Algorithmic Arithmetic Geometry

Madhavan Venkatesh

विष्णवे वेदात्मने ।

Acknowledgements

I begin by expressing immense gratitude to my advisors Nitin Saxena and Manindra Agrawal.

I am fortunate to be advised by Nitin. His unrelenting style of inquiry with the tendency to go for the problem's jugular is absolutely inspirational. I only hope I can emulate it in some way.

I am ever grateful to Manindra for giving me the opportunity to work on some exciting projects, and for encouraging me to start a PhD in the first place.

I thank Somnath Jha profusely for his constant encouragement, and for serving on various committees over the course of my PhD.

I thank Kiran Kedlaya for discussions, in particular for bringing my attention to the circle of problems studied in this thesis.

I am indebted to my mentors over the years: Miles Reid, Jürg Kramer and the late MS Narasimhan. Their mathematical tastes have certainly influenced mine, which I believe is reflected in this work.

Many thanks to Pierre Deligne for his delightful contributions to mathematics.

I have benefited greatly from the kindness and generosity of several researchers: TN Venkataramana, Arvind Nair, CS Rajan, Robin de Jong, Rachel Newton, Jonathan Pila, Steven Galbraith, Brendan Creutz, Felipe Voloch, Guhan Venkat, Anilatmaja Aryasomayajula, Emre Sertöz, Joël Ouaknine and Ben Worrell, whom I wish to thank. I hope to get the chance to be helpful to young researchers down the line and pay it forward.

I thank the institutions of ICTS, TIFR, MIT, the University of Auckland, the University of Canterbury, Ashoka University, and IISER Tirupati for hosting me at various times. I thank C3iHub; particularly Prof. Sandeep Shukla and Dr. Tanima Hajra for facilitating optimal working conditions, and for granting a research fellowship that supported this work. I thank the Department of CSE, IITK, the Research-I-Foundation and Nitin's JC Bose Fellowship for travel funding.

I thank my collaborators Hyuk Jun Kweon and Diptajit Roy for several discussions. I thank the other members of Nitin's group I overlapped with: Prateek Dwivedi, CS Bhargav, Anindya Ganguly, Tufan Singha Mahapatra, and Foram Lakhani. My friends at IITK and C3iHub have made my time in Kanpur whimsically enjoyable.

Salutations to the city of प्रयाग, which; apart from being the hometown of both my advisors, is where I began writing this thesis.

The final parts of this thesis were completed during a sojourn in Europe, in the wonderful cities of Luxembourg, Trieste and Leiden. I thank the University of Luxembourg (and the organisers of Journées Arithmétiques), ICTP Trieste, the Lorentz center, Universiteit Leiden and MPI-SWS Saarbrücken for providing excellent working conditions and travel support.

I am forever grateful to my family for their constant, unconditional support.

Contents

List of works

(i) "*Complexity of conting points on curves, and the factor $P_1(T)$ of the zeta function of surfaces*", with Diptajit Roy and Nitin Saxena [RSV24].

Submitted for publication to a complexity theory journal. Presented in a short talk at the ANTS XVI conference at MIT, and in a seminar at TIFR Mumbai, 2024.

(ii) "*Bornes de torsion et un théorème effectif du pgcd*", with Hyuk Jun Kweon [KV25].

Submitted for publication to a mathematics journal. Presented in a seminar at ICTS Bengaluru, 2024.

(iii) "*Counting points on surfaces in polynomial time*", with Nitin Saxena [SV25].

Submitted for publication to a mathematics journal. Presented at 33èmes Journées Arithmetiques, Luxembourg and at the workshop 'Explicit Arithmetic Geometry' at ICTP Trieste, 2025.

Chapter 1

Introduction

In this chapter, we introduce the problem studied in this thesis, and state the main results.

1.1 The problem

This work concerns the arithmetic geometry of varieties over finite fields. Specifically, the focus is on effective methods and algorithms. The main motivation is the following fundamental question of Serre [Ser16, Preface].

Question. Let $\mathcal{X}$ be a $\mathbb{Z}-$scheme of finite type. Does there exist an algorithm that, on input a prime p, computes the point count $\#X(\mathbb{F}_p)$ of the reduction X in time polynomial in $\log p$?

Equivalently, one asks for the computation of the local zeta function

$$Z(X/\mathbb{F}_p, T) = \exp\left(\sum_{j=1}^{\infty} \#X(\mathbb{F}_{p^j})\frac{T^j}{j}\right). \tag{1.1}$$

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

$$Z(X/\mathbb{F}_q, T) = \frac{P_1(X/\mathbb{F}_q, T)\cdots P_{2n-1}(X/\mathbb{F}_q, T)}{P_0(X/\mathbb{F}_q, T)\cdots P_{2n}(X/\mathbb{F}_q, T)},$$

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. The question is well understood in certain cases, due to the work of Schoof [Sch85] addressing elliptic curves, and Pila [Pil90] addressing curves and abelian varieties.

In [CE11, Epilogue], the existence of an algorithm that computes the point count $\#X(\mathbb{F}_q)$ of a *surface* X 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.

1.2 Main results

Let $\mathcal{X} \subset \mathbb{P}^N$ be a smooth, projective geometrically irreducible variety of dimension n and degree D, over a number field K, presented via homogeneous forms $f_1, \ldots, f_m$. Let $\mathfrak{p}$ be a prime of good reduction, write $\mathbb{F}_q := \mathcal{O}_K/\mathfrak{p}$ and denote the variety $X/\mathbb{F}_q$ upon reduction.

Theorem 1.1. *There exists a polynomial $\Phi(x) \in \mathbb{Z}[x]$ independent of q and $\deg X = D$, such that for any extension $\mathbb{F}_Q/\mathbb{F}_q$ with*

$$[\mathbb{F}_Q : \mathbb{F}_q] > \Phi(D),$$

we have for any $u_1, u_2 \in U(\mathbb{F}_Q)$ chosen uniformly at random,

$$P_{n-1}(X/\mathbb{F}_Q, T) = \gcd\left(P_{n-1}(X_{u_1}/\mathbb{F}_Q, T), P_{n-1}(X_{u_2}/\mathbb{F}_Q, T)\right);$$

with probability $> 2/3$.

This is proved as Theorem 3.21. Considering the embedding dimension N to be fixed, [1] one obtains the following algorithmic consequence, via an application of the Lefschetz hyperplane theorem.

Corollary 1.2. *There is a randomised polynomial time reduction for zeta function computations of smooth projective varieties to the middle cohomology.*

Let $\mathcal{X} \subset \mathbb{P}^N$ now be a fixed smooth, projective geometrically irreducible **surface** of degree D, over a number field K, presented via homogeneous forms $f_1, \ldots, f_m$, each having coefficients of Weil height bounded by $H \in \mathbb{R}_{>0}$. Let $\mathfrak{p}$ be a prime of good reduction and write $\mathbb{F}_q := \mathcal{O}_K/\mathfrak{p}$.

Theorem 1.3. *There exists an algorithm, that, on input X and a prime $\mathfrak{p}$ as above, outputs $Z(X/\mathbb{F}_q, T)$ in time bounded by a polynomial in $\log q$.*

This is proved as Theorem 6.6.

A common permeating theme in the proofs of the results is the yoga of vanishing cycles, originally due to Picard and Lefschetz, adapted to the $\ell-$adic setting by Grothendieck, Katz and Deligne.

1.3 Prior work

It is possible to interpret (1.1) via a trace formula in a suitable *Weil cohomology theory*. Examples include ℓ-adic cohomology, for primes ℓ distinct from the characteristic, developed by Grothendieck [G+77]; and rigid cohomology, an extension of crystalline cohomology due to Berthelot [Ber86]. In general, algorithms for computing the zeta function can be classified broadly into two distinct families, ℓ-adic or p-adic, usually based on the nature of the cohomology theory being employed. The progenitor of the ℓ-adic class of algorithms is the work of Schoof [Sch85], who gave an algorithm to compute the zeta function of an elliptic curve over $\mathbb{F}_q$ with complexity polynomial in $\log q$. This method was generalised by Pila [Pil90] to curves (of fixed genus g), and abelian varieties, with

[1] as is the case with algorithms

improvements for some special cases due to Huang-Ierardi [HI98] and Adleman-Huang [AH01]. The complexity of these algorithms, while polynomial in $\log q$ is exponential or worse in g. A common theme is the realisation of the étale cohomology $\mathrm{H}^1(X, \mu_\ell)$ as the ℓ-torsion $\mathrm{Pic}^0(X)[\ell]$ in the Picard scheme. This has, so far, limited their application to varieties where this realisation can be made explicit, namely curves and abelian varieties. There has been work showing the computability of étale cohomology in higher degrees as well [MO15], but it has not proven amenable to complexity analysis yet.

On the other hand, p-adic methods encompass a more diverse range of algorithms. Some early examples are Satoh's algorithm for elliptic curves [Sat00] using canonical lifts and Kedlaya's algorithm for hyperelliptic curves [Ked01] using Monsky-Washnitzer cohomology (and extensions thereof [DV06, CDV06]). Lauder-Wan [LW06], inspired by work of Dwork on the rationality of the zeta function [Dwo60], proposed a more general algorithm capable of handling arbitrary varieties. Lauder [Lau04] also developed an algorithm for hypersurfaces based on p-adic deformation theory. More recently, there is the 'non-cohomological' work of Harvey [Har15], who devised an algorithm based on a novel trace formula. The complexity of these algorithms, while polynomial in the degree D of the variety, is exponential in $\log p$. A common theme is that they involve a p-adic lift of the Frobenius, which necessitates working with $O(p)$ monomials in the basis for the respective p-adic cohomology theory.

1.4 Leitfaden

The thesis is divided into two independent but related results. In Part I, we begin with an introductory chapter discussing the complexity of counting points on curves, based on the work [RSV24, §2], which is joint with Roy and Saxena. Chapter 3 is on an effective, probabilistic version of Deligne's gcd theorem, based on joint work with Kweon [KV25]. It contains material on bounding torsion in the Betti cohomology of varieties (3.2), followed by a revisit of the theory of Lefschetz pencils and monodromy (3.3, 3.4), which combined with certain probability estimates on linear algebraic groups (3.5), culminates in the proof of the theorem (3.6).
Part II is based on joint work with Saxena [SV25], which resolves a conjecture of Couveignes and Edixhoven in computing the étale cohomology groups with constant torsion coefficients of a surface, thereby providing an algorithm to count points on surfaces in polynomial time. After a preliminary chapter on cohomology computations (4), we recall and develop new subroutines to compute monodromy and vanishing cycles (5), followed by a description of the main algorithm (6), complexity analyses (7), and a collection of supplementary but known material (8) that is useful for the algorithm.

The results of this thesis are original unless otherwise stated.

Part I

Curves and more

Chapter 2

Zeta function of curves

In this chapter, we present an $\mathrm{AM} \cap \mathrm{coAM}$ protocol for certifying the zeta function of a curve $C/\mathbb{F}_q$. We assume the input to be a smooth, projective, absolutely irreducible curve $C_0 \subset \mathbb{P}^N$ of genus $g > 0$ and degree δ, presented as a system of homogeneous polynomials $f_1, \ldots, f_m$ with coefficients in $\mathbb{F}_q$ and of degree $\leq d$. Denote by C the base change to the algebraic closure $\overline{\mathbb{F}}_q$. The zeta function has the form

$$Z(C/\mathbb{F}_q, T) = \frac{P_1(C/\mathbb{F}_q, T)}{(1-T)(1-qT)},$$

where $P_1(C/\mathbb{F}_q, T) \in \mathbb{Z}[T]$ is of degree $2g$, with constant term 1. We will certify $P_1(C/\mathbb{F}_q, T)$ and the abelian group structure of the Jacobian variety over the base field, addressing a question of Kedlaya [Ked06, §9] on verifying the order of the Jacobian as a black-box group.

Theorem 2.1 (Zeta & Jacobian). *Given an input polynomial $P(T) \in \mathbb{Z}[T]$, deciding whether $P(T)$ is the numerator polynomial of the zeta function of the smooth, projective curve C, given as above (with variable $g \log q$), is in $\mathrm{AM} \cap \mathrm{coAM}$. Moreover, given a finite Abelian group G (via additive generators), the verification problem*

$$G \overset{?}{\simeq} \mathrm{Jac}(C)(\mathbb{F}_q) \quad \textit{is in} \quad \mathrm{AM} \cap \mathrm{coAM}\,.$$

We begin with the preliminary sections 2.1 and 2.2 consisting of standard material. The $\mathrm{AM} \cap \mathrm{coAM}$ protocol of Theorem 2.1 and its proof is presented in 2.3.

2.1 Preliminaries

A *divisor* D on C is a formal sum $D = \sum_{i=1}^{r} n_i P_i$, where $P_i \in C(\overline{\mathbb{F}}_q)$ and $n_i \in \mathbb{Z} \setminus \{0\}$. The set of points P_i occurring in the sum above is called the *support* of D. The sum $\sum_i n_i$ is called the *degree* of D.

We denote the group of divisors by $\mathrm{Div}(C)$ and the subgroup of degree zero divisors by $\mathrm{Div}^0(C)$. Let K denote the function field of C. We have a map $\mathrm{div} : K^* \hookrightarrow \mathrm{Div}^0(C)$, sending a function to the sum of its zeros and poles. The image of this map is called the subgroup of *principal divisors*, denoted $\mathrm{Div}^{\mathrm{pr}}(C)$. We call a divisor D *effective*, if $n_i \geq 0$ for all i, which we denote by $D \geq 0$.

Definition 2.1. There exists an abelian variety (of dimension g) called the *Jacobian*, denoted $\mathrm{Jac}(C)$, whose $\overline{\mathbb{F}}_q$-rational points correspond to elements of the quotient group $\mathrm{Div}^0(C)/\mathrm{Div}^{\mathrm{pr}}(C)$.

Let D be a divisor on C. We recall the *Riemann-Roch space* of D.

$$\mathcal{L}(D) := \{f \in K^* \mid \operatorname{div}(f) + D \geq 0\} \cup \{0\}.$$

Further, denoting by K_C the canonical divisor of C, the Riemann-Roch theorem states

$$\dim \mathcal{L}(D) = \deg(D) + 1 - g + \dim \mathcal{L}(K_C - D).$$

Addition on the Jacobian is performed by using an effective Riemann-Roch theorem. However, in order to invoke algorithms [HI94, ABCL02] computing the Riemann-Roch spaces, we first reduce our curve to a *planar* model.

In particular, we seek to find a curve $C' \subset \mathbb{P}^2$ birational to C, given by a homogeneous form F. A singular point $P \in C'$ is said to be a *node* if it is an ordinary double point, i.e., has multiplicity two, with distinct tangents. A curve is *nodal* if all its singularities are nodes. We recall [Har13, IV.3.11].

Lemma 2.2 (Planar model)**.** *Let $C \subset \mathbb{P}^N$ be as above. There is a randomised algorithm that computes a nodal curve $C' \subset \mathbb{P}^2$ and a birational morphism $\phi : C \to C'$ that runs in time polynomial in $g \log q$.*

Proof. We describe how to obtain an equation defining C' algorithmically. The key idea is to choose a random point $O \in \mathbb{P}^N$, with $O \notin C$, and project C onto a hyperplane from O. For generic O (lying outside any secant or tangent of C) and $N \geq 4$, the resulting map is an embedding. Repeating the process, we get a sequence of morphisms $C \to \mathbb{P}^{N-1} \to \cdots \to \mathbb{P}^3$. Again, generically[1], by [Har13, Theorem V.3.10] for $O \in \mathbb{P}^3$, the image of the projection of C from O onto $\mathbb{P}^2$ has at worst nodal singularities. Denote by $\phi : C \to \mathbb{P}^2$ the composite morphism of all projections. It is a birational morphism with $\deg(\phi(C)) \leq \delta$. Therefore, the polynomial F cutting out C' in $\mathbb{P}^2$ has total degree at most δ. Writing the linear projection ϕ explicitly and computing the image of $\Theta(\delta^2)$ many points $P_i \in C$, we can recover F by a bivariate interpolation algorithm. □

Sampling points in $C(\mathbb{F}_q)$ (which exist after an extension) can be achieved in randomised polynomial-time as follows. Consider an affine piece of C in $\mathbb{A}^N$ (with coordinates $(y_1, \ldots, y_N)$) by taking the complement of a hyperplane. Fixing a value of y_1 amounts to intersecting with a hyperplane in $\mathbb{A}^N$, giving a finite set of points. The Weil bound (see Theorem 2.3 below) for C guarantees that with high probability, after $2g \leq 4\delta^2$ fixings of y_1 in $\mathbb{F}_q$, the resulting zero-dimensional system has $\mathbb{F}_q$-rational points. Extracting them can be done in randomised polynomial-time by using the main result of [LL91] for the $\mathbb{F}_q$ -root-finding of a zero-dimensional N-variate system.

We conclude this section with a statement of the Weil-Riemann hypothesis for curves [Wei48a, Wei48b].

Theorem 2.3 (Weil)**.** $|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$.

2.2 Jacobian arithmetic

Recall the standard results showing that elements of $\operatorname{Jac}(C)(\mathbb{F}_q)$ can be presented concisely and divisor arithmetic therein can be performed efficiently. We know by [Ser12, §8] that C injects into its Jacobian, by the choice of a rational point, which we call ∞.

[1] the locus of 'bad' projections forms a subvariety of $\mathbb{P}^3$ of dimension at most 2, with degree bounded by a polynomial in $\delta := \deg(C)$. Hence, this locus can be avoided with high probability at the cost of a field extension of degree at worst $\operatorname{poly}(\delta)$.

Lemma 2.4 (Reduced form)**.** *Given $D \in \mathrm{Jac}(C)$, $\exists\ 0 \le i \le g$ and a unique* effective *divisor E of degree $g - i$ such that $D = E - (g - i)(\infty)$ in $\mathrm{Jac}(C)(\overline{\mathbb{F}}_q)$.*

Proof. By the Riemann-Roch theorem, we have $\dim \mathcal{L}(D + g(\infty)) = 1 + \dim \mathcal{L}(K_C - D - g(\infty)) > 0$. Iteratively, subtracting ∞ from the divisor $D + g(\infty)$, we choose the largest $0 \le i \le g$ so that $\dim \mathcal{L}(D + (g - i)(\infty))$ is still positive. In particular, for such an i, we have $\dim \mathcal{L}(D + (g - i)(\infty)) = 1$. Thus, one gets a 'unique' (upto a constant) rational function f in the basis of $\mathcal{L}(D + (g - i\infty))$. Therefore, one obtains a unique effective divisor $E := \mathrm{div}(f) + D + (g-i)(\infty) \ge 0$, which is the same as saying $D = E - (g-i)(\infty)$ in the arithmetic of $\mathrm{Jac}(C)(\overline{\mathbb{F}}_q)$. □

We recall next a method to compute bases of Riemann-Roch spaces.

Proposition 2.5 (Riemann-Roch basis)**.** *Let D be a divisor on a curve C of degree and support-size $\le \delta$. A basis of the Riemann-Roch space $\mathcal{L}(D)$ can be computed efficiently in $O(\delta^{12} \log q)$ time.*

Proof. After computing a plane model $\phi : C \to C' \subset \mathbb{P}^2$ one uses [HI94, §2] to compute the Riemann-Roch space of a divisor on the normalisation of C' (which is isomorphic to C). While [HI94] requires the singular points of C' to lie over the base field (essentially to ensure an efficient resolution of singularities), this can be bypassed by using [Koz94] instead. The complexity follows from [HI94, §2.5]. This strategy was also utilised in the algorithm of [Ked06, §6] as a preprocessing step to do basic arithmetic in the class group (=$\mathrm{Jac}(C)$). □

Using Proposition 2.5, we can now check when a divisor of degree zero is trivial in the Jacobian. Recall that for $D \in \mathrm{Div}^0(C)$, we have $\dim \mathcal{L}(D) = 1$ if and only if $D \in \mathrm{Div}^{\mathrm{pr}}(C)$. This implies the following.

Lemma 2.6 (Zero test)**.** *Given $D \in \mathrm{Div}^0(C)$, whether $D \in \mathrm{Div}^{\mathrm{pr}}(C)$ is testable in polynomial time. In other words zero-tests in $\mathrm{Jac}(C)$ can be performed in polynomial time.*

Combining Lemma 2.4, Proposition 2.5 and Lemma 2.6, one obtains a polynomial time algorithm to put a given divisor $D \in \mathrm{Jac}(C)(\mathbb{F}_q)$ into reduced form. Indeed by Lemma 2.4, one knows that the support of D can be chosen to be of size at most $\mathrm{poly}(g)$. Then, Proposition 2.5 can be applied to obtain the effective divisor E and the integer i, so that $D = E - (g - i)\infty$ is in reduced form as an element of $\mathrm{Jac}(C)$.

