta_{z_1} \rangle, \ldots, \langle \gamma, \delta_{z_r} \rangle)$$

and for any r − tuple $(a_1, \ldots, a_r) \in (\mathbb{Z}/\ell\mathbb{Z})^r$

$$\beta(a_1, \ldots, a_r) = a_1 \cdot \delta_{z_1} + a_2 \cdot \sigma_1(\delta_{z_2}) + \ldots + a_r \cdot \left(\prod_{j=1}^{r-1} \sigma_j \right) (\delta_{z_r}).$$

The cohomology groups of the above complex are related to the cohomology of X, i.e.,

$$\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z}) \simeq \begin{cases} \ker(\alpha), \ i = 1; \\ (\ker(\beta)/\mathrm{im}(\alpha)) \oplus < \gamma_E > \oplus < \gamma_F >, \ i = 2; \\ \mathrm{coker}(\beta), \ i = 3. \end{cases} \tag{2.6}$$

In particular, we have that $\mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) \simeq \ker(\beta)/\mathrm{im}(\alpha)$. If the situation is over a finite field, it is sufficient to compute the action of the Frobenius $F_q^\star$ on $\mathrm{H}^1(\mathbb{P}^1, \mathcal{F})$ as it acts as 'multiplication by q' on $< \gamma_E >$ and $< \gamma_F >$.

This simplification of the concerned cohomology groups lends itself to the following rough computation strategy.

- Make the cospecialisation maps $\mathcal{F}_{z_j} \hookrightarrow \mathcal{F}_{\overline{\eta}}$ explicit.
- Identify the δ_{z_j} as elements of $\mathcal{F}_{\overline{\eta}}$ consistently.
- Compute pairings in $\mathcal{F}_{\overline{\eta}}$.

This is carried out in Sections 3 and 4, using the method of Puiseux series and lifting to characteristic zero (which is where our situation arises).

[3] action of the étale fundamental group on $\mathcal{F}_{\overline{\eta}}$

2.2. **Cohomology of a smooth fibre.** Let X_u be a smooth fibre of the Lefschetz pencil $\pi : X \to \mathbb{P}^1$ at a point $u \in U$. The objective of this subsection is to state how to compute and efficiently represent the $\ell -$ torsion in the Jacobian of X_u, i.e., the group $\mathrm{Pic}^0(X_u)[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$. Algorithms for this procedure are known, see e.g., [HI98] and [Pil90]. The two are markedly different, in that the former works with the Jacobian by means of divisor arithmetic whereas the latter requires an explicit embedding of the Jacobian including equations and addition law. We use both for different applications.

Remark. Over a finite field, knowing the zeta function of X_u, an algorithm of Couveignes [Cou09, Theorem 1] also computes $\mathrm{Pic}^0(X_u)[\ell]$, but any (known) algorithm that computes $Z(X_u/\mathbb{F}_Q, T)$ in time $\mathrm{poly}(\log Q)$ also computes the $\ell -$ torsion in the Jacobian for small primes ℓ first as a subroutine.

Theorem 2.1 (Arithmetic on Jacobians via divisors)**.** *Given a curve C of genus g over an effective field k, and a divisor E on C of degree d, there exists an algorithm that computes a basis for the Riemann-Roch space $\mathcal{L}(E)$ in time*

$$\mathrm{poly}(g \cdot d).$$

Moreover, arithmetic on $\mathrm{Pic}^0(C)$ can be performed in polynomial time.

Proof. Apply [HI94] or [LGS20] for computing Riemann-Roch spaces. Divisor arithmetic on the Jacobian can be done using [KM04, KM07]. □

Theorem 2.2 (Huang-Ierardi)**.** *Let $C \subset \mathbb{P}^N$ be a smooth, projective curve of genus g over an effective field k and let ℓ be a prime coprime to the characteristic of k. There exists an algorithm to compute $\mathrm{Pic}^0(C)[\ell]$ via divisor representatives in time $\mathrm{poly}(\ell)$. If $k = \mathbb{F}_q$ is a finite field, the complexity is polynomial in $\log q$ as well.*

Proof. See [HI98, §5]. □

Theorem 2.3 (Pila)**.** *Let $C \subset \mathbb{P}^N$ be a smooth, projective curve of genus g over an effective field k and let ℓ be a prime coprime to the characteristic of k. Assume $\mathrm{Pic}^0(C) = \mathrm{Jac}(C)$ is provided as an abelian variety via homogeneous polynomial equations in $\mathbb{P}^M$ along with addition law. Then, there exists an algorithm to compute the points representing $\mathrm{Pic}^0(C)[\ell]$ in $\mathbb{P}^M$ in time polynomial in ℓ. If $k = \mathbb{F}_q$ is a finite field, the complexity is polynomial in $\log q$ as well.*

Proof. See [Pil90, §2, §3]. □

2.3. **Cohomology of a nodal fibre.** Let X_z be a nodal curve, obtained as a critical fibre of the Lefschetz pencil in the previous subsection. The objective of this subsection is to state how we may represent and compute the cohomology $\mathrm{H}^1(X_z, \mu_\ell) \simeq \mathrm{Pic}^0(X_z)[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g-1}$ concisely. Let $\widetilde{X}_z \to X_z$ be the normalisation of this nodal curve. Let $P_z \in X_z$ denote its singularity and let $D_z = Q_z + R_z$ denote the exceptional divisor on $\widetilde{X}_z$, where $Q_z, R_z \in \widetilde{X}_z$. It is possible to describe $\mathrm{Pic}^0(X_z)$ in terms of $\mathrm{Pic}^0(\widetilde{X}_z)$ and D_z. First, write

$$\mathrm{Div}_{D_z}(\widetilde{X}_z) := \mathrm{Div}(\widetilde{X}_z \setminus \{Q_z, R_z\})$$

and let $k(\widetilde{X}_z)$ denote the function field of $\widetilde{X}_z$. For $f \in k(\widetilde{X}_z)^*$, we say

$$f \equiv 1 \bmod D_z \ \text{ if } \ v_{Q_z}(1-f) \geq 1 \ \text{ and } \ v_{R_z}(1-f) \geq 1.$$

Define

$$\mathrm{Pic}^0_{D_z}(\widetilde{X}_z) := \mathrm{Div}^0_{D_z}(\widetilde{X}_z)/\langle\{\mathrm{div}(f) \mid f \equiv 1 \mod D_z\}\rangle. \tag{2.7}$$

Then, it is possible to show [Ser12, Chapter V][4] that $\mathrm{Pic}^0(X_z) \simeq \mathrm{Pic}^0_{D_z}(\widetilde{X}_z)$. In particular, we have

$$\mathrm{Pic}^0(X_z)[\ell] \simeq \mathrm{Pic}^0_{D_z}(\widetilde{X}_z)[\ell]. \tag{2.8}$$

The upshot is that we may also represent the elements (and group law) of the LHS in the isomorphism 2.8, using effective Riemann-Roch algorithms on the normalisation. In particular, one can isolate the subspace generated by the vanishing cycle at z, namely $\langle\delta_z\rangle \subset \mathrm{Pic}^0(X_z)[\ell]$, as the kernel of the natural induced map

$$\mathrm{Pic}^0_{D_z}(\widetilde{X}_z)[\ell] \longrightarrow \mathrm{Pic}^0(\widetilde{X}_z)[\ell].$$

Remark. We may compute the elements of $\mathrm{Pic}^0(X_z)[\ell]$ via specialisation to z of the ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ computing the ℓ – torsion in the generic fibre using Algorithm 2. By a result of Igusa [Igu56a, Theorem 3], we know that the $\overline{k}$ – roots of this specialisation contain the ℓ^{2g-1} torsion elements of the generalised Jacobian $\mathrm{Pic}^0(X_z)[\ell]$. The other roots correspond to singularities of the completion of the generalised Jacobian $\mathrm{Pic}^0(X_z)$ by Theorem C.3.

It requires more work to completely identify the vanishing cycle δ_z (upto sign), this is done in Section 3 using the Picard-Lefschetz formulas (2.4).

2.4. **Cohomology of the generic fibre.** As a result of the Lefschetz fibration $\pi : X \to \mathbb{P}^1$, we may think of the surface X as defining a relative curve over $k(t)$, the function field of the projective line. We refer to this notion as the 'generic fibre' of the pencil, $X_{\overline{\eta}}$. Scheme-theoretically, this corresponds to the fibre of π over a geometric generic point $\overline{\eta} \to \mathbb{P}^1$. The stalk $\mathcal{F}_{\overline{\eta}} \simeq \mathrm{Pic}^0(X_{\overline{\eta}})[\ell]$ corresponds to the ℓ – torsion in the Jacobian of this relative curve of genus g. [5]

The main objective of this subsection is to describe a zero-dimensional radical ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ over $k(t)$[6], whose $\overline{k(t)}$ – roots correspond exactly to elements of $\mathcal{F}_{\overline{\eta}}$. First, we bound the degree of this system. We know that $\mathcal{F}_{\overline{\eta}} \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ as an abelian group, so the system has ℓ^{2g} – many $\overline{k(t)}$ – roots. It remains to bound the degree of the system in t, i.e., the degree of the polynomials in t occurring as coefficients of the above system. First, we note by [RSV24, §4.2]

$$\#Z \leq D^{N+1} \quad \text{and} \quad g \leq D^2 - 2D + 1. \tag{2.9}$$

Next, denote by κ the minimal Galois extension of $\overline{k}(t)$ that all the elements of $\mathcal{F}_{\overline{\eta}}$ can be defined over. We know that the extension $\kappa/\overline{k}(t)$ has its Galois group as a subgroup of $\mathrm{Sp}(2g, \mathbb{F}_\ell)$, so in particular, its degree is bounded above by ℓ^{4g^2}. Further, we see that the system ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ when viewed as a one–dimensional scheme over $\overline{k}$ corresponds (after normalisation) to a curve V obtained by normalising the function field of U in κ. In particular, the (minimal) étale cover $V \to U$ trivialises the locally constant sheaf $\mathcal{F}|_U$ to a *constant* sheaf

[4] see also [Lev22, Lemma 2.3.8]

[5] The genus of any smooth fibre over $u \in U$ will also be g.

[6] i.e., one-dimensional over k

$\mathcal{G}$ on V. More specifically, V is a cover of $\mathbb{P}^1$ of degree bounded by ℓ^{4g^2}, tamely ramified at Z. Therefore, the product

$$\#Z \cdot \ell^{4g^2} \leq D^{N+1}\ell^{4(D+1)^4}$$

which is polynomial in ℓ, serves as an upper bound for the genus g_V of V[7]; and hence, also for the complexity of the system ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ in the variable t.

Remark. Mascot [Mas23, Algorithm 2.2] also proposes an algorithm to compute ℓ – division polynomials for the Jacobian of a curve over $\mathbb{Q}(t)$, based on (p', t) – adically lifting torsion points for a small, auxiliary prime p'. It is however mentioned [Mas23, Remark 4.3] that parts of his algorithm are not rigorous.

Algorithm 2 `Computing the` ℓ – `division ideal of` $\mathrm{Pic}^0(X_{\overline{\eta}})$

```
• Input: A Lefschetz pencil $\pi : X \to \mathbb{P}^1$.
• Output: A radical ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ over $k(t)$ whose $\overline{k(t)}$ – roots correspond to the $\ell$ – torsion points of $\mathrm{Pic}^0(X_{\overline{\eta}})$.
Compute equations for $\mathrm{Pic}^0(X_{\overline{\eta}}) = \mathrm{Jac}(X_{\overline{\eta}})$ using Theorem D.1, realising it as a subvariety of $\mathbb{P}^M$.
Compute the multiplication by $\ell$ – map as a morphism on $\mathrm{Pic}^0(X_{\overline{\eta}})$ by Theorem D.1.
Compute the equations for the pre-image of the identity element of the Jacobian.
Return the ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ so obtained.
```

Remark. Algorithm 2 also provides an algorithm to compute the ℓ – division ideal corresponding to $\mathrm{Pic}^0(X_u)$ for a smooth $u \in U$ by simply specialising ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ to u.

3. Essential subroutines

The objective of this section is to collect procedures essential to our main algorithm of computing the cohomology groups of a surface. Specifically, we recall pairing algorithms, review Puiseux series, cospecialisation at singular points, and specialisation to smooth points with the final motive of gathering all the vanishing cycles in the cohomology of a smooth fibre over a finite field.

3.1. **Pairing.**

The objective of this subsection is to define the Weil pairing on the ℓ – torsion points on the Jacobian of a curve and delineate an efficient algorithm to compute it.

Definition 3.1. *Let C be a smooth projective curve over an algebraically closed field k, let J be its Jacobian and let ℓ be a prime number. The* mod – ℓ *Weil pairing on J is a map*

$$J[\ell] \times J[\ell] \longrightarrow \mu_\ell$$

given by

$$(D_1, D_2) \mapsto \langle D_1, D_2 \rangle.$$

Let $\ell \cdot D_1 = \mathrm{div}(f)$ and $\ell \cdot D_2 = \mathrm{div}(g)$ for $f, g \in k(C)^*$. Then, $\langle D_1, D_2 \rangle = \frac{f(D_2)}{g(D_1)}$.

[7] by the Riemann-Hurwitz formula

Theorem 3.2. *There exists an algorithm, that, on input a smooth, projective curve C over $\mathbb{F}_q$, a prime number ℓ coprime to q, two ℓ – torsion divisors $D_1, D_2 \in \mathrm{Pic}^0(C)[\ell]$, computes the Weil pairing $\langle D_1, D_2 \rangle$ in time*

$$\mathrm{poly}(\log q \cdot \ell).$$

Proof. See [CF+12, §16.1] or [Cou09, Lemma 10]. □

Algorithm 3 `Computing the Weil pairing`

```
• Input: A smooth projective curve $C$ over $\mathbb{F}_q$ and two divisors $D_1, D_2 \in \mathrm{Pic}^0(C)[\ell]$.
• Output: The value $\langle D_1, D_2 \rangle \in \mu_\ell(\overline{\mathbb{F}}_q)$.
Find $f, g \in k(C)^*$ such that $\mathrm{div}(f) = \ell \cdot D_1$ and $\mathrm{div}(g) = \ell \cdot D_2$ using an effective Riemann-Roch algorithm from Theorem 2.1.
Evaluate $\frac{f(D_2)}{g(D_1)}$ using [Cou09, Lemma 10].
Return the value of $\frac{f(D_2)}{g(D_1)}$.
```

Remark. While the algorithm from [Cou09] runs with stated complexity over a finite field, it works over a number field as well, with similar dependence on ℓ. We note that for a curve C over a number field K, the ℓ – torsion is defined over an extension K' of K of degree a polynomial in ℓ as $\mathrm{Gal}(K'/K) \subset \mathrm{GL}(2g, \mathbb{F}_\ell)$, where g is the genus of C. The height of the ℓ – torsion elements is bounded, by Theorem B.4. Additionally, we note that there are also pairing algorithms running in time polynomial in ℓ that work directly with an embedding of the Jacobian of the curve. See [LR10, LR15].

