COMPLEXITY OF THE CHARACTERISTIC POLYNOMIAL OF FROBENIUS ON THE FIRST ÉTALE COHOMOLOGY GROUP

V. MADHAVAN, DIPTAJIT ROY, AND NITIN SAXENA

Abstract. Let $X_0 \subset \mathbb{P}^N$ be a smooth, projective variety of dimension n and degree D over the finite field $\mathbb{F}_q$. Denote $X = X_0 \times \overline{\mathbb{F}}_q$. Let prime ℓ be coprime to q, and $P_1(T)$ be the characteristic polynomial of the geometric Frobenius $F_q^\star$ on $\mathrm{H}^1(X, \mathbb{Q}_\ell)$; it is a well-studied factor of the Hasse-Weil zeta function of X. We show that the problem of computing $P_1(T)$ is in the complexity class AM $\cap$ coAM (= a randomised version of NP $\cap$ coNP) for fixed N. As a by-product of our methods, we obtain: (1) a randomised polynomial-time algorithm to compute $P_1(T)$ for constant D, and (2) a quantum algorithm to compute $P_1(T)$ that is polynomial-time in both D and $\log q$. Also, when X_0 is a surface, the respective algorithms output the dimension of $\mathrm{H}^2(X, \mathbb{Q}_\ell)$.

Our technique is to first reduce to the case of a surface, which is fibred as a Lefschetz pencil of hyperplane sections over $\mathbb{P}^1$. The formalism of vanishing cycles, and the inherent big monodromy, enable us to prove an effective version of Deligne's 'théorème du pgcd' using the hard-Lefschetz theorem and an equidistribution result due to Katz. Ultimately, this reduces the problem to that of computing the zeta function of a curve defined over a finite field extension $\mathbb{F}_Q/\mathbb{F}_q$ of poly-bounded degree; yielding the first complexity upper bounds.

1. Introduction

Let X_0 be a smooth, projective variety of dimension n over the finite field $\mathbb{F}_q$ of characteristic $p > 0$. Denote by X the base-change to the algebraic closure. To encode the number of its points over all finite field extensions, the zeta function of X is defined as

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

Let ℓ be a prime distinct from p. By the foundational work of Grothendieck et al.[G$^+$77] on ℓ-adic cohomology, it is known that the zeta function can be written as a rational function:

$$Z(X/\mathbb{F}_q, T) = \frac{P_1(T)P_3(T)\cdots P_{2n-1}(T)}{P_0(T)P_2(T)\cdots P_{2n}(T)} \in \mathbb{Q}(T)\,, \tag{1.1}$$

where $P_i(T) = \det(1 - TF_q^\star \mid \mathrm{H}^i(X, \mathbb{Q}_\ell))$ is the characteristic polynomial[1] of the map $F_q^\star$ induced on the cohomology by the geometric Frobenius. Further, the zeta function satisfies the functional equation

$$Z(X/\mathbb{F}_q, 1/(q^n T)) = \pm q^{n\cdot\chi/2} \cdot T^\chi \cdot Z(X/\mathbb{F}_q, T),$$

where $\chi = \sum_{i=0}^{2n} (-1)^i \cdot \dim \mathrm{H}^i(X, \mathbb{Q}_\ell)$ is the ℓ-adic Euler-Poincaré characteristic of X. Denote $\beta_i := \dim \mathrm{H}^i(X, \mathbb{Q}_\ell)$, also called the ith Betti number. As a result of Deligne's proof [Del74] of the Weil-Riemann hypothesis, we have $P_i(T) = \prod_{j=1}^{\beta_i}(1 - \alpha_{i,j}T) \in \mathbb{Z}[T]$, with $\alpha_{i,j}$

2020 *Mathematics Subject Classification.* Primary 11Y16 11G25 68Q25 14G15.

Key words and phrases. Zeta function, Weil conjectures, ell-adic, étale, cohomology, Frobenius, Jacobian variety, Lefschetz pencils, vanishing cycles, equidistribution, monodromy, Arthur-Merlin protocol, quantum.

[1] or *reversed* characteristic polynomial, according to another convention

being algebraic numbers such that $|\iota(\alpha_{i,j})| = q^{i/2}$ for any embedding $\iota : \mathbb{Q}(\alpha_{i,j}) \to \mathbb{C}$. In particular, it follows that the $P_i(T)$ are independent of ℓ.

The complexity of computing the zeta function of a variety over a finite field is a natural question, being the generalisation of the ancient problem of counting the number of congruent solutions of a given polynomial equation modulo a prime p. Let $X \subset \mathbb{P}^N$ be a smooth, projective variety of dimension n and degree D, presented as the zero set of homogeneous polynomials $f_1, \ldots, f_m$ each of total degree $\le d$. The dimension of the variety n (and that of its embedding space) is considered *fixed* as allowing it to vary runs into the known NP-complete problem of 3-SAT (see [AB09] for NP- and #P-hardness). So, in practice, one seeks algorithms to compute $Z(X/\mathbb{F}_q, T)$ efficiently in the other parameters, namely $\log q$ and D. Such an algorithm which is polynomial-time in both is unknown, despite being a well-studied problem in the intersection of mathematics and computer science. In particular, even for the simple to present, hyperelliptic curves $y^2 = f(x) \bmod p$, that are quite useful in cryptography [CFA$^+$05], there is no fast algorithm known to compute the zeta function, in time polynomial in $\log p$ and $\deg(f)$. Thus, instead, one asks the following (see [LPP03, Question 15]):