Remark. The points occurring in the support of the effective divisor E associated to the reduced form of D in the above description each lie in a $\mathrm{poly}(g)$ extension of $\mathbb{F}_q$. However, one never needs to go to an extension of $\mathbb{F}_q$ containing *all* of them simultaneously (which may be exponentially large in degree). The issue is handled exactly the same way in [Ked06, §6]. See also [HI94, §3] for more on this *implicit representation* of divisors used in their algorithm to do Jacobian arithmetic.

We are now ready to describe a randomised polynomial-time Algorithm 1 to compute the sum of two elements in $\mathrm{Jac}(C)$ in the canonical representation described above.

Algorithm 1 Adding two points on the Jacobian

- **Input:** Two divisors $D_1 = E_1 - m_1(\infty)$ and $D_2 = E_2 - m_2(\infty)$ of degree zero, with $m_1, m_2 \leq g$ lying in the Jacobian of a smooth projective curve $C/\mathbb{F}_q$, presented in the reduced form as per Lemma 2.4.
- **Output:** $D_3 = D_1 + D_2$ as $D_3 = E_3 - m_3(\infty)$ where E_3 is effective of degree m_3.

```
(Reduction loop) For each $i$, compute $\mathcal{L}(D_1 + D_2 + (g-i)(\infty))$ using Proposition 2.5,
    starting from $i = 0$. If $\dim \mathcal{L}(D_1 + D_2 + (g-i)(\infty)) = 1$ then we get a unique effective
    divisor $E := \mathrm{div}(f) + D_1 + D_2 + (g-i)(\infty)$, where the representation of $\mathrm{div}(f)$ can
    be found in randomised polynomial-time [LL91]. Choose the largest such $i$ and set
    $m_3 = g - i$ and $E_3 = E$.
Output $E_3 - m_3(\infty)$.
```

2.3 $\mathrm{AM} \cap \mathrm{coAM}$ protocol

In this section, we present an $\mathrm{AM} \cap \mathrm{coAM}$ protocol to certify the order (and group structure) of $\mathrm{Jac}(C)(\mathbb{F}_q)$. We then show how to certify the zeta function of C using this. We first recall a result of Weil [Wei48a, pp.70-71] which generalises a theorem of Hasse [Has36, p.206] from elliptic curves ($g = 1$) to abelian varieties ($g \geq 1$).

Proposition 2.7 (Hasse-Weil interval). *For an abelian variety A of dimension g over the finite field $\mathbb{F}_q$, the number of $\mathbb{F}_q$-rational points is in the following range:*

$$(\sqrt{q} - 1)^{2g} \ \leq \#A(\mathbb{F}_q) \ \leq (\sqrt{q} + 1)^{2g} .$$

Reduced gap. Given an input curve of genus g we want to choose q so that the above gap is small enough, namely, $((\sqrt{q}+1)/(\sqrt{q}-1))^{2g} < 2$. In particular, we require

$$1 + \frac{2}{\sqrt{q} - 1} \ < \ 2^{1/2g} \ = \ \exp\left(\frac{\log 2}{2g}\right) = 1 + \frac{\log 2}{2g} + \frac{(\log 2)^2}{8g^2} + \ldots$$

Truncating, we notice that $q > (8g+1)^2$ suffices.

Hash functions are pseudorandom maps from large strings to small strings, in a way that minimizes *collision* as much as possible. Let $h : \{0,1\}^n \mapsto \{0,1\}^k$; $k \ll n$ be from a hash family. We require that for $X \in \{0,1\}^n$ and a random $Y \in \{0,1\}^k$, $\Pr_{h,Y}[h(X) = Y] = 1/2^k$. One can show that, for a random $k \times n$ matrix A over $\mathbb{F}_2$, and a random vector $b \in \{0,1\}^k$, $h : X \mapsto AX + b$ satisfies this property (see [AB09, Theorem 8.15]). Using this concept, Algorithm 2 is the $\mathrm{AM} \cap \mathrm{coAM}$ protocol to verify the Jacobian size, over $\mathbb{F}_Q \supseteq \mathbb{F}_q$ assuming $Q > (8g+1)^2$.

Lemma 2.8 (Probability of Algorithm 2). *In Algorithm 2 (given candidate $\mathcal{N}$), if $\#\mathrm{Jac}(C)(\mathbb{F}_Q) = \mathcal{N}$, then Arthur accepts with probability $> 2/3$. Else, Arthur* rejects *with probability $> 2/3$.*

Proof. We adapt the protocol from [AB09, §9.4]. Let $S \subset \{0,1\}^{2g \log Q}$ denote the set $\mathrm{Jac}(C)(\mathbb{F}_Q)$ with the elements written as binary strings. Let $\mathcal{G}$ be the group generated by the divisors D_i's that Merlin provided. Suppose it has size $\mathcal{N}$, as Merlin claimed. In particular, $\mathcal{G} = S$ as we have made the Hasse-Weil 'gap' small enough so that only a unique multiple of $\mathcal{N}$ can lie in that interval. For a random $y \in \{0,1\}^{L+1}$ and a random

Algorithm 2 Verifying the size and structure of the Jacobian of $C/\mathbb{F}_Q$

Input: A smooth projective *curve* $C \subset \mathbb{P}^N$ of genus g and degree δ, given by polynomials $(f_i)_{1\leq i\leq m}$. A *candidate* integer $\mathcal{N}$ lying in the Hasse-Weil interval. Set L: $2^{L-1} < \mathcal{N} \leq 2^L$.

1: **Arthur**: Choose a random hash function $h : \{0,1\}^{2g\log Q} \to \{0,1\}^{L+1}$ by picking a matrix A and a vector b randomly as stated above. Pick a random $y \in \{0,1\}^{L+1}$ and send (h, y) to Merlin as a *challenge*. **Note:** Arthur could send $O(L)$ many such independently chosen pairs (h, y) to reduce the error probability exponentially. Below, we use only one pair for the simplicity of exposition.

2: **Merlin**:

- Pick r generators $D_i \in \mathrm{Jac}(C)(\mathbb{F}_Q)$ $(i \in [r])$ such that

  $$\mathrm{Jac}(C)(\mathbb{F}_Q) \;\simeq\; \langle D_1\rangle \times \ldots \times \langle D_r\rangle$$

  with each D_i of order n_i, with $n_i|n_{i+1}$ and $\prod_{i=1}^r n_i = \mathcal{N}$. Each D_i is presented in canonical form as $D_i = E_i - m_i(\infty)$, with E_i effective of degree m_i. The divisors E_i in turn are presented as a sum of $\overline{\mathbb{F}}_Q$ – rational points of C, each defined over an extension of $\mathbb{F}_Q$ of degree at most poly(g) thanks to Lemma 2.4.

- Send a *response* consisting of r quadruples $\{(c_i, D_i, n_i, P_i)\}_{1\leq i\leq r}$ with the claim that the divisor $\sum_i c_iD_i =: x$, for $c_i \in \mathbb{Z}/n_i\mathbb{Z}$, satisfies $h(x) = y$. Every P_i is a set of pairs: each consisting of a prime factor of n_i and the corresponding exponent in its factorisation.

3: **Arthur**:

- Check whether D_i indeed represents a point in $\mathrm{Jac}(C)(\mathbb{F}_Q)$. This is done by evaluating the Frobenius F_Q on $D_i = E_i - m_i(\infty)$ and checking for invariance. If not, *Reject*.

- Check the factorization data P_i of each n_i. Check the order n_i as follows: verify $n_iD_i = 0$, and for each distinct prime factor $p_{i,j}$ of n_i, verify $(n_i/p_{i,j})D_i \neq 0$. Check that $\mathcal{N} = \prod_{i=1}^r n_i$. If a check fails, *Reject*. Calculate $x = \sum_i c_iD_i$.

- Check $h(x) = h\left(\sum_i c_iD_i\right) = y$, if yes then *Accept*; otherwise *Reject*. All the checks can be easily performed by Arthur using: basic arithmetic, or Algorithm 1, combined with the standard trick of repeated-doubling.

hash function h (chosen from a uniform distribution over matrices A and vectors b such that $h : x \mapsto Ax + b$), the probability that there is an $x \in \mathcal{G} = S$, such that $h(x) = y$ is

$$\begin{aligned}\Pr[\exists x \in \mathcal{G} = S,\ h(x) = y] \geq \binom{\#S}{1} \cdot \frac{1}{2^{L+1}} - \binom{\#S}{2} \cdot \frac{1}{2^{2(L+1)}} &> \frac{\#S}{2^{L+1}} - \frac{(\#S)^2}{2^{2(L+1)+1}} \\ &> \frac{\#S}{2^{L+1}}\left(1 - \frac{\#S}{2^{L+2}}\right) \geq 0.75 \cdot \frac{\#S}{2^{L+1}} . \qquad (2.1)\end{aligned}$$

from the inclusion-exclusion-principle, and applying the inequality $2^{L-1} < \#S = \mathcal{N} \leq 2^L$.

Conversely, suppose $\#S \neq \mathcal{N}$, as Merlin bluffed (so, $\mathcal{G} \neq S$). Since Arthur checked that the product of the orders of the divisors D_i's equals $\mathcal{N}$, we deduce that $\#\mathcal{G} \leq \#S/2$ (as the order of the subgroup $\mathcal{G}$ properly divides that of the group S). So, simply by the union-bound we get

$$\Pr[\exists x \in \mathcal{G},\ h(x) = y] \leq \binom{\#\mathcal{G}}{1} \cdot \frac{1}{2^{L+1}} \leq 0.5 \cdot \frac{\#S}{2^{L+1}} . \qquad (2.2)$$

Thus, Eqns.2.1-2.2 have a noticeable difference in the probability estimate. Now, we can repeat, with Arthur choosing several (h, y) pairs, take the 'majority vote', and use the Chernoff bound [AB09, §7.4.1]. This *amplification* trick brings the probabilities above 2/3 (in Eqn.2.1) and below 1/3 (in Eqn.2.2) respectively. The number of repetitions will be inverse-polynomial in $\#S/2^{L+1} > 1/4$; which is only a constant blowup in our time complexity. □

Remark. The steps of Merlin require exponential resources (i.e. Step 2), so we do not know how to compute them in polynomial-time in practice. The purpose is to only provide a concise certificate, using which Arthur can verify the Jacobian-size efficiently and reliably (with high probability).

Lemma 2.9 (Complexity of Algorithm 2)**.** *Arthur's verification algorithm runs in randomised polynomial-time.*

Proof. Step 1 simply involves addition and multiplication, of matrices over $\mathbb{F}_2$, so it needs $\text{poly}(g \log Q) = \text{poly}(g \log q)$ time. In Step 3, since the number of prime factors of any integer n is $O(\log n)$, the prime factor checking computation can be performed in $\text{poly}(\log \mathcal{N})$ time. Applying the Hasse-Weil bound, this is $\text{poly}(g \log q)$ time. For the Jacobian arithmetic, Arthur uses Algorithm 1 and repeated-doubling. This sums up the complexity of our protocol to $\text{poly}(g, \log q)$-time. □

The zeta function is intimately connected to the order of the Jacobian. From [Ked06, §8]:

Lemma 2.10 (Count to zeta function)**.** *Assume we are given $\#\text{Jac}(C)(\mathbb{F}_{q^j})$, for every $1 \leq j \leq \max(18, 2g)$. Then, $P_1(C/\mathbb{F}_q, T)$ can be reconstructed from these counts, in poly($g \log q$)-time.*

Kedlaya [Ked06, §8] also shows the following, connecting the zeta function of a larger Frobenius to that of a *smaller* Frobenius.

Lemma 2.11 (Base zeta function)**.** *Let primes m_1, m_2 with $m_1 < m_2$, be such that $m_j - 1$ is divisible by a prime greater than $2g$, for $j \in \{1, 2\}$. Assume further that $q^{m_1} > (8g+1)^2$. Then, $P_1(C/\mathbb{F}_q, T)$ can be recovered from $P_1(C/\mathbb{F}_{q^{m_j}}, T)$, $j \in \{1, 2\}$, in time polynomial in $g \log q$. Further, the existence of such m_1, m_2 bounded by a polynomial in $g \log q$ is guaranteed.* [2]

[2] by [Har05, Theorem 1.2]

Proof of Theorem 2.1. Using Algorithm 2, we can verify the structure of $\mathrm{Jac}(C)(\mathbb{F}_Q)$ for any $Q > (8g+1)^2$. This implies $P_1(C/\mathbb{F}_q, T)$ can be certified by first certifying $P_1(C/\mathbb{F}_{q^{m_1}}, T)$ and $P_1(C/\mathbb{F}_{q^{m_2}}, T)$ and next applying Lemma 2.11. Each $P_1(C/\mathbb{F}_{q^{m_j}}, T)$ can be computed, uniquely, using the counts $\#\mathrm{Jac}(C)(\mathbb{F}_{q^{im_j}})$, for $1 \leq i \leq \max(18, 2g)$, by Lemma 2.10. This completes the proof of the first part of the theorem, verifying the zeta function.

Group structure. In the second part of the theorem statement, suppose a candidate G has been provided via additive generators $\{A_1, \ldots, A_r\}$, with each A_i of order n_i such that G decomposes as a direct sum of the subgroups $\langle A_i \rangle$, where $n_i \mid n_{i+1}$. We need to verify whether $\mathrm{Jac}(C)(\mathbb{F}_q) \simeq G$. For this, Merlin first convinces Arthur of the structure of $\mathrm{Jac}(C)(\mathbb{F}_Q)$, and provides the additive generators for $Q > (8g+1)^2$. Using this, Arthur can compute $P_1(C/\mathbb{F}_q, T)$, thereby obtaining the count $\#\mathrm{Jac}(C)(\mathbb{F}_q) = P_1(C/\mathbb{F}_q, 1)$. For the subgroup $\mathrm{Jac}(C)(\mathbb{F}_q) \subset \mathrm{Jac}(C)(\mathbb{F}_Q)$, Merlin presents divisors D_i with support in $C(\mathbb{F}_Q)$, that are candidates corresponding to each A_i. Arthur first checks whether the D_i all belong to $\mathrm{Jac}(C)(\mathbb{F}_q)$ (by evaluating the q-Frobenius on them and verifying invariance). Next, Arthur verifies the independence of the D_i as in Algorithm 2. This provides a lower bound for $\#G$. Comparing it with the verified count $\#\mathrm{Jac}(C)(\mathbb{F}_q)$ certifies the structure. The proof then follows from Lemmas 2.8-2.9. □

Chapter 3

Effective gcd theorem

In this chapter, we prove an effective, probabilistic version of Deligne's 'théorème du pgcd' [Del80, Théorème 4.5.1] for a smooth, projective, geometrically integral (nice) variety $X_0 \subset \mathbb{P}^N$ over $\mathbb{F}_q$ of dimension n and degree D, obtained via good reduction from a nice variety $\mathcal{X}_0$ over a number field K at a prime $\mathfrak{p} \subset \mathcal{O}_K$. As a consequence of the hard-Lefschetz theorem for X, Deligne [Del80, Théorème 4.5.1] showed the following.

Theorem. *The polynomial $P_{n-1}(X/\mathbb{F}_q, T)$ is the least common multiple of all polynomials*

$$f(T) = \prod_j (1 - \alpha_j T) \in \mathbb{C}[T],$$

satisfying the condition that for any $t \in U(\mathbb{F}_{q^r})$, the polynomial

$$f(T)^{(r)} := \prod_j (1 - \alpha_j^r T)$$

divides $P_{n-1}(X_t/\mathbb{F}_{q^r}, T)$.

Treating the embedding dimension N as constant, our result is as follows.

Theorem. *There exists a polynomial $\Phi(x) \in \mathbb{Z}[x]$ independent of q and* $\deg X = D$*, such that for any extension $\mathbb{F}_Q/\mathbb{F}_q$ with*

$$[\mathbb{F}_Q : \mathbb{F}_q] > \Phi(D),$$

we have for any $u_1, u_2 \in U(\mathbb{F}_Q)$ chosen uniformly at random,

$$P_{n-1}(X/\mathbb{F}_Q, T) = \gcd\left(P_{n-1}(X_{u_1}/\mathbb{F}_Q, T), P_{n-1}(X_{u_2}/\mathbb{F}_Q, T)\right);$$

with probability $> 2/3$.

The main ingredients include bounding torsion in the Betti cohomology of $\mathcal{X}_0$, a mod $-$ ℓ big monodromy result and equidistribution of Frobenius in the representation associated to the sheaf of vanishing cycles modulo ℓ. One has the following algorithmic consequence.

Corollary. *There is a polynomial-time reduction for the zeta function computation of nice varieties (coming from number fields via good reduction) over finite fields to that of the middle cohomology.*

This chapter is based on joint work with Hyuk Jun Kweon [KV25], generalising the case for surfaces in [RSV24, Theorem 4.6] [1], which is joint work with Diptajit Roy and Nitin Saxena.

[1] addressing the first cohomology

Credits

I thank Saugata Basu, Chris Hall, Donu Arapura, Nitin Saxena, Jeff Achter, TN Venkataramana, Arvind Nair, Santosh Nadimpalli, Bruno Kahn, Daniel Litt and Jason Fulman for various discussions regarding this work. I thank Alan Lauder and George Walker for making the thesis [Wal09] available. I thank Jason Fulman and Robert Guralnick for informing me of their work [FG25]. Part of this work was conceived during the 'Mordell Conjecture: 100 years later' conference at MIT in 2024, for which I'd like to thank the organisers. I thank the Research-I Foundation of Department of CSE, IIT Kanpur; and the Simons Foundation for travel funding support.

3.1 Ideas

In the DPhil dissertation of Walker [Wal09, 1.2.2], the possibility of using Deligne's gcd theorem is discussed in the context of developing algorithms to compute the zeta function of smooth, projective varieties. By the weak-Lefschetz theorem, cohomology in degrees other than the middle band of $n-1$, n, $n+1$ maps isomorphically to the cohomology of a hyperplane section. Further, in [RSV24, Theorem 1.4], an algorithm was given to compute $P_1(T)$ for any smooth, projective variety by proving the effective gcd theorem in the surface case (the torsion bounds here are due to [Kwe21]), and reducing to known algorithms for curves. This present work is a generalisation to n dimensions, in particular, handling both the cases of symplectic and orthogonal monodromy. In the light of Theorem 6.6, our theorem gives rise to algorithms to compute $P_2(T)$ for any smooth, projective variety as well.

Our proof strategy begins by finding a prime ℓ of reasonable size, for which the hard-Lefschetz theorem holds with $\mathbb{Z}/\ell\mathbb{Z}$ – coefficients; which reduces to the condition of the integral ℓ-adic cohomology groups being torsion free. To this regard, we first obtain torsion bounds in the characteristic zero Betti setting using cylindrical algebraic decomposition.

Choosing a torsion-free ℓ, hard-Lefschetz modulo ℓ implies the irreducibility of the representation associated to the local system of vanishing cycles modulo ℓ on U. If the ℓ–adic monodromy is infinite, this implies that the monodromy image is 'big', using a result of Hall [Hal08]. An equidistribution theorem of Katz [KS99] then dictates the likelihood of two Frobenii having coprime characteristic polynomials, which we make precise by bounding the error term therein.

3.2 Torsion bounds

The aim of this section is to give explicit upper bounds on the order of the torsion subgroups of cohomology groups. The bound is singly exponential in the degree of the defining polynomials and triply exponential in the dimension of the ambient projective space. To obtain these upper bounds, we will use a regular cellular decomposition of the variety. The number of cells will then provide an upper bound on the order of the torsion subgroups. The main tool for finding such a cellular decomposition is cylindrical algebraic decomposition, introduced by Collins [Col76].