3.2. **Cospecialisation at a singular fibre.** In this subsection, we indicate how to make the cospecialisation maps (2.3) from the cohomology of a special fibre to that of the generic fibre, explicit.

Let $\pi : \mathcal{X} \to \mathbb{P}^1$ be a Lefschetz pencil of hyperplane sections on a nice surface over a number field K. We fix an embedding $\overline{K} \hookrightarrow \mathbb{C}$ at the outset. Denote by $Z \subset \mathbb{P}^1$ the finite subset parametrising the critical (nodal) fibres and write $U = \mathbb{P}^1 \setminus Z$. Denote by $\mathcal{F} := R^1\pi_\star\mu_\ell$, the first derived pushforward sheaf on $\mathbb{P}^1$ and let $\overline{\eta} \to \mathbb{P}^1$ be a geometric generic point. Let $z \in Z$. Consider the strictly Henselian ring $\widehat{\mathcal{O}}_{\mathbb{P}^1,z}$. By [Mil98, Proposition 4.10], it can be understood as the elements of

$$\overline{K}[[t-z]] \cap \overline{K(t)},$$

i.e., those power series in $t - z$ which are algebraic over $\overline{K}(t)$. Let $\mathtt{K}_z$ denote a separable closure of the field of fractions of $\widehat{\mathcal{O}}_{\mathbb{P}^1,z}$. After [Mil98, §20], we know that the choice of a cospecialisation map

$$\phi_z : \mathcal{F}_z \hookrightarrow \mathcal{F}_{\overline{\eta}}$$

depends on an embedding $\mathtt{K}_z \hookrightarrow \overline{K(t)}$. We begin with the following.

Definition 3.3 (Puiseux series)**.** *Let $\mathbb{K}$ be a field. A formal Puiseux series $f(t)$ over $\mathbb{K}$ in the variable t is an expression of the form*

$$f(t) = \sum_{j \geq M}^{\infty} a_j t^{j/n}$$

for some $M \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ and $a_j \in \mathbb{K}$. The field of formal Puiseux series is denoted $\mathbb{K}\langle\langle t\rangle\rangle$. In particular, we have

$$\mathbb{K}\langle\langle t\rangle\rangle = \bigcup_{n=1}^{\infty} \mathbb{K}((t^{1/n})),$$

where $\mathbb{K}((t))$ is the field of formal Laurent series in t with coefficients in $\mathbb{K}$. It is a classical result that if $\mathbb{K}$ is algebraically closed of characteristic zero, then $\mathbb{K}\langle\langle t\rangle\rangle$ is the algebraic closure of $\mathbb{K}((t))$.

We notice that the field $\overline{K}\langle\langle t-z\rangle\rangle$ of Puiseux series in $t-z$, contains both $\mathtt{K}_z$ and a copy of $\overline{K(t)}$, so we seek to fix the stated embedding therein. We are only concerned with the finite field extension $\mathbf{K}$ of $K(t)$ that all the points of $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$ are defined over. It is the splitting field of the ℓ – division ideal ${}^{(\ell)}\mathcal{I}$ of $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})$ computed in Section 2.4. We observe

$$[\mathbf{K} : K(t)] \leq \#\mathrm{GL}(2g, \mathbb{F}_\ell), \tag{3.1}$$

where g is the genus of $\mathcal{X}_{\overline{\eta}}$. Therefore, we may write $\mathbf{K} = K(t)\,(\boldsymbol{\tau})$, where $\boldsymbol{\tau}$ is a primitive element for $\mathbf{K}/K(t)$. By (3.1), we may assume $\boldsymbol{\tau}$ has a minimal polynomial $\mu(x)$ with coefficients in $K(t)$, of degree bounded by a polynomial in ℓ. The height of the coefficients can also be assumed to be bounded by a polynomial in ℓ by Appendix B. In order to fix an embedding $\mathbf{K} \hookrightarrow \overline{K}\langle\langle t-z\rangle\rangle$, we simply pick a Puiseux series expansion λ_z of $\boldsymbol{\tau}$ in $t-z$, as a root of $\mu(x)$. This is made possible using the following classical theorem-algorithm due to Newton and Puiseux.

Theorem 3.4 (Newton-Puiseux)**.** *Let $\mu(x,t) = 0$ be a curve in $\mathbb{C}^2$. Let d_x be the degree of μ in the variable x. Then, around any $u \in \mathbb{C}$, there exist d_x many Puiseux expansions*

$$x_i(t) = \sum_{j \geq M}^{\infty} \alpha_{i,j}(t-u)^{j/N}$$

satisfying $\mu(x_i,t) = 0$. Each $x_i(t)$ converges for values of t in an open neighbourhood of u. Moreover, given a positive integer m, there exists an algorithm that outputs the first m coefficients of all the expansions of x_i in time

$$\mathrm{poly}(d_x \cdot m).$$

Proof. For the existence, see [Wal04, Theorem 2.1]. The algorithm with stated complexity is from [Wal00, Theorem 1]. □

Remark. We see that if $\lambda(t) = \sum_j \alpha_j t^{j/M}$ is an algebraic Puiseux series as a solution of $\mu(x,t) = 0$, so are its conjugates $\sum_j \alpha_j \zeta_M^{ij} t^{j/M}$, for ζ_M a primitive M^{th} – root of unity and $0 \leq i < M$. We note that there is no ambiguity in the function defined by a Puiseux series, as the function $t^{1/M}$ refers locally to a unique branch of the M^{th} – root function, and the other branches are given as conjugates by ζ_M^i. Specifically, for w a nonzero complex number written as $w = (r, \psi)$ in polar form, where $r \in \mathbb{R}_{>0}$ and $0 \leq \psi < 2\pi$, we have $w^{1/M} = (r^{1/M}, \psi/M)$.

So, for each $z \in Z$, we use Theorem 3.4 to write $\boldsymbol{\tau}$ as a Puiseux series in $t-z$, after making a choice of the series expansion to use. Essentially, this identifies $\boldsymbol{\tau}$ with a root of $\mu(x)$ over $\overline{K}\langle\langle t-z\rangle\rangle$.

This choice of embedding $\mathbf{K} \hookrightarrow \overline{K}\langle\langle t-z\rangle\rangle$ determines completely the cospecialisation map $\phi_z : \mathcal{F}_z \hookrightarrow \mathcal{F}_{\overline{\eta}}$. Following work of Igusa (Theorem C.5) we know that the elements of $\mathcal{F}_z$ can be identified as those solutions of the ℓ – torsion ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ of $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})$ as a zero-dimensional ideal over $\overline{K}(t)$, which are in fact rational over $\overline{K}((t-z))$. The other elements of $\mathcal{F}_{\overline{\eta}}$ can be represented using polynomial expressions in $\boldsymbol{\tau}$, which has in turn been identified with the Puiseux series λ_z using our embedding. We sum up our efforts in Algorithm 4.

Algorithm 4 `Computing a cospecialisation map at a singular point`

```
• Input: A singular fibre $\mathcal{X}_z$ of the Lefschetz pencil $\pi : \mathcal{X} \to \mathbb{P}^1$ for a fixed $z \in Z$.
• Output: The elements of $\mathrm{Pic}^0(\mathcal{X}_z)[\ell]$ represented as $\overline{K(t)}$ – rational points in a projective space $\mathbb{P}^M$ using convergent Puiseux series around $z$.
1: Compute the $\ell$ – division ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ of $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})$ using Algorithm 2.
2: Represent the $\ell^{2g}$ solutions of ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ over $\overline{K(t)}$ using a primitive element $\boldsymbol{\tau}$ and a zero-dimensional system solving algorithm such as [Rou99]. In particular, an element $\gamma$ of $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$ is represented as a point in $\mathbb{P}^M$ with its coordinates being polynomials in $\boldsymbol{\tau}$ with coefficients from a poly($\ell$) – degree extension of $K$. This identifies each $\gamma$ uniquely by Lemma 3.5.
3: Expand $\boldsymbol{\tau}$ as a Puiseux series $\lambda_z$ around $z$ using the algorithm from Theorem 3.4. Similarly polynomial functions in $\boldsymbol{\tau}$ also have convergent Puiseux series representations.
4: Return a representation of each $\gamma$ as a tuple
       $$[X_0^{(\gamma)}(t) : \ldots : X_M^{(\gamma)}(t)],$$
   where $X_i^{(\gamma)}(t)$ are Puiseux series in $t - z$.
```

Remark. By Theorem 3.4, all the Puiseux expansions $X_i^{(\gamma)}(t)$ converge for all t in a neighbourhood of z. In other words, they all converge for $|t-z| < \varepsilon_z$, where $\varepsilon_z \in \mathbb{R}_{>0}$ is the minimum of the radii of convergence of all the $X_i^{(\gamma)}(t)$.

Lemma 3.5. *It suffices to specify*

$$\mathrm{poly}(\ell)$$

coefficients of the Puiseux expansion of each $\gamma \in \mathcal{F}_{\overline{\eta}}$ around $z \in Z$, in order to identify it uniquely. Further, the Weil height of each coefficient is bounded by a polynomial in ℓ.

Proof. The first statement follows from [Wal00, pg 3].(See also [HS83, Theorem 4.5]). The bound for the height of the coefficients is provided by [Wal00, Theorem 1]. □

Remark. We 'store' an algebraic number α, by a pair consisting of its minimal polynomial and a floating point approximation, to distinguish α from its conjugates.

We conclude this subsection with the following.

Lemma 3.6 (Radius of convergence). *There exists a polynomial $\Psi(x) \in \mathbb{Z}[x]$, with coefficients and degree independent of ℓ, such that the common radius of convergence ε_z satisfies*

$$\varepsilon_z > \frac{1}{\exp(\Psi(\ell))}.$$

Proof. Denote by

$$\left(X_i^{(\gamma)}(t)\right)_{\gamma \in \mathcal{F}_{\overline{\eta}}}$$

the system of Puiseux expansions one obtains for the elements of $\mathcal{F}_{\overline{\eta}}$ around z. In particular, they are Laurent series in $\boldsymbol{t} = (t-z)^{1/M}$ for some M bounded by a polynomial in ℓ. Write

$$X_i^{(\gamma)}(t) = \sum_j \alpha_{i,j}^{(\gamma)} \boldsymbol{t}^j.$$

It converges on a disc $|\boldsymbol{t}| < \varepsilon_z$ where

$$\frac{1}{\varepsilon_z} = \limsup_{j \to \infty} |\alpha_{i,j}^{(\gamma)}|^{\frac{1}{j}}.$$

Applying [HM17, Corollary 4.6] [8], we see that

$$|\alpha_{i,j}^{(\gamma)}| \leq \exp\left(\Psi(\ell) \cdot j\right),$$

where $\Psi(x)$ is a polynomial with coefficients and degree independent of j and ℓ. Taking the limit gives the result.

□

3.3. **Specialisation to a smooth fibre.** Consider the setup of Section 3.2. Let $z \in Z$. In this subsection, we indicate how we may specialise elements of $\mathcal{F}_{\overline{\eta}}$ realised as Puiseux expansions around z using Algorithm 4, to elements of $\mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ for a 'nearby' smooth fibre $\mathcal{X}_{u_z}$. We recall the following.

Lemma 3.7. *Let $u \in U$. Then, any cospecialisation map*

$$\phi_u : \mathcal{F}_u \to \mathcal{F}_{\overline{\eta}}$$

is an isomorphism. Its inverse ϕ_u^{-1} associates a divisor in $\mathcal{F}_{\overline{\eta}}$ to the intersection with $\mathcal{X}_u$ of its closure in $\mathcal{X}$.

Proof. The first statement follows from the fact that $\mathcal{F}|_U$ is a locally constant sheaf on U. See [Mil80] for more details. □

Now, consider again the splitting field $\mathbf{K}$ of ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$. Under the natural embedding $\overline{K}(t) \hookrightarrow \overline{K}((t-u))$, we know that the elements of $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$ are rational over $\overline{K}((t-u))$ as the ℓ – torsion of the generic fibre is unramified at u. We show the following next.

Lemma 3.8. *The specialisation $\phi_u^{-1} : \mathcal{F}_{\overline{\eta}} \to \mathcal{F}_u$ is unique and does not depend on a $\overline{K}(t)$ – linear embedding $\overline{K(t)} \hookrightarrow \overline{K((t-u))}$.*

Proof. Consider the Jacobian $\mathcal{J}_{\overline{\eta}} = \mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})$ of $\mathcal{X}_{\overline{\eta}}$. It is an abelian variety defined over $K(t)$, and can be thought of as being defined over $K((t-u))$ in a natural way. Specialising $\mathcal{J}_{\overline{\eta}}$ to u gives the Jacobian $\mathcal{J}_u$ of $\mathcal{X}_u$ by [Igu56a]. Then, by a generalisation of Hensel's lemma [Cho02, Corollary pg 546], we know each ℓ – torsion point ρ_j of $\mathcal{J}_u$ lifts uniquely to an ℓ – torsion point ω_j of $\mathcal{J}_{\overline{\eta}}$ and ρ_j is the specialisation at u of ω_j. □

[8] see also Theorem 2.3 of loc. cit.

Lemma 3.9. *The specialisation ϕ_u^{-1} preserves the Weil pairing, i.e., for any $\gamma_1, \gamma_2 \in \mathcal{F}_{\overline{\eta}}$, we have*

$$\langle \gamma_1, \gamma_2 \rangle = \langle \phi_u^{-1}(\gamma_1), \phi_u^{-1}(\gamma_2) \rangle,$$

where the pairing on the left is the Weil pairing on $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$ *and the one on the right is the Weil pairing on* $\mathrm{Pic}^0(\mathcal{X}_u)[\ell]$.