Question (Motivation)**.** Given a rational function $Q(T)$ and some 'data', is there a polynomial time algorithm to *verify* that $Q(T)$ is the zeta function of X? In other words, is the zeta function computation problem in NP, or in coNP? More generally, given input polynomials $Q_i(T) \in \mathbb{Z}[T]$, for all i, is *verifying*

$$Q_i(T) \stackrel{?}{=} P_i(T) \quad \text{in} \quad \mathrm{NP} \cap \mathrm{coNP}\,?$$

In this work, we take the first steps towards answering the above question about verifying the zeta function. We show initially that for a smooth, projective, geometrically irreducible curve C, the problem of verifying its zeta function is in AM $\cap$ coAM. AM is a computational complexity class which is considered 'similar' in the complexity hierarchy to NP. The problems of this class can be verified by an *Arthur-Merlin protocol* consisting of two parties called the *prover* (Merlin) and *verifier* (Arthur). Merlin tries to convince Arthur about a decision problem, by sending some 'data' (*certificate*) which is verified by Arthur in probabilistic polynomial time. After a fixed number of steps, Arthur either accepts or rejects. If we restrict the number of interactions between the two parties to just two (e.g., a *challenge* followed by a *response*), this is a randomised version of the classic NP protocol.

We show that under a fixed ambient representation (keeping the number of variables constant), computing $P_1(T)$ for a smooth projective variety is in AM $\cap$ coAM. A problem in the class AM $\cap$ coAM is considered unlikely to be NP-hard, as otherwise, the complexity class called Polynomial Hierarchy (PH) will collapse (see [AB09, 9.3] for details).

In terms of actual algorithms, we obtain the first polynomial-time (in $\log q$) algorithm to compute $P_1(T)$ for smooth varieties (of dimension ≥ 2) of fixed degree D, extending a line of work that goes back to elliptic curves [Sch85] and abelian varieties [Pil90]. Further, generalising work of Kedlaya [Ked06] (which was restricted to curves), we obtain the first quantum algorithm for computing $P_1(T)$ that is polynomial-time in both $\log q$ and D.

1.1. **Prior work.** It is possible to interpret Eqn.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 resp. 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 genus g), and abelian varieties, with 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 on computing étale cohomology in higher degrees [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 more than p monomials in the basis.

1.2. **Main results.** We assume the input is a smooth, projective variety $X_0 \subset \mathbb{P}^N$ of dimension[2] $n \geq 1$ and degree D, over the finite field $\mathbb{F}_q$, presented as a system of m homogeneous polynomials $f_1, \ldots, f_m$ of degree $\leq d$[3]. Denote by X the base-change to $\overline{\mathbb{F}}_q$.

The technical heart of the results in this work lies in the proof of Theorem 3.6; an effective version of Deligne's 'théorème du pgcd' (from the celebrated work [Del80]). This allows us to reduce the computation of $P_1(T)$[4] for X to the computation of the zeta function of smooth curves obtained by taking successive hyperplane sections of X; and then we give new complexity upper bounds for the curve case . As consequences, we obtain the following.

Theorem 1.1 (Certify P_1)**.** *Given $Q_1(T) \in \mathbb{Z}[T]$, deciding whether $Q_1(T) = P_1(X/\mathbb{F}_q, T)$, for X_0 given as above, is in* $\mathrm{AM} \cap \mathrm{coAM}$.

The curve case is handled separately in Theorem 1.4. For a curve C of genus g, the above protocol reduces to the verification of a few group orders $\mathcal{N}_j := \#\mathrm{Jac}(C)(\mathbb{F}_{q^j})$ of the Jacobian of C, which entails the verification of independence for a set of generators. The well-known "mod-ℓ pairing"-based arguments do not give a protocol immediately; as, the order $\ell \mid \mathcal{N}_j$ of a generator can be very large. In which case, it can require an exponential degree extension $\mathbb{F}_Q/\mathbb{F}_q$ for the Tate pairing to be non-degenerate on $\mathrm{Jac}(\mathbb{F}_Q)[\ell]$ [FR94].

For varieties of constant degree D, after reduction to the case of curves and applying work of Pila [Pil90] and Huang-Ierardi [HI98], we have the following.

[2] the dimension of the embedding space, N, is considered to be fixed. The degree D and field size q are allowed to vary.

[3] the complexity can be measured in D or d, as for N fixed, each is bounded by a polynomial function in the other.

[4] we write $P_1(X/\mathbb{F}_q, T)$ to specify the q-power Frobenius.