Theorem 3.1. *Let $X \subset \mathbb{R}^N$ be a compact real algebraic variety defined by m polynomials of degree $\leq d$. Then there is a regular cell complex, with number of cells at most*

$$(2d)^{3^{N+1}} m^{2^N}.$$

Proof. Collins' algorithm computes a cylindrical algebraic decomposition of X with at most $(2d)^{3^{N+1}} m^{2^N}$ cells [Col76, Theorem 12]. Although this may not yield a regular cellular decomposition [DLS20, Example 2.1], performing a generic linear change of coordinates before running the algorithm ensures that the cylindrical algebraic decomposition becomes a regular cell complex [SS83, Theorem 2]. □

The theorem above depends on the number m of polynomials defining the variety X. This is bounded by the number of monomials of degree $\leq d$, meaning that

$$m \leq \binom{N+d}{N}.$$

Lemma 3.2. *Let M be an $m \times n$ matrix representing a linear transformation*

$$\varphi \colon \mathbb{Z}^n \to \mathbb{Z}^m.$$

Suppose that all entries of M are either -1, 0, or 1. Then

$$\#\mathrm{coker}(\varphi)_{\mathrm{tors}} \leq \min\{m!, n!\}.$$

Proof. Let D be the Smith Normal Form of M, with diagonal entries $d_0, d_1, \ldots, d_{r-1}$. Then

$$\begin{aligned} \mathrm{coker}(\varphi)_{\mathrm{tors}} &\simeq \mathbb{Z}/d_0\mathbb{Z} \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_{r-1}\mathbb{Z} \\ \#\mathrm{coker}(\varphi)_{\mathrm{tors}} &= d_0 d_1 \cdots d_{r-1}. \end{aligned}$$

Moreover, $d_0 d_1 \cdots d_{r-1}$ is the greatest common divisor of the determinants of all $r \times r$ minors of M. Since the Leibniz expansion for such a minor consists of $r!$ terms,

$$d_0 d_1 \cdots d_{r-1} \leq r! \leq \min\{m!, n!\}.$$ □

Now, Theorem 3.1 together with Lemma 3.2 gives the following theorem.

Theorem 3.3. *Let $X \subset \mathbb{R}^N$ be a compact real algebraic variety defined by polynomials of degree $\leq d$. Then*

$$\#\mathrm{H}^i_{\mathrm{B}}(X, \mathbb{Z})_{\mathrm{tors}} \leq \left((2d)^{3^{N+1}} \binom{N+d}{N}^{2^N} \right)!.$$

Remark. We denote Betti cohomology with $\mathrm{H}^i_{\mathrm{B}}$ and étale cohomology with H^i.

The above theorem applies only when X is a real affine variety, and the set of its $\mathbb{R}$-points is compact. We aim to obtain a similar bound for the case where X is a complex projective variety. This can be achieved by using the standard embedding $\mathbb{CP}^N \to \mathbb{C}^{(N+1)^2}$ and dividing each complex coordinate into two real coordinates.

Theorem 3.4. *Let $X \subset \mathbb{CP}^N$ be a complex projective variety defined by homogeneous polynomials of degree $\leq d$. Then*

$$\#\mathrm{H}^i_{\mathrm{B}}(X,\mathbb{Z})_{\mathrm{tors}} \leq \left((2d)^{3^{(N+1)^2+1}} \binom{(N+1)^2+d}{(N+1)^2}^{2^{(N+1)^2}} \right)!.$$

Proof. Recall that the standard embedding $\mathbb{CP}^N \to \mathbb{C}^{(N+1)^2}$ is given by

$$(z_0 : z_1 : \cdots : z_N) \mapsto \frac{1}{\sum_{i=0}^N |z_i|^2} \begin{pmatrix} z_0\overline{z_0} & z_0\overline{z_1} & \cdots & z_0\overline{z_N} \\ z_1\overline{z_0} & z_1\overline{z_1} & \cdots & z_1\overline{z_N} \\ \vdots & \vdots & \ddots & \vdots \\ z_N\overline{z_0} & z_N\overline{z_1} & \cdots & z_N\overline{z_N} \end{pmatrix}.$$

The image is defined by polynomials of degree ≤ 2. A hypersurface in $\mathbb{CP}^N$ defined by a homogeneous polynomial f can be expressed by several polynomials of the same degree in $\mathbb{C}^{(N+1)^2}$. Since the image of the embedding is a Hermitian matrix, half of the real coordinates can be reconstructed from the other half. Thus, applying Theorem 3.3 yields the desired result. □

Corollary 3.5. *Let $X \subset \mathbb{CP}^N$ be a complex projective variety defined by homogeneous polynomials of degree $\leq d$. Then*

$$\#\mathrm{H}^i_{\mathrm{B}}(X,\mathbb{Z})_{\mathrm{tors}} \leq 2^{d^{2^{3N^2}}}.$$

Proof. We may assume that $d \geq 2$ and $N \geq 4$, because projective spaces, hypersurfaces and curves do not have torsion in their cohomology groups. For simplicity let $M = N+1$ and

$$L = (2d)^{3^{M^2+1}} \binom{M^2+d}{M^2}^{2^{M^2}}.$$

Since

$$\binom{M^2+d}{M^2} \leq (M^2+d)^{M^2} \leq \left(d^M\right)^{M^2} = d^{M^3},$$

we obtain

$$L \leq \left(d^2\right)^{3^{M^2+1}} \left(d^{M^3}\right)^{2^{M^2}} \leq d^{2\cdot 3^{M^2+1}+M^3 2^{M^2}}.$$

As a result,

$$\log_d \log_2 L! \leq 2\log_d L = 4\cdot 3^{M^2+1} + M^3 2^{M^2} \leq 2^{3(M-1)^2}.$$ □

Corollary 3.6. *Let $X \subset \mathbb{CP}^N$ be a complex projective variety defined by homogeneous polynomials of degree at most d. Then there exists a prime number*

$$\ell \leq d^{2^{4N^2}}$$

such that $\mathrm{H}^i_B(X,\mathbb{Z})$ is torsion-free for all i.

Proof. By Corollary 3.5,

$$\# \prod_{i=0}^N \mathrm{H}^i_{\mathrm{B}}(X,\mathbb{Z})_{\mathrm{tors}} < \left(2^{d^{2^{3N^2}}}\right)^N = 2^{Nd^{2^{3N^2}}}.$$

Therefore, there exists a prime number ℓ among the first

$$k = Nd^{2^{3N^2}}$$

primes such that $\prod_{i=0}^{N} \mathrm{H}^i_B(X, \mathbb{Z})$ is ℓ-torsion-free. Since $k \geq 4$, [Ros39, Theorem 2] implies that the k-th prime number is smaller than

$$k(\log k + 2 \log \log k) \leq k^2 \leq \left(Nd^{2^{3N^2}}\right)^2 \leq d^{2^{4N^2}}. \qquad \square$$

The sum of the Betti numbers of X has an upper bound that is polynomial in d and singly exponential in N [Mil64, Corollary 2].

Theorem 3.7 (Milnor)**.** *Let $X \subset \mathbb{CP}^N$ be a complex projective variety defined by homogeneous polynomials of degree $\leq d$. Then*

$$\sum_{i \geq 0} \operatorname{rank} \mathrm{H}^i_{\mathrm{B}}(X, \mathbb{Z}) \leq Nd(2d-1)^{2N+1}.$$

This bound is derived by bounding the number of critical points of a Morse function. Since a Morse cohomology is generated by these critical points, the number of generators of the torsion subgroups is also bounded by the same value. Thus, if the order of each generator is not excessively large, we expect to obtain an upper bound on the order of $\mathrm{H}^i_B(X, \mathbb{Z})_{\mathrm{tors}}$ that is singly exponential in d and doubly exponential in N. However, determining the boundary map in Morse homology requires solving differential equations arising from a pseudo-gradient field, and these solutions do not form a semi-algebraic set. This is the technical reason why it is difficult to derive a bound doubly exponential in N.

Further, as we are in the realm of complex, smooth, projective varieties, one may also look at other methods towards obtaining such bounds for torsion. Note firstly, using the Künneth formula, that it suffices to bound torsion in cohomology in even degree. Next, torsion therein can be of two types, algebraic or transcendental. Guaranteed that the torsion is algebraic, it may be possible to bound it using the connected components of the Chow variety of X. Examples with transcendental torsion seem to have the order depend on the degree of the variety in question (see [SV05, Theorem 3] for concrete examples using Godeaux surfaces). This line of work, involving explicitly constructing transcendental torsion algebraic cycles began with Atiyah and Hirzebruch [AH61], who thereby provided counterexamples to the integral Hodge conjecture. One is led to conjecture that the torsion coming from transcendental cycles can likewise be controlled uniformly by the degree of the variety.

Over fields of positive characteristic, Gabber's theorem [Gab83] guarantees the torsion-freeness of the integral ℓ –adic étale cohomology groups for all but finitely many ℓ, so one is tempted to make the analogous conjecture over arbitrary base fields as well.

Conjecture. There exist polynomials $\psi(x), \phi(x) \in \mathbb{Z}[x]$ such that for any smooth, projective variety $X \subset \mathbb{P}^N$ of dimension n and degree D over an algebraically closed field k, we have

$$\mathrm{H}^i(X, \mathbb{Z}_\ell)_{\mathrm{tors}} = 0$$

for $0 \leq i \leq 2n$, when

$$\ell > \psi(D^{\phi(N)})$$

is any prime number distinct from the characteristic of k.

3.3 Lefschetz pencils

Let $X_0/\mathbb{F}_q$ be a smooth, projective, geometrically irreducible variety of dimension $n > 1$ and degree $D > 0$. We suppose that it is presented as a subvariety of $\mathbb{P}^N$, given by a homogeneous ideal I generated by m polynomials $f_1, \dots, f_m$ of degree $\leq d$ for $d \in \mathbb{Z}_{>0}$. Denote by X the base change to the algebraic closure. Let ℓ be a prime distinct from the characteristic of the base field. We recall the following.

Definition 3.1. A *hyperplane section* of X is a codimension 1 subvariety $Y \subset X$ obtained by intersecting X with a hyperplane $H \subset \mathbb{P}^N$. A hyperplane H is said to intersect X *transversally* at $x \in X$ if $T_xX \not\subset H$, i.e., H does not contain the tangent space to X at x. Equivalently, this translates to the condition that $X \cap H$ is smooth at x. In general, H intersects X *transversally* if $H \cap X$ is a smooth, irreducible subvariety of codimension 1 of X.

Denote by $(\mathbb{P}^N)^\vee$ the dual projective space, parameterising hyperplanes in $\mathbb{P}^N$. We construct the *dual variety* to X, denoted $\check{X} \subset (\mathbb{P}^N)^\vee$ as follows. Let

$$\Omega := \{(x, H) \in X \times (\mathbb{P}^N)^\vee \mid x \in H,\ T_xX \subset H\}.$$

It is a closed subvariety of $X \times (\mathbb{P}^N)^\vee$. We define $\check{X}$ to be the projection of Ω onto its second factor. In particular, $\check{X}$ parameterises those hyperplanes that *do not* intersect transversally with X. We now state an effective version of Bertini's theorem, that ensures the availability of smooth hyperplane sections. The following is [Bal03, Theorem 1].

Proposition 3.8 (Effective Bertini)**.** *Let $W \subset \mathbb{P}^N$ be a smooth, irreducible variety of dimension n and degree D, defined over $\mathbb{F}_q$. Let $\mathbb{F}_Q/\mathbb{F}_q$ be an extension such that $Q > D(D-1)^n$. Then, there exists a hyperplane H defined over $\mathbb{F}_Q$ that intersects transversally with W.*

Definition 3.2. Let $X/\overline{\mathbb{F}}_q$ be as above. A *Lefschetz pencil* on X is a collection of hyperplanes $(H_t)_{t\in\mathbb{P}^1}$ such that there exists a line $L \simeq \mathbb{P}^1 \subset (\mathbb{P}^N)^\vee$; for e.g., $(\lambda, \mu) \mapsto \lambda F = \mu G$, for linear forms F, G on $\mathbb{P}^N$, satisfying the following conditions

- the *axis*, of the pencil, $\Delta := (F = 0) \cap (G = 0)$ in $\mathbb{P}^N$ intersects X transversally, i.e., $X \cap \Delta$ is smooth of codimension 2,
- there is a dense open subset $U \subset \mathbb{P}^1$ on which the associated intersections $(\lambda, \mu) \to X \cap (\lambda F = \mu G)$ are smooth and geometrically irreducible for $(\lambda, \mu) \in U$; and have only an ordinary double point as singularity for the finitely many $(\lambda, \mu) \notin U$.

It is a fundamental theorem that Lefschetz pencils exist on any smooth projective variety of dimension ≥ 2, over an algebraically closed field (see [Kat73]). Over arbitrary fields, Lefschetz pencils exist, subject to a degree ≥ 3 Veronese embedding.[2] We recall [JS12, Theorem 3].

Proposition 3.9. *There exists a nonempty open subscheme (after possibly passing to a degree ≥ 3 Veronese embedding) in the Grassmannian of lines $W_X \subset \mathrm{Gr}(1, (\mathbb{P}^N)^\vee)$ such that every $L \in W_X$ defines a Lefschetz pencil for X.*

[2] this adds an overhead of only a polynomial in the degree D of X.

Algorithm 3 Lefschetz pencil on a variety

- **Input:** A smooth projective variety $X_0/\mathbb{F}_q$ of degree D presented as a system of homogeneous polynomials of degree $\leq d$ in the projective space $\mathbb{P}^N$.
- **Pre-processing:** Replace X with the degree 3 Veronese image of X in $\mathbb{P} := \mathbb{P}^{\binom{N+3}{3}-1}$.
- **Output:** Hyperplanes F and G in $\mathbb{P}$ such that the line L through them in the dual $(\mathbb{P})^\vee$, is a Lefschetz pencil on X.

```
1: Take a field extension $\mathbb{F}_Q/\mathbb{F}_q$ with degree bounded by a polynomial in $D$, such that smooth hyperplane sections exist as in Proposition 3.8.
2: Select two random linear forms $F$ and $G$ on $\mathbb{P}$, such that they intersect transversally with $X$ (this is possible by Proposition 3.8).
3: The line $L$ in $(\mathbb{P})^\vee$ through $F$ and $G$ is a candidate Lefschetz pencil on $X$.
```

Lemma 3.10. *Algorithm 3 succeeds with probability at least* $1 - O(1/Q)$.

Proof. Indeed for $Q \gg D$, the locus of hyperplanes in $\mathbb{P}^\vee$ defined over $\mathbb{F}_Q$ that do not intersect transversally with X is given by the dual variety $\check{X}$, which by the Lang-Weil estimates, can be avoided with probability $1 - O(1/Q)$. Further, for two hyperplanes H_1 and H_2 that intersect transversally with X, the condition that they define a Lefschetz pencil on X is equivalent to the condition that the line through the corresponding points in $\mathbb{P}^\vee$ does not intersect the singular locus $\mathring{X}$ of $\check{X}$. For two randomly chosen hyperplanes, this is also ensured with probability greater than $1 - O(1/Q)$, again by a Lang-Weil argument.

One checks that the output is correct by computing the finite subset Z of 'bad' hyperplanes (which is possible in poly-time) and verifying that the associated fibres are indeed nodal curves. The latter can be done by blowing up at a singular point and checking that the exceptional divisor intersects the transformed curve at two points, which has a polynomial-time algorithm. □

3.4 Monodromy of vanishing cycles

In this section, we recall the notion of monodromy in the context of a Lefschetz pencil of hyperplane sections on a smooth, projective variety. The main objective is to show that the mod $-\ \ell$ monodromy is as large as possible for primes ℓ of a reasonable size.

Let X be a nice variety satisfying our main assumptions. We may fibre X as a Lefschetz pencil of hyperplane sections $\pi : \tilde{X} \to \mathbb{P}^1$, where $\tilde{X}$ is the variety obtained by blowing up X at the axis of the pencil, and the fibres of π are the hyperplane sections. Denote by $U \subset \mathbb{P}^1$ the locus of smooth fibres and by $Z := \mathbb{P}^1 \setminus U$, the finite set parameterising the nodal fibres. Let ℓ be coprime to q. Consider the constructible sheaf $\mathcal{F} := R^{n-1}\pi_\star\mathbb{Q}_\ell$ on $\mathbb{P}^1$. The restriction $\mathcal{F}|_U$ defines a local system on U, and we can speak of the monodromy action of the geometric étale fundamental group $\pi_1(U, u)$, where $u \to U$ is a geometric point. We know further, that $\pi_1(U, u)$ is topologically generated by $\#Z$ – many elements σ_i satisfying the relation $\prod_i \sigma_i = 1$. Further, for each $z \in Z$, one obtains a vanishing cycle $\delta_z \in \mathrm{H}^{n-1}(X_{\overline{\eta}}, \mathbb{Z}/\ell\mathbb{Z})$ via the exact sequence

$$0 \longrightarrow \mathrm{H}^{n-1}(X_z, \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{H}^{n-1}(X_{\overline{\eta}}, \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathbb{Z}/\ell\mathbb{Z}$$

with the final arrow being given by $\gamma \mapsto \langle \gamma, \delta_z \rangle$, where

$$\langle \cdot, \cdot \rangle : \mathrm{H}^{n-1}(X_{\overline{\eta}}, \mathbb{Z}/\ell\mathbb{Z}) \times \mathrm{H}^{n-1}(X_{\overline{\eta}}, \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathbb{Z}/\ell\mathbb{Z}$$

is the Poincaré duality pairing. Furthermore, δ_z is unqiuely determined upto sign by the Picard-Lefschetz formulas

$$\sigma_z(\gamma) = \gamma \pm \epsilon_z \cdot \langle \gamma, \delta_z \rangle \cdot \delta_z, \tag{3.1}$$

where for a uniformising parameter θ_z at z, we have $\sigma_z(\theta_z^{1/\ell}) = \epsilon_z \theta_z^{1/\ell}$. In the limit, we obtain an integral $\ell-$adic vanishing cycle in $\mathrm{H}^{n-1}(X_{\overline{\eta}}, \mathbb{Z}_\ell)$ which is defined upto torsion, and becomes unique upto sign upon tensoring with $\mathbb{Q}_\ell$. We call by $\mathcal{E}_{\overline{\eta}}$ the space generated by all the vanishing cycles δ_z[3] for $z \in Z$ in $\mathrm{H}^{n-1}(X_{\overline{\eta}}, \mathbb{Q}_\ell)$ and by $\mathcal{E}_u$ for $u \in U$, the image of $\mathcal{E}_{\overline{\eta}}$ under the specialisation isomorphism $\mathcal{F}_{\overline{\eta}} \to \mathcal{F}_u$.

By the hard-Lefschetz theorem [Del80, Theorem 4.3.9], we have for $u \in U$,

$$\mathcal{F}_u \simeq \mathrm{H}^{n-1}(X_u, \mathbb{Q}_\ell) \simeq \mathrm{H}^{n-1}(X, \mathbb{Q}_\ell) \oplus \mathcal{E}_u \ , \tag{3.2}$$

where $\mathcal{E}_u$ is the space of vanishing cycles at u. In particular,

$$\mathrm{H}^{n-1}(X, \mathbb{Q}_\ell) = \mathrm{H}^{n-1}(X_u, \mathbb{Q}_\ell)^{\pi_1(U,u)} = \mathcal{E}_u^{\perp} \ ,$$

with respect to the Poincaré duality pairing on $\mathrm{H}^{n-1}(X_u, \mathbb{Q}_\ell)$ and $\mathcal{E}_u \cap \mathcal{E}_u^{\perp} = 0$. Further, the sheaf $\mathcal{F}|_U$ decomposes as

$$\mathcal{F}|_U \simeq \underline{\mathcal{V}} \oplus \mathcal{E}$$

where $\underline{\mathcal{V}}$ is the constant sheaf on U associated to $\mathrm{H}^{n-1}(X, \mathbb{Q}_\ell)$ and $\mathcal{E}$ is the sheaf of vanishing cycles. The sheaf $\mathcal{E}$ is locally constant on U of rank, say, $r \in \mathbb{Z}_{\geq 0}$. Write $\mathcal{E}^{\mathbb{Z}_\ell}$ for the sheaf of integral $\ell-$adic vanishing cycles and denote by $\mathcal{E}^\ell := \mathcal{E}^{\mathbb{Z}_\ell} \otimes \mathbb{F}_\ell$ the sheaf of mod $-\ \ell$ vanishing cycles. We begin by showing the following.