Proof. Clear from the definition of specialisation. □

Lemma 3.10. *Let $\gamma \in \mathcal{F}_{\overline{\eta}}$, and assume we have computed*

$$\gamma = [X_0^{(\gamma)}(t) : \dots : X_M^{(\gamma)}(t)]$$

as a tuple of Puiseux series around $z \in Z$ (truncated upto $\mathrm{poly}(\ell)$ *coefficients so that any two $\gamma_1 \neq \gamma_2$ in $\mathcal{F}_{\overline{\eta}}$ can be distinguished), with respect to the cospecialisation ϕ_z. Then, for any $u_z \in U$ with $|z - u_z| < \varepsilon_z/2$, the tuple representing γ converges at u_z to the specialisation $\phi_{u_z}^{-1}(\gamma) \in \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ of γ at u_z.*

Proof. It follows from the convergence properties of the associated Puiseux series (see [Wal04, 2.2] for more details) that at u_z, γ converges to a root of the zero-dimensional ideal ${}^{(\ell)}\mathcal{I}_{u_z}$, or in other words, an ℓ torsion point $\gamma_{u_z} \in \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$. Now, as u_z is a smooth specialisation for the ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$, we may, by Lemma 3.8, uniquely Hensel-lift this point γ_{u_z} to a set of expansions

$$\phi_{u_z}(\gamma_{u_z}) = [Y_0(t) : \dots Y_M(t)]$$

where $Y_i(t) \in \overline{K}((t - u_z))$ converge in neighbourhood W of u_z. The uniqueness of the lift (i.e., cospecialisation) of γ_{u_z} implies that the tuples $[X_i^{(\gamma)}(t)]$ and $[Y_i(t)]$ represent the same analytic germs [9] on $W \cap \{u \in \mathbb{C} \mid |z - u| < \varepsilon_z/2\}$. This proves the claim.

□

We intend to use the above lemma to make the specialisation explicit. It remains to prove $\mathrm{poly}(\ell)$ – bounds to separate roots of ${}^{(\ell)}\mathcal{I}_{u_z}$ and derive the level of precision to determine which root it is that the associated expansions of γ converge to. We deal with the first item initially, using a classical result from diophantine approximation.

Lemma 3.11. *Let υ_1 and υ_2 be algebraic numbers occurring as roots of a polynomial $f(x) \in K[x]$ of degree $\mathbf{d}$ and height $\mathbf{h}$. Then*

$$|\upsilon_1 - \upsilon_2| \geq \Gamma(\mathbf{d}, \mathbf{h}) := \frac{\sqrt{3}}{(\mathbf{d}+1)^{(2\mathbf{d}+1)/2} \cdot \mathbf{h}^{\mathbf{d}-1}}.$$

Proof. See [Bug04, Corollary A.2]. □

In our context, $\mathbf{h}$ and $\mathbf{d}$ are both bounded by polynomials in ℓ. This is because for a smooth $u \in U$ of bounded height, the ℓ – division system ${}^{(\ell)}\mathcal{I}_u$ associated to $\mathrm{Pic}^0(\mathcal{X}_u)$ has degree polynomial in ℓ, and the algebraic numbers occurring as coefficients also have height bounded by a polynomial in ℓ (by Theorem B.4). Hence, we may write

$$\Gamma(\ell) := \frac{1}{\exp(\Phi(\ell))} \leq \Gamma(\mathbf{d}, \mathbf{h})$$

where $\Phi(x) \in \mathbb{Z}[x]$ is a polynomial with coefficients and degree independent of ℓ.

[9] being solutions of ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$, which are all distinct and ℓ^{2g} in number

Lemma 3.12 (Convergence-testing). *Let $\Lambda_1(t) = \sum_j \alpha_j t^{j/\ell}$ be an algebraic Puiseux series in t occurring in a tuple representing $\gamma \in \mathcal{F}_{\overline{\eta}}$ in the context of Lemma 3.10, around $z = 0$ wlog. Write $\Lambda_2(t) = \sum_j \zeta_\ell^j \alpha_j t^{j/\ell}$ for its conjugate and let u be an algebraic number of height bounded by a polynomial in ℓ, with*

$$|u|^{1/\ell} < \frac{1}{2 \cdot \exp((\Psi(\ell))}$$

such that both $\Lambda_1(t)$ and $\Lambda_2(t)$ converge at u to distinct, conjugate algebraic numbers υ_1 and υ_2 respectively. Then, it requires at most $\mathrm{poly}(\ell)$ precision to distinguish υ_1 from υ_2, i.e., to determine which series converges to which number.

Proof. Write $\mathbf{t} := t^{1/\ell}$, so we regard Λ and Λ' as power series in $\mathbf{t}$. We show firstly, that with $\mathrm{poly}(\ell)$ terms, we can approximate Λ and Λ' at u to within $\Gamma(\ell)/4$ of υ_1 and υ_2 respectively. Denote by $\lambda_1^{(m)}(\mathbf{t})$ and $\lambda_2^{(m)}(\mathbf{t})$ the m^{th} partial sums of $\Lambda_1(\mathbf{t})$ and $\Lambda_2(\mathbf{t})$ respectively. Then, applying Lemma 3.6

$$|\Lambda_1(u) - \lambda_1^{(m)}(u)| = \sum_{j>m} |\alpha_j| \cdot (|u|^{1/\ell})^j \leq \sum_{j>m} (\exp(\Psi(\ell)) \cdot u)^j \leq \sum_{j>m} \frac{1}{2^j},$$

which can clearly be made less than $\Gamma(\ell)/4$ for a value of m polynomial in ℓ. So, we have

$$|\upsilon_1 - \lambda_1^{(m)}(u)| < \Gamma(\ell)/4 \quad \text{and} \quad |\upsilon_2 - \lambda_2^{(m)}(u)| < \Gamma(\ell)/4$$

for $m \in \mathbb{Z}_{>0}$ bounded by a polynomial in ℓ. By Lemma 3.11, these truncations specify υ_1 and υ_2 uniquely and unambiguously as $|\upsilon_1 - \upsilon_2| > \Gamma(\ell)$.

□

Combining Lemmas 3.10, 3.11 and 3.12, we have shown the following.

Theorem 3.13 (Approximation). *Let $\gamma \in \mathcal{F}_{\overline{\eta}}$ and let $z \in Z$. Assume we have computed γ as a tuple $[X_0^{(\gamma)} : \ldots : X_M^{(\gamma)}(t)]$ of Puiseux expansions truncated upto $\mathrm{poly}(\ell)$ coefficients. Then, for u_z of height bounded by $\mathrm{poly}(\ell)$ such that $|z - u_z| < \varepsilon_z/2$, it is possible to determine with*

$\mathrm{poly}(\ell)$ space, time and precision complexity,

the unique specialisation $\gamma_{u_z} = \phi_{u_z}^{-1}(\gamma)$ as the tuple $[x_0 : \ldots : x_M]$ that $[X_0^{(\gamma)}(t) : \ldots : X_M^{(\gamma)}(t)]$ converges to at u_z.

□

The next task is to make the specialisation map from Lemma 3.8 explicit. Let $z \in Z$. In Algorithm 4, we obtained a representation of $\mathcal{F}_{\overline{\eta}}$ as Puiseux series around z, with the common minimal radius of convergence ε_z. In Algorithm 5, we indicate how to compute, for $\gamma \in \mathcal{F}_{\overline{\eta}}$ obtained via Puiseux series expansions around z; the specialisation $\phi_{u_z}^{-1}(\gamma) \in \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ for $u_z \in U$ such that $|z - u_z| < \varepsilon_z$.

3.4. **Computing the vanishing cycle.** The goal of this subsection is to compute the vanishing cycle δ_z for $z \in Z$, as an element in $\mathrm{Pic}^0(\mathcal{X}_{u_z})$ via specialisation, for a suitably chosen u_z. We accomplish this by use of the Picard-Lefschetz formulas (2.4).

Remark. The vanishing cycle δ_z depends on the chosen cospecialisation $\phi_z : \mathcal{F}_z \hookrightarrow \mathcal{F}_{\overline{\eta}}$. Hence, it would be more accurate to write $\phi_z(\delta_z) \in \mathcal{F}_{\overline{\eta}}$ for the vanishing cycle, but we abuse

Algorithm 5 Re-centering

```
• Input: An element $\gamma \in \mathcal{F}_{\overline{\eta}}$ represented by a tuple $[X_0^{\gamma}(t) : \dots : X_M^{(\gamma)}(t)]$ of Puiseux series around $z$ as a $\mathbf{K}$ – rational point in $\mathbb{P}^M$ (via Algorithm 4), and a smooth point $u \in U$ with $|u - z| < \varepsilon_z$.
• Output: The specialisation $\phi_{u_z}^{-1}(\gamma) \in \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$.
1: Specialise the ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ at $u_z$ to obtain the $\ell$ – division ideal ${}^{(\ell)}\mathcal{I}_{u_z}$ for $\mathrm{Pic}^0(\mathcal{X}_z)$ by Appendix C.
2: Compute the $\ell^{2g}$ distinct $\ell$ – torsion elements $\mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ via a zero-dimensional system solving algorithm ([Rou99]) applied to ${}^{(\ell)}\mathcal{I}_{u_z}$.
3: The input tuple $[X_0^{(\gamma)}(t) : \dots : X_M^{(\gamma)}(t)]$ actually converges at $u_z$ to a point $[x_0 : \dots : x_M] \in \mathrm{Pic}^0(\mathcal{X}_{u_z})$. Determine the point as a tuple of algebraic numbers by using Theorem 3.13 and matching with the points computed in Step 2.
```

notation by referring to it as just δ_z. This is because the cospecialisations ϕ_z have already been chosen or determined, as will be seen below.

As stated in Section 3.2, for $z \in Z$, the vanishing cycle $\delta_z \in \mathcal{F}_{\overline{\eta}}$ is determined uniquely upto sign by the Picard-Lefschetz formulas after picking a $\overline{K}(t)$ – embedding $\mathbf{K} \hookrightarrow \overline{K}\langle\langle t - z \rangle\rangle$. Firstly, write $Z = \{z_1, \dots, z_r\}$ as an ordered set of distinct points for $r \in \mathbb{Z}_{>0}$. We make certain preliminary simplifications following the discussion before [Mil80, Theorem 3.23].

Choose $\zeta_s := \exp(2\pi i/s)$ as a generator of $\mu_s(\overline{K})$ for each s so that $\zeta_l = \zeta_{sl}^s$. Let $I_{z_j}^{\mathrm{t}}$ denote the tame inertia group at z_j and let σ_j be its generator. We need to choose embeddings $I_{z_j}^{\mathrm{t}} \hookrightarrow \mathrm{Gal}(\overline{K(t)}/\overline{K}(t))$ in such a way that the σ_j together generate the tame fundamental group $\pi_1(U, \overline{\eta})$ and $\prod_{j=1}^r \sigma_j = 1$. This implies that we are freely permitted to choose the embeddings for $1 \leq j \leq r-1$ but the embedding for $j = r$ is decided by the others, so that

$$\sigma_r = \prod_{j=1}^{r-1} \sigma_{r-j}^{-1} \in \pi_1^{\mathrm{t}}(U, \overline{\eta}).$$

Further, for all $1 \leq j \leq r$, the canonical generator σ_j of the inertia $I_{z_j}^{\mathrm{t}}$ acts as

$$\sigma_j \left(t - z_j\right)^{1/s} = \zeta_s \left(t - z_j\right)^{1/s}.$$

What this means for us, is that the cospecialisation maps $\phi_{z_j} : \mathcal{F}_{z_j} \hookrightarrow \mathcal{F}_{\overline{\eta}}$ are determined by arbitrary embeddings for $1 \leq j \leq r-1$, but once these choices have been made, the *last cospecialisation* $\phi_{z_r} : \mathcal{F}_{z_r} \hookrightarrow \mathcal{F}_{\overline{\eta}}$ is completely determined by the previously made choices. With these simplifications, the Picard-Lefschetz formula (2.4) becomes

$$\sigma_j(\gamma) = \gamma - \langle \gamma, \delta_{z_j} \rangle \delta_{z_j} \tag{3.2}$$

for $\gamma \in \mathcal{F}_{\overline{\eta}}$ and $1 \leq j \leq r$. We now give a method, such that given $z_j \in Z$ for $1 \leq j \leq r-1$, and $u_j \in U$ with $|z_j - u_j| < \varepsilon_{z_j}$, we compute $\phi_{u_j}^{-1}(\delta_{z_j})$ as an element of $\mathrm{Pic}^0(\mathcal{X}_{u_j})[\ell]$.

Theorem 3.14. *Algorithm 6 uniquely determines the vanishing cycle at each $z \in Z \setminus \{z_r\}$, upto sign.*

Algorithm 6 `Computing the vanishing cycle`

```
  • Input: A singular point $z \in Z \setminus \{z_r\}$ and a smooth point $u_z$ such that $|z - u_z| < \varepsilon_z$.
  • Output: An element $\delta_z \in \mathcal{F}_{\overline{\eta}}$ unique upto sign, that is the vanishing cycle at $z$ with
    respect to the cospecialisation $\phi_z$ of Algorithm 4, specialised to an element of $\mathcal{F}_{u_z}$.
    In other words, the element $\phi_{u_z}^{-1}(\delta_z) \in \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ is returned.
1: Obtain a representation of $\mathcal{F}_{\overline{\eta}}$ as Puiseux series around $z$ using Algorithm 4.
2: Choose $\gamma = [X_0^{(\gamma)}(t) : \ldots : X_M^{(\gamma)}(t)] \in \mathcal{F}_{\overline{\eta}} \setminus \phi_z(\mathcal{F}_z)$. This reduces to choosing a $\gamma$ for which
   at least one of the Puiseux series $X_j^{(\gamma)}(t)$ is ramified at $z$, i.e., is a true Puiseux series
   and not in fact a Laurent series.
3: Writing
       $X_i^{(\gamma)}(t) = \sum_j \alpha_{i,j}^{(\gamma)} (t-z)^{j/\ell}$
   evaluate
       $\sigma_z(\gamma) = [X_0^{(\sigma_z(\gamma))}(t) : \ldots : X_M^{(\sigma_z(\gamma))}(t)]$
   where
       $X_i^{(\sigma_z(\gamma))}(t) = \sum_j \alpha_{i,j}^{(\gamma)} \zeta_\ell^j (t-z)^{j/\ell}.$
4: Compute the element $\phi_{u_z}^{-1}(\sigma_z(\gamma)) \in \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ using the specialisation of Algorithm 5.
5: Compute $\phi_{u_z}^{-1}(\gamma)$ using Algorithm 5.
6: Compute
       $\delta := \phi_{u_z}^{-1}(\sigma_z(\gamma)) - \phi_{u_z}^{-1}(\gamma)$
   using the explicit group law on $\mathrm{Pic}^0(\mathcal{X}_{u_z})$ (using Theorem D.1).
7: Use the inverse of the abstract Abel map of Appendix D (Algorithm 10) to represent the
   $\ell$ – torsion points $\phi_{u_z}^{-1}(\gamma)$ and $\delta$ as divisors on $\mathcal{X}_{u_z}$.
8: Use the divisorial representation in Step 7 to compute the Weil pairing
       $a := \langle \phi_{u_z}^{-1}(\gamma), \delta \rangle \in \mathbb{Z}/\ell\mathbb{Z}$
   on $\mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ using Algorithm 3.
9: Applying (3.3), compute
       $\phi_{u_z}^{-1}(\delta_z) = \pm(\sqrt{-a^{-1}}) \cdot \delta \in \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$
   via the explicit addition law (Theorem D.1), and make an arbitrary choice of sign.
10: Return $\phi_{u_z}^{-1}(\delta_z)$.
```

Proof. Let $\gamma \in \mathcal{F}_{\overline{\eta}} \setminus \phi_z(\mathcal{F}_z)$. By Section 3.2, we know that after a choice of embedding, we may write

$$\gamma = [X_0^{(\gamma)}(t) : \ldots : X_M^{(\gamma)}(t)]$$

as a tuple of Puiseux series around z, representing a $\overline{K(t)}$ – rational point of $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})$. By Theorem C.5, we know that the image $\phi_z(\mathcal{F}_z)$ is all rational over $\overline{K}((t-z))$, so in order to choose γ from outside $\mathcal{F}_z$, it suffices to ensure one associated Puiseux expansion ramifies at z.