Theorem 1.2 (Fixed degree)**.** *There exists an algorithm that, given X_0 as above of fixed degree D, computes $P_1(X/\mathbb{F}_q, T)$ in time polynomial in $\log q$. Moreover, if X_0 is a surface, the algorithm also outputs the second Betti number $\dim \mathrm{H}^2(X, \mathbb{Q}_\ell) = \deg(P_2(X/\mathbb{F}_q, T))$.*

A major obstacle to computing the above was the lack of a concise and explicit representation, in general, for the étale cohomology group $\mathrm{H}^1(X, \mu_\ell)$; despite it being known to be isomorphic to the ℓ-torsion in the Picard scheme of X. A priori, elements therein are a formal sum of codimension-1 subvarieties (modulo an equivalence relation), and it is uncertain how one may directly produce ℓ-torsion elements due to the highly *non-explicit* nature of the group law. There has been a strategy laid out by Levrat [Lev22, IV.3.5, VI.4] for surfaces, under some strongly restrictive hypotheses; but the general-case complexity is either unclear or exponential-time.

We also give the first quantum polynomial-time algorithm (allowing the degree D to vary) to compute $P_1(X/\mathbb{F}_q, T)$, by applying Kedlaya's algorithm [Ked06] for the curve case.

Theorem 1.3 (Quantum)**.** *There exists a quantum algorithm that computes $P_1(X/\mathbb{F}_q, T)$ in time polynomial in $D \log q$, for any X_0 given as above. Moreover, if X_0 is a surface, the algorithm outputs the second Betti number $\dim \mathrm{H}^2(X, \mathbb{Q}_\ell)$; yielding $\deg(P_i(T))$ for all i.*

For a smooth, projective, geometrically irreducible curve $C \subset \mathbb{P}^N$ of genus $g > 0$, the zeta function has the form $Z(C/\mathbb{F}_q, T) = P_1(C/\mathbb{F}_q, T)/\left((1-T)(1-qT)\right)$, where $P_1(C/\mathbb{F}_q, T) \in \mathbb{Z}[T]$ is of degree $2g$, with constant term 1. Somewhat surprisingly, we will not only verify $P_1(C/\mathbb{F}_q, T)$ but also the abelian group structure of the Jacobian variety over the base field.

Theorem 1.4 (Certify 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, is in $\mathrm{AM} \cap \mathrm{coAM}$. Moreover, given a finite Abelian group G (via additive generators), the verification problem*

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

These results, in the curve case, address a question of Kedlaya [Ked06, §9] on verifying the order of the Jacobian as a black-box group.

1.3. **New techniques and proof ideas.** Certifying the zeta function of a smooth curve $C/\mathbb{F}_q$ of genus g boils down to a certification of the group orders $\#\mathrm{Jac}(C)(\mathbb{F}_{q^j})$ for $1 \le j \le 2g$. By a theorem of Voloch (Theorem 2.4), elements in $\mathrm{Jac}(C)(\mathbb{F}_q)$ can be represented as a formal sum of $C(\mathbb{F}_q)$ points, when $q > \Omega(g^2)$. Further, the addition law on the Jacobian can be made explicit (after reducing to a plane model) by an effective Riemann-Roch algorithm (Algorithm 1). Utilising the additive structure of $\mathrm{Jac}(C)(\mathbb{F}_q) \simeq \mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_r$ (with $n_i | n_{i+1}$ and $r \le 2g$) as an abelian group, it suffices to certify that a candidate generating-set of divisors $(D_i)_{1 \le i \le r}$, with each D_i of order n_i, actually generates the full group. Using the Weil bound for the size of the Jacobian, we are able to certify, with high probability, the 'independence' of the divisors D_i (Algorithm 2). This is done by random sampling in a family of hash functions— a classical technique that originated in the famous protocol of Goldwasser-Sipser [GS86] to certify the lower bound of a, possibly exponential-size, set.

More generally, for smooth projective varieties X, the theory of étale cohomology, in particular the Kummer sequence, allows us to relate the group $\mathrm{H}^1(X, \mathbb{Z}/\ell\mathbb{Z}) \simeq \mathrm{Pic}^0(X)[\ell]^\vee$ to the ℓ-torsion in the Picard scheme of X. Define the ℓ-adic versions of the cohomology,

$$\mathrm{H}^1(X, \mathbb{Z}_\ell) := \lim_{\leftarrow j} \mathrm{H}^1(X, \mathbb{Z}/\ell^j\mathbb{Z}) \quad \text{and} \quad \mathrm{H}^1(X, \mathbb{Q}_\ell) := \mathrm{H}^1(X, \mathbb{Z}_\ell) \otimes \mathbb{Q}_\ell\,.$$

By an application of the weak-Lefschetz theorem (Theorem 3.3), we notice that to compute $P_1(X/\mathbb{F}_q, T)$, it is sufficient to compute $P_1(Y/\mathbb{F}_q, T)$ where Y is a smooth projective *surface* obtained by successively taking smooth hyperplane sections of X. By Algorithm 3, we produce a Lefschetz pencil of hyperplane sections on Y, denoted $(H_t)_{t\in\mathbb{P}^1}$, with $Y_t := H_t \cap Y$ being smooth *curves*, for t in an open dense subscheme $U_0 \subseteq \mathbb{P}^1$. Denote $U := U_0 \times \overline{\mathbb{F}}_q$.