Lemma 3.11. *Let ℓ be a prime coprime to q, such that the cohomology groups $\mathrm{H}^i(X, \mathbb{Z}_\ell)$ are all torsion-free for $0 \leq i \leq 2n$. Let X_u be a smooth hyperplane section of X from the above Lefschetz pencil. Then the cohomology groups $\mathrm{H}^j(X_u, \mathbb{Z}_\ell)$ for $0 \leq j \leq 2n-2$ are all torsion-free.*

Proof. By the Lefschetz hyperplane theorem [4], we know that the induced map $\mathrm{H}^j(X, \mathbb{Z}_\ell) \to \mathrm{H}^j(X_u, \mathbb{Z}_\ell)$ is an isomorphism for $j < n-1$. Moreover, we also know, by Poincaré duality, the Gysin map $\mathrm{H}^j(X_u, \mathbb{Z}_\ell) \to \mathrm{H}^{j+2}(X, \mathbb{Z}_\ell)$ is an isomorphism for $j > n-1$. It remains to show that $\mathrm{H}^{n-1}(X_u, \mathbb{Z}_\ell)$ is torsion-free. We recall the universal coefficient theorem for the affine variety $X \setminus X_u$ on cohomology with compact support

$$\mathrm{H}_c^{n-1}(X \setminus X_u, \mathbb{Z}/\ell\mathbb{Z}) = \left(\mathrm{H}_c^{n-1}(X \setminus X_u, \mathbb{Z}_\ell) \otimes \mathbb{Z}/\ell\mathbb{Z}\right) \oplus \mathbf{Tor}_1^{\mathbb{Z}_\ell}\left(\mathrm{H}_c^{n}(X \setminus X_u, \mathbb{Z}_\ell), \mathbb{Z}/\ell\mathbb{Z}\right). \tag{3.3}$$

By Artin vanishing and Poincaré duality, we know $\mathrm{H}_c^{n-1}(X \setminus X_u, \mathbb{Z}/\ell\mathbb{Z}) = 0$, so we have from (3.3) that $\mathrm{H}_c^{n}(X \setminus X_u, \mathbb{Z}_\ell)$ is torsion-free. Therefore, from the relative long exact sequence associated to the pair $(X, X \setminus X_u)$,

[3] abusing notation

[4] also known as the weak-Lefschetz theorem

$$\ldots \to \mathrm{H}^j_c(X \setminus X_u, \mathbb{Z}_\ell) \to \mathrm{H}^j(X, \mathbb{Z}_\ell) \to \mathrm{H}^j(X_u, \mathbb{Z}_\ell) \to \ldots \tag{3.4}$$

we see that

$$\mathrm{H}^{n-1}(X_u, \mathbb{Z}_\ell)/\mathrm{H}^{n-1}(X, \mathbb{Z}_\ell)$$

is torsion-free. We conclude the proof using the torsion-freeness assumption on $\mathrm{H}^{n-1}(X, \mathbb{Z}_\ell)$. □

Lemma 3.12. *Let ℓ be a prime coprime to q, such that the cohomology groups $\mathrm{H}^i(X, \mathbb{Z}_\ell)$ are all torsion-free for $0 \le i \le 2n$ and let X_u be a hyperplane section of X from the above Lefschetz pencil. Then, the hard-Lefschetz theorem holds modulo ℓ, i.e., we have*

$$\mathrm{H}^{n-1}(X_u, \mathbb{Z}/\ell\mathbb{Z}) \simeq \mathrm{H}^{n-1}(X, \mathbb{Z}/\ell\mathbb{Z}) \oplus \mathcal{E}^\ell_u. \tag{3.5}$$

Proof. From the diagram [Del80, (4.3.3.2)], we see that the exact sequence

$$0 \to \mathcal{E}^{\mathbb{Z}_\ell}_u \to \mathrm{H}^{n-1}(X_u, \mathbb{Z}_\ell) \to \mathrm{H}^{n+1}(X, \mathbb{Z}_\ell) \to 0$$

splits as the terms involved are all torsion-free. Next, one notices that the hard-Lefschetz map

$$\lambda : \mathrm{H}^{n-1}(X, \mathbb{Z}_\ell) \to \mathrm{H}^{n+1}(X, \mathbb{Z}_\ell)$$

obtained by taking cup-product with the class of X_u is injective by the hard-Lefschetz theorem and the fact that $\mathrm{H}^{n-1}(X, \mathbb{Z}_\ell)$ is torsion-free. The map is also surjective as we know

$$\mathrm{H}^{n-1}(X_u, \mathbb{Z}_\ell)/\mathrm{H}^{n-1}(X, \mathbb{Z}_\ell)$$

is torsion-free. Further, we note that $\mathrm{H}^{n-1}(X, \mathbb{Z}_\ell) \cap \mathcal{E}^{\mathbb{Z}_\ell}_u \subset \mathrm{H}^{n-1}(X_u, \mathbb{Z}_\ell)_{\mathrm{tors}} = 0$, by assumption. Therefore, we have

$$\mathrm{H}^{n-1}(X_u, \mathbb{Z}_\ell) \simeq \mathrm{H}^{n-1}(X, \mathbb{Z}_\ell) \oplus \mathcal{E}^{\mathbb{Z}_\ell}_u.$$

Tensoring by $\mathbb{Z}/\ell\mathbb{Z}$ and using torsion-freeness once more gives the result. □

Lemma 3.13 (Irreducibility)**.** *The representation $\rho_\ell : \pi_1(U, u) \to \mathrm{GL}(r, \mathbb{Z}/\ell\mathbb{Z})$ associated to the local system $\mathcal{E}^\ell$ of mod – ℓ vanishing cycles on U is irreducible.*

Proof. Let W denote the representation corresponding to the mod – ℓ vanishing cycles $\mathcal{E}^\ell_u$ and let $W' \subset W$ be a subspace fixed under the action of $\pi_1(U, u)$. Let $\gamma \in W'$ be such that $\gamma \neq 0$. We claim firstly that $\langle \gamma, \delta_z \rangle \neq 0$ for a vanishing cycle δ_z for some $z \in Z$. Otherwise, we would have $\gamma \in W^\perp \cap W$, which is trivial by Lemma 3.12. In particular, by the Picard-Lefschetz formula (3.1), we have $\sigma_z(\gamma) - \gamma = \langle \gamma, \delta_z \rangle \cdot \delta_z \in W'$, implying $\delta_z \in W'$. However, by [Ill06, Theorem 5.2], the vanishing cycles are all conjugate under the action of $\pi_1(U, u)$, so we must have $W' = W$. □

Theorem 3.14 (Big monodromy)**.** *Assume the sheaf $\mathcal{E}^{\mathbb{Z}_\ell}$ has big monodromy, i.e., the associated representation $\rho : \pi_1(U, u) \to \mathrm{GL}(\mathcal{E}^{\mathbb{Z}_\ell}_u)$ has Zariski dense image in the corresponding symplectic or orthogonal groups. Then the sheaf $\mathcal{E}^\ell$ has big monodromy, i.e., the mod – ℓ representation $\rho_\ell : \pi_1(U, u) \to \mathrm{GL}(r, \mathbb{Z}/\ell\mathbb{Z})$ has maximal image. In particular, if n is even, then $\mathrm{im}(\rho_\ell) = \mathrm{Sp}(r, \mathbb{Z}/\ell\mathbb{Z})$ and if n is odd, $\mathrm{im}(\rho_\ell)$ is one of the following subgroups of the orthogonal group $\mathrm{O}(r, \mathbb{Z}/\ell\mathbb{Z})$*

(a) the kernel of the spinor norm,

(b) the kernel of the product of the spinor norm and the determinant map,

(c) the full orthogonal group.

Proof. We intend to apply [Hal08, Theorem 3.1] to W. Assume firstly that n is even. In this case, the Poincaré duality pairing is alternating and W is even-dimensional. Then, the elements $\rho_\ell(\sigma_i)$ act via the Picard-Lefschetz formulas (4.4) as transvections on W. Using the irreducibility from Lemma 3.13, we may conclude that the image of ρ_ℓ is the full symplectic group $\mathrm{Sp}(r, \mathbb{F}_\ell)$.

In the case n is odd, the pairing is symmetric, so the monodromy is orthogonal. Here, the Picard-Lefschetz formulas act by reflections, in particular, even as isotropic shears. We again appeal to [Hal08, Theorem 3.1] to conclude that the geometric mod $-\ \ell$ monodromy must be one of the subgroups of the orthogonal group of index at most two (other than the special orthogonal group), as listed above. □

Remark. We note that using work of Katz [Kat04, Theorem 2.2.4], we may assume that $\mathcal{E}^{\mathbb{Z}_\ell}$ has big monodromy always (i.e., its image is infinite), at the cost of a Veronese embedding of constant degree.

3.5 Linear algebraic groups over finite fields

In this section, we provide probability estimates for the likelihood of characteristic polynomials being coprime in symplectic and orthogonal groups, for use in the proof of our effective gcd theorem. Subsequent to the writing of this section, we were informed of recent work of Fulman and Guralnick [FG25], that also addresses this issue [5] using different methods.

3.5.1 Symplectic monodromy

Let V be a vector space of rank $2r$, for $r \in \mathbb{Z}_{>0}$, over the finite field $\mathbb{F}_\ell$ of characteristic $\ell > 0$, equipped with a symplectic (i.e., alternating, nondegenerate, bilinear) pairing $\langle \cdot, \cdot \rangle$.

Definition 3.3. The group of *symplectic similitudes*, $\mathrm{GSp}(2r, \mathbb{F}_\ell)$ is defined as

$$\mathrm{GSp}(2r, \mathbb{F}_\ell) := \{A \in \mathrm{GL}(2r, \mathbb{F}_\ell) \mid \exists\ \gamma \in \mathbb{F}_\ell^* \text{ such that } \langle Av, Aw \rangle = \gamma \cdot \langle v, w \rangle\ \forall v, w \in V\}.$$

For $A \in \mathrm{GSp}(2r, \mathbb{F}_\ell)$, the associated $\gamma \in \mathbb{F}_\ell^*$ is called the *multiplicator* of A. We denote by $\mathrm{GSp}(2r, \mathbb{F}_\ell)^\gamma$ the subset of matrices with multiplicator γ. The matrices with multiplicator $\gamma = 1$ form a subgroup known as the *symplectic group*, denoted $\mathrm{Sp}(2r, \mathbb{F}_\ell)$. We have the following exact sequence

$$1 \longrightarrow \mathrm{Sp}(2r, \mathbb{F}_\ell) \longrightarrow \mathrm{GSp}(2r, \mathbb{F}_\ell) \xrightarrow{\text{mult}} \mathbb{F}_\ell^* \longrightarrow 1.$$

For any $\gamma \in \mathbb{F}_\ell^*$, collect the 'relevant' characteristic polynomials f in the set

$$M_r^\gamma := \{f(T) = 1 + a_1 T + \ldots + a_{2r-1} T^{2r-1} + \gamma^r T^{2r} \mid a_i \in \mathbb{F}_\ell,\ a_{2r-i} = \gamma^{r-i} a_i,\ 0 \le i \le 2r\}.$$

[5] Theorems 2.5, 2.7 and 2.8 of loc. cit.

We now give an estimate for the number of matrices with given characteristic polynomial $f(T)$. See [Cha97, Theorem 3.5] for a proof.

Lemma 3.15. *Fix $f(T) \in M_r^\gamma$. For $\ell > 4$, we have*

$$(\ell-3)^{2r^2} \;\leq\; \#\{A \in \mathrm{GSp}(2r, \mathbb{F}_\ell)^\gamma \mid f(T) = \det(1-TA)\} \;\leq\; (\ell+3)^{2r^2}\,.$$

We may identify M_r^γ with the points of the affine space $\mathbb{A}^r_{\mathbb{F}_\ell}$ with coordinates $(y_1, \ldots, y_r)$, by sending a polynomial $f(T) = 1 + \sum_{i=1}^{2r-1} a_i T^i + \gamma^r T^{2r}$ to the tuple $(a_1, \ldots, a_r)$.

Our goal is to obtain estimates for the proportion of characteristic polynomials that are *not* coprime to a given $f(T) \in M_r^\gamma$. Let $W \subset \mathbb{A}^r_{\mathbb{F}_\ell}$ parameterise such polynomials. It is a hypersurface, given by the vanishing of $F(y_1, \ldots, y_r)$, described as the resultant of a formal polynomial of the type

$$g(T) \;=\; 1 + \sum_{i=1}^{r} y_i T^i + \sum_{i=1}^{r-1} \gamma^{r-i} y_i T^{2r-i} + \gamma^r T^{2r}$$

with $f(T)$ w.r.t. T. The polynomial F is of total degree at most $4r$ in the y_i. The number of its rational points, $\#W(\mathbb{F}_\ell)$, gives the count we need. But, by [BS86, pg 45], we have $\#W(\mathbb{F}_\ell) \leq 4r\ell^{r-1}$. Further, recalling the order formula for the symplectic group, we have

$$\ell^{2r^2}(\ell-1)^r \;\leq\; \#\mathrm{Sp}(2r, \mathbb{F}_\ell) \;=\; \ell^{r^2}\prod_{j=1}^{r}(\ell^{2j}-1) \;\leq\; \ell^{2r^2+r}\,.$$

Therefore, combining with Lemma 3.15, the proportion of matrices in $\mathrm{GSp}(2r, \mathbb{F}_\ell)^\gamma$ with characteristic polynomial *not* coprime to $f(T)$ is at most

$$\frac{4r\ell^{r-1}\cdot(\ell+3)^{2r^2}}{\ell^{2r^2}(\ell-1)^r} \;=\; \frac{4r}{\ell}\left(1+\frac{1}{\ell-1}\right)^r\left(1+\frac{3}{\ell}\right)^{2r^2}\,,$$

which is less than $1/4$, for $\ell > 16e^2r^2$, where $e := \exp(1)$. We summarise what we have shown in the following.

Lemma 3.16 (Common eigenvalue)**.** *Let $r \in \mathbb{Z}_{>0}$ and let $\ell > 4$ be a prime. Let $f(T)$ be the characteristic polynomial of a matrix in $\mathrm{GSp}(2r, \mathbb{F}_\ell)^\gamma$ for some $\gamma \in \mathbb{F}_\ell^*$. Denote by $C \subset \mathrm{GSp}(2r, \mathbb{F}_\ell)$ the set of matrices with characteristic polynomial not coprime with $f(T)$. Then for $\ell > 119r^2$,*

$$\frac{\#\left(C \cap \mathrm{GSp}(2r, \mathbb{F}_\ell)^\gamma\right)}{\#\mathrm{Sp}(2r, \mathbb{F}_\ell)} \;\leq\; 1/4\,.$$

The orthogonal case is, as always, slightly trickier to handle given its non-simply-connected nature (of the special orthogonal group). Our methods for the estimate here are cruder and more geometric, but could really also be applied to the symplectic case.

3.5.2 Orthogonal monodromy

We are now concerned with the case when $n = \dim X$ is odd. In particular, we have that the action of Frobenius on $\mathrm{H}^{n-1}(X_u, \mathbb{Z}/\ell\mathbb{Z})$ is via an orthogonal similitude, i.e., the image $\rho_\ell(\pi_1(U_0, u)) \subset \mathrm{GO(V)}$, where V is the subspace $\mathcal{E}_u^\ell \subset \mathrm{H}^{n-1}(X_u, \mathbb{Z}/\ell\mathbb{Z})$ of dimension s, regarded as an $\mathbb{F}_\ell$ – vector space. We begin by recalling the well-known bounds for the size of the orthogonal group.

Lemma 3.17. *We have*

$$2\ell^{2r^2}(\ell-1)^r \leq \#\mathrm{O}(2r+1,\mathbb{F}_\ell) = 2\ell^{r^2}\prod_{i=1}^{r}(\ell^{2i}-1) \leq 2\ell^{2r^2+r}$$

and

$$\ell^{2r^2}(\ell-1)^r \leq \#\mathrm{O}(2r,\mathbb{F}_\ell) \leq 2\ell^{2r^2+r}$$

Let N_r^λ now be the space of reciprocal polynomials of degree at most $s = 2r$, or $s = 2r+1$ in one variable, with mulitplier λ and coefficients in $\mathbb{F}_\ell$. Like in the symplectic case, we have an exact sequence

$$1 \to \mathrm{O}(s,\mathbb{F}_\ell) \to \mathrm{GO}(s,\mathbb{F}_\ell) \to \mathbb{F}_\ell^* \to 1 \tag{3.6}$$

We may identify it with the affine space $\mathbb{A}^r$. For $\lambda \in \mathbb{F}_\ell^*$, consider a map

$$\Psi : \mathrm{GO}(s,\overline{\mathbb{F}}_\ell)^\lambda \to \mathbb{A}^r_{\overline{\mathbb{F}}_\ell}$$

where a matrix is mapped to its (reversed) characteristic polynomial. The map Ψ is a morphism of algebraic varieties. We know that $\dim \mathrm{O}(V) = s(s-1)/2$. Given $f(T)$ that we know is the characteristic polynomial of a matrix in $\mathrm{GO}(s,\mathbb{F}_\ell)$, we seek to estimate the size of $\Psi^{-1}(W) \cap \mathrm{GO}(s,\mathbb{F}_\ell)^\lambda$, where $W \subset \mathbb{A}^r$ parametrises those polynomials which have a factor common with $f(T)$. The map Ψ is clearly surjective over $\overline{\mathbb{F}}_\ell$, so applying the theorem on fibre dimension, we see that generically, for x in an open subset of $\mathbb{A}^r$, we have

$$\dim \Psi^{-1}(x) = s(s-1)/2 - r \leq 2r^2.$$

We observe the following next.

Lemma 3.18. *The fibre dimension of Ψ is constant and minimal on the open subset Y of $\mathbb{A}^r$ parametrising those characteristic polynomials with distinct roots. Moreover, writing $V = \mathbb{A}^r \setminus Y$, we have*

$$\frac{\#V(\mathbb{F}_\ell)}{\ell^r} \leq O(1/\ell)$$

where the implied constant is independent of ℓ and depends linearly on r. Further,

$$\frac{\#\Psi^{-1}(Y)(\mathbb{F}_\ell)}{\mathrm{O}(s,\mathbb{F}_\ell)} \geq 1 - \Omega(1/\ell),$$

where now, the implied constant is independent of ℓ and of the form $\exp(\mathrm{poly}(r))$.

Proof. For a characteristic polynomial in Y, its fibre consists of those matrices in $\mathrm{GO}(s,\mathbb{F}_\ell)^\lambda$ with distinct eigenvalues prescribed by the roots of said polynomial. This imposes r independent conditions on the fibre, and hence the generic fibre dimension of

$$s(s-1)/2 - r$$

is achieved here.

The complement V of Y is a hypersurface in $\mathbb{A}^r$ of degree at most $8r$, obtained via the vanishing of the discriminant associated to a formal characteristic polynomial. We conclude the first estimate using [BS86, pg 45]. For the second estimate, we note that $\Psi^{-1}(V)$ is now a proper, closed subvariety of $\mathrm{GO}(s)^\lambda$ of degree $\exp(\mathrm{poly}(r))$. The number of its $\mathbb{F}_\ell$ – rational points can be bounded via the Lang-Weil estimates [CM06, Theorem 7.5], and can thus be avoided with high probability.

□

Proposition 3.19. *Let $f(T) \in Y(\mathbb{F}_\ell) \subset N_r^\lambda$ be the reversed characteristic polynomial of a matrix in* $\mathrm{GO}(s, \mathbb{F}_\ell)^\lambda$*. Denote by Λ the set of matrices in* $\mathrm{GO}(s, \mathbb{F}_\ell)^\lambda$ *such that their reversed characteristic polynomial has a common factor with $f(T)$. Then*

$$\frac{\#\Lambda}{\#\mathrm{O}(s, \mathbb{F}_\ell)} \leq O(1/\ell),$$

where the implied constant is independent of ℓ and of the form $\exp(\mathrm{poly}(r))$*.*

Proof. Given $f(T)$, let $W_f \subset \mathbb{A}^r$ parametrise those polynomials which have a factor common with $f(T)$. It is a hypersurface, given by the vanishing of the formal resultant with $f(T)$ (see [RSV24, §3.3]). Then, the set Λ is just the set of $\mathbb{F}_\ell$ – rational points of $\Psi^{-1}(W_f) \subset \mathrm{GO}(s)$, which is a proper, closed subvariety of degree at most $r^{\mathrm{poly}(r)}$. Then, we may conclude by the Lang-Weil estimates [CM06, Theorem 7.5] applied to $\Psi^{-1}(W_f)$.