Having chosen compatible generators ζ_s for $\mu_s(\overline{K})$, we may identify the inertia I_z^{t} at z as

$$I_z^{\mathrm{t}} \simeq \prod_{\ell' \text{ prime}} \mathbb{Z}_{\ell'}.$$

Our choice of topological generator σ_z sends $(t-z)^{1/\ell}$ to $\zeta_\ell(t-z)^{1/\ell}$, and acts termwise on the Puiseux expansions associated to γ. In this way, the action of σ_z is realised as an automorphism of $\mathcal{F}_{\overline{\eta}}$, that precisely fixes $\phi_z(\mathcal{F}_z)$. In particular, since $\gamma \notin \phi_z(\mathcal{F}_z)$, we have $\sigma_z(\gamma) \neq \gamma$. Therefore, by the Picard-Lefschetz formula (3.2), we know $\langle \gamma, \delta_z \rangle \neq 0$.

For a u_z such that $|z - u_z| < \varepsilon_z$, we know that the Puiseux series $X_i^{(\gamma)}(t)$ all converge at $t = u_z$. Further, by Section 3.3, Algorithm 5 computes the unique (and distinct) specialisations $\phi_{u_z}^{-1}(\sigma_z(\gamma))$ and $\phi_{u_z}^{-1}(\gamma)$ of γ to the $\ell-$torsion of $\mathrm{Pic}(\mathcal{X}_{u_z})$. Set

$$\delta := \phi_{u_z}^{-1}(\sigma_z(\gamma)) - \phi_{u_z}^{-1}(\gamma) = \phi_{u_z}^{-1}(\sigma_z(\gamma) - \gamma),$$

and $a := \langle \phi_{u_z}^{-1}(\gamma), \delta \rangle$. Note that a priori, $a \in \mu_\ell(\overline{K})$, but we have then taken its discrete logarithm with respect to the generator ζ_ℓ. It remains to show the following.

Lemma 3.15. *The vanishing cycle δ_z at z can be computed as*

$$\delta_z = \pm \phi_{u_z}\left((\sqrt{-a^{-1}}) \cdot \delta \right) \tag{3.3}$$

Proof. First, we see that $a \neq 0$ as an element of $\mathbb{Z}/\ell\mathbb{Z}$. Indeed,

$$a = \langle \phi_{u_z}^{-1}(\gamma), \delta \rangle = \langle \phi_{u_z}^{-1}(\gamma), \phi_{u_z}^{-1}(\sigma_z(\gamma) - \gamma) \rangle = \langle \gamma, \sigma_z(\gamma) - \gamma \rangle = \langle \gamma, \sigma_z(\gamma) \rangle \neq 0.$$

Further, we know by the Picard-Lefschetz formulas, or Appendix C, Theorem C.4 that $\phi_{u_z}(\delta) = \sigma_z(\gamma) - \gamma \ \in <\delta_z> \subset \mathcal{F}_{\overline{\eta}}$. Therefore, writing

$$c \cdot \phi_{u_z}(\delta) = \delta_z$$

for some $c \in (\mathbb{Z}/\ell\mathbb{Z})^*$, we see

$$\sigma_z(\gamma) - \gamma = -\langle \gamma, \delta_z \rangle \delta_z = -c \cdot (\langle \gamma, c \cdot \phi_{u_z}(\delta) \rangle) \cdot \phi_{u_z}(\delta) = -c^2 \cdot (\langle \gamma, \phi_{u_z}(\delta) \rangle) \cdot \phi_{u_z}(\delta) = \phi_{u_z}(\delta).$$

Equating coefficients, we have

$$a = \langle \phi_{u_z}^{-1}, \delta \rangle = \langle \gamma, \phi_{u_z}(\delta) \rangle = -c^{-2}.$$

Therefore, we see

$$c = \pm\sqrt{-a^{-1}}.$$

□

Thus, the specialised vanishing cycle $\phi_{u_z}^{-1}(\delta_z) \in \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ is computed. This completes the proof of Theorem 3.14.

□

Remark. We check that $-a$ is indeed a square in $\mathbb{Z}/\ell\mathbb{Z}$ as

$$-a = -\langle \gamma, \phi_{u_z}(\delta) \rangle = -\langle \gamma, \sigma_z(\gamma) \rangle = -\langle \gamma, -(\langle \gamma, \delta_z \rangle) \cdot \delta_z \rangle = (\langle \gamma, \delta_z \rangle)^2.$$

We emphasise again that the cospecialisations $\phi_{z_j} : \mathcal{F}_{z_j} \to \mathcal{F}_{\overline{\eta}}$ have only been made explicit for $1 \leq j \leq r-1$, as arbitrary choices were allowed for the associated embeddings $I^{\mathfrak{t}}_{z_j} \hookrightarrow \mathrm{Gal}\left(\overline{K(t)}/\overline{K}(t)\right)$. However, the final embedding $I^{\mathfrak{t}}_{z_r} \hookrightarrow \mathrm{Gal}\left(\overline{K(t)}/\overline{K}(t)\right)$ is completely determined by the previous ones, via the relation $\prod_{j=1}^{r} \sigma_j = 1$ in $\pi_1^{\mathfrak{t}}(U, \overline{\eta})$. Hence, an explicit representation of the *last vanishing cycle* δ_{z_r} and its specialisation is postponed to Section 3.5, Algorithm 7.

3.5. **Gathering the vanishing cycles.** The goal of this subsection is to demonstrate how to collect vanishing cycles at all the distinct $z \in Z = \{z_1, \ldots, z_r\}$, inside $\mathcal{F}_{\overline{\eta}}$ under a common representation. In the previous subsection, given a point $z \in Z \setminus \{z_r\}$, we worked with a $u_z \in U$ that lay within the common radius of convergence ε_z of the concerned Puiseux series around z. While this approach helped us to compute $\phi_{u_z}^{-1}(\delta_z)$ as an element of $\mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$, given another $z' \neq z$ in Z, it is not necessary that z' would lie within ε_z of z. Further, we are yet to compute the *last vanishing cycle* δ_{z_r} as well. To address both these issues, we give a strategy that involves moving to characteristic $p > 0$, and working with the prime ideal $\mathfrak{p}$ given in our input. We begin with the following.

Lemma 3.16. *Let X be the reduction of $\mathcal{X}$ modulo the input prime ideal $\mathfrak{p}$, and let $\mathbb{F}_q = \mathcal{O}_K/\mathfrak{p}$. Let $\mathsf{u} \in U(\mathbb{F}_q)$. Then for each $z \in Z$, there exists $u_z \in U$ with $|z - u_z| < \varepsilon_z$ and height $h(u_z) < \mathrm{poly}(\ell \cdot \log q)$ such that $u_z \equiv \mathsf{u} \mod \mathfrak{p}$. Moreover, u_z can be computed and effectively represented with space and time complexity*

$$\mathrm{poly}(\ell \cdot \log q).$$

Proof. By Lemma 3.6, we know that $\varepsilon_z > 1/\exp(\Psi(\ell))$, for some polynomial $\Psi(x) \in \mathbb{Z}[x]$, with coefficients independent of ℓ. Consider the localisation $R := (\mathcal{O}_K)_{(\mathfrak{p})}$ of $\mathcal{O}_K$ at the prime ideal $\mathfrak{p}$. We know that R is dense in $\mathbb{C}$ so the reduction map on the restriction

$$S := R \cap (z - \varepsilon_z, z + \varepsilon_z) \to \mathbb{F}_q$$

is still surjective. It remains to show that we can compute a pre-image of u in S, of bounded height, in polynomial time. Without loss, we show how this is done, for $z = 0$, from which the general case follows. First, lift the finite field element u to a $u \in K$ of bounded height, that maps to u under the mod– $\mathfrak{p}$ reduction map. Then, simply chose $\iota \in \mathbb{Z}_{>0}$ such that

$$u' := \frac{u}{q^{\iota} + 1} \quad \text{with} \quad |u'| < \frac{1}{\exp(\Psi(\ell))}.$$

Clearly, ι can be chosen to be at most $\mathrm{poly}(\ell \cdot \log q)$. Then, one checks that u' maps to u modulo $\mathfrak{p}$ and $|u'| < \varepsilon_0$. This u' is our candidate around $z = 0$.

□

Proposition 3.17 (Reduction to positive characteristic)**.** *Let $\mathsf{u} \in U(\mathbb{F}_Q)$. For each $z \in Z \setminus \{z_r\}$, choose $u_z \in U$ such that $|z - u_z| < \varepsilon_z$ and $u_z \equiv \mathsf{u} \mod \mathfrak{p}$. There exists an algorithm that computes the reduction isomorphism*

$$\varrho_{u_z} : \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell] \to \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$$

in time

$$\mathrm{poly}(\ell \cdot \log q).$$

Proof. For each u_z, denote by K_{u_z} the minimal field extension of K that the points of $\mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ are all defined over. It is the splitting field of the ideal ${}^{(\ell)}\mathcal{I}_{u_z}$. We know that $\mathrm{Gal}(K_{u_z}/K) \subseteq \mathrm{GL}(2g, \mathbb{F}_\ell)$, so the degree $[K_{u_z} : K]$ is bounded by a polynomial in ℓ. Denote by $\mathcal{K}$ the compositum of the fields K_{u_z} for all $z \in Z$. It follows that $[\mathcal{K} : K]$ is also bounded by a polynomial in ℓ. Since $\mathfrak{p}$ is a prime of good reduction for $\mathcal{X}$ and hence also, for each $\mathcal{X}_{u_z}$, we have that $\mathfrak{p}$ is unramified over the extension $\mathcal{K}/K$. Write $\mathcal{K} = K(\varpi)$ for a primitive element $\varpi \in \mathcal{K}$ and let f be the minimal polynomial of ϖ. Assume $\mathfrak{p}$ splits over this extension as

$$\mathfrak{p} = \prod_j \mathfrak{p}_j$$

for distinct primes $\mathfrak{p}_j \subset \mathcal{O}_{\mathcal{K}}$. If $\overline{f}$ is the reduction of f modulo $\mathfrak{p}$, it splits as

$$\overline{f} = \prod_j \overline{f}_j.$$

Now, lifting $\overline{f}_j$ arbitrarily to a polynomial f_j over K, we have that $\mathfrak{p}_j =< \mathfrak{p}, f_j(\varpi) >$. Choose a prime ideal $\mathfrak{p}_1|\mathfrak{p}$ in this manner, by factoring $\overline{f}$ over a finite field.[10]

Having chosen a prime $\mathfrak{p}_1$ lying above $\mathfrak{p}$, we can now make the promised map ϱ_{u_z} explicit and consistent across the different u_z. For a tuple $\omega = [x_0 : \ldots : x_M] \in \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$, its image $\varrho_{u_z}(\omega)$ is given by the tuple $[\overline{x}_0 : \ldots : \overline{x}_M]$ where $\overline{x}_j = x_j \mod \mathfrak{p}_1$. □

We observe next the following, to provide a complete picture of the situation, when reducing to positive characteristic.

Lemma 3.18. *Consider now the positive-characteristic Lefschetz pencil $\pi : X \to \mathbb{P}^1_{\overline{\mathbb{F}}_q}$. Let $\overline{\xi} \to \mathbb{P}^1_{\overline{\mathbb{F}}_q}$ be the geometric generic point, and $X_{\overline{\xi}}$ the corresponding generic fibre. Then, the diagram of isomorphisms for $z \in Z \setminus \{z_r\}$*

$$\begin{tikzcd}
\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell] \arrow[r, "\phi_{u_z}^{-1}"] \arrow[d, "\varrho_{\overline{\eta}}"'] & \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell] \arrow[d, "\varrho_{u_z}"] \\
\mathrm{Pic}^0(X_{\overline{\xi}})[\ell] \arrow[r, "\varphi_{\mathsf{u}}^{-1}"] & \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]
\end{tikzcd}$$

commutes, where $\varrho_{\overline{\eta}}$ is the $\mathrm{mod} - \mathfrak{p}_1$ *reduction map on the generic fibres and $\varphi_{\mathsf{u}}^{-1}$ is the specialisation to* u.

Proof. The fact that the maps are isomorphisms follows from the proper-smooth base change theorem. The commutativity of the diagram follows from the construction of the reduction maps. □

Theorem 3.19. *Algorithm 7 collects the images of all the vanishing cycles $\delta_z \in \mathcal{F}_{\overline{\eta}}$ consistently in* $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$.