This procedure gives us (implicitly) a morphism[5] $\pi : \tilde{Y} \to \mathbb{P}^1$, whose fibre at any $t \in \mathbb{P}^1$ is Y_t. By the Leray spectral sequence, we have $\mathrm{H}^1(Y, \mathbb{Q}_\ell) \simeq \mathrm{H}^1(\tilde{Y}, \mathbb{Q}_\ell) \simeq \mathrm{H}^0(\mathbb{P}^1, \mathcal{F})$, where $\mathcal{F} := R^1\pi_\star\mathbb{Q}_\ell$ is the étale sheaf, on the projective line, obtained by the first direct image relative to π. Further, by the proper base-change theorem, we have for any $t \in \mathbb{P}^1$, the stalk $\mathcal{F}_t \simeq \mathrm{H}^1(Y_t, \mathbb{Q}_\ell)$. We notice that $\mathcal{F}|_U$ is a locally constant sheaf on U and has as a subsheaf $\mathcal{E} \subset \mathcal{F}|_U$, the sheaf of vanishing cycles. The sheaf $\mathcal{E}$ is locally constant and of rank (say) $2r$.

We prove an effective version (Theorem 3.6) of Deligne's 'théorème du pgcd' ("polynomial gcd theorem" from the celebrated work [Del80]). In particular, we show that there exists an extension $\mathbb{F}_Q/\mathbb{F}_q$ of bounded degree such that we can recover (with high probability) $P_1(Y/\mathbb{F}_Q, T)$, merely from the curve-case polynomials $P_1(Y_{u_i}/\mathbb{F}_Q, T)$ with $u_i \in U(\mathbb{F}_Q)$ chosen randomly, for $1 \leq i \leq 2$; by computing their gcd. The ingredients are as follows.

The hard-Lefschetz theorem (Theorem 4.2) states $\mathrm{H}^1(Y_u, \mathbb{Q}_\ell) = \mathrm{H}^1(Y, \mathbb{Q}_\ell) \oplus \mathcal{E}_u$ for $u \in U$. We proceed to understand the action of the Frobenius at u on $\mathcal{E}_u$, which for our purposes behaves as a 'random group' contribution. The sheaf $\mathcal{E}_{\mathbb{Z}_\ell} \subset R^1\pi_\star\mathbb{Z}_\ell|_U$ of ℓ-adic integral vanishing cycles on U corresponds to a representation of the étale fundamental group $\rho : \pi_1(U_0, u) \to \mathrm{GL}(2r, \mathbb{Z}_\ell)$ via its action on the stalk of $\mathcal{E}_{\mathbb{Z}_\ell}$ at u. We next study the geometric mod-ℓ monodromy $\overline{\rho}_\ell : \pi_1(U, u) \to \mathrm{GL}(2r, \mathbb{F}_\ell)$. Methods of Hall [Hal08] imply that $\mathrm{im}(\overline{\rho}_\ell) = \mathrm{Sp}(2r, \mathbb{F}_\ell)$, the symplectic group. An equidistribution theorem due to Katz dictates the proportion of Frobenius elements $F_{Q,v} \in \pi_1(U_0, u)$ for $v \in U(\mathbb{F}_Q)$, whose image lies in a conjugacy-stable subset of the mod-ℓ arithmetic monodromy group. The error term therein, and an analysis of the proportion of matrices in the group of symplectic similitudes $\mathrm{GSp}(2r, \mathbb{F}_\ell)$ with characteristic polynomial coprime to a given one; provide the reasonable bounds for ℓ and Q to obtain our computational complexity result.

2. Zeta function of curves

In this section, 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 $\overline{\mathbb{F}}_q$. We begin with some preliminaries.

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

[5] $\tilde{Y}$ is a smooth projective surface obtained by blowing up Y along $\Delta \cap Y$, where Δ is the axis of the pencil.

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.

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

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 exists a nodal curve $C' \subset \mathbb{P}^2$ and a birational morphism $\phi : C \to C'$.*

We now 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[6], 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 subsection with a statement of the Weil-Riemann hypothesis for curves [Wei48a, Wei48b].

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

---

[6]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 $\mathrm{poly}(\delta)$.

2.2. **Jacobian arithmetic.** In this subsection we recall certain results with the goal of showing that elements of $\mathrm{Jac}(C)(\mathbb{F}_q)$ can be presented concisely and divisor arithmetic therein can be performed efficiently.

We know by [Ser88, Section 8] that C injects into its Jacobian, by the choice of a rational point, which we call ∞. By the Weil-Riemann hypothesis for C, rational points exist after taking an extension of $\mathbb{F}_q$ of degree $\mathrm{poly}(g)$. Let G_C denote the group generated by the points $C(\mathbb{F}_q)$ in $\mathrm{Jac}(C)(\mathbb{F}_q)$. Using Weil and the Riemann-Hurwitz theorems, Voloch [Vol00] shows the following explicitness result.

Theorem 2.4 (Voloch)**.** *If $q \geq (8g-2)^2$, then $G_C = \mathrm{Jac}(C)(\mathbb{F}_q)$.*

We now recall a result that enables one to compute $\mathcal{L}(D)$ for a divisor D on C.