We remark finally, that our bounds can be improved using very recent work of Fulman and Guralnick [FG25, Theorems 2.5-2.8], who show that the probability of a random matrix in $\mathrm{O}(s, \mathbb{F}_\ell)$ or $\mathrm{Sp}(s, \mathbb{F}_\ell)$ having a given characteristic polynomial is at most

$$\frac{\mathrm{poly}(\log_\ell(s))}{\ell^{s/2-1}}.$$

This shows that the implied constant in our bounds can be assumed to be at most polynomial in r.

□

3.6 The effective gcd theorem

We begin by recalling a version of Deligne's equidistribution theorem [Del80] due to Katz [KS99, Theorem 9.7.13]. Let $U_0/\mathbb{F}_q$ be a smooth, affine, geometrically irreducible curve. Let U be the base change to the algebraic closure. Pick a geometric point $u \to U$, lying over a closed point $u_0 \in U(\mathbb{F}_q)$ and denote by $\overline{\pi}_1 := \pi_1(U, u)$ the geometric étale fundamental group. Let π_1 denote the arithmetic fundamental group $\pi_1(U_0, u)$. For any closed point $v \in U(\mathbb{F}_q)$, there exists an element $F_{q,v} \in \pi_1$ well-defined upto conjugacy, called the *Frobenius element* at v. It is defined as follows. Writing $v = \mathrm{Spec}(\mathbb{F}_q) \to U$, we obtain an induced map of fundamental groups

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to \pi_1(U_0, v) \simeq \pi_1.$$

The element $F_{q,v} \in \pi_1$ is simply the image in π_1 of the Frobenius element in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ under the composition of the above morphisms.

Given a map $\rho : \pi_1 \to G$ to a finite group, and a conjugacy-stable subset $C \subset G$, we seek to understand the proportion of points $v \in U(\mathbb{F}_{q^w})$ such that $\rho(F_{q^w,v})$ lies in C.

Theorem 3.20 (Katz)**.** *Assume there is a commutative diagram*

$$\begin{tikzcd}
1 \arrow[r] & \overline{\pi}_1 \arrow[r] \arrow[d, "\overline{\rho}"'] & \pi_1 \arrow[r] \arrow[d, "\rho"] & \hat{\mathbb{Z}} \arrow[r] \arrow[d, "1 \mapsto -\gamma"] & 1 \\
1 \arrow[r] & \overline{G} \arrow[r] & G \arrow[r, "\mu"] & \Gamma \arrow[r] & 1
\end{tikzcd}$$

where G is a finite group, Γ is abelian, $\overline{\rho}$ is surjective and tamely ramified. Let $C \subset G$ be stable under conjugation by elements of G. Then

$$\left| \frac{\#\{v \in U(\mathbb{F}_{q^w}) \mid \rho(F_{q^w,v}) \in C\}}{\#U(\mathbb{F}_{q^w})} - \frac{\#(C \cap G^{\gamma^w})}{\#\overline{G}} \right| \leq |\chi(U)| \frac{\#G\sqrt{q^w}}{\#U(\mathbb{F}_{q^w})},$$

where $G^{\gamma^w} = \mu^{-1}(\gamma^w)$ and $\chi(U) = \sum_{i=0}^{1}(-1)^i \dim \mathrm{H}^i(U, \mathbb{Q}_\ell)$ is the ℓ-adic Euler-Poincaré characteristic of U.

Proof. See [Cha97, Theorem 4.1]. □

With the above in mind, we can now prove our effective gcd theorem. We recall our assumptions. Let $\mathcal{X} \subset \mathbb{P}^N$ be a smooth, projective geometrically irreducible variety of dimension n and degree D, over a number field K. Let $\mathfrak{p}$ be a prime of good reduction, write $\mathbb{F}_q := \mathcal{O}_K/\mathfrak{p}$ and denote the variety $X/\mathbb{F}_q$ upon reduction. Let $(X_t)_{t\in\mathbb{P}^1}$ be a Lefschetz pencil of hyperplane sections on X. Denote by $Z \subset \mathbb{P}^1$ the finite set of nodal fibres and by $U = \mathbb{P}^1 \setminus Z$, the subscheme parameterising the smooth fibres.

Theorem 3.21. *There exists a polynomial $\Phi(x) \in \mathbb{Z}[x]$ independent of D and q, such that for any extension $\mathbb{F}_Q/\mathbb{F}_q$ with*

$$[\mathbb{F}_Q : \mathbb{F}_q] > \Phi(D),$$

we have for any $u_1, u_2 \in U(\mathbb{F}_Q)$ chosen uniformly at random,

$$P_{n-1}(X/\mathbb{F}_Q, T) = \gcd\left(P_{n-1}(X_{u_1}/\mathbb{F}_Q, T), P_{n-1}(X_{u_2}/\mathbb{F}_Q, T)\right);$$

with probability $> 2/3$.

Proof. Let ℓ be a large enough prime such that the groups $\mathrm{H}^i(X, \mathbb{Z}_\ell)$ are all torsion-free. We can choose ℓ to be $\Omega(D^{2^{4N^2}})$ by the proof of Corollary 3.6. Consider now the locally constant sheaf $\mathrm{R}^1\pi_\star\mathbb{Z}_\ell|_U$ on U. It has as subsheaf $\mathcal{E}^{\mathbb{Z}_\ell}$ the sheaf of vanishing cycles. Write $\mathcal{E}^\ell = \mathcal{E}^{\mathbb{Z}_\ell} \otimes \mathbb{F}_\ell$ for the locally constant sheaf of mod $-$ ℓ vanishing cycles. Let $\rho_\ell : \pi_1(U_0, u) \to \mathrm{GL}(s, \mathbb{F}_\ell)$ be the associated representation, and denote by $\overline{\rho}_\ell := \rho_\ell|\pi_1(U, u)$ the restriction to the geometric fundamental group. We begin by assuming that the sheaf $\mathcal{E}^{\mathbb{Z}_\ell}$ has big monodromy. Indeed by the results of [Del80, 4.4], we know that the monodromy is either big or finite, with the latter only happening in the orthogonal case.

We begin with the case of symplectic monodromy, i.e., n is even, and by Theorem 3.14, the image of $\overline{\rho}_\ell$ is $\mathrm{Sp}(s, \mathbb{F}_\ell)$. We seek to apply Theorem 3.20 to this setup with $\overline{G} = \mathrm{Sp}(s, \mathbb{F}_\ell)$. Let $\mathbb{F}_Q/\mathbb{F}_q$ be an extension where $Q := q^w$ and choose $u_1 \in U(\mathbb{F}_Q)$ randomly. We estimate the number of $v \in U(\mathbb{F}_Q)$ such that $P(\mathcal{E}_v/\mathbb{F}_Q, T)$ is coprime to $f(T) := P(\mathcal{E}_{u_1}/\mathbb{F}_Q, T)$. Write $\overline{f}(T) := f(T) \bmod \ell$.

Denote by $C \subset \mathrm{GSp}(2r, \mathbb{F}_\ell)$ the subset of matrices with characteristic polynomial not coprime to $\overline{f}(T)$. It is stable under conjugation by elements from $\mathrm{GSp}(2r, \mathbb{F}_\ell)$. Applying Theorem 3.20 to C, we get

$$\frac{\#\{v \in U(\mathbb{F}_Q) \mid \rho_\ell(F_{Q,v}) \in C\}}{\#U(\mathbb{F}_Q)} \leq \frac{\#(C \cap \mathrm{GSp}(2r, \mathbb{F}_\ell)^{\gamma^w})}{\#\mathrm{Sp}(2r, \mathbb{F}_\ell)} + |\chi(U)| \frac{\#\mathrm{GSp}(2r, \mathbb{F}_\ell)\sqrt{q^w}}{\#U(\mathbb{F}_Q)}.$$

By Lemma 3.16 (since $\ell > 119r^2$), the first summand on the RHS is $\leq 1/4$. From the calculation[6] of the étale cohomology of U (the projective line with $\#Z$ punctures), we deduce that $|\chi(U)| \leq \#Z \leq D^{N+1}$. Further, we see that s, which is the dimension of the space of vanishing cycles, is bounded above by the sum of the Betti numbers of the hyperplane section of X, which by Theorem 3.7, is at most $ND(2D-1)^{2N+1}$. Therefore, for $q^w > 2D^{N+1}$, we have

$$|\chi(U)|\frac{\#\mathrm{GSp}(s,\mathbb{F}_\ell)\sqrt{q^w}}{\#U(\mathbb{F}_Q)} \;\leq\; D^{N+1}\ell^{2s^2+s+1}\frac{\sqrt{q^w}}{q^w - D^{N+1}} \;\leq\; D^{N+1}D^{2^{4N^2}\cdot 4N^2D^2(2D)^{6N}}\frac{\sqrt{q^w}}{q^w/2}\,.$$

In particular, if

$$Q = q^w > \Omega\left(D^{2^{8N^2}\cdot N^2\cdot D^{4N}}\right),$$

we have

$$\frac{\#\{v \in U(\mathbb{F}_Q) \mid \rho_\ell(F_{Q,v}) \notin C\}}{\#U(\mathbb{F}_Q)} \;>\; 2/3\,,$$

which completes the proof for the symplectic case.

Now, we deal with the big orthogonal case, i.e., n is odd and the image of $\overline{\rho}_\ell$ is one of the subgroups $\overline{\mathrm{G}}$ of $\mathrm{O}(s,\mathbb{F}_\ell)$ of index at most two in Theorem 3.14. [7] Denote by G its extension by an appropriate subgroup of $\mathbb{F}_\ell^*$ via (3.6). Let $C' \subset \mathrm{GO}(V,\mathbb{F}_\ell)$ be the subset of matrices with characteristic polynomial having distinct roots. Then, applying Theorem 3.20, we see

$$\frac{\#\{v \in U(\mathbb{F}_Q) \mid \rho_\ell(F_{Q,v}) \in C'\}}{\#U(\mathbb{F}_Q)} \geq \frac{\#(C' \cap \mathrm{G}^{\gamma^w})}{\#\overline{\mathrm{G}}} - |\chi(U)|\frac{\#\mathrm{G}\sqrt{q^w}}{\#U(\mathbb{F}_Q)}.$$

By Lemma 3.18, the first term of the RHS can be maximised with growing ℓ, and the error term is minimised similar to the symplectic case. Now, for another trial $v' \in U(\mathbb{F}_Q)$ chosen uniformly at random, we maximise the probability of the associated characteristic polynomial being coprime to that of the earlier trial via a similar estimate using Proposition 3.19. □

[6] see [Sta18, Tag 03RR]

[7] We may assume the orthogonal monodromy is big by the remark after Theorem 3.14.

Part II

Surfaces

Synopsis

In this part, a randomised polynomial-time algorithm to compute the local zeta function of a surface at large primes of good reduction is developed. This is based on joint work with Nitin Saxena [SV25].

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 (4.5) coming from the Galois cohomology of the tame fundamental group of the line with the critical locus (i.e., the finite set $\mathcal{Z} = \mathbb{P}^1 \setminus \mathcal{U}$ where the fibres are nodal) removed. In particular, one needs to be able to compute 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 compute the local monodromy using this Puiseux expansion. Additionally, 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 also compute each vanishing cycle as an element in the cohomology $\mathcal{F}_{\overline{\eta}}$ of the generic fibre.

Following this, we move to the étale open cover $\mathcal{V} \to \mathcal{U}$ trivialising the locally constant sheaf $\mathcal{F} = \mathrm{R}^1\pi_\star\mu_\ell$ on $\mathcal{U}$. The normalisation of $\mathbb{P}^1$ in the function field of $\mathcal{V}$ yields a morphism of smooth projective curves $\tilde{\mathcal{V}} \to \mathbb{P}^1$ ramified exactly at $\mathcal{Z}$. Calling the representation $\rho_\ell : \pi_1(\mathcal{U}, \overline{\eta}) \to \mathrm{Aut}(\mathcal{F}_{\overline{\eta}})$, we write $G := \mathrm{im}(\rho_\ell)$, and note that the cover $\mathcal{V} \to \mathcal{U}$ has Galois group G. The group G acts naturally on $\tilde{\mathcal{V}}$ via automorphisms, which extends to an action on $\mathrm{H}^1(\tilde{\mathcal{V}}, \mu_\ell) \simeq \mathrm{Jac}(\tilde{\mathcal{V}})[\ell]$.

Further, to compute the part of $\mathrm{H}^2(\mathcal{X}, \mu_\ell)$ corresponding to $\mathrm{H}^1(\mathcal{U}, \mathcal{F})$, it suffices to compute the invariant subspace of $\mathrm{H}^1(\tilde{\mathcal{V}}, \mu_\ell) \otimes_{\mathbb{Z}/\ell\mathbb{Z}} \mathcal{F}_{\overline{\eta}}$, under the diagonal action of G. This is done by choosing an auxiliary prime $\mathfrak{P}$ with characteristic distinct from ℓ and of size $O(\ell)$, of good reduction and isolating the subspace spanned by the images of all G- equivariant homomorphisms from $\mathcal{F}_{\overline{\eta}}^\vee$ to $\mathrm{Jac}(\tilde{\mathcal{V}}_{\mathfrak{P}})[\ell]$ (which we call the mod-$\mathfrak{P}$ Edixhoven subspace) in the cohomology of the reduced curve. We then $\mathfrak{P}-$adically lift the concerned subspace to the char zero Edixhoven subspace $\mathbb{E}$, using work of Mascot [Mas20] on Hensel-lifting torsion points. With this, the arithmetic Galois action follows, along with zeta function and point counts, for large primes of good reduction.

Credits

I thank Jean-Pierre Serre for comments, particularly with regard to his question from [Ser16]. I thank Joe Silverman for references to the literature on heights. I thank Robin de Jong for references, discussions and detailed comments that have significantly improved the exposition. I thank Felipe Voloch for discussions that led to the discovery of an error in a previous version.

I am grateful to T.N. Venkataramana, Arvind Nair, Kiran Kedlaya, Eamonn O'Brien, and Ronald van Luijk for discussions, and the institutions University of Auckland, University of Canterbury, Ashoka University, ICTS, TIFR and MIT for their hospitality. I 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.

Chapter 4

Cohomological preliminaries

In this background chapter, we collect results on the cohomology of surfaces and algorithmic results on computing with the cohomology of the smooth, nodal, and generic fibres of a Lefschetz pencil on a surface.

4.1 Cohomology of a surface

In this section, we briefly recall cohomology computations for surfaces. A standard reference is [Mil80, V.3]. Let k be a separably closed field and let X be a smooth, projective geometrically irreducible surface over it. 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. Let ℓ be a prime distinct from the characteristic of k and write $\mathcal{F} := \mathrm{R}^1\pi_\star\mu_\ell$ 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]

$$\mathrm{H}^i(\tilde{X}, \mathbb{Q}_\ell) \simeq \begin{cases} \mathrm{H}^i(X, \mathbb{Q}_\ell),\ i \neq 2; \\ \mathrm{H}^2(X, \mathbb{Q}_\ell) \oplus \mathrm{H}^0(\Upsilon \cap X, \mathbb{Q}_\ell)(-1),\ i = 2 \end{cases} \tag{4.1}$$

so it suffices to compute the zeta function of $\tilde{X}$ (see Section 8.1). In Algorithm 4, we detail a method to compute equations for the blowup.

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

$$\mathrm{H}^i(X, \mu_\ell) \simeq \begin{cases} \mu_\ell,\ i = 0; \\ \mathrm{H}^0(\mathbb{P}^1, \mathcal{F}), i = 1; \\ \mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) \oplus \langle \gamma_E \rangle \oplus \langle \gamma_F \rangle,\ i = 2; \\ \mathrm{H}^2(\mathbb{P}^1, \mathcal{F}),\ i = 3; \\ \mu_\ell^\vee,\ i = 4; \\ 0,\ i > 4. \end{cases} \tag{4.2}$$

Algorithm 4 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.
```

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[1]

$$\phi_{z_j} : \mathcal{F}_{z_j} \hookrightarrow \mathcal{F}_{\overline{\eta}} \tag{4.3}$$

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 $\pi_1^{\mathrm{t}}(U, \overline{\eta})$, 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 $\gamma \in \mathcal{F}_{\overline{\eta}}$

$$\sigma_j(\gamma) = \gamma - \epsilon_j \cdot \langle \gamma, \delta_{z_j} \rangle \cdot \delta_{z_j}, \tag{4.4}$$

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 [2] 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 $\mathbb{F}_\ell^{2g}$, as it has to preserve the Weil pairing on $\mathcal{F}_{\overline{\eta}}$.

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

$$\mathcal{F}_{\overline{\eta}} \xrightarrow{\alpha} (\mathbb{Z}/\ell\mathbb{Z})^r \xrightarrow{\beta} \mathcal{F}_{\overline{\eta}} \tag{4.5}$$

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

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

[1] 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 5.2

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

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.,

$$\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z}) \simeq \begin{cases} \ker(\alpha), \ i = 1; \\ (\ker(\beta)/\mathrm{im}(\alpha)) \oplus < \gamma_E > \oplus < \gamma_F >, \ i = 2; \\ \mathrm{coker}(\beta), \ i = 3. \end{cases} \tag{4.6}$$

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 $< \gamma_F >$. More generally, the Galois action on $< \gamma_E >$ and $< \gamma_F >$ is via the cyclotomic character.

4.2 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 section is to state how to compute and efficiently represent the ℓ – 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 ℓ – torsion in the Jacobian for small primes ℓ first as a subroutine.

Theorem 4.1 (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 4.2 (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 distinct from 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 4.3 (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 distinct from the characteristic of k. Assume $\operatorname{Pic}^0(C) = \operatorname{Jac}(C)$ 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 $\operatorname{Pic}^0(C)[\ell]$ 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]. □

4.3 Cohomology of a nodal fibre

Let X_z be a nodal curve, obtained as a critical fibre of the Lefschetz pencil in the previous section. The objective of this section is to state how we may represent and compute the cohomology $\mathrm{H}^1(X_z, \mu_\ell) \simeq \operatorname{Pic}^0(X_z)[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g-1}$ 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 $\operatorname{Pic}^0(X_z)$ in terms of $\operatorname{Pic}^0(\widetilde{X}_z)$ and D_z. First, write

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

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

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

Define

$$\operatorname{Pic}^0_{D_z}(\widetilde{X}_z) := \operatorname{Div}^0_{D_z}(\widetilde{X}_z)/\langle \{\operatorname{div}(f) \mid f \equiv 1 \mod D_z\}\rangle. \tag{4.7}$$

Then, it is possible to show [Ser12, Chapter V][3] that $\operatorname{Pic}^0(X_z) \simeq \operatorname{Pic}^0_{D_z}(\widetilde{X}_z)$. In particular, we have

$$\operatorname{Pic}^0(X_z)[\ell] \simeq \operatorname{Pic}^0_{D_z}(\widetilde{X}_z)[\ell]. \tag{4.8}$$

The upshot is that we may also represent the elements (and group law) of the LHS in the isomorphism 4.8, using effective Riemann-Roch algorithms on the normalisation. In particular, one can isolate the subspace generated by the vanishing cycle at z, namely $\langle \delta_z \rangle \subset \operatorname{Pic}^0(X_z)[\ell]$, as the kernel of the natural induced map

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

Remark. We may compute the elements of $\operatorname{Pic}^0(X_z)[\ell]$ via specialisation to z of the ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ computing the $\ell-$torsion in the generic fibre using Algorithm 5. 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 $\operatorname{Pic}^0(X_z)[\ell]$. The other roots correspond to singularities of the completion of the generalised Jacobian $\operatorname{Pic}^0(X_z)$ by Theorem 8.6.

It requires more work to completely identify the vanishing cycle δ_z (upto sign), this is done in Section 5 using the Picard-Lefschetz formulas (4.4).

[3] see also [Lev22, Lemma 2.3.8]

4.4 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 curve 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 $\mathcal{F}_{\overline{\eta}} \simeq \mathrm{Pic}^0(X_{\overline{\eta}})[\ell]$ is the ℓ – torsion in the Jacobian of this relative curve of genus g. [4]

The main objective of this section is to describe a zero-dimensional radical ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ over $k(t)$[5], 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]

$$\#Z \leq D^{N+1} \quad \text{and} \quad g \leq D^2 - 2D + 1. \tag{4.9}$$

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 curve V obtained by normalising the function field of U in κ gives an étale cover $V \to U$ which trivialises the locally constant sheaf $\mathcal{F}|_U$ to a constant sheaf $\mathcal{G}$ 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[6]; 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 5 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 8.9, 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 8.9.
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 5 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.

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

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

[6] by the Riemann-Hurwitz formula

Chapter 5

Explicit Picard-Lefschetz theory

In this chapter, we compute and explicitly present the monodromy representation of the étale fundamental group associated to the sheaf of vanishing cycles. Specifically, we recall pairing algorithms and Puiseux series to construct the cospecialisation maps at singular points, and specialisation to smooth points with the final motive of computing the monodromy action on the cohomology of the generic fibre. As a by product, we also explcitly compute local monodromy, and the vanishing cycle at each singular point.

5.1 The Weil pairing

Now, we define the Weil pairing on the $\ell-$torsion points on the Jacobian of a curve and delineate an efficient algorithm to compute it.

Definition 5.1. 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 $-\ \ell$ 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 $\ell \cdot D_1 = \operatorname{div}(f)$ and $\ell \cdot D_2 = \operatorname{div}(g)$ for $f, g \in k(C)^*$. Then, $\langle D_1, D_2 \rangle = \frac{f(D_2)}{g(D_1)}$.

Theorem 5.1. *There exists an algorithm, that, on input a smooth, projective curve C over $\mathbb{F}_q$, a prime number ℓ coprime to q, two $\ell-$torsion divisors $D_1, D_2 \in \operatorname{Pic}^0(C)[\ell]$, computes the Weil pairing $\langle D_1, D_2 \rangle$ in time*

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

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

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 $\ell-$torsion is defined over an extension K' of K of degree a polynomial in ℓ as $\operatorname{Gal}(K'/K) \subset \operatorname{GL}(2g, \mathbb{F}_\ell)$, where g is the genus of C. The height of the $\ell-$torsion elements is bounded, by Theorem 8.2. 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].

Algorithm 6 `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 $\langle D_1, D_2 \rangle \in \mu_\ell(\overline{\mathbb{F}}_q)$.