[10] which can be done in randomised polynomial time

Algorithm 7 `Collecting all the vanishing cycles` δ_z `for each` $z \in Z$.

```
  • Input: A smooth point $\mathsf{u} \in U(\mathbb{F}_Q)$.
  • Output: For each $z_j \in Z$, the elements $\varrho_{u_j}(\phi_{u_j}^{-1}(\delta_{z_j})) \in \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$.
1: For each $z_j \in Z \setminus \{z_r\}$, choose $u_j \equiv \mathsf{u} \mod \mathfrak{p}$ such that $|z_j - u_j| < \varepsilon_j/2$, where $\varepsilon_j$ is
   the minimum radius of convergence of all Puiseux expansions associated to $\mathcal{F}_{\overline{\eta}}$ around
   $z_j$ using Lemma 3.16.
2: Compute $\phi_{u_j}^{-1}(\delta_{z_j})$ as an element of $\mathrm{Pic}^0(\mathcal{X}_{u_j})[\ell]$ using Algorithm 6.
3: Obtain the reduction $\varrho_{u_j}\left(\phi_{u_j}^{-1}(\delta_{z_j})\right) \in \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$ using Proposition 3.17 to compute
   the reduction maps
       $\varrho_{u_j} : \mathrm{Pic}^0(\mathcal{X}_{u_j})[\ell] \to \mathrm{Pic}^0(X_{\mathsf{u}})[\ell].$
4: Return
       $\overline{\delta}_{z_j} := \varrho_{u_j}(\phi_{u_j}^{-1}(\delta_{z_j}))$
   for $1 \leq j \leq r-1$.
5: It remains to compute the last vanishing cycle $\overline{\delta}_{z_r}$. Our strategy is to mimic Step 9 of
   Algorithm 6. Pick an element $\vartheta \in \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$ randomly.
6: Compute $\sigma_r(\vartheta)$ using the fact that $\sigma_r = \prod_{j=1}^{r-1} \sigma_{r-j}^{-1}$, where $\sigma_j^{-1}$ acts on $\vartheta$ as
   (3.4)    $\sigma_j^{-1}(\vartheta) = \vartheta + \langle \vartheta, \overline{\delta}_{z_j} \rangle \overline{\delta}_{z_j}.$
   Perform arithmetic on $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$ using the explicit addition law (Theorem D.1), and
   compute pairings using divisorial notation (after inverting the abstract Abel map using
   Algorithm 10) via Algorithm 3.
7: If $\sigma_r(\vartheta) = \vartheta$ return to Step 5 and choose another $\vartheta$. Otherwise, compute $\nu := \sigma_r(\vartheta) - \vartheta \neq$
   $0$ and $b := \langle \vartheta, \nu \rangle$.
8: Compute
       $\overline{\delta}_{z_r} = \pm(\sqrt{-b^{-1}}) \cdot \nu \in \mathrm{Pic}^0(X_{\mathsf{u}})[\ell],$
   and make a choice of sign.
9: Return $\overline{\delta}_{z_r}$.
```

Proof. The correctness of Steps 1-4 of Algorithm 7 is guaranteed by the commutativity of the diagram in Lemma 3.18. We address now the correctness of the computation of the image of the final vanishing cycle δ_{z_r}. Let σ_r be a generator of the local inertia $I_{z_r}^{\mathrm{t}}$. We note firstly that the embeddings $I_{z_j}^{\mathrm{t}} \hookrightarrow \mathrm{Gal}\left(\overline{K(t)}/\overline{K}(t)\right)$ must be in such a way that the σ_j all together topologically generate the tame fundamental group $\pi_1^{\mathrm{t}}(U, \overline{\eta})$ and satisfy $\prod_{j=1}^{r} \sigma_j = 1$.

This allows us freedom to choose the initial cospecialisations ϕ_{z_j} for $1 \leq j \leq r-1$ arbitrarily as we have done so. We bypass computation of the last cospecialisation as we already have a description of the action of σ_r, in terms of the other σ_j. This then boils down to being able to compute pairings with the other δ_{z_j} for $1 \leq j \leq r-1$, which we have consistently obtained in $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$.

In Step 5, an arbitrary element $\vartheta \in \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$ is unfixed by σ_r with probability $1 - 1/\ell$. This can be tested, as the computation of the action of σ_r is at our disposal. Having chosen

ϑ unfixed by σ_r, the exact computation of the image of δ_{z_r} (up to sign) follows, in the same manner as in the proof of Theorem 3.14 (and Lemma 3.15).

□

4. Computing cohomology

4.1. **Passage to positive characteristic.** Continuing with the notations of the previous section, we observe the following.

Theorem 4.1. *Consider the sequence*

$$\mathrm{Pic}^0(X_{\mathsf{u}})[\ell] \xrightarrow{\overline{\alpha}} (\mathbb{Z}/\ell\mathbb{Z})^r \xrightarrow{\overline{\beta}} \mathrm{Pic}^0(X_{\mathsf{u}})[\ell] \tag{4.1}$$

with, for any $\gamma \in \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$

$$\overline{\alpha}(\gamma) = (\langle \gamma, \overline{\delta}_{z_1} \rangle, \dots, \langle \gamma, \overline{\delta}_{z_r} \rangle)$$

and for any r *– tuple* $(a_1, \dots, a_r) \in (\mathbb{Z}/\ell\mathbb{Z})^r$

$$\overline{\beta}(a_1, \dots, a_r) = a_1 \cdot \overline{\delta}_{z_1} + a_2 \cdot \sigma_1(\overline{\delta}_{z_2}) + \dots + a_r \cdot \left(\prod_{j=1}^{r-1} \sigma_j \right) (\overline{\delta}_{z_r}).$$

Then, the cohomology groups are

$$\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z}) \simeq \begin{cases} \ker(\overline{\alpha}), \;\; i = 1; \\ \big(\ker(\overline{\beta})/\mathrm{im}(\overline{\alpha})\big) \oplus < \overline{\gamma}_E > \oplus < \overline{\gamma}_F >, \;\; i = 2; \\ \mathrm{coker}(\overline{\beta}), \;\; i = 3. \end{cases} \tag{4.2}$$

Proof. This follows from the results in Section 2.1, the proper-smooth base change theorem and the fact that pairings are invariant under specialisation. □

4.2. **Algorithms.** In this subsection, we state and prove our main result.

Theorem 4.2 (Main theorem)**.** *Let $X \subset \mathbb{P}^N$ be a nice surface of fixed degree D over a finite field $\mathbb{F}_q$, obtained via good reduction from a nice surface $\mathcal{X}$ defined over a number field K at a prime $\mathfrak{p} \subset \mathcal{O}_K$. Further, assume the coefficients of the equations defining $\mathcal{X}$ have Weil–height bounded by $H \in \mathbb{R}_{>0}$ and write $\Delta = [K : \mathbb{Q}]$. Then, there exists a randomised algorithm that outputs*

- *on input a prime number ℓ coprime to q, the étale cohomology groups* $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$ *for $0 \leq i \leq 4$ along with the Frobenius action in time*
$$\mathrm{poly}(\ell \cdot H \cdot \Delta)$$
- *the zeta function $Z(X/\mathbb{F}_q, T)$, and the point-count $\#X(\mathbb{F}_q)$ in time*
$$\mathrm{poly}(\log q \cdot H \cdot \Delta).$$

Proof. Using Theorem 4.1, we see that Algorithm 8 outputs the first cohomology and Algorithm 9 outputs the second and third cohomology groups (all with Galois actions). The Galois action on the zeroth and fourth cohomology groups is computed trivially. The runtime of the algorithms as stated is proved in Section 5. The zeta-function and point count are recovered from the cohomology groups by Appendix A. □

[11] may need to take an extension $\mathbb{F}_Q/\mathbb{F}_q$ to ensure a smooth fibre actually exists

Algorithm 8 Computing $\mathrm{H}^1(X, \mathbb{Z}/\ell\mathbb{Z})$

```
• Input: A smooth projective surface $\mathcal{X} \subset \mathbb{P}^N$ of degree $D$ over a number field $K$ presented as a system of homogeneous polynomials of degree $\leq d$, a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ of good reduction and a prime number $\ell$ coprime to $p$ and of size $O(\log q)$, where $q = \#(\mathcal{O}_K/\mathfrak{p})$. Call $X$ the reduction of $\mathcal{X}$ modulo the ideal $\mathfrak{p}$.
• Pre-processing: Fibre $\mathcal{X}$ as a Lefschetz pencil $\pi : \mathcal{X} \to \mathbb{P}^1$. Let $Z \subset \mathbb{P}^1$ parametrise the singular fibres and $U = \mathbb{P}^1 \backslash Z$ the smooth ones. Embed the Jacobian of the generic fibre $\mathcal{X}_{\overline{\eta}}$ into $\mathbb{P}^M$ obtaining the $\ell$ – torsion $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$ as the $\overline{K(t)}$ – roots of the ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ using Algorithm 2. Pick a $\mathsf{u} \in U(\mathbb{F}_Q)$ [11] which is a smooth fibre of the reduced pencil $\pi : X \to \mathbb{P}^1_{\overline{\mathbb{F}}_q}$.
• Output: $\mathrm{H}^1(X, \mathbb{Z}/\ell\mathbb{Z})$ presented as an $\mathbb{F}_\ell$ – vector space with basis and $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_Q)$ – action.
1: For each $z \in Z$, compute the images $\overline{\delta}_z \in \mathrm{Pic}^0(X_\mathsf{u})[\ell]$ of the vanishing cycle $\delta_z$ using Algorithm 7.
2: Recall the sequence (4.1). This involves arithmetic over $\mathrm{Pic}^0(X_\mathsf{u})[\ell]$ which can be performed using the explicit addition law on $\mathrm{Pic}^0(X_\mathsf{u})$ provided by Appendix D, Theorem D.1.
3: Compute the map $\overline{\alpha}$ as follows. For each $\gamma \in \mathrm{Pic}^0(X_\mathsf{u})[\ell]$ and each $\overline{\delta}_z$, compute their inverse images of the abstract Abel map to obtain divisorial representations. Then compute the Weil pairings $\langle \gamma, \overline{\delta}_z \rangle$ using Algorithm 3.
4: A priori the output of a pairing is an element in $\mu_\ell(\overline{\mathbb{F}}_Q)$, which can then be identified with an element in $\mathbb{Z}/\ell\mathbb{Z}$ by taking the discrete logarithm with respect to the modulo $\mathfrak{p}_1$ generator $\overline{\zeta}_\ell$ as the image of $\zeta_\ell$ under the reduction map.
5: Determine the $\gamma \in \mathrm{Pic}^0(X_\mathsf{u})[\ell]$ which lie in $\ker(\overline{\alpha})$ by obtaining the images of the corresponding divisor representatives via the abstract Abel map.
6: Choose a basis of $\ker(\overline{\alpha})$ as an $\mathbb{F}_\ell$ – vector space and determine the action of the $F_Q$ – Frobenius on it as an $\mathbb{F}_\ell$ – matrix $M_1$, by evaluating it on the coordinates and expressing the result in terms of the basis chosen.
7: Compute the characteristic polynomial of $M_1$ and return it. This is in fact
       $$\det\left(1 - TF_Q^\star \mid \mathrm{H}^1(X, \mathbb{Z}/\ell\mathbb{Z})\right).$$
```

5. Complexity analyses

In this section, we prove the upper bounds for the complexities stated of the subroutines used in the earlier sections. We do not deduce the exact complexities beyond showing that they are bounded by polynomial functions of ℓ and $\log q$. We also keep track of the heights of the algebraic numbers involved in the computations.

5.1. **Algorithms of Section 2.**

Noting that the complexity of Algorithm 1 is independent of ℓ, we begin with the following.

Lemma 5.1. *Algorithm 2 runs in time* $\mathrm{poly}(\ell)$.

Proof. Pila [Pil90, §2] shows that the data representing the multiplication by ℓ map is bounded by a polynomial in ℓ. Further, the coefficients occurring in the ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ have

Algorithm 9 `Computing` $\mathrm{H}^2(X, \mathbb{Z}/\ell\mathbb{Z})$ `and` $\mathrm{H}^3(X, \mathbb{Z}/\ell\mathbb{Z})$

```
• Input: A smooth projective surface $\mathcal{X} \subset \mathbb{P}^N$ of degree $D$ over a number field $K$
  presented as a system of homogeneous polynomials of degree $\leq d$, a prime ideal
  $\mathfrak{p} \subset \mathcal{O}_K$ of good reduction and a prime number $\ell$ coprime to $p$ and of size $O(\log q)$,
  where $q = \#(\mathcal{O}_K/\mathfrak{p})$. Call $X$ the reduction of $\mathcal{X}$ modulo the ideal $\mathfrak{p}$.
• Pre-processing: Fibre $\mathcal{X}$ as a Lefschetz pencil $\pi : \mathcal{X} \to \mathbb{P}^1$. Let $Z \subset \mathbb{P}^1$ parametrise
  the singular fibres and $U = \mathbb{P}^1 \backslash Z$ the smooth ones. Embed the Jacobian of the generic
  fibre $\mathcal{X}_{\overline{\eta}}$ into $\mathbb{P}^M$ obtaining the $\ell$ – torsion $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$ as the $\overline{K(t)}$ – roots of the ideal
  ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ using Algorithm 2. Pick a $\mathsf{u} \in U(\mathbb{F}_Q)$ which is a smooth fibre of the reduced
  pencil $\pi : X \to \mathbb{P}^1_{\overline{\mathbb{F}}_q}$.
• Output: $\mathrm{H}^2(X, \mathbb{Z}/\ell\mathbb{Z})$ and $\mathrm{H}^3(X, \mathbb{Z}/\ell\mathbb{Z})$ presented as $\mathbb{F}_\ell$ – vector spaces with bases
  and $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_Q)$ – action.
1: Continuing from Algorithm 8, we work with (4.1). Compute the map $\overline{\beta}$ using arithmetic
   on $\mathrm{Pic}^0(X_{\mathsf{u}})$ on the codomain. The action of each $\sigma_j$ is computed using the Picard-
   Lefschetz formula (3.2). Pairings as usual are computed by moving to divisorial notation.
2: List the elements of $\ker(\overline{\beta})$ by computing which elements map to the neutral element of
   $\mathrm{Pic}^0(X_{\mathsf{u}})$ under $\overline{\beta}$ in Step 1.
3: List the elements of $\mathrm{im}(\overline{\alpha})$ by computing the pairings
       $$\left(\langle \gamma, \overline{\delta}_{z_1} \rangle, \ldots, \langle \gamma, \overline{\delta}_{z_r} \rangle\right)$$
   for each $\gamma \in \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$ using the abstract Abel map (Algorithm 10) and Algorithm 3.
4: Construct a basis $(\omega_j)$ for the quotient $\ker(\overline{\beta})/\mathrm{im}(\overline{\alpha})$, and identify a tuple $(a_1, \ldots, a_r) \in$
   $(\mathbb{Z}/\ell\mathbb{Z})^r$ with the tuple
       $$\left((\overline{\zeta}_\ell)^{a_1}, \ldots, (\overline{\zeta}_\ell)^{a_r}\right),$$
   as elements in $\overline{\mathbb{F}}_q$.
5: Compute the action of the Frobenius $F_Q^\star$ as follows
       $$F_Q^\star(a_1, \ldots, a_r) = \overline{Q} \cdot (a_1, \ldots, a_r),$$
   where $\overline{Q} = Q \mod \ell$. Express $F_Q^\star(\omega_j)$ as an $\mathbb{F}_\ell$ – linear combination of the basis elements
   and thereby compute the action of $F_Q^\star$ as a matrix $M_2$.
6: Return the characteristic polynomial of the matrix $M_2$. This is in fact
       $$\det\left(1 - TF_Q^\star \mid \mathrm{H}^1(\mathbb{P}^1, R^1\pi_\star\mathbb{Z}/\ell\mathbb{Z})\right).$$
7: List the elements of $\mathrm{im}(\overline{\beta}) \subseteq \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$, using the computation of the map $\overline{\beta}$ in Step 1.
8: Choose a basis of representatives of $\mathrm{coker}(\overline{\beta}) = \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]/\mathrm{im}(\overline{\beta})$ as an $\mathbb{F}_\ell$ – vector
   space, and evaluate the Frobenius $F_Q^\star$ coordinate-wise. Express the result in terms of the
   basis chosen, performing zero-tests with knowledge of which elements belong in $\mathrm{im}(\overline{\beta})$
   due to Step 7. This obtains the action of $F_Q^\star$ on $\mathrm{coker}(\overline{\beta})$ as an $\mathbb{F}_\ell$ – matrix $M_3$.
9: Return the characteristic polynomial of $M_3$. This is in fact
       $$\det\left(1 - TF_Q^\star \mid \mathrm{H}^3(X, \mathbb{Z}/\ell\mathbb{Z})\right).$$
```

height bounded by a polynomial in ℓ due to Theorem B.4 and the fact that the Faltings height of the (normalisation of the) curve ${}^{(\ell)}\mathfrak{C}$ over K given by ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ is bounded by a polynomial in ℓ [Jav14, Theorem 6.0.6].