Proposition 2.5 (Riemann-Roch basis)**.** *Let D be a degree zero divisor on a curve C of degree $\leq \delta$. 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 the above, 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. *Let $D \in \mathrm{Div}^0(C)$. Deciding whether $D \in \mathrm{Div}^{\mathrm{pr}}(C)$ can be done in polynomial time.*

We recall a canonical method to represent elements in $\mathrm{Jac}(C)$.

Lemma 2.7 (Reduced form)**.** *Let $D \in \mathrm{Jac}(C)$. Then, there exists $0 \leq i \leq g$ so that there is a unique effective divisor E of degree $g-i$ such that $D = E - (g-i)(\infty)$ in $\mathrm{Jac}(C)$.*

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 $0 \leq i \leq g$ so that $\dim \mathcal{L}(D + (g-i)(\infty))$ is still > 0. In particular, for such an i, we have $\dim \mathcal{L}(D + (g-i)(\infty)) = 1$. Applying Proposition 2.5, one gets a unique rational function f in the basis. Thus, one gets an expression for a unique effective divisor $E := \mathrm{div}(f) + D + (g-i)(\infty) \geq 0$; which is the same as saying $D = E - (g-i)(\infty)$ in $\mathrm{Jac}(C)$'s arithmetic. □

Based on this proof, we describe now a randomised polynomial-time Algorithm 1 that details how to compute the sum of two elements in $\mathrm{Jac}(C)$ in this canonical representation.

2.3. AM **protocol.** In this subsection, 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 ($g \geq 1$).

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 $m_1, m_2 \le g$ lying in the Jacobian of a smooth projective curve $C/\mathbb{F}_q$, presented in the reduced form as per Lemma 2.7.
- **Output:** $D_3 = D_1 + D_2$ as $D_3 = E_3 - m_3(\infty)$ where E_3 is effective of degree m_3.

1: *(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]. Set $m_3 = g - i$ and $E_3 = E$.
2: Output $E_3 - m_3(\infty)$.

Proposition 2.8 (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:*

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

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 objects, important in computer science, to map large strings to small strings, in a way that minimizes *collision* as much as possible. Hashing[7] forms the main tool for our $\mathrm{AM} \cap \mathrm{coAM}$ protocol. Let $h : \{0,1\}^n \mapsto \{0,1\}^k$; $k \ll n$ be a hash function. One requires that for any boolean string $X \in \{0,1\}^n$ and a random string $Y \in \{0,1\}^k$, $\Pr_{h,Y}[h(X) = Y] = 1/2^k$. 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]). Algorithm 2 introduces the $\mathrm{AM} \cap \mathrm{coAM}$ protocol to verify the size of the Jacobian over $\mathbb{F}_Q \supseteq \mathbb{F}_q$ with the assumption that $Q > (8g+1)^2$.

Lemma 2.9 (Probability of Algorithm 2)**.** *In Algorithm 2, 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 hash function h, the probability that there is an $x \in \mathcal{G} = S$, such that $h(x) = y$ is

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

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

[7] see [AB09, Definition 8.14]

Algorithm 2 Verifying the size 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 homogeneous polynomials $(f_i)_{1\le i\le m}$. A positive integer $\mathcal{N}$ lying in the Hasse-Weil interval. Set L:
$$2^{L-1} < \mathcal{N} \le 2^L.$$

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 can be assumed to be a sum of $C(\mathbb{F}_Q)$ points by Theorem 2.4.
- Send a *response* consisting of r quadruples $\{(c_i, D_i, n_i, P_i)\}_{1\le i\le r}$ with the claim that the divisor $\sum_i c_i D_i =: x$, 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 the support of D_i indeed comprises of $C(\mathbb{F}_Q)$ points; this is done by a simple substitution in the polynomial system defining C. If not, *Reject*.
- Check the factorization data P_i of each n_i. Check the order n_i as follows: verify $n_i D_i = 0$, and for each distinct prime factor $p_{i,j}$ of n_i, verify $(n_i/p_{i,j})D_i \ne 0$. Check that $\mathcal{N} = \prod_{i=1}^r n_i$. If a check fails, *Reject*. Calculate $x = \sum_i c_i D_i$.
- Check $h(x) = h\left(\sum_i c_i D_i\right) = y$, 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.

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

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

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. $\square$

Lemma 2.10 (Complexity of Algorithm 2)**.** *The protocol runs in polynomial time.*

Proof. Step 1 simply involves addition and multiplication, of matrices over $\mathbb{F}_2$, so it needs $\mathrm{poly}(g\log Q) = \mathrm{poly}(g\log q)$ 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.

Next, for the Jacobian arithmetic, Arthur uses Algorithm 1 and repeated-doubling. This gets done in $\text{poly}(\delta, g, \log q)$; which sums up the complexity of our protocol. □

The zeta function is intimately connected to the order of the Jacobian. We recall the following from [Ked06, §8].

Lemma 2.11 (Count to zeta function)**.** *Assume we have the counts $\#\text{Jac}(C)(\mathbb{F}_{q^j})$, for every $1 \le j \le \max(18, 2g)$. Then, $P_1(C/\mathbb{F}_q, T)$ can be reconstructed from these counts, in time polynomial in $g \log q$.*

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

Lemma 2.12 (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 by [Har05, Theorem 1.2]. Using the above, we can now prove Theorem 1.4.