```
1: 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 4.1.
2: Evaluate $\frac{f(D_2)}{g(D_1)}$ using [Cou09, Lemma 10].
3: Return the value of $\frac{f(D_2)}{g(D_1)}$.
```

5.2 Cospecialisation at a singular fibre

In this section, we make the cospecialisation maps (4.3) 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 $\mathcal{Z} \subset \mathbb{P}^1$ the finite subset parametrising the critical (nodal) fibres and write $\mathcal{U} = \mathbb{P}^1 \setminus \mathcal{Z}$. Denote by $\mathcal{F} := \mathrm{R}^1\pi_\star\mu_\ell$, the first derived pushforward sheaf on $\mathbb{P}^1$ and let $\overline{\eta} \to \mathbb{P}^1$ be a geometric generic point. Let $z \in \mathcal{Z}$. 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 an embedding $\mathtt{K}_z \hookrightarrow \overline{K(t)}$ determines the cospecialisation morphism

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

In particular, this choice is the étale analogue of a path or '*chemin*'. We begin with the following.

Definition 5.2 (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 4.4. We observe

$$[\mathbf{K} : K(t)] \leq \#\mathrm{GL}(2g, \mathbb{F}_\ell), \tag{5.1}$$

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 (5.1), 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 Section 8.2. 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 5.2 (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 $w^{1/M} = (r^{1/M}, \psi/M)$, corresponding to the principal branch.

So, for each $z \in \mathcal{Z}$, we use Theorem 5.2 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 $\overline{K}\langle\langle t-z\rangle\rangle$.

As stated earlier, 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 8.8) 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 rational function 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 7.

Algorithm 7 `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 $z \in \mathcal{Z}$.
- **Output:** The elements of $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$ represented as $\overline{K(t)}$ – rational points in a projective space $\mathbb{P}^M$ using convergent Puiseux series around z.

```
Compute the $\ell$ – division ideal ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$ of $\mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})$ using Algorithm 5.
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 rational functions in $\boldsymbol{\tau}$ with coefficients from a poly($\ell$) – degree extension of $K$.
Expand $\boldsymbol{\tau}$ as a Puiseux series $\lambda_z$ around $z$ using the algorithm from Theorem 5.2, upto poly($\ell$) precision. Similarly rational functions in $\boldsymbol{\tau}$ also have convergent Puiseux series representations. This identifies each $\gamma$ uniquely by Lemma 5.3.
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 5.2, 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 5.3. *It suffices to specify*

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

coefficients of the Puiseux expansion of each $\gamma \in \mathcal{F}_{\overline{\eta}}$ around $z \in \mathcal{Z}$, 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 next note the following.

Lemma 5.4 (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*

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

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] [1], 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.

□

5.3 Specialisation to a smooth fibre

Consider the setup of Section 5.2. Let $z \in \mathcal{Z}$. In this section, we indicate how we may specialise elements of $\mathcal{F}_{\overline{\eta}}$ realised as Puiseux expansions around z using Algorithm 7, 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 5.5. *Let $u \in \mathcal{U}$. 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 $\mathcal{F}|_{\mathcal{U}}$ 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 $\ell-$torsion of the generic fibre is unramified at u. We show the following next.

Lemma 5.6. *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 5.7. *Let $\gamma \in \mathcal{F}_{\overline{\eta}}$, and assume we have computed*

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

as a tuple of Puiseux series around $z \in \mathcal{Z}$ (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 $u_z \in \mathcal{U}$ with $|z - u_z| < \varepsilon_z/2$, the tuple representing γ converges at u_z to a specialisation $\phi_{u_z}^{-1}(\gamma) \in \mathrm{Pic}^0(\mathcal{X}_{u_z})[\ell]$ of γ at u_z.

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

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, 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 of γ_{u_z} implies that the tuples $[X_i^{(\gamma)}(t)]$ and $[Y_i(t)]$ represent the same analytic germs [2] on $W \cap \{u \in \mathbb{C} \mid |z-u| < \varepsilon_z/2\}$. This proves the claim. □

Remark. Having fixed a cospecialisation ϕ_z at z, one automatically determines cospecialisation morphsisms ϕ_u for all u in a neighbourhood of z via the above lemma. We call these *analytically compatible* cospecialisations.

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 5.8. *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 $u \in \mathcal{U}$ 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 8.2). 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.

Lemma 5.9 (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 5.7, 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.*

[2] being solutions of ${}^{(\ell)}\mathcal{I}_{\overline{\eta}}$, which are all distinct and ℓ^{2g} in 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 poly(ℓ) 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 5.4

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

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

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

for $m \in \mathbb{Z}_{>0}$ bounded by a polynomial in ℓ. By Lemma 5.8, these truncations specify υ_1 and υ_2 uniquely and unambiguously as $|\upsilon_1 - \upsilon_2| > \Gamma(\ell)$.

□

Combining Lemmas 5.7, 5.8 and 5.9, we have shown the following.

Theorem 5.10 (Approximation). *Let $\gamma \in \mathcal{F}_{\overline{\eta}}$ and let $z \in \mathcal{Z}$. Assume we have computed γ as a tuple $[X_0^{(\gamma)} : \ldots : X_M^{(\gamma)}(t)]$ of Puiseux expansions truncated upto* poly(ℓ) *coefficients, with respect to the cospecialisation ϕ_z. Then, for u_z of height bounded by* poly(ℓ) *such that $|z - u_z| < \varepsilon_z/2$, it is possible to determine with*

poly(ℓ) *space, time and precision complexity,*

the unique analytically compatible 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 explicit. Let $z \in \mathcal{Z}$. In Algorithm 7, 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 8, 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 $u_z \in \mathcal{U}$ such that $|z - u_z| < \varepsilon_z$.

Algorithm 8 Re-centering

- **Input:** An element $\gamma \in \mathcal{F}_{\overline{\eta}}$ represented by a tuple $[X_0^{\gamma}(t) : \ldots : X_M^{(\gamma)}(t)]$ of Puiseux series around z as a $\mathbf{K}$ − rational point in $\mathbb{P}^M$ (via Algorithm 7), and a smooth point $u \in \mathcal{U}$ 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 Section 8.3.
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 $[X_0^{(\gamma)}(t) : \ldots : X_M^{(\gamma)}(t)]$ actually converges at $u_z$ to a point $[x_0 : \ldots : x_M] \in \mathrm{Pic}^0(\mathcal{X}_{u_z})$. Determine the point as a tuple of algebraic numbers by using Theorem 5.10 and matching with the points computed in Step 2.
```

5.4 Computing vanishing cycles and monodromy

The goal of this section is to compute the monodromy action on $\mathcal{F}_{\overline{\eta}}$. Additionally, we also compute the local monodromy at each singular point, explicitly computing each vanishing cycle in the process. This algebraic computation of monodromy can be understood as an algebraic, finite coefficient analogue of the work [LPPV24] extended to the case of a Lefschetz pencil on an arbitrary smooth projective surface (as opposed to a hypersurface).

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 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 5.2, for $z \in \mathcal{Z}$, 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 (4.4) becomes

$$\sigma_j(\gamma) = \gamma - \langle \gamma, \delta_{z_j} \rangle \delta_{z_j} \tag{5.2}$$

for $\gamma \in \mathcal{F}_{\overline{\eta}}$ and $1 \leq j \leq r$. We now give a method, such that given $z_j \in \mathcal{Z}$ for $1 \leq j \leq r-1$, and $u_j \in \mathcal{U}$ 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 5.11. *Algorithm 9 uniquely determines the vanishing cycle at each $z \in \mathcal{Z} \setminus \{z_r\}$, upto sign.*

Proof. Let $\gamma \in \mathcal{F}_{\overline{\eta}} \setminus \phi_z(\mathcal{F}_z)$. By Section 5.2, we know that after a choice of embedding, we may write

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

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 8.8, we know that the image $\phi_z(\mathcal{F}_z)$ is all rational over $\overline{K}((t-z))$, so in

Algorithm 9 `Computing vanishing cycles`

```
• Input: A singular point $z \in \mathcal{Z} \setminus \{z_r\}$ 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 7.

1:  Obtain a representation of $\mathcal{F}_{\overline{\eta}}$ as Puiseux series around $z$ using Algorithm 7.
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 8.
5:  Compute $\phi_{u_z}^{-1}(\gamma)$ using Algorithm 8.
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 8.9).
7:  Use the inverse of the abstract Abel map of Section 8.4 (Algorithm 13) 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 6.
9:  Applying (5.3), 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 8.9), and make an arbitrary choice of sign.
10: With knowledge of $\phi_{u_z}^{-1}(\delta_z)$, identify it with the correct tuple of Puiseux expansions
    around $z$ and return $\delta_z$ as a rational function in the primitive element $\boldsymbol{\tau}$.
```

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 (5.2), 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 5.3, Algorithm 8 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 5.12. *The vanishing cycle δ_z at z can be computed as*

$$\delta_z = \pm \phi_{u_z}\left((\sqrt{-a^{-1}}) \cdot \delta \right) \tag{5.3}$$

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

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

Further, we know by the Picard-Lefschetz formulas, or Section 8.3, Theorem 8.7 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 5.11.

□

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 $I^{\mathrm{t}}_{z_j} \hookrightarrow \mathrm{Gal}\left(\overline{K(t)}/\overline{K}(t)\right)$. However, the final embedding $I^{\mathrm{t}}_{z_r} \hookrightarrow \mathrm{Gal}\left(\overline{K(t)}/\overline{K}(t)\right)$ is completely determined by the previous ones, via the relation $\prod_{j=1}^{r} \sigma_j = 1$ in $\pi_1^{\mathrm{t}}(U, \overline{\eta})$. Hence, an explicit representation of the *last vanishing cycle* δ_{z_r} can be computed by just using the knowledge of the action of the other inertia generators. We sum up, with an algorithm computing the action of the generators σ_j for $1 \leq j < r$, of the geometric monodromy.

Algorithm 10 `Computing the monodromy`

- **Input:** An element $\gamma \in \mathcal{F}_{\overline{\eta}}$ presented as a tuple of rational functions in the primitive element $\boldsymbol{\tau}$.
- **Output:** For each $z_j \in \mathcal{Z} \setminus \{z_r\}$, the element $\sigma_j(\gamma)$, again presented as a tuple of rational functions in $\boldsymbol{\tau}$.

```
For $z \in \mathcal{Z} \setminus \{z_r\}$, expand $\gamma$ as a Puiseux series around $z$ and compute $\sigma_z(\gamma)$ as in Step 3 of Algorithm 9.
Express $\sigma_z(\gamma)$, which is now represented as a tuple of Puiseux expansions around $z$, as a tuple of rational functions in $\boldsymbol{\tau}$, using the Puiseux expansion $\lambda_z$ for $\boldsymbol{\tau}$ and linear algebra.
Return the tuple of rational functions in $\boldsymbol{\tau}$.
```

We conclude with a table drawing a parallel with monodromy computations in the complex analytic setting, such as [LPPV24].

Analytic side	**Étale side**
$\pi_1^{\mathrm{top}}(\mathcal{U}, u)$	$\pi_1^{\text{ét}}(\mathcal{U}, \overline{u})$
Generator $\boldsymbol{\sigma}_j$	Topological generator σ_j
Loop based at u going around a puncture z	Embedding $I_z \hookrightarrow \mathrm{Gal}(\overline{K(t)}/K(t))$, together with isomorphism of fiber fuctors at u and geometric generic point $\overline{\eta} = \mathrm{Spec}(\overline{K(t)})$.

Table 5.1: Analytic-étale comparison

Chapter 6

Algorithms for cohomology

6.1 The Edixhoven subspace

In this section, we describe how to compute the Galois action on the second étale cohomology. We begin with a high-level description of the strategy.

- Having computed the monodromy, compute the normalisation of $\mathbb{P}^1$ in the function field of the étale cover $\mathcal{V} \to \mathcal{U}$ trivialising the locally constant sheaf $\mathrm{R}^1\pi_\star\mu_\ell$.

- Let $\tilde{\mathcal{V}} \to \mathbb{P}^1$ now be the smooth curve so obtained, ramified at $\mathcal{Z}$. Then, the Galois action on $\mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) \subset \mathrm{H}^2(\mathcal{X}, \mu_\ell)$ can be computed from the action of Galois on the subspace of $\mathrm{H}^1(\tilde{\mathcal{V}}, \mu_\ell) \otimes_{\mathbb{F}_\ell} \mathcal{F}_{\overline{\eta}}$, given by those tensors invariant under the diagonal action of G.

- The action of G on $\tilde{\mathcal{V}}$ extends naturally to an action on $\mathrm{H}^1(\tilde{\mathcal{V}}, \mu_\ell)$. One then isolates the *Edixhoven subspace* $\mathbb{E} \subset \mathrm{H}^1(\tilde{\mathcal{V}}, \mu_\ell)$, i.e., the subspace spanned by all copies of M inside it, by working over a finite field, modulo an auxiliary prime $\mathfrak{P}$ of good reduction, distinct from ℓ.

- Calling $\tilde{\mathcal{V}}_{\mathfrak{P}}$ the curve obtained upon reduction, we obtain its zeta function by counting points, and isolate the Edixhoven subspace $\mathbb{E}_{\mathfrak{P}}$ (which is defined over a poly-bounded extension) with knowledge of the monodromy action.

- The subspace $\mathbb{E}_{\mathfrak{P}}$ is then lifted $\mathfrak{P}$ - adically, using Hensel's lemma, to the characteristic zero subspace $\mathbb{E}$ following Mascot [Mas20], from which the Galois action is subsequently computed.

6.1.1 The trivialising cover

The étale cover $\mathcal{V} \to \mathcal{U}$ that trivialises the locally constant sheaf is obtained by normalising the function field of $\mathbb{P}^1$ in the Galois closure of the field $\overline{K}(\mathrm{Jac}(\mathcal{X}_{\overline{\eta}})[\ell])$ that the relative ℓ – torsion $\mathrm{Jac}(\mathcal{X}_{\overline{\eta}})[\ell]$ of the Jacobian of the generic fibre is defined over. Passage to the Galois closure of a field is efficiently possible, simply by computing a primitive element, and going to its splitting field.

As seen earlier, this extension is of degree bounded by a polynomial in ℓ, and a birational planar model of the curve representing this extension can be computed via a primitive element. Call $\mathcal{V}$ the curve so obtained, and denote its normalisation by $\tilde{\mathcal{V}}$. A representation for the latter is computed via resolution of singularities, for which there is a polynomial-time (in the genus $\mathfrak{g}$ of the curve) algorithm [Koz94]. Further, the associated map $\mathfrak{j} : \mathcal{V} \to \mathcal{U}$ can be computed in polynomial-time. The map on the smooth compactifications $\tilde{\mathfrak{j}} : \tilde{\mathcal{V}} \to \mathbb{P}^1$ is ramified only at $\mathcal{Z}$, and its degree is bounded by a polynomial in ℓ.

Theorem 6.1. *We have the following isomorphism of* $\mathrm{Gal}(\overline{K}/K)$ *– modules*

$$\mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) \simeq \left(\mathrm{H}^1(\tilde{\mathcal{V}}, \mu_\ell) \otimes M\right)^G \tag{6.1}$$

where $M = \mathcal{F}_{\overline{\eta}}$.

Proof. First, consider the Hochschild-Serre spectral sequence [Mil98, Theorem 14.9]

$$\mathrm{H}^i(G, \mathrm{H}^j(\mathcal{V}, \mathcal{F}|_{\mathcal{V}})) \Rightarrow \mathrm{H}^{i+j}(\mathcal{U}, \mathcal{F})$$

associated to the Galois cover $\mathcal{V} \to \mathcal{U}$. One has the five-term long exact sequence

$$0 \to \mathrm{H}^1(G, M) \to \mathrm{H}^1(\mathcal{U}, \mathcal{F}) \to \mathrm{H}^1(\mathcal{V}, \mathcal{F}|_{\mathcal{V}})^G \to \mathrm{H}^2(G, M) \to \mathrm{H}^2(\mathcal{U}, \mathcal{F}).$$

Now, for large enough ℓ (i.e., so that the integral ℓ - adic cohomology groups are torsion-free) we know by [KV25, Theorem 13], that $G = \mathrm{Sp}(\mathcal{E}_{\overline{\eta}})$, where $\mathcal{E} \subset \mathcal{F}|_U$ is the locally constant subsheaf of vanishing cycles. In particular, by mod-ℓ hard Lefschetz, we may write $M \simeq M' \oplus M''$, where $M' = \mathcal{E}_{\overline{\eta}}$ and $M'' \simeq \mathrm{H}^1(\mathcal{X}, \mu_\ell)$ is a trivial G - module. Thus, for such ℓ, we have that $\mathrm{H}^i(G, M) = 0$ for $1 \leq i \leq 2$, as after splitting, the centre has order 2 and acts non-trivially on M' (for $\ell > 2$, which we assume anyway). The passage to $\tilde{\mathcal{V}}$ follows from a purity argument by moving to positive characteristic, thanks to Deligne's main theorem [Del80, Théorème 2].

□

6.1.2 Geometric Galois action

In this subsection, we describe how to compute the G-action on points of $\tilde{\mathcal{V}}$.

- Consider the primitive element $\boldsymbol{\tau}$ for the field extension $\overline{K}(\tilde{\mathcal{V}})/\overline{K}(\mathbb{P}^1)$.

- The extension has Galois group G, the geometric monodromy group. For each generator $\rho_\ell(\sigma_j) \in G$ for $1 \leq j < r$, express $\sigma_j(\boldsymbol{\tau})$ as a rational function of $\boldsymbol{\tau}$, akin to Algorithm 10.

- As each σ_j gives rise to a birational automorphism of the smooth projective curve $\tilde{\mathcal{V}}$, it hence extends to an isomorphism, which can be given in terms of polynomials.

- Hence simply evaluate the corresponding isomorphism on the input point, this gives the G – action on the points of $\tilde{\mathcal{V}}$.

- This extends to an action on $\mathrm{Jac}(\tilde{\mathcal{V}})$, via divisors.

Algorithm 11 Computing the Edixhoven subspace modulo $\mathfrak{P}$

```
• Input: The curve $\tilde{\mathcal{V}}$ and a prime $\mathfrak{P}$.
• Output: The mod-$\mathfrak{P}$ Edixhoven subspace $\mathbb{E}_{\mathfrak{P}} \subset \mathrm{Jac}(\tilde{\mathcal{V}}_{\mathfrak{P}})[\ell]$.