□

5.2. **Algorithms of Section 3.**

Lemma 5.2. *Algorithm 4 runs in time* $\mathrm{poly}(\ell)$*.*

Proof.

- Step 1: The complexity of Algorithm 2 has been shown to be polynomial in ℓ.
- Step 2: Zero-dimensional system solving can be done using a primitive element in time polynomial in the degree of the system by [Rou99].
- Step 3: Computing the first m coefficients of a branch can be done in $\mathrm{poly}(m)$ time by Theorem 3.4. It suffices to compute the first $\mathrm{poly}(\ell)$ coefficients to uniquely specify a branch by Lemma 3.5.
- Step 4: Once a choice of Puiseux series for $\boldsymbol{\tau}$ is made, simple arithmetic (addition, squaring) can be performed using it in polynomial time.

□

Lemma 5.3. *Algorithm 5 runs in time* $\mathrm{poly}(\ell)$*.*

Proof.

- Step 1: Specialisation of the ideal ${}^{(\ell}\mathcal{I}_{\overline{\eta}}$ to u mearly involves making the substitution $t = u$.
- Step 2: The specialised ideal ${}^{(\ell)}\mathcal{I}_u$ is now zero-dimensional over $\overline{K}$ and its roots can be found by a system solver [Rou99]. The Weil height of the $\ell-$ torsion points is bounded by a polynomial in ℓ by Theorem B.4.
- Step 3: Convergence to an algebraic number with $\mathrm{poly}(\ell)$ precision is guaranteed by Theorem 3.13.

□

Lemma 5.4. *Algorithm 6 runs in time* $\mathrm{poly}(\ell)$*.*

Proof.

- Step 1: Follows from the complexity of Algorithm 4.
- Step 2: An element $\gamma \in \mathcal{F}_{\overline{\eta}} \setminus \phi_z(\mathcal{F}_z)$ can be chosen by ensuring that at least one of the tuple of Puiseux expansions associated to γ is ramified at z, i.e., is in fact belongs to $\overline{K}\langle\langle t-z\rangle\rangle \setminus \overline{K}((t-z))$.
- Step 3: As each Puiseux expansion is specified only upto the first $\mathrm{poly}(\ell)$ coefficients by Lemma 3.5, one has to simply multiply each (non-constant) coefficient by a power of ζ_ℓ.
- Steps 4 & 5: The complexity follows from that of Algorithm 5.
- Step 6: The addition of the group law can be performed efficiently by Theorem D.1.
- Step 7: The complexity of computing the abstract Abel map and its inverse (Algorithm 10) is given by Theorem D.1.
- Step 8: Pairings can be computed in polynomial time using a divisorial description by Algorithm 3.

- Step 9: Square root over $\mathbb{Z}/\ell\mathbb{Z}$ can be found in randomised polynomial time.

□

Lemma 5.5. *Algorithm 7 runs in time* $\mathrm{poly}(\ell \cdot \log q)$.

Proof.

- Step 1: For $z_j \in Z$, a u_j with $u_j \equiv \mathsf{u} \mod \mathfrak{p}$ and $|z_j - u_j| < \varepsilon_z$ can be found by Lemma 3.16 with $\mathrm{poly}(\ell)$ precision.
- Step 2: Follows from the complexity of Algorithm 5.
- Steps 3 & 4: The reduction maps ϱ_{u_j} can be computed in time $\mathrm{poly}(\ell \cdot \log q)$ by Proposition 3.17.
- Step 5: If an element $\vartheta \in \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$, the probability that it is unfixed by σ_r is $1 - 1/\ell$.
- Step 6: The action of σ_r can be computed by computing the action of the σ_j^{-1} for $1 \leq j \leq r-1$. The action of the product $\sigma_r = \prod_j^{r-1} \sigma_{r-j}^{-1}$ is computed iteratively using the formula (3.4).
- Step 7: The complexity is $\mathrm{poly}(\ell \cdot \log q)$ following from the complexity of the explicit addition law on $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$ (Theorem‘ D.1), the pairing of Algorithm 3 and the abstract Abel map of Algorithm 10.
- Step 8: Again, computing a square root over $\mathbb{Z}/\ell\mathbb{Z}$ can be done in randomised polynomial time. Computing $\overline{\delta}_{z_r}$ reduces to addition on $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$, which is also poly-time.

□

5.3. **Algorithms of Section 4.**

Lemma 5.6. *Algorithm 8 runs in time* $\mathrm{poly}(\ell \cdot \log q)$.

Proof.

- Step 1: Follows from the complexity of Algorithm 7.
- Step 2: Arithmetic on $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$ is poly-time.
- Step 3: The inverse of the abstract Abel map is computed using Algorithm 10, which runs in polynomial time. Pairings are computed in poly-time by Alorithm 3.
- Step 4: A discrete logarithm can be computed in $\mathbb{Z}/\ell\mathbb{Z}$ by brute force in $\mathrm{poly}(\ell)$ time.
- Step 5: The complexity of computing $\overline{\alpha}$ is dominated by that of computing pairings in $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$, which is poly-time. The abstract Abel map (Algorithm 10) is computed in polynomial time. The elements of $\ker(\overline{\alpha})$ are at most ℓ^{2g} in number and can be listed one by one.
- Step 6: The Frobenius F_Q is evaluated on an ℓ – torsion point $\omega \in \mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$ coordinate-wise via repeated squaring. The output $F_Q(\omega)$ can be written uniquely in terms of the chosen basis in $\mathrm{poly}(\ell)$ – time even by a brute force trial-and-error search using arithmetic on $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$.
- Step 7: The matrix M_1 representing the linear map F_Q on $\ker(\overline{\alpha})$ is of size at most $2g \times 2g$ with entries in $\mathbb{F}_\ell$. Computing its characteristic polynomial can be done in polynomial time.

□

Lemma 5.7. *Algorithm 9 runs in time* $\mathrm{poly}(\ell \cdot \log q)$.

Proof.

- Steps 1 & 2: The kernel of $(\overline{\beta})$ can be computed by writing down its action on each $r-$tuple element in $(\mathbb{Z}/\ell\mathbb{Z})^r$, and seeing which elements map to the neutral element in $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$. The map $\overline{\beta}$ itself is computed using the Picard-Lefschetz formulas, which boils down to arithmetic and pairings on $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$.
- Step 3: Computation of the map $\overline{\alpha}$ has been discussed in the previous lemma.
- Step 4: A basis for the quotient $\ker(\overline{\beta})/\mathrm{im}(\overline{\alpha})$ can be constructed by simply taking the reduction of a basis $\ker(\overline{\beta})$ and removing redundant elements. Testing linear dependence in $\ker(\overline{\beta})/\mathrm{im}(\overline{\alpha})$ reduces to testing zero-ness there, and hence membership in $\mathrm{im}(\overline{\alpha})$, which is done in polynomial time by simple list of all its elements.
- Step 5: The action of the Frobenius $F_Q^\star$ is obtained by coordinate-wise multiplication by $\overline{Q} := Q \mod \ell$ on $\ker(\overline{\beta})/\mathrm{im}(\overline{\alpha})$. We choose a basis and compute the action of $F_Q^\star$ with respect to this basis as a matrix M_2, while testing linear independence as in Step 4.
- Step 6: This step computes the characteristic polynomial of a matrix whose dimension is independent of ℓ, and has entries in $\mathbb{F}_\ell$. Clearly this can be done in polynomial time.
- Step 7: The map $\overline{\beta}$ was computed in Step 1. Here, we simply list the elements of its image, which are at most ℓ^{2g} in number.
- Step 8: A basis for the quotient $\mathrm{coker}(\overline{\beta})$ can be chosen simply by picking a basis of $\mathrm{Pic}^0(X_{\mathsf{u}})[\ell]$ and discarding redundant elements, i.e., those which become linearly dependent modulo $\mathrm{im}(\overline{\beta})$. Zero-tests can be performed in $\mathrm{coker}(\overline{\beta})$ using the list of elements in $\mathrm{im}(\overline{\beta})$ computed in Step 7. The Frobenius $\mathbb{F}_Q^\star$ is evaluated on a basis akin to Step 6 of Algorithm 8, coordinate-wise via repeated squaring. The result of the action of $F_Q^\star$ on a basis is re-written in terms of the basis using linear dependence testing in $\mathrm{coker}(\overline{\beta})$, which reduces to a question of membership in $\mathrm{im}(\overline{\beta})$, which we know is in polynomial time. Denote by M_3 the matrix obtained as a result of $\mathbb{F}_Q^\star$ acting on $\mathrm{coker}(\overline{\beta})$ with respect to the basis chosen.
- Step 9: The characteristic polynomial of M_3 is returned. Here M_3 is a matrix of size at most $2g \times 2g$ with entries in $\mathbb{F}_\ell$, so this step is accomplished in polynomial time as well.

□

6. Conclusion

In this article, we have provided an algorithm to compute the number of points on a nice surface (of fixed degree) in polynomial time, having made its étale cohomology groups explicit. An area for improvement would be the dependence on the degree of the total complexity, which is, at the moment, multiply exponential. In another direction, one could ask if in the realm of *quantum* algorithms, the dependence on the degree could be made polynomial.

The immediate next question, with regard to point counting, is that of algorithms for varieties of a higher dimension, to begin with, threefolds. The techniques described in this paper (particularly that of Puiseux expansions to realise the cospecialisation maps) use crucially the fact that the first cohomology is an abelian scheme, i.e., can be described by solutions to polynomial equations. This does not continue to hold for the second cohomology, so it appears that new inputs are needed.

Acknowledgements

We thank Jean-Pierre Serre for comments on an earlier draft, particularly with regard to his question from [Ser16]. We thank Joe Silverman and Robin de Jong for pointing us to the literature on heights. We thank Robin de Jong for detailed comments on an earlier draft, that has significantly improved our exposition. We are grateful to T.N. Venkataramana, Arvind Nair and Kiran Kedlaya for discussions, and the institutions Ashoka, ICTS, TIFR and MIT for their hospitality. We thank the organisers and attendees of the special sessions on 'Arithmetic geometry & Number theory' and 'Computational number theory' at the Joint Meeting of the NZMS, AustMS and AMS, held in Auckland, for their feedback on a preliminary talk based on this work. This research work was partially supported by the Research-I Foundation of the Department of Computer Science & Engineering of IIT-Kanpur. N.S. thanks the funding support from DST-SERB (CRG/2020/45 + JCB/2022/57) and N. Rama Rao Chair. M.V. is supported by a C3iHub research fellowship.

References

[And97] Greg W Anderson. An explicit algebraic representation of the Abel map. *IMRN: International Mathematics Research Notices*, 1997(11), 1997. 35

[And02] Greg W Anderson. Abeliants and their application to an elementary construction of Jacobians. *Advances in Mathematics*, 172(2):169–205, 2002. 34, 35, 36, 37

[And04] Greg W Anderson. Edited 4-Θ embeddings of Jacobians. *Michigan Mathematical Journal*, 52(2):309–339, 2004. 35, 37

[Bug04] Yann Bugeaud. *Approximation by algebraic numbers*. Cambridge University Press, 2004. 15

[CE11] Jean-Marc Couveignes and Bas Edixhoven. *Computational aspects of modular forms and Galois representations*. Princeton University Press, 2011. 2

[CF⁺12] Henri Cohen, Gerhard Frey, et al. *Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition*. Chapman & Hall/CRC, 2nd edition, 2012. 11

[Cho54] Wei-Liang Chow. The Jacobian variety of an algebraic curve. *American Journal of Mathematics*, 76(2):453–476, 1954. 34, 35

[Cho02] Wei-Liang Chow. The criterion for unit multiplicity and a generalization of Hensel's lemma. In *The Collected Papers of Wei-Liang Chow*, pages 333–346. World Scientific, 2002. 14

[Cou06] Jean-Marc Couveignes. Hard Homogeneous Spaces. Cryptology ePrint Archive, Paper 2006/291, 2006. 3

[Cou09] Jean-Marc Couveignes. Linearizing torsion classes in the Picard group of algebraic curves over finite fields. *Journal of Algebra*, 321(8):2085–2118, 2009. 4, 8, 11

[CTS21] Jean-Louis Colliot-Thélène and Alexei N Skorobogatov. *The Brauer-Grothendieck group*, volume 71. Springer, 2021. 3

[Del74] Pierre Deligne. La conjecture de Weil : I. *Publications Mathématiques de l'IHÉS*, 43:273–307, 1974. 2, 32

[Gab83] Ofer Gabber. Sur la torsion dans la cohomologie ℓ-adique d'une variété. *CR Acad. Sci. Paris Sér. I Math*, 297(3):179–182, 1983. 32

[Gel84] Stephen Gelbart. An elementary introduction to the Langlands program. *Bulletin of the American Mathematical Society*, 10(2):177–219, 1984. 2

[Har15] David Harvey. Computing zeta functions of arithmetic schemes. *Proceedings of the London Mathematical Society*, 111(6):1379–1401, 2015. 3

[HI94] Ming-Deh Huang and Doug Ierardi. Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve. *Journal of Symbolic Computation*, 18(6):519–539, 1994. 8