Proof of Theorem 1.4. Using Algorithm 2, we can verify the structure of $\text{Jac}(C)(\mathbb{F}_Q)$ 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 applying Lemma 2.12. Each $P_1(C/\mathbb{F}_{q^{m_j}}, T)$ can be computed, uniquely, using the counts $\#\text{Jac}(C)(\mathbb{F}_{q^{im_j}})$, for $1 \le i \le \max(18, 2g)$, by Lemma 2.11. 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 $\text{Jac}(C)(\mathbb{F}_q) \simeq G$. For this, Merlin first convinces Arthur of the structure of $\text{Jac}(C)(\mathbb{F}_Q)$, 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 $\#\text{Jac}(C)(\mathbb{F}_q) = P_1(C/\mathbb{F}_q, 1)$. For the subgroup $\text{Jac}(C)(\mathbb{F}_q) \subset \text{Jac}(C)(\mathbb{F}_Q)$, 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 $\text{Jac}(C)(\mathbb{F}_q)$ (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 $\#\text{Jac}(C)(\mathbb{F}_q)$ certifies the structure. The proof then follows from Lemmas 2.9-2.10. □

3. $P_1(T)$ FOR SMOOTH PROJECTIVE VARIETIES

3.1. **Reduction to smooth projective surfaces.** In this subsection, we demonstrate a reduction of the problem of computing the characteristic polynomial of geometric Frobenius on the first (ℓ-adic) étale cohomology of a smooth projective variety over a finite field $\mathbb{F}_q$ of fixed dimension $r > 1$, to that of a smooth projective *surface*. This reduction is polynomial in the input data, namely the degree of the polynomials defining the variety and $\log q$.

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 $f_1, \ldots, f_m$ of degree $\le d$ 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. Let X be as above. 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 3.2 (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.*

Remark. In the proof of the above theorem, it is shown [Bal03, Lemma 1] that $\check{W}$ is a variety of degree at most $D(D-1)^N \le D^{N+1}$. The singular locus of $\check{W}$, denoted $\mathring{W}$ is a subvariety of $(\mathbb{P}^N)^\vee$ of codimension at least 2 and degree (by Bézout) at most $D^{(N+1)^2}$.

We now recall the following theorem, which is the key step in our reduction to surfaces. See [Fu11, §8.5.5] for the proof of the more general theorem, of which this is a special case.

Theorem 3.3 (Weak-Lefschetz)**.** *Let $Y \hookrightarrow X$ be a smooth hyperplane section. Then the induced map*

$$\mathrm{H}^1(X, \mathbb{Q}_\ell) \to \mathrm{H}^1(Y, \mathbb{Q}_\ell)$$

is an isomorphism if $n = \dim(X) > 2$ and an injection if $n = 2$.

With this setup, we notice that with an application of Bertini's theorem on the existence of smooth hyperplane sections, we can inductively reduce the dimension of X by intersecting with a generic hyperplane in $\mathbb{P}^N$. In particular, there is a chain of smooth hyperplane sections $Y := Y_2 \subset Y_3 \subset \ldots \subset Y_{n-1} \subset X$, where Y_i are smooth varieties of dimension i. Applying the weak-Lefschetz theorem, we get an isomorphism

$$\mathrm{H}^1(X, \mathbb{Q}_\ell) \to \mathrm{H}^1(Y, \mathbb{Q}_\ell),$$

compatible with the action of the respective geometric Frobenii. Writing

$$P_1(X/\mathbb{F}_q, T) := \det\left(1 - TF_q^\star | \mathrm{H}^1(X, \mathbb{Q}_\ell)\right)$$

and assuming Y is also defined over $\mathbb{F}_q$, we have $P_1(X/\mathbb{F}_q, T) = P_1(Y/\mathbb{F}_q, T)$. So, it suffices to compute $P_1(Y/\mathbb{F}_q, T)$ for Y a smooth subvariety obtained from X after intersection with $n-2$ hyperplanes in general position.

Remark. We note that the ideal defining Y now is generated by the forms f_i, L_j with $1 \le i \le m$ and $1 \le j \le n-2$, where the L_j are linear forms representing the generic hyperplanes in $\mathbb{P}^N$ that we have intersected X with, to obtain Y.

3.2. **Lefschetz pencils on a surface.** To study the zeta function of a surface, intuitively, one wants to break it up into those of curves, each parameterized by a single variable t, and then invoke the methods of Section 2. It is not so easy because Theorem 3.3 does not give an isomorphism when X is a surface, e.g., $\mathrm{H}^1(Y, \mathbb{Q}_\ell)$ can be a larger group for a generic curve Y lying on the surface X, which will make the zeta function of Y 'larger' than that of X, introducing errors called vanishing cycles (see Section 4.1).

To explore these issues, in this subsection, we introduce the classic machinery of Lefschetz pencils and describe an algorithm to fibre a given smooth projective surface $X \subseteq \mathbb{P}^N$ of degree D over the projective line so that the fibres are curves with singularities at worst being ordinary double points. We assume X is given by m homogeneous forms $f_1, \ldots, f_m$, each of total degree $\leq d \in \mathbb{Z}_{>0}$. Denote by $(\mathbb{P}^N)^\vee$, the dual projective space.