1: Compute the zeta function $Z(\tilde{\mathcal{V}}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{P}}, T)$ by counting points on $\tilde{\mathcal{V}}$ over extensions of
   $\mathbb{F}_{\mathfrak{P}}$, using a $\mathfrak{P}$ - adic algorithm such as Harvey's [Har15].
2: Compute a basis of each space
       $$\mathcal{S}_i := \mathrm{Jac}(\tilde{\mathcal{V}}_{\mathfrak{P}})[\ell](\mathbb{F}_{\mathfrak{P}^i})$$
   as sums of $\tilde{\mathcal{V}}_{\mathfrak{P}}$ – points.
3: Compute the $G$ – action on each subspace $\mathcal{S}_i$. In particular, for each generator $\rho_\ell(\sigma_j)$,
   compute its action on $\mathcal{S}_i$ for each $i$ upto a bound $J = \mathrm{poly}(\ell)$, using 6.1.2 and [Cou09,
   Theorem 1].
4: Compute each element $\phi \in \mathrm{Hom}_G(M_{\mathfrak{P}}^\vee, \mathcal{S}_i)$ as a matrix, and a basis of the sum of the
   images. Write
       $$\mathbb{E}_{\mathfrak{P}}^{(i)} = \sum_{\phi \in \mathrm{Hom}_G(M_{\mathfrak{P}}^\vee, \mathcal{S}_i)} \mathrm{im}(\phi).$$
5: Compute the invariant space $(\mathbb{E}_{\mathfrak{P}}^{(i)} \otimes_{\mathbb{F}_\ell} M_{\mathfrak{P}})^G$ and its dimension. If it equals $\beta_2 - 2$,
   return $\mathbb{E}_{\mathfrak{P}}^{(i)}$.
```

6.1.3 Arithmetic Galois action

We first give a method to isolate the Edixhoven subspace $\mathbb{E} \subset \mathrm{H}^1(\tilde{\mathcal{V}}, \mu_\ell)$ that is relevant for the Galois contribution on the second étale cohomology of the input surface. For this, we make use of an auxiliary prime $\mathfrak{P}$ of good reduction, distinct from ℓ, and work with the positive-characteristic curve $\tilde{\mathcal{V}}_{\mathfrak{P}}$.

Remark. We abuse notation by using G to also refer to the monodromy of the mod-$\mathfrak{P}$ Lefschetz pencil. Provided $\mathfrak{P}$ is large enough compared to the data of the surface, there is an equality between the number of singular fibres in char zero and in positive char. Further, let $u \in \mathcal{U}$ and $\mathsf{u} \in \mathcal{U}_{\mathfrak{P}}$ such that $u \equiv \mathsf{u} \mod \mathfrak{P}$. Let $\overline{\xi} = \mathrm{spec}(\overline{\mathbb{F}_{\mathfrak{P}}(t)})$ be the geometric generic point. Then, we can consistently transport the G-action on $\mathcal{F}_{\overline{\eta}}$ to $\mathcal{F}_{\overline{\xi}}$ via the diagram

$$\begin{tikzcd}
\mathcal{F}_{\overline{\eta}} \arrow[r, "\phi_u^{-1}"] \arrow[d] & \mathcal{F}_u \arrow[d, "\varrho_u"] \\
\mathcal{F}_{\overline{\xi}} \arrow[r, "\varphi_{\mathsf{u}}^{-1}"] & \mathcal{F}_{\mathsf{u}}
\end{tikzcd}$$

where ϕ_u is a choice of cospecialisation at u, φ_{u} is the corresponding positive characteristic choice (obtained via coefficient-wise reduction of Laurent series), and ϱ_u is the char-zero to positive-char comparison isomorphism coming from reduction mod $\mathfrak{P}$. Thus, we have an unambiguous G - action on $M_{\mathfrak{P}} = \mathcal{F}_{\overline{\xi}}$.

Lemma 6.2. *The quantity J in Step 3 of Algorithm 11 can be assumed to be bounded by a polynomial in ℓ.*

Proof. We need to show that the Edixhoven subspace $\mathbb{E}_{\mathfrak{P}} \subset \mathrm{Jac}(\tilde{\mathcal{V}}_{\mathfrak{P}})[\ell]$ is defined over a field extension of $\mathbb{F}_{\mathfrak{P}}$ of degree at most bounded by a polynomial in ℓ. We notice that via its action on the positive characteristic surface $\mathcal{X}_{\mathfrak{P}}$, we have a Galois representation

$$\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{P}}) \to \mathrm{GL}\left(\mathrm{H}^2(\mathcal{X}_{\mathfrak{P}}, \mu_\ell)\right).$$

The general linear group is of rank β_2 (the second Betti number of $\mathcal{X}$) over the field $\mathbb{F}_\ell$, hence has size bounded by a polynomial in ℓ. Further, this restricts to an action on $\mathrm{H}^1(\mathbb{P}^1, \mathcal{F})$. Therefore, by Theorem 6.1, it is sufficient to show that $\mathbb{E}_{\mathfrak{P}}$ has dimension independent of ℓ. Using the tensor-hom duality, we see that $\mathbb{E}_{\mathfrak{P}}$ can be identified with the sum of the images of each $\phi \in \mathrm{Hom}_G(M^\vee, \mathrm{H}^1(\tilde{\mathcal{V}}_{\mathfrak{P}}, \mu_\ell))$. The hom space has dimension bounded by β_2, and the dimension of M is independent of ℓ, so this gives the result. □

Remark. See also [Lev24, Lemma 5.6] for an alternate proof.

Theorem 6.3. *Algorithm 11 outputs the subspace* $\mathbb{E}_{\mathfrak{P}} \subset \mathrm{H}^1(\tilde{\mathcal{V}}_{\mathfrak{P}}, \mu_\ell)$.

Proof. We note that $\mathbb{E}_{\mathfrak{P}}$ is the sum of all subspaces of $\mathrm{Jac}(\tilde{\mathcal{V}})[\ell]$ isomorphic to $M_{\mathfrak{P}}$ as G-modules. Further, by Lemma 6.2, it can be found within a poly-bounded extension. The algorithm only stops when the invariant subspace has the correct dimension, indicating that we have found the Edixhoven subspace. □

We now indicate how to Hensel- lift torsion points $\mathfrak{P}$ – adically, following work of Mascot [Mas20]. We recall the following.

Theorem 6.4 (Mascot)**.** *Let C be a model for a nice algebraic curve of genus g' over a number field L given via equations, and let ρ be a mod-ℓ $\mathrm{Gal}(\overline{L}/L)$ representation contained in a subspace $S \subset \mathrm{Jac}(C)[\ell]$ of dimension s. Let $\mathfrak{P} \subset \mathcal{O}_L$ be a prime of good reduction for C distinct from ℓ, and assume we are given $P_1(C_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{P}}, T)$. Further, assume we can isolate the subspace $S_{\mathfrak{P}} \subset \mathrm{Jac}(C_{\mathfrak{P}})[\ell]$. Then, given an accuracy parameter e, there exists an algorithm to $\mathfrak{P}$-adically lift the torsion subspace $S_{\mathfrak{P}}$ to S and compute the associated $\mathrm{Gal}(\overline{L}/L)$ representation in time*

$$\widetilde{O}(\mathrm{poly}(g' \cdot \log(\#\mathbb{F}_{\mathfrak{P}}) \cdot e \cdot \ell^s)).$$

Proof. This is the main result of [Mas20]. □

We now give a brief, informal sketch of Mascot's algorithm for completeness, based on the outline [Mas20, §1.2]. For simplicity, assume the base number field is $\mathbb{Q}$, and we have a rational prime $\mathbf{p}$.

- Compute a basis of $S_{\mathbf{p}} \subset \mathrm{Jac}(C_{\mathbf{p}})[\ell](\mathbb{F}_{\mathbf{q}})$, where $\mathbb{F}_{\mathbf{q}}/\mathbb{F}_{\mathbf{p}}$ is an extension over which the subspace $S_{\mathbf{p}}$ becomes rational.
- Given the accuracy parameter e, Hensel-lift the basis points to approximation $O(\mathbf{p}^e)$ in $\mathrm{Jac}(C)(\mathbb{Q}_{\mathbf{q}})$, i.e., points of $\mathrm{Jac}(C)(\mathbb{Z}_{\mathbf{q}}/\mathbf{p}^e)$.
- Compute all the possible $\mathbb{F}_\ell$ – linear combinations of this basis. This is a model of S over $\mathbb{Z}_{\mathbf{q}}/\mathbf{p}^e$, consisting of ℓ^s points.
- Write a rational map $\boldsymbol{\alpha} : \mathrm{Jac}(C) \dashrightarrow \mathbb{A}^1$ defined over the field $\mathbb{Q}$, and evaluate at the ℓ^s points constructed in the above step. Make sure the values are distinct, else use another rational map.
- Form the monic polynomial whose roots are these values and output it.

6.1.4 Height of divisors in the Edixhoven subspace

In this subsection, we bound the height of the divisors we are interested in, coming from the Edixhoven subspace. The main estimate is the following.

Theorem 6.5. *For each $x \in \mathbb{E} \subset \mathrm{Jac}(\tilde{\mathcal{V}})[\ell]$, we have*

$$h(\mathbf{D}_x) \leq \mathrm{poly}(\ell), \tag{6.2}$$

where $\mathbf{D}_x$ is a representation of the degree zero divisor in $\mathrm{Jac}(\tilde{\mathcal{V}})[\ell]$ corresponding to x, as a sum of points in $\tilde{\mathcal{V}}$.

Proof. We have to show that for $x \in \mathbb{E} \subset \mathrm{Jac}(\tilde{\mathcal{V}})[\ell]$, each point in the support of the divisor representing it, in the framework of Khuri-Makdisi's algorithms [KM07, KM04] (as used by Mascot), has (logarithmic) Weil height bounded by a polynomial in ℓ. The strategy is to make use of [CE11, Theorem 9.1.3] applied to the curve $\tilde{\mathfrak{j}} : \tilde{\mathcal{V}} \to \mathbb{P}^1$. We first note that Theorems 9.1.3, 9.2.1, and 9.2.5 of [CE11] are directly applicable to our setting, as they are concerned with a general algebraic curve or Riemann surface defined over a number field. We address each term in the inequality of [CE11, Theorem 9.1.3] separately, showing polynomial bounds.

1. **Faltings height of the curve $\tilde{\mathcal{V}}$.**
As a first step, we invoke Theorem 8.3, applied to the curve $\tilde{\mathcal{V}}$, which is the normalisation of $\mathbb{P}^1$ in the function field of the cover $\mathfrak{j} : \mathcal{V} \to \mathcal{U}$. Noting that the ramification locus $\mathcal{Z} = \mathbb{P}^1 \setminus \mathcal{U}$ has cardinality and height depending only on the surface $\mathcal{X}$ and independent of ℓ, we see that the theorem directly gives that the Faltings height $\mathfrak{h}_F(\tilde{\mathcal{V}})$ of the Jacobian of $\tilde{\mathcal{V}}$ is bounded above by

$$\deg(\mathfrak{j})^a,$$

where the quantity a is independent of ℓ. Noting that $\deg(\mathfrak{j})$ is bounded by a polynomial in ℓ gives the result.

2. **Sup norm bounds for the Arakelov-Green's functions** The sup-norm of the Arakelov-Green's functions g is bounded above in terms of Faltings' delta invariant $\delta_F(\cdot)$, by [Wil16, Corollary 4.6.2]. The quantity $\delta_F(\tilde{\mathcal{V}})$ is in turn bounded in Javanpeykar's result [Jav14, Theorem 6.0.4], by a polynomial in ℓ.

3. **Bounds for the theta function** For the norm of the theta function $||\vartheta||$ on $\mathrm{Pic}^{\mathfrak{g}-1}(\tilde{\mathcal{V}})$, we have by [Jav14, Lemma 2.4.2]

$$\log ||\vartheta||_{\max} \leq \frac{\mathfrak{g}}{4} \log \max(1, \mathfrak{h}_F(\tilde{\mathcal{V}})) + (4\mathfrak{g}^3 + 5\mathfrak{g} + 1) \log 2,$$

which is clearly bounded by a polynomial in ℓ, as both the genus $\mathfrak{g}$ of $\tilde{\mathcal{V}}$ and its Faltings height $\mathfrak{h}_F(\tilde{\mathcal{V}})$ are.

4. **An integral bound** Consider the integral

$$\int_{\tilde{\mathcal{V}}} \log(1 + |\tilde{\mathfrak{j}}|^2) \mu_{\tilde{\mathcal{V}}},$$

where $\mu_{\tilde{\mathcal{V}}}$ is the Arakelov 1-1 form associated to $\tilde{\mathcal{V}}$, regarded as a Riemann surface. By pushing forward to $\mathbb{P}^1$, one may conclude a polynomial upper bound for the integral as the degree, the number of poles and (logarithmic) height of the polynomials defining the function $\tilde{\mathrm{j}}$ are bounded by a polynomial in ℓ. Further, the ramification locus is bounded independently of ℓ as well.

5. **Bounds for intersection numbers** For an ℓ - torsion divisor $\mathbf{D}_x$ corresponding to $x \in \mathbb{E}$, one can bound the intersection numbers due to work of Wilms [Wil16, Propositions 1, 2] (see also [dJ04, Proposition 2.6.1], and more generally, the discussion in §2.6 of loc. cit.).

With bounds for the above quantities, it follows that for each point P_x in the support of $\mathbf{D}_x$, the absolute Weil height $h(\tilde{\mathrm{j}}(P_x))$ is bounded by a polynomial in ℓ, by a similar argument as in [CE11, Proposition 11.7.1]. This implies, the same for $h(P_x)$ as the map $\tilde{\mathrm{j}}$ itself has height and degree bounded by a polynomial in ℓ. □

Remark. We note that in the proofs of each of the above components, we require $\tilde{\mathcal{V}}$ to be semistable over K. This is possible after an extension, but the degree of the extension can be exponential in the genus $\mathfrak{g}$ and hence ℓ. This does not affect the bounds as the inequalities (in particular, for the intersection number as well) are normalised by the degree $[K : \mathbb{Q}]$, as in [CE11, Theorem 9.1.1], ultimately giving polynomial height bounds.

Remark. As an aside, we mention that the result of Javanpeykar, Theorem 8.3, provides a heruistic towards Theorem 6.5 in the following sense. An ℓ-torsion point in $\mathrm{Jac}(\tilde{\mathcal{V}})[\ell]$ is understood as a divisor $\mathbf{D}$, corresponding to an étale μ_ℓ-torsor $\mathrm{j}' : \mathcal{W} \to \tilde{\mathcal{V}}$. The composite map

$$\tilde{\mathrm{j}} \circ \mathrm{j}' : \mathcal{W} \to \mathbb{P}^1$$

is ramified exactly at $\mathcal{Z}$, and is of degree bounded by a polynomial in ℓ. Further, the curve $\mathcal{W}$ also has genus bounded by a polynomial in ℓ thanks to the Riemann-Hurwitz formula, hence has Faltings height bounded by a polynomial in ℓ by Theorem 8.3. This suggests that the (logarithmic) Weil height of the algebraic numbers that appear in a "minimal" expression for the divisor $\mathbf{D}$ should also likewise be bounded by a polynomial in ℓ.

We conclude with the below table, drawing a rough comparison with the leitmotif of the work [CE11].

Couveignes-Edixhoven	**This work**
Modular curve $\mathrm{X}_1(5\ell)$	The curve $\tilde{\mathcal{V}}$
The Ramanujan subspace $\mathrm{V} \subset \mathrm{J}_1(5\ell)[\ell]$	The Edixhoven subspace $\mathbb{E} \subset \mathrm{Jac}(\tilde{\mathcal{V}})[\ell]$
Hecke action to compute V	Monodromy action to compute $\mathbb{E}$.

Table 6.1: Comparison to Couveignes-Edixhoven

6.2 Main theorem

In this section, we state and prove our main result.

Theorem 6.6. *Let $\mathcal{X}$ be a fixed, nice surface of degree D defined over a number field K. Then, there exists a randomised algorithm that*

(i) on input a prime number ℓ, outputs the étale cohomology groups $\mathrm{H}^i(\mathcal{X}, \mu_\ell)$ for $0 \leq i \leq 4$ along with the $\mathrm{Gal}(\overline{K}/K)$ action in time

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

(ii) on input a prime $\mathfrak{p} \subset \mathcal{O}_K$ of good reduction with $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_q$, outputs the zeta function of the reduction $Z(X/\mathbb{F}_q, T)$, and the point-count $\#X(\mathbb{F}_q)$ in time

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

Proof. The computation of the cohomology groups $\mathrm{H}^i(\mathcal{X}, \mu_\ell)$ for $i = 1, 2$ is in Algorithm 12. The computation for $i = 3$ follows from that of $i = 1$ using Poincaré duality, while the cases $i = 0, 4$ are via suitable twists of the cyclotomic character. The complexity is proved in Lemma 7.7.

Part (ii) follows in a manner similar to that mentioned in [Mas20, Remark 1.2]. One uses an efficient algorithm to compute the image of the Frobenius element at large primes, upto conjugacy, such as [DD13], combined with Section 8.1 to recover the zeta function and point count. □

Algorithm 12 `Computing the cohomology groups` $\mathrm{H}^i(\mathcal{X}, \mu_\ell)$

- **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 $\leq d$ and a prime number ℓ.

- **Pre-processing:** Fibre $\mathcal{X}$ as a Lefschetz pencil $\pi : \mathcal{X} \to \mathbb{P}^1$. Let $\mathcal{Z} \subset \mathbb{P}^1$ parametrise the singular fibres and $\mathcal{U} = \mathbb{P}^1 \setminus Z$ the smooth ones. Embed the Jacobian of the generic fibre $\mathcal{X}_{\overline{\eta}}$ into $\mathbb{P}^M$ obtaining the ℓ – 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 5.

- **Output:** The cohomology groups $\mathrm{H}^i(\mathcal{X}, \mu_\ell)$ for $1 \leq i \leq 2$ presented as $\mathbb{F}_\ell$ – vector spaces with bases and $\mathrm{Gal}(\overline{K}/K)$ – action.