[HI98] Ming-Deh Huang and Doug Ierardi. Counting points on curves over finite fields. *Journal of Symbolic Computation*, 25(1):1–21, 1998. 4, 8

[HM17] Michel Hickel and Mickaël Matusinski. On the algebraicity of puiseux series. *Revista Matemática Complutense*, 30:589–620, 2017. 14

[HS83] David Lee Hilliker and EG Straus. Determination of bounds for the solutions to those binary Diophantine equations that satisfy the hypotheses of Runge's theorem. *Transactions of the American Mathematical Society*, 280(2):637–657, 1983. 13

[Igu56a] Jun-Ichi Igusa. Fibre systems of Jacobian varieties. *American Journal of Mathematics*, 78(1):171–199, 1956. 9, 14, 34, 37

[Igu56b] Jun-Ichi Igusa. Fibre Systems of Jacobian Varieties:(II. Local Monodromy Groups of Fibre Systems). *American Journal of Mathematics*, 78(4):745–760, 1956. 34, 35, 37

[Igu58] Jun-Ichi Igusa. Abstract vanishing cycle theory. *Proceedings of the Japan Academy*, 34(9):589–593, 1958. 34, 35

[Jav14] Ariyan Javanpeykar. Polynomial bounds for Arakelov invariants of Belyi curves. *Algebra & Number Theory*, 8(1):89–140, 2014. 26

[Ked06] Kiran S Kedlaya. Quantum computation of zeta functions of curves. *computational complexity*, 15(1):1–19, 2006. 4, 33

[KM04] Kamal Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Mathematics of Computation*, 73(245):333–357, 2004. 8

[KM07] Kamal Khuri-Makdisi. Asymptotically fast group operations on jacobians of general curves. *Mathematics of Computation*, 76(260):2213–2239, 2007. 8

[KV] Hyuk Jun Kweon and Madhavan Venkatesh. Bornes de torsion et un théorème effectif du pgcd. *in preparation*. 3

[Lev22] Christophe Levrat. Calcul effectif de la cohomologie des faisceaux constructibles sur le site étale d'une courbe. *arXiv preprint arXiv:2209.10221*, 2022. 3, 9

[Lev23] Christophe Levrat. Computing the cohomology of constructible étale sheaves on curves. *arXiv preprint arXiv:2306.03283*, 2023. 3, 4

[LGS20] Aude Le Gluher and Pierre-Jean Spaenlehauer. A fast randomized geometric algorithm for computing Riemann-Roch spaces. *Mathematics of Computation*, 89(325):2399–2433, 2020. 8

[LR87] Robert P Langlands and Michael Rapoport. Shimuravarietäten und Gerben. *Journal für die reine und angewandte Mathematik*, 378:113–220, 1987. 3

[LR10] David Lubicz and Damien Robert. Efficient pairing computation with theta functions. In *International Algorithmic Number Theory Symposium*, pages 251–269. Springer, 2010. 11

[LR15] David Lubicz and Damien Robert. A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties. *Journal of Symbolic Computation*, 67:68–92, 2015. 11

[LW06] Alan G.B. Lauder and Daqing Wan. Counting points on varieties over finite fields of small characteristic. *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, 2006. 3

[Mas23] Nicolas Mascot. Explicit computation of Galois representations occurring in families of curves. *arXiv preprint arXiv:2304.04701*, 2023. 10

[Mil80] James S Milne. *Etale cohomology (PMS-33)*. Princeton university press, 1980. 5, 7, 14, 17

[Mil98] James S Milne. Lectures on étale cohomology. Available on-line at `http://www.jmilne.org/math/CourseNotes/LEC.pdf`, 1998. 6, 11

[MO15] David Madore and Fabrice Orgogozo. Calculabilité de la cohomologie étale modulo ℓ. *Algebra & Number Theory*, 9(7):1647–1739, 2015. 3

[Mor00] Atsushi Moriwaki. Arithmetic height functions over finitely generated fields. *Inventiones mathematicae*, 140:101–142, 2000. 34

[Pil90] Jonathan Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):745–763, 1990. 2, 3, 8, 24, 37

[PTvL15] Bjorn Poonen, Damiano Testa, and Ronald van Luijk. Computing Néron–Severi groups and cycle class groups. *Compositio Mathematica*, 151(4):713–734, 2015. 3

[PW21] Fabien Pazuki and Martin Widmer. Bertini and Northcott. *Research in Number Theory*, 7:1–18, 2021. 34

[Rém10] Gaël Rémond. Nombre de points rationnels des courbes. *Proceedings of the London Mathematical Society*, 101(3):759–794, 2010. 34

[Rou99] Fabrice Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999. 13, 17, 26

[RSV24] Diptajit Roy, Nitin Saxena, and Madhavan Venkatesh. Complexity of counting points on curves, and the factor $P_1(T)$ of the zeta function of surfaces. *Preprint*, 2024. 3, 5, 6, 9, 32

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of computation*, 44(170):483–494, 1985. 2, 3

[Ser12] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117. Springer Science & Business Media, 2012. 9

[Ser16] Jean-Pierre Serre. *Lectures on $N_X(p)$*. CRC Press, 2016. 2, 29

[Sil83] Joseph H. Silverman. Heights and the specialization map for families of abelian varieties. *Journal für die reine und angewandte Mathematik*, 342:197–211, 1983. 34

[Wal00] P Walsh. A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function. *Mathematics of Computation*, 69(231):1167–1182, 2000. 12, 13

[Wal04] C. T. C. Wall. *Singular Points of Plane Curves*. London Mathematical Society Student Texts. Cambridge University Press, 2004. 12, 15

[ZM72] Ju G Zarhin and Ju I Manin. Height on families of abelian varieties. *Mathematics of the USSR-Sbornik*, 18(2):169, 1972. 33

Appendix A. Recovering zeta

The objective of this section of the appendix is to show how to recover the zeta function of a smooth, projective surface from the action of Frobenius on its étale cohomology groups. As usual, let $X \subset \mathbb{P}^N$ be a nice surface of degree D obtained via good reduction from a nice surface $\mathcal{X}$ over a number field K, at a prime $\mathfrak{p} \subset \mathcal{O}_K$. Assume we have computed the action of the Frobenius endomorphism $F_q^\star$ on the cohomology groups $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$ for $0 \leq i \leq 4$. We show how to recover the zeta function $Z(X/\mathbb{F}_q, T)$ and the point-count $\#X(\mathbb{F}_q)$ as follows. Firstly, denote $\tilde{P}_i(T) := \det\left(1 - TF_q^\star \mid \mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})\right) \in \mathbb{F}_\ell[T]$. Consider the following exact sequence of étale sheaves on X following [Gab83]

$$0 \longrightarrow \mathbb{Z}_\ell \longrightarrow \mathbb{Z}_\ell \longrightarrow \mathbb{Z}/\ell\mathbb{Z} \longrightarrow 0.$$

As a result, we obtain the following from the associated long-exact-sequence on cohomology

$$0 \longrightarrow \mathrm{H}^i(X, \mathbb{Z}_\ell)/(\ell \cdot \mathrm{H}^i(X, \mathbb{Z}_\ell)) \longrightarrow \mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{H}^{i+1}(X, \mathbb{Z}_\ell)[\ell] \longrightarrow 0. \tag{A.1}$$

Writing

$$P_i'(T) := \det\left(1 - TF_q^\star \mid \mathrm{H}^i(X, \mathbb{Z}_\ell)[\ell]\right) \text{ and } \overline{P}_i(T) := \det\left(1 - TF_q^\star \mid \mathrm{H}^i(X, \mathbb{Q}_\ell)\right) \bmod \ell,$$

we see from (A.1) that

$$\tilde{P}_i(T) = \overline{P}_i(T) \cdot P_i'(T) \cdot P_{i+1}'(T).$$

In particular if we write $Z(X/\mathbb{F}_q, T) = P(T)/Q(T)$ for $P(T), Q(T) \in \mathbb{Z}[T]$, we see that

$$\frac{\overline{P}(T)}{\overline{Q}(T)} = \prod_{i=0}^{4} (\tilde{P}_i(T))^{(-1)^{i+1}}$$

where $\overline{P}(T) := P(T) \bmod \ell$ and $\overline{Q}(T) := Q(T) \bmod \ell$. This implies that the zeta function can be recovered as an application of the Chinese remainder theorem using the polynomials $\tilde{P}_i(T)$ for finitely many primes ℓ. We now give bounds for the number and size for the primes required. Write

$$\beta_i := \dim \mathrm{H}^i(X, \mathbb{Q}_\ell) = \deg P_i(X/\mathbb{F}_q, T)$$

for the i^{th} $\ell-$adic Betti number of X. By [RSV24, §4.2], we know $\beta_1 = \beta_3 \leq 2D^2$ and $\beta_2 \leq 2D^{N+1}$. As a result of Deligne's proof [Del74] of the Weil-Riemann hypothesis for X, we know that the reciprocal roots of $P_i(X/\mathbb{F}_q, T)$ have absolute value $q^{i/2}$. This implies that the coefficients of each polynomial $P_i(T)$ are bounded above by

$$\binom{2D^{N+1}}{D^{N+1}} q^{D^{N+1}}.$$

In particular, it suffices to compute $P_i(T) \bmod \ell$ for all primes $\ell \leq A \log q$ where $A = 9 \cdot D^{N+1} + 3$. Further, observe that

$$\frac{d}{dT} \log Z(X/\mathbb{F}_q, T) = \sum_{j=1}^{\infty} \#X(\mathbb{F}_{q^j}) T^{j-1} = \frac{Q(T)\dot{P}(T) - P(T)\dot{Q}(T)}{P(T)Q(T)},$$

so $\#X(\mathbb{F}_q)$ can be read off as the constant term of the power-series expansion associated to the logarithmic derivative of $Z(X/\mathbb{F}_q, T)$.

Remark. We note that we may need to work over field extensions $\mathbb{F}_Q/\mathbb{F}_q$ (e.g., to ensure the existence of a smooth fibre of π) and compute the F_Q – zeta function. The base zeta function can be recovered from any two such, via a recipe due to Kedlaya [Ked06, §8].

Appendix B. Height bounds

In this section of the appendix, we recall the theory of heights and state certain height bounds towards our results in Section 3.5.

Let $K/\mathbb{Q}$ be a number field. Denote by M_K the set of places of the ring of integers $\mathcal{O}_K$ and denote by $v_\mathfrak{p}$ for $\mathfrak{p} \in M_K$ the associated $\mathfrak{p}$ – adic valuation. Let $K_\mathfrak{p}$ denote the completion of K and set $n_{v_\mathfrak{p}} = [K_\mathfrak{p} : \mathbb{Q}_\mathfrak{p}]$.

Definition B.1. *Let $P = [x_0 : \ldots : x_N] \in \mathbb{P}^N(K)$ be a point. The Weil height $h(P)$ is defined as*

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{\mathfrak{p}} n_{v_\mathfrak{p}} \cdot \left(\log(\max_j \|x_j\|_{v_\mathfrak{p}}) \right).$$

Definition B.2. *Let C be a curve over K and let J denote its Jacobian. The Néron-Tate height, denoted $\hat{h}$ for a point $P \in J$ is defined as follows*

$$\hat{h}(P) := \lim_{j\to\infty} \frac{h(2^j P)}{4^j}. \tag{B.1}$$

It is clear that the Néron-Tate height vanishes on torsion points. We next recall the following, that relates the two height functions introduced above, on an abelian variety.

Theorem B.3 (Zarhin-Manin)**.** *Let A be a polarised abelian variety over a number field K, together with an ample, symmetric line bundle Θ. Then, there exist constants c_1 and c_2, depending on A and g such that for any $P \in A(\overline{K})$,*

$$\hat{h}(P) - c_1 \leq h(P) \leq \hat{h}(P) + c_2 \tag{B.2}$$

with

$$c_1 = \left(\frac{2^{2g-1}}{3} + 1\right) \cdot h_\Theta(A) + \left(2^{2g-2} + \frac{67}{12}\right) \cdot g \cdot \log 2 \;\text{ and }\; c_2 = (2^{2g} - 1) \cdot h_\Theta(A) + (2^{2g+1} - \frac{1}{3}) \cdot g \cdot \log 2,$$

where $h_\Theta(A)$ is the height of the neutral element 0_A of A.

Proof. Apply [ZM72, 3.2] to the divisor $4 \cdot \Theta$. □

Theorem B.4 (Height of torsion point)**.** *Let $C \subset \mathbb{P}^N$ be a smooth, projective curve of genus g and degree D over a number field K, and denote by J its Jacobian. Let ℓ be a prime number, and let $P \in J[\ell]$ be an ℓ – torsion point. Consider the embedding of J into $\mathbb{P}^M$ given by Theorem D.1. Then, we have*

$$|h(P)| \leq C,$$

where C is a constant that depends only on N, g, D, the height of the coefficients of the equations defining C, the extension degree, and the logarithm of the discriminant of the number field $K/\mathbb{Q}$. The dependence is polynomial in the last three items. In particular, the height of an ℓ – torsion point is bounded by a quantity independent of ℓ.

Proof. As P is assumed to be torsion, we know $\hat{h}(P) = 0$. We note firstly, that by Theorem D.2, the height of the Jacobian constructed in Theorem D.1 is bounded above by the height associated to the $4 \cdot \Theta$ – embedding. The result then follows from Theorem B.3, combined with the results of [PW21, §2] and [Rém10, §1]. □

Remark. Theorem B.4 holds with the base field K replaced by a function field $\mathbb{F}_q(t)$ or a function field over a number field $K(t)$. We merely change the notion of height, in the former case, one uses a geometric height function, and in the latter case, a height function that captures both the geometric and arithmetic data, such as Moriwaki's height function [Mor00]. The general underlying principle is that the naive height only differs from the canonical height by a bounded amount (see [Sil83, §4]).

Appendix C. Results of Igusa

In this appendix, we recall certain results of Igusa related to fibre systems of Jacobian varieties, their embeddings, and specialisation. This is then applied to the context of a Lefschetz pencil on a surface and the specialisation of the ℓ – torsion in the Jacobian of the generic fibre. The treatment is based on the works [Igu56a, Igu56b, Igu58].