Definition 3.4. 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 $L \subset (\mathbb{P}^N)^\vee$; for e.g., $(\lambda, \mu) \mapsto \lambda F = \mu G$, for linear forms F, G on $\mathbb{P}$; satisfying the following conditions

- the *axis*, of the pencil, $\Delta := F \cap G$ 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.[8] We recall [JS12, Theorem 3].

Proposition 3.5. *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.*

Algorithmically, to construct a Lefschetz pencil, we first take a field extension to ensure the existence of a transversal hyperplane section. We saw that the dual variety $\check{X}$ parameterises those hyperplanes that do not intersect transversally with X. Further, its singular locus $\mathring{X}$ parameterises those hyperplanes that intersect X with singularity worse than a single ordinary double point. In other words, $\check{X} \setminus \mathring{X}$ consists of those hyperplanes H such that $H \cap X$ has a single node (see [Mil98, Theorem 31.2] or [Kat73]). In light of Proposition 3.2, it suffices to randomly take two linear forms $F, G \in (\mathbb{P}^N)^\vee$. With high probability, they intersect transversally with X and the line joining them in $(\mathbb{P}^N)^\vee$ intersects $\check{X}$ at finitely many points and completely misses $\mathring{X}$.

Blowing up X along $X \cap \Delta$ gives a smooth projective surface $\tilde{X}$ and a morphism $\pi : \tilde{X} \to \mathbb{P}^1$ such that the fibre of a $[\lambda : \mu] \in \mathbb{P}^1$ is the curve $X \cap (\lambda F = \mu G)$. Algorithmically, the locus $\Delta \cap X$ may not all be defined over $\mathbb{F}_q$ and going to a field extension which contains all of the points therein may be expensive. Further, computing the blowup $\tilde{X} \to X$ and the morphism $\pi : \tilde{X} \to \mathbb{P}^1$ may also be exponential in the input data. Fortunately, we are able to leave π implicit, i.e., the only knowledge we need is that the fibre of $u \in \mathbb{P}^1$ under π is $H_u \cap X$, where H_u is the hyperplane associated to u. We describe the required construction in Algorithm 3.

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

Algorithm 3 Lefschetz pencil on a *surface*

- **Input:** A smooth projective *surface* $X_0/\mathbb{F}_q$ of degree D presented as a system of homogeneous polynomials of degree $\leq d$ in the projective space $\mathbb{P}^N$.

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 3.2.
Replace X with the degree 3 Veronese image of X in $\mathbb{P} := \mathbb{P}^{\binom{N+3}{3}-1}$.
Select two random linear forms F and G on $\mathbb{P}$, such that they intersect transversally with X (this is possible with high probability by Proposition 3.2).
The line L in $(\mathbb{P})^\vee$ through F and G is a Lefschetz pencil on X with high probability.

Now, consider the étale sheaf $R^1\pi_\star\mathbb{Q}_\ell$ on $\mathbb{P}^1$. It is locally constant of rank $2g$ on U, where g is the genus of the generic fibre $\tilde{X}_\eta$ (which is a curve over the function field of $\mathbb{P}^1$), where $\eta \to \mathbb{P}^1$ is a geometric generic point. By the proper base-change theorem, for a point $u \in \mathbb{P}^1$, we have $(R^1\pi_\star\mathbb{Q}_\ell)_u \simeq \mathrm{H}^1(\tilde{X}_u, \mathbb{Q}_\ell) = \mathrm{H}^1(X \cap H_u, \mathbb{Q}_\ell)$. Further, by [Mil98, Lemma 33.2], we have $\mathrm{H}^1(\tilde{X}, \mathbb{Q}_\ell) \simeq \mathrm{H}^1(X, \mathbb{Q}_\ell)$.

We now establish bounds for the genus g of the generic smooth fibre and for the critical locus which we call $Z := \mathbb{P}^1 \setminus U$. Pick $u \in U$, the fibre $X \cap H_u$ is a curve in $\mathbb{P}$ of degree $D = \deg(X)$. By the results of [GLP83] (see also [Mac19]), we have $g \leq D^2 - 2D + 1$. Further, the number of critical points, i.e., $\#Z$ is bounded by the size of $L \cap \check{X}$, which by the remark following Proposition 3.2 and Bézout's theorem, is at most D^{N+1}. Denote the Betti numbers $\beta_i := \dim \mathrm{H}^i(X, \mathbb{Q}_\ell)$. Clearly, we have[9] $\beta_3 = \beta_1 \leq 2g \leq 2D^2$. By [Mil80, V, Theorem 3.12], we have $\beta_2 = \#Z + 2\beta_1 + 2 - 4g \leq 2D^{N+1}$.

3.3. **An effective gcd theorem.** As before, let $X_0/\mathbb{F}_q$ be a smooth, projective, geometrically irreducible surface of degree $D > 0$. We assume that X_0 is presented as $X_0 \subset \mathbb{P}^N$, given by a homogeneous ideal I generated by m polynomials $f_1, \ldots, f_m$ of degree $\leq d$ for $d \in \mathbb{Z}_{>0}$. Denote by X the base change to the algebraic closure. Let ℓ be an odd prime, distinct from the characteristic. In this subsection, we prove an effective version of Deligne's 'théorème du pgcd' [Del80, Théorème 4.5.1], that enables one to recover $P_1(X/\mathbb{F}_q, T)$ from the zeta function of hyperplane sections of X (namely, simply by taking their gcd).