```
Choose a point $u \in \mathcal{U}(\overline{K})$ of bounded height and degree, to serve as base point.
Compute a cospecialisation $\phi_u : \mathcal{F}_u \to \mathcal{F}_{\overline{\eta}}$, by making a choice of expansion for the primitive element $\boldsymbol{\tau}$ around $u$, hence obtaining each $\gamma \in \mathcal{F}_{\overline{\eta}}$ as Laurent series around $u$.
Compute the image of the monodromy fixed subspace, i.e., those elements $\gamma \in \mathcal{F}_{\overline{\eta}}$ fixed by each $\sigma_j$ for $1 \leq j < r$, with the monodromy action as computed in Algorithm 10.
Compute the Galois action on the monodromy fixed subspace $\mathcal{F}_u^G := \phi_u^{-1}(\mathcal{F}_{\overline{\eta}}^G)$ element-wise, using the cospecialisation $\phi_u$. This gives $\mathrm{H}^1(\mathcal{X}, \mu_\ell)$ with $\mathrm{Gal}(\overline{K}/K)$ action.
Now, for the second cohomology work with the curve $\tilde{\mathcal{V}}$. Choose an auxiliary prime of good reduction $\mathfrak{P}$ of size $O(\ell)$, distinct from $\ell$, and compute the subspace $\mathbb{E}_{\mathfrak{P}} \subset \mathrm{H}^1(\tilde{\mathcal{V}}_{\mathfrak{P}}, \mu_\ell)$ using Algorithm 11.
Lift the subspace $\mathbb{E}_{\mathfrak{P}}$ to the characteristic zero subspace $\mathbb{E} \subset \mathrm{H}^1(\tilde{\mathcal{V}}, \mu_\ell)$ using Theorem 6.4.
Compute the space of invariant tensors
    $$(\mathbb{E} \otimes \mathcal{F}_u)^G$$
  with knowledge of the $G$ - action.
Compute the diagonal $\mathrm{Gal}(\overline{K}/K)$ action as a matrix on the subspace of tensors which has been isolated in the above step, element-wise. This gives the space $\mathrm{H}^1(\mathbb{P}^1, \mathcal{F})$ with $\mathrm{Gal}(\overline{K}/K)$ - action. To obtain the full $\mathrm{H}^2(\mathcal{X}, \mu_\ell)$, we just add the space $< \gamma_E > \oplus < \gamma_F >$, on which Galois acts via the cyclotomic character on each component.
```

Chapter 7

Complexity analyses

In this chapter, we provide 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.

7.1 Algorithms of Chapter 4

Noting that the complexity of Algorithm 4 is independent of ℓ, we begin with the following.

Lemma 7.1. *Algorithm 5 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 height bounded by a polynomial in ℓ due to Theorem 8.2 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].

□

7.2 Algorithms of Chapter 5

Lemma 7.2. *Algorithm 7 runs in time* $\mathrm{poly}(\ell)$.

Proof.

- Step 1: The complexity of Algorithm 5 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 5.2. It suffices to compute the first $\mathrm{poly}(\ell)$ coefficients to uniquely specify a branch by Lemma 5.3.
- 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 7.3. *Algorithm 8 runs in time* poly(ℓ).

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 8.2.

- Step 3: Convergence to an algebraic number with poly(ℓ) precision is guaranteed by Theorem 5.10.

□

Lemma 7.4. *Algorithm 9 runs in time* poly(ℓ).

Proof.

- Step 1: Follows from the complexity of Algorithm 7.

- 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 poly(ℓ) coefficients by Lemma 5.3, 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 8.

- Step 6: The addition of the group law can be performed efficiently by Theorem 8.9.

- Step 7: The complexity of computing the abstract Abel map and its inverse (Algorithm 13) is given by Theorem 8.9.

- Step 8: Pairings can be computed in polynomial time using a divisorial description by Algorithm 6.

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

- Step 10: The rational functions in $\boldsymbol{\tau}$ corresponding to Puiseux expansions around z, can be found in polynomial time via linear algebra combined with poly(ℓ) truncations.

□

Lemma 7.5. *Algorithm 10 runs in time* poly(ℓ).

Proof.

- Step 1: Follows from the complexity of Algorithm 9.

- Steps 2 and 3 : This boils down to the problem of expressing elements in the splitting field of the ℓ − torsion of the Jacobian of the generic fibre, as rational functions in a primitive element for the field extension. This can be solved on the level of Puiseux series as well, with $\mathrm{poly}(\ell)$ truncation, by Lemma 5.3.

□

7.3 Algorithms of Chapter 6

Lemma 7.6. *Algorithm 11 runs in time* $\mathrm{poly}(\ell \cdot \mathrm{char}(\mathbb{F}_{\mathfrak{P}}) \cdot \log(\#\mathbb{F}_{\mathfrak{P}}))$.

Proof.

- Step 1: One can use a $\mathfrak{P}$ – adic algorithm such as Harvey's [Har15] to count points on $\tilde{\mathcal{V}}_{\mathfrak{P}}$ to output its zeta function with the stated complexity. It is sufficient to count points upto an extension of degree bounded by the genus $\mathfrak{g}$, which in this case is bounded by a polynomial in ℓ.

- Step 2: A basis for the space $\mathcal{S}_i$ can be computed in polynomial time using random sampling on the curve, following [Cou09].

- Step 3: The G - action is computed on the points of the curve $\tilde{\mathcal{V}}_{\mathfrak{P}}$ following 6.1.2 in polynomial time. The number J is bounded by a polynomial in ℓ by Lemma 6.2.

- Step 4: Firstly, the dual $M^{\vee}$ can be identified with M for the G − action via the self-duality given by the symplectic Weil pairing. Next, the dimension of the space $\mathrm{Hom}_G(M^{\vee}, \mathcal{S}_i)$ is bounded independently of ℓ, and each G − equivariant homomorphism can be computed as a matrix via linear algebra. In other words, there are only $\mathrm{poly}(\ell)$ homs, and a basis for the sum of their images can be found using [Cou09].

- Step 5: One can list all the invariant tensors with knowledge of the G − action. Further, zero-testing is efficient and can be done in polynomial time, so it simply remains to count the number of invariant tensors in each space, which is always bounded by a polynomial in ℓ. Finally the Betti number β_2 can be computed as $\#\mathcal{Z} + 2\beta_1 + 2 - 4g$, where g is the genus of the generic fibre of the pencil.

□

Lemma 7.7. *Algorithm 12 runs in time* $\mathrm{poly}(\ell)$.

Proof.

- Step 1: This can be done in polynomial time.

- Step 2: The complexity is the same as that of computing a Puiseux series expansion, except we are now working around a smooth point. The $\mathrm{poly}(\ell)$ truncation bounds remain, and the total complexity is the same as that of Algorithm 7.

- Step 3: Follows from the complexity of Algorithm 10.

- Step 4: The arithmetic $\mathrm{Gal}(\overline{K}/K)$ action on $\mathcal{F}_u^G$ factors via a finite extension K'/K that the subspace is rational over. This extension has degree bounded by a polynomial in ℓ, as its Galois group is a subgroup of $\mathrm{GL}(\mathcal{F}_u^G)$, whose rank is independent of ℓ.

- Step 5: Follows from the complexity of Algorithm 11.

- Step 6: Follows from [Mas20], i.e., the complextiy of Theorem 6.4. The preceision e required depends on the complexity of the algebraic numbers occurring in an explicit description of the Edixhoven subspace. We know by Theorem 6.5 that the heights are bounded by a polynomial in ℓ. Further, the points occurring in the support of the divisors concerned, each also have degree bounded by a polynomial in ℓ, as the Edixhoven subspace becomes rational over such an extension.

- Step 7: The G- action on the space of tensors can be computed element by element, as its dimension is independent of ℓ.

- Step 8: Again the $\mathrm{Gal}(\overline{K}/K)$ action factors through a finite extension K''/K, with degree bounded by a polynomial in ℓ. Its action on $\mathbb{E}$ is obtained via points on $\tilde{\mathcal{V}}$, and the action on $\mathcal{F}_u$ can be computed akin to Step 4.

□

Chapter 8

Ancillaries

This supplementary chapter serves the purpose of an appendix, including 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.

8.1 Recovering zeta

The objective of this section 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 $\tilde{P}_i(T) := \det\big(1 - TF_q^\star \mid \mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})\big) \in \mathbb{F}_\ell[T]$. 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

$$0 \longrightarrow \mathrm{H}^i(X, \mathbb{Z}_\ell)/(\ell \cdot \mathrm{H}^i(X, \mathbb{Z}_\ell)) \longrightarrow \mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{H}^{i+1}(X, \mathbb{Z}_\ell)[\ell] \longrightarrow 0. \tag{8.1}$$

Writing

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

we see from (8.1) 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} ℓ – 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 $P_i(T)$ mod ℓ 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].

8.2 Höhentheorie

In this section, we recall the theory of heights and state certain height bounds to complement our algorithms.

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 8.1. 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 8.2. 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

$$\hat{h}(P) := \lim_{j \to \infty} \frac{h(2^j P)}{4^j}. \tag{8.2}$$

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 8.1 (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 $P \in A(\overline{K})$,*

$$\hat{h}(P) - c_1 \leq h(P) \leq \hat{h}(P) + c_2 \tag{8.3}$$

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 8.2 (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 8.9. 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 8.10, the height of the Jacobian constructed in Theorem 8.9 is bounded above by the height associated to the $4 \cdot \Theta$ – embedding. The result then follows from Theorem 8.1, combined with the results of [PW21, §2] and [Rém10, §1]. □

Remark. Theorem 8.2 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]).

We now recall a result of Javanpeykar, which resolves a conjecture of Edixhoven-de Jong-Schepers [EDJS10, Conjecture 5.1], that bounds the Faltings height of the Jacobian of a ramified covering of the projective line.

Theorem 8.3 (Javanpeykar)**.** *Let $U \subset \mathbb{P}^1_{\mathbb{Z}}$ be a nonempty open subscheme. There exist integers $a, b \in \mathbb{Z}_{>0}$ such that for any prime ℓ, and any connected finite étale cover*

$$\Psi : V \to U_{\mathbb{Z}[1/\ell]},$$

the Faltings height of the Jacobian of the normalisation of $\mathbb{P}^1$ in the function field of V is bounded by

$$(\deg \Psi)^a$$

where a is a constant that depends only on the height of $Z = \mathbb{P}^1_{\mathbb{Q}} \setminus U_{\mathbb{Q}}$ and the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *– on Z. In particular,*

$$a = 6 + \log\left(13 \cdot 10^6 \mathrm{A} \cdot (4\mathrm{AB})^{45\mathrm{A}^3 2^{\mathrm{A}-2}\mathrm{A}!}\right)$$

where A *is the number of elements in the orbit of Z under the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *and* B *is a bound for the height of the elements of Z.*

Proof. See [Jav14, Theorem 6.0.6]. □

8.3 Results of Igusa

In this section, 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 $\mathcal{F} := \mathrm{R}^1\pi_\star\mu_\ell$ 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 $\mathbb{P}^M$ [1].

Theorem 8.4. *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, $\tilde{\mathcal{J}_z}$ is the completion of the generalised Jacobian [2] $\mathcal{J}_z$ of $\mathcal{X}_z$.*

Proof. See [Igu56a, Theorem 3]. □

Theorem 8.5. *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 5.2, this completely determines a cospecialisation map $\phi_z : \mathcal{F}_z \hookrightarrow \mathcal{F}_{\overline{\eta}}$. We have the following.

Theorem 8.6. *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]. □

Theorem 8.7. *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.*

[1] using e.g., Chow's method ([Cho54] or [Igu56a, Appendix]) or Anderson's method ([And02]) sketched in Section 8.4, both of which involve the Θ – divisor

[2] also called Rosenlicht variety

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

Theorem 8.8. *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]. □

8.4 Abstract Abel map and embeddings of Jacobians

This section 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

$$\operatorname{abel}(\mathcal{D})_{ij} = \begin{vmatrix} \widehat{\underline{v}^{(0)}} \\ \vdots \\ \widehat{\underline{v}^{(i)}} \\ \vdots \end{vmatrix} \cdot \begin{vmatrix} \vdots \\ \widehat{\underline{u}^{(i)}} \\ \vdots \\ \widehat{\underline{u}^{(w+1)}} \end{vmatrix} \cdot \begin{vmatrix} \vdots \\ \widehat{\underline{v}^{(j)}} \\ \vdots \\ \widehat{\underline{v}^{(w+1)}} \end{vmatrix} \cdot \begin{vmatrix} \widehat{\underline{u}^{(0)}} \\ \vdots \\ \widehat{\underline{u}^{(j)}} \\ \vdots \end{vmatrix} \tag{8.4}$$

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 $S = \mathrm{supp}(E)$, $A = \mathrm{H}^0(S, \mathcal{O}_C)$ 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 $\mathrm{div}(\lambda) = \lambda_+ - \lambda_-$, 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.

Remark. The only dependence on ℓ in Algorithm 13 is the input divisor $D \in \mathrm{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$. By Theorem 4.2, we know that D can be efficiently represented $\mathrm{poly}(\ell)$ time and the bases for the Riemann-Roch spaces $\mathrm{H}^0(\mathcal{X}_{\overline{\eta}}, E \pm D)$ are computed using Theorem 4.1.

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 8.9. *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]. □

Algorithm 13 `Abstract Abel map and its inverse on` $\ell -$ `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 $D \in \operatorname{Pic}^0(\mathcal{X}_{\overline{\eta}})[\ell]$ represented using Theorem 4.2.

- **Output:** The image $\operatorname{abel}(D)$ of the map in (8.4) as a point in projective space $\mathbb{P}^M$ lying on the Jacobian $\mathcal{J}_{\overline{\eta}}$, satisfying the conditions of the paragraph above.

```
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 $\lambda$, with $K(t)$ – coefficients on $\mathcal{X}_{\overline{\eta}}$. We may assume $\operatorname{div}(\lambda) = \lambda_+ - \lambda_-$, with $\lambda_+$ and $\lambda_-$ 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.
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 4.1.
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.
Compute the map (8.4) using these pullbacks.
For any $u \in \mathbb{P}^1$, the embedding of the Jacobian $\operatorname{Pic}^0(\mathcal{X}_u) \hookrightarrow \mathbb{P}^M$ is given by the divisor $E_u$. If we specialise the input divisor $D$ to $u$, we get $D_u \in \operatorname{Pic}^0(\mathcal{X}_u)[\ell]$.
To invert the Abel map on $\operatorname{Pic}^0(\mathcal{X}_u)[\ell]$, given a point in $\mathbb{P}^M$ corresponding to an element of $\operatorname{Pic}^0(\mathcal{X}_u)[\ell]$, we simply go through all the $\ell^{2g}$ divisorial representatives of $\ell -$ torsion as a result of the algorithm from Theorem 4.2 and check which of them map to our given point via the divisor $E_u$ and the map (8.4). There will be a unique pre-image as the Abel map is injective.
```

Theorem 8.10. *The embedding described in Theorem 8.9 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]. □

Bibliography

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[ABCL02] Simon Abelard, Elena Berardini, Alain Couvreur, and Grégoire Lecerf. Computing Riemann–Roch spaces via Puiseux expansions. *Journal of Complexity*, 73, 2002.

[AH61] M.F. Atiyah and F. Hirzebruch. Vector bundles and homogeneous spaces. *Proc. Sympos. Pure Math.*, 3:7–38, 1961.

[AH01] Leonard M Adleman and Ming-Deh Huang. Counting rational points on curves and abelian varieties over finite fields. *Journal of Symbolic Computation*, 32(6):171–189, 2001.

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

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

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

[Bal03] Edoardo Ballico. An effective Bertini theorem over finite fields. *Advances in Geometry*, 3(4):361–363, 2003.

[Ber86] Pierre Berthelot. Géométrie rigide et cohomologie des variétés algébriques de caractéristique p. *Groupe de travail d'analyse ultramétrique*, 9(3):J1–J18, 1986.

[BS86] Zenon Ivanovich Borevich and Igor Rostislavovich Shafarevich. *Number theory*. Academic press, 1986.

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

[CDV06] Wouter Castryck, Jan Denef, and Frederik Vercauteren. Computing zeta functions of nondegenerate curves. *International Mathematics Research Papers*, 2006:72017, 2006.

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

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

[Cha97] Nick Chavdarov. The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy. *Duke Mathematical Journal*, 87(1):151 – 180, 1997.

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

[CM06] Antonio Cafure and Guillermo Matera. Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields and Their Applications*, 12(2):155–185, 2006.

[Col76] George E Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition: a synopsis. *ACM SIGSAM Bulletin*, 10(1):10–12, 1976.

[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.

[DD13] Tim Dokchitser and Vladimir Dokchitser. Identifying frobenius elements in galois groups. *Algebra & Number Theory*, 7(6):1325–1352, 2013.

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

[Del80] Pierre Deligne. La conjecture de Weil : II. *Publications Mathématiques de l'IHÉS*, 52:137–252, 1980.

[dJ04] Robin S de Jong. *Explicit Arakelov Geometry.* PhD thesis, Universiteit van Amsterdam, 2004.

[DLS20] James H Davenport, Acyr F Locatelli, and Gregory K Sankaran. Regular cylindrical algebraic decomposition. *Journal of the London Mathematical Society*, 101(1):43–59, 2020.

[DV06] Jan Denef and Frederik Vercauteren. Counting points on C_{ab} curves using Monsky–Washnitzer cohomology. *Finite Fields and Their Applications*, 12(1):78–102, 2006.

[Dwo60] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math*, 82:631–648, 1960.

[EDJS10] Bas Edixhoven, Robin De Jong, and Jan Schepers. Covers of surfaces with fixed branch locus. *International Journal of Mathematics*, 21(07):859–874, 2010.

[FG25] Jason Fulman and Robert Guralnick. Derangements in finite classical groups and characteristic polynomials of random matrices. *arXiv:2507.21025*, 2025.

[G$^+$77] Alexander Grothendieck et al. Cohomologie ℓ-adique et fonctions L (SGA V). *Lecture Notes in Math*, 589, 1977.

[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.

[Hal08] Chris Hall. Big symplectic or orthogonal monodromy modulo ℓ. *Duke Mathematical Journal*, 141(1):179 – 203, 2008.

[Har05] Gilbert Harman. On the greatest prime factor of $p-1$ with effective constants. *Mathematics of Computation*, 74(252):2035–2041, 2005.

[Har13] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

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

[Has36] Helmut Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. 1936.

[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.

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

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

[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.

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

[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.

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

[Ill06] Luc Illusie. Vanishing cycles over general bases after P. Deligne, O. Gabber, G. Laumon and F. Orgogozo (Algebraic Number Theory and Related Topics). *Institute of Mathematical Analysis Kokyuroku*, 1521:35–53, 2006.

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

[JS12] Uwe Jannsen and Shuji Saito. Bertini theorems and Lefschetz pencils over discrete valuation rings, with applications to higher class field theory. *Journal of Algebraic Geometry*, 21(4):683–705, 2012.

[Kat73] Nicholas M Katz. Pinceaux de Lefschetz: théoréme d'existence, expose XVII in Groupe de Monodromy en Geometrie Algebrique [SGA 7 II]. *Lecture Notes in Math*, 340, 1973.

[Kat04] Nicholas M Katz. Larsen's alternative, moments, and the monodromy of Lefschetz pencils. Contributions to automorphic forms, geometry, and number theory, 521–560, 2004.

[Ked01] Kiran S Kedlaya. Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology. *J. Ramanujan Math. Soc.*, 2001.

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

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

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

[Koz94] Dexter Kozen. Efficient Resolution of Singularities of Plane Curves. *Foundation of Software Technology and Theoretical Computer Science*, 141:1 – 11, 1994.

[KS99] Nicholas M Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45. American Mathematical Soc., 1999.

[KV25] Hyuk Jun Kweon and Madhavan Venkatesh. Bornes de torsion et un théorème effectif du pgcd. *Preprint*, 2025.

[Kwe21] Hyuk Jun Kweon. Bounds on the torsion subgroups of Néron–Severi groups. *Transactions of the American Mathematical Society*, 374(1):351–365, 2021.

[Lau04] Alan G.B. Lauder. Deformation theory and the computation of zeta functions. *Proceedings of the London Mathematical Society*, 88(3):565–602, 2004.

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

[Lev24] Christophe Levrat. Computing the cohomology of constructible étale sheaves on curves. *Journal de théorie des nombres de Bordeaux*, 36(3):1085–1122, 2024.

[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.

[LL91] Yagati N Lakshman and Daniel Lazard. On the complexity of zero-dimensional algebraic systems. In *Effective methods in algebraic geometry*, pages 217–225. Springer, 1991.

[LPPV24] Pierre Lairez, Eric Pichon-Pharabod, and Pierre Vanhove. Effective homology and periods of complex projective hypersurfaces. *Mathematics of Computation*, 93(350):2985–3025, 2024.

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

[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.

[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.

[Mas20] Nicolas Mascot. Hensel-lifting torsion points on Jacobians and Galois representations. *Mathematics of Computation*, 89(323):1417–1455, 2020.

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

[Mil64] John Milnor. On the Betti numbers of real varieties. *Proceedings of the American Mathematical Society*, 15(2):275–280, 1964.

[Mil80] James S Milne. *Etale cohomology (PMS-33)*. Princeton University Press, 1980.

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

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

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

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

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

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

[Ros39] Barkley Rosser. The n-th Prime is greater than $n \log n$. *Proceedings of the London Mathematical Society*, 2(1):21–44, 1939.

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

[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.

[Sat00] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *Journal-Ramanujan Mathematical Society*, 15(4):247–270, 2000.

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

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

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

[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.

[SS83] Jacob T Schwartz and Micha Sharir. On the "piano movers" problem. II. General techniques for computing topological properties of real algebraic manifolds. *Advances in applied Mathematics*, 4(3):298–351, 1983.

[Sta18] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu, 2018.

[SV05] Christophe Soulé and Claire Voisin. Torsion cohomology classes and algebraic cycles on complex projective manifolds. *Advances in Mathematics*, 198(1):107–127, 2005.

[SV25] Nitin Saxena and Madhavan Venkatesh. Counting points on surfaces in polynomial time. *Preprint*, 2025.

[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.

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

[Wal09] George Walker. *Computing zeta functions of varieties via fibration*. PhD thesis, University of Oxford, 2009.

[Wei48a] André Weil. *Sur les courbes algébriques et les variétés qui s' en déduisent*. Number 1041. Actualités Sci. Ind, 1948.

[Wei48b] André Weil. *Variétés abéliennes et courbes algébriques*, volume 32. Paris, 1948.

[Wil16] Robert Wilms. *The delta invariant in Arakelov geometry*. PhD thesis, Universitäts-und Landesbibliothek Bonn, 2016.

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