Let $\mathcal{X} \subset \mathbb{P}^N$ be a nice surface over a number field K and let $\pi : \mathcal{X} \to \mathbb{P}^1$ be a Lefschetz pencil of hyperplane sections. Denote by $Z \subset \mathbb{P}^1$ the finite subset parametrising the nodal fibres and let $U = \mathbb{P}^1 \setminus Z$. Let $\overline{\eta} \to \mathbb{P}^1$ be a geometric generic point and let the genus of the generic fibre $\mathcal{X}_{\overline{\eta}}$ (as a curve over the field $\overline{K}(t)$) be g. Write $\mathcal{F} := R^1\pi_\star\mu_\ell$ for the derived pushforward. Consider an embedding of the Jacobian $\mathcal{J}_{\overline{\eta}} = \mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})$ into a projective space $\mathbb{P}^M$ [12].

Theorem C.1. *For $z \in Z$, let $\widetilde{\mathcal{J}}_z$ be the specialisation of $\mathcal{J}_{\overline{\eta}}$ to z, over the specialisation $\mathcal{X}_{\overline{\eta}} \to \mathcal{X}_z$. Then, $\widetilde{\mathcal{J}}_z$ is the completion of the generalised Jacobian* [13] *$\mathcal{J}_z$ of $\mathcal{X}_z$.*

Proof. See [Igu56a, Theorem 3]. □

Theorem C.2. *The singular locus of $\widetilde{\mathcal{J}}_z$ is $\widetilde{\mathcal{J}}_z \setminus \mathcal{J}_z$. Further, if ω is a $\overline{K}(t)$ – rational point of $\mathcal{J}_{\overline{\eta}}$, then the specialisation ω_z of ω to z is a smooth point of $\widetilde{\mathcal{J}}_z$.*

Proof. See [Igu56b, pg 746, Theorem 1]. □

Now, under the natural inclusion $\overline{K}(t) \hookrightarrow \overline{K}((t-z))$, fix an embedding $\overline{K(t)} \hookrightarrow \overline{K}\langle\langle t-z\rangle\rangle$. As we saw in Section 3.2, this completely determines a cospecialisation map $\phi_z : \mathcal{F}_z \hookrightarrow \mathcal{F}_{\overline{\eta}}$. We have the following.

Theorem C.3. *Write ς for the 0 – cycle on $\mathcal{J}_{\overline{\eta}}$ comprising of its ℓ – torsion $\mathcal{J}_{\overline{\eta}}[\ell]$. Then the specialisation of ς to z is the 0 – cycle on $\widetilde{\mathcal{J}}_z$ written $\overline{\varsigma} + \overline{\varsigma}'$ where $\overline{\varsigma}$ consists of the ℓ – torsion of the generalised Jacobian $\mathcal{J}_z[\ell]$ and $\overline{\varsigma}'$ is a positive cycle, each of which is a multiple point of $\widetilde{\mathcal{J}}_z$ arising from the singularities of the curve ${}^{(\ell)}\mathfrak{C} \subset \mathbb{P}^M$ over $\overline{K}$ corresponding to the ℓ – division ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ of $\mathcal{J}_{\overline{\eta}}$.*

Proof. See [Igu56b, Theorem 2]. □

[12] using e.g., Chow's method ([Cho54] or [Igu56a, Appendix]) or Anderson's method ([And02]) sketched in Appendix D, both of which involve the Θ – divisor

[13] also called Rosenlicht variety

Theorem C.4. *Let $\gamma \in \mathcal{F}_{\overline{\eta}} \setminus \phi_z(\mathcal{F}_z)$. Then $\sigma_z(\gamma)$ and γ specialise to the same point in $\widetilde{\mathcal{J}}_z$. Further, $\sigma_z(\gamma) - \gamma$ lies in the space generated by the vanishing cycle at z.*

Proof. See the proof of [Igu56b, Theorem 3]. □

Theorem C.5. *Now, consider $\mathcal{J}_{\overline{\eta}}$ as being defined over $\overline{K}((t-z))$. Then, all the points of $\phi_z(\mathcal{F}_z)$ are rational over $\overline{K}((t-z))$ and the splitting field $\mathbb{K}$ of $\mathcal{F}_{\overline{\eta}}$ over $\overline{K}((t-z))$ satisfies*

$$[\mathbb{K} : \overline{K}((t-z))] = \ell,$$

i.e., $\mathbb{K}$ is the field obtained by adjoining $\overline{K}((t-z))$ with an ℓ^{th} – root of $t - z$.

Proof. See [Igu58, Theorem 2]. □

Appendix D. Abstract Abel map and embeddings of Jacobians

This section of the appendix aims to provide equations for the Jacobian of smooth projective curves and the generalised Jacobian of a nodal curve. A construction of the Jacobian of a smooth curve was described by Chow [Cho54], however our treatment follows Anderson [And02], who provides an 'elementary' algebraic construction of the Abel map [And97]. In [And04], it is shown that the construction matches with an 'edited' $4 \cdot \Theta$ – embedding associated to the Θ – divisor on the Jacobian of a curve.

We explain briefly Anderson's construction of the 'abstract Abel map'. Let $C \subset \mathbb{P}^N$ be a smooth, projective curve of genus g over a field $\mathbb{K}$. Let $\mathcal{E}$ be a line bundle of degree $w \geq 2g+1$ and let $\mathcal{D}$ be a line bundle of degree zero. Let $\underline{u}$ be a basis for $\mathrm{H}^0(C, \mathcal{D}^{-1} \otimes \mathcal{E})$ and let $\underline{v}$ be a basis for $\mathrm{H}^0(C, \mathcal{D} \otimes \mathcal{E})$. Denote by $C^{\{0,\ldots,w+1\}}$ the $w+2$ – fold power of C with numbering remembered, and for a section f of a line bundle on C, denote by $f^{(i)}$ the pullback by the i^{th} projection. Then the abstract Abel map sends $\mathcal{D}$ to the $w \times w$ matrix with entries

$$\text{abel}(\mathcal{D})_{ij} = \begin{vmatrix} \widehat{\underline{v}^{(0)}} \\ \vdots \\ \widehat{\underline{v}^{(i)}} \\ \vdots \end{vmatrix} \cdot \begin{vmatrix} \vdots \\ \widehat{\underline{u}^{(i)}} \\ \vdots \\ \widehat{\underline{u}^{(w+1)}} \end{vmatrix} \cdot \begin{vmatrix} \vdots \\ \widehat{\underline{v}^{(j)}} \\ \vdots \\ \widehat{\underline{v}^{(w+1)}} \end{vmatrix} \cdot \begin{vmatrix} \widehat{\underline{u}^{(0)}} \\ \vdots \\ \widehat{\underline{u}^{(j)}} \\ \vdots \end{vmatrix} \tag{D.1}$$

for $1 \leq i, j \leq w$, where the leftmost term in the product denotes the determinant of the $w \times w$ matrix obtained by stacking the $\underline{v}^{(t)}$ as row vectors numbered 0 to $w+1$ and removing the rows numbered 0 and i. In particular, the construction maps classes of degree zero line bundles to $w \times w$ matrices with the entry from the i^{th} row and j^{th} column being from the space

$$\mathrm{H}^0\left(C^{\{0,\ldots,w+1\}}, \frac{\bigotimes_{s=0}^{w+1} \left(\mathcal{E}^{(s)}\right)^{\otimes 4}}{\left(\mathcal{E}^{0}\right)^{\otimes 2} \otimes \left(\mathcal{E}^{(i)}\right)^{\otimes 2} \otimes \left(\mathcal{E}^{(j)}\right)^{\otimes 2} \otimes \left(\mathcal{E}^{(w+1)}\right)^{\otimes 2}}\right).$$

In summary, the abstract Abel map gives a way to realise any degree zero divisor on C as a point on its Jacobian, embedded into projective space.

We now sketch below how to obtain the equations for the Jacobian, i.e., the ideal of polynomials vanishing on the image of the abstract Abel map.

(1) Fix an effective divisor E of C with $\deg(E) \geq 2g+1$.

(2) Set $w = \dim \mathcal{L}(E) = \deg(E) - g + 1$.
(3) Write $S = \operatorname{supp}(E)$, $A = \mathrm{H}^0(S, \mathcal{O}_C)$ and $L = \mathcal{L}(2E)$.

Then, the Jacobian of C is given by the projective algebraic variety J of $\mathbb{K}$ – proportionality classes of Jacobi matrices of type $(\mathbb{K}, w, A, L)$. A proof is given in [And02, Theorem 4.4.6]. From [And02, 3.7.3], we see that the complexity of the construction is at worst $\exp(\mathrm{poly}(g))$.

In the case $\mathbb{K} = k(t)$ is the function field of the projective line, and C is a curve over $\mathbb{K}$, we want to choose an effective divisor E on C for the embedding so that upon specialisation to a smooth value $t = u$, the corresponding embedding of the Jacobian of C_u is given by E_u. This is achieved as follows.

- Choose an effective divisor E of C of degree $\geq 2g + 1$ via taking all the zeros of a rational function λ on C, with $k(t)$ – coefficients. We may assume $\operatorname{div}(\lambda) = \lambda_+ - \lambda_-$, with λ_+ and λ_- effective of degree $\geq 2g + 1$, and no redundancies between them. Also assume that the divisor $\mathcal{E}$ specialised to any $u \in \mathbb{P}^1$ contains no singular point of $\mathcal{X}_u$ in its support.
- For a smooth point u, the associated divisor E_u is obtained by specialising λ_+ to u.
- The Jacobian of the curve C_u corresponds to the specialisation of the Jacobian of C at $t = u$, via the divisor E_u.

Algorithm 10 `Abstract Abel map and its inverse on` ℓ `– torsion`

- **Input:** The generic fibre $\mathcal{X}_{\overline{\eta}}$ of a Lefschetz pencil $\pi : \mathcal{X} \to \mathbb{P}^1$ on a smooth projective surface $\mathcal{X}$ over a number field K, and a degree zero divisor $D \in \mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$ represented using Theorem 2.2.
- **Output:** The image $\mathrm{abel}(D)$ of the map in (D.1) as a point in projective space $\mathbb{P}^M$ lying on the Jacobian $\mathcal{J}_{\overline{\eta}}$, satisfying the conditions of the paragraph above.

1: Choose an effective divisor E of $\mathcal{X}_{\overline{\eta}}$ of degree $w \geq 2g + 1$ via taking all the zeros of a rational function λ, with $K(t)$ – coefficients on $\mathcal{X}_{\overline{\eta}}$. We may assume $\operatorname{div}(\lambda) = \lambda_+ - \lambda_-$, with λ_+ and λ_- effective of degree $\geq 2g + 1$, and no redundancies between them. Also assume that the divisor E specialised to any $u \in \mathbb{P}^1$ contains no singular point of $\mathcal{X}_u$ in its support.

2: Compute bases $\underline{v}$ for $\mathrm{H}^0(\mathcal{X}_{\overline{\eta}}, E + D)$ and $\underline{u}$ for $\mathrm{H}^0(\mathcal{X}_{\overline{\eta}}, E - D)$ using an effective Riemann-Roch algorithm via Theorem 2.1.

3: Maintaining $w + 2$ sets of variables, compute the pullbacks $\underline{u}^{(i)}$ and $\underline{v}^{(j)}$ for each $i, j \in \{0, \dots, w + 1\}$. These are merely the same rational functions associated to a specific set of variables.

4: Compute the map (D.1) using these pullbacks.

5: For any $u \in \mathbb{P}^1$, the embedding of the Jacobian $\mathrm{Pic}^0(\mathcal{X}_u) \hookrightarrow \mathbb{P}^M$ is given by the divisor E_u. If we specialise the input divisor D to u, we get $D_u \in \mathrm{Pic}^0(\mathcal{X}_u)[\ell]$.

6: To invert the Abel map on $\mathrm{Pic}^0(\mathcal{X}_u)[\ell]$, given a point in $\mathbb{P}^M$ corresponding to an element of $\mathrm{Pic}^0(\mathcal{X}_u)[\ell]$, we simply go through all the ℓ^{2g} divisorial representatives of ℓ – torsion as a result of the algorithm from Theorem 2.2 and check which of them map to our given point via the divisor E_u and the map (D.1). There will be a unique pre-image as the Abel map is injective.

Remark. The only dependence on ℓ in Algorithm 10 is the input divisor $D \in \mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$. By Theorem 2.2, we know that D can be efficiently represented poly(ℓ) time and the bases for the Riemann-Roch spaces $\mathrm{H}^0(\mathcal{X}_{\overline{\eta}}, E \pm D)$ are computed using Thorem 2.1.

By [Igu56a, Theorem 3] (see also [Igu56b]), we know that the specialisation of the Jacobian of the generic fibre $\mathcal{X}_{\overline{\eta}}$ of a Lefschetz pencil $\pi : \mathcal{X} \to \mathbb{P}^1$ on a surface $\mathcal{X}$ to a singular $z \in Z$ is the completion of the generalised Jacobian of $\mathcal{X}_z$. In summary, we have the following.

Theorem D.1. *Let $\mathcal{X} \subset \mathbb{P}^N$ be a nice surface of degree D over a number field K and let $\pi : \mathcal{X} \to \mathbb{P}^1$ be a Lefschetz pencil of hyperplane sections on $\mathcal{X}$. Let $U \subset \mathbb{P}^1$ be the subscheme parametrising the smooth fibres and let $Z = \mathbb{P}^1 \setminus U$ parametrise the singular nodal fibres. Then, there exists an algorithm that computes*

(i) *the Jacobian $\mathcal{J}_{\overline{\eta}}$ of $\mathcal{X}_{\overline{\eta}}$ in a projective space $\mathbb{P}^M$ as a system of homogeneous polynomial equations,*

(ii) *an explicitisation of the Abel map $\mathcal{X}_{\overline{\eta}} \hookrightarrow \mathcal{J}_{\overline{\eta}}$,*

(iii) *an explicit addition law on the Jacobian $\mathcal{J}_{\overline{\eta}}$ with atlases, in the sense of Pila [Pil90]. This provides a translation between the language of divisor arithmetic on $\mathcal{X}_{\overline{\eta}}$ and points on $\mathcal{J}_{\overline{\eta}}$. Moreover, for any specialisation to $u \in \mathbb{P}^1$, the group law on $\mathcal{J}_{\overline{\eta}}$ specialises to that on $\mathcal{J}_u$.*

Proof. See [And02, §4]. □

Theorem D.2. *The embedding described in Theorem D.1 factors through (and corresponds exactly to, upto linear hull) an 'edited' $4 \cdot \Theta$ – embedding, i.e., the complete linear system associated to the divisor $4 \cdot \Theta$ on the Jacobian, consisting of those theta-functions which vanish at the origin with order ≤ 1.*

Proof. See [And04, §3]. □

Department of Computer Science & Engineering, IIT Kanpur, India
Email address: nitin@cse.iitk.ac.in

Department of Computer Science & Engineering, IIT Kanpur, India
Email address: madhavan@cse.iitk.ac.in