Following Algorithm 3, we may fibre X as a Lefschetz pencil of hyperplane sections $\pi : \tilde{X} \to \mathbb{P}^1$ over $\mathbb{F}_q$ (after possibly replacing $\mathbb{F}_q$ by an extension of degree at most polynomial in D). Denote by $U \subset \mathbb{P}^1$ the open subscheme[10] where the fibres are smooth, and Z its complement. Let g be the genus of the geometric generic fibre X_η.

Let $u \in U(\mathbb{F}_q)$. From the formalism of vanishing cycles and the so-called 'hard-Lefschetz theorem' [Del80, 4.3.9], we have the decomposition

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

where X_u denotes the fibre of π over u, and $\mathcal{E}_u$ is the space generated by the vanishing cycles in $\mathrm{H}^1(X_u, \mathbb{Q}_\ell)$. In particular, we have that

$$P_1(X_u/\mathbb{F}_q, T) = P_1(X/\mathbb{F}_q, T) \cdot P(\mathcal{E}_u/\mathbb{F}_q, T) ,$$

where $P(\mathcal{E}_u/\mathbb{F}_q, T)$ denotes the characteristic polynomial of $F_q^\star$ acting on $\mathcal{E}_u$.

[9] by Poincaré duality

[10] write U_0 for the associated $\mathbb{F}_q$-scheme.

A theorem of Deligne (Theorem 4.3) states that $P_1(X/\mathbb{F}_q, T)$ can be recovered from $P_1(X_{u_i}/\mathbb{F}_{q^j}, T)$ for $u_i \in U(\mathbb{F}_{q^j})$ over all extensions $\mathbb{F}_{q^j}$. We show that there is a 'small' extension, and a small number of fibres over that extension to sample, to recover $P_1(X/\mathbb{F}_q, T)$.

Firstly, consider the representation $\rho : \pi_1(U_0, u) \to \mathrm{GL}(2r, \mathbb{Z}_\ell)$ of the étale fundamental group of U_0 associated to the torsion-free lisse $\mathbb{Z}_\ell$-sheaf $\mathcal{E}_{\mathbb{Z}_\ell} \subset R^1\pi_\star\mathbb{Z}_\ell|_U$, of vanishing cycles. Denote by $\overline{\rho} := \rho \mid \pi_1(U, u)$, the restriction to the geometric fundamental group. By [Del74, 5.10], we know that the Zariski-closure of the image of $\overline{\rho}\otimes\mathbb{Q}_\ell$ in $\mathrm{GL}(2r, \mathbb{Q}_\ell)$ is the symplectic group $\mathrm{Sp}(2r, \mathbb{Q}_\ell)$. Using methods of Hall [Hal08], we deduce that the mod-ℓ monodromy of the family, i.e., the image of $\overline{\rho}_\ell : \pi_1(U, u) \to \mathrm{GL}(2r, \mathbb{F}_\ell)$ is the symplectic group $\mathrm{Sp}(2r, \mathbb{F}_\ell)$.

Next, we note that for $u \in U(\mathbb{F}_{q^j})$ the 'vanishing term' $P(\mathcal{E}_u/\mathbb{F}_{q^j}, T)$ is equidistributed (mod-ℓ) in the family, à la Katz (see [Cha97, Theorem 4.1] or [KS99, Theorem 9.7.13]), so can be eliminated with high probability after two samplings. This is done by first moving to a large enough extension $\mathbb{F}_Q$ of $\mathbb{F}_q$ (to minimise the error term coming from the aforementioned equidistrubution theorem) and sampling points uniformly randomly in $U(\mathbb{F}_Q)$. Then the zeta functions of the associated fibres are computed and their gcd is taken. With high probability, this procedure gives $P_1(X/\mathbb{F}_Q, T)$, from which $P_1(X/\mathbb{F}_q, T)$ can be easily recovered.

Theorem 3.6 (Effective gcd)**.** *There exists an extension $\mathbb{F}_Q/\mathbb{F}_q$, with degree $[\mathbb{F}_Q : \mathbb{F}_q]$ bounded by a polynomial in D, such that for any two distinct randomly chosen $u_1, u_2 \in U(\mathbb{F}_Q)$, we have with probability $> 2/3$*

$$\gcd(P_1(X_{u_1}/\mathbb{F}_Q, T), P_1(X_{u_2}/\mathbb{F}_Q, T)) \;=\; P_1(X/\mathbb{F}_Q, T)\,.$$

Proof. Let $\ell \in [(4D)^4/2\,, (4D)^4]$ be a prime distinct from p. Consider the locally constant sheaf $R^1\pi_\star\mathbb{Z}_\ell|_U$ on U. It has as subsheaf, $\mathcal{E}_{\mathbb{Z}_\ell}$, the sheaf of $\mathbb{Z}_\ell$-vanishing cycles of rank (say) $2r$. Denote by $\rho : \pi_1(U_0, u) \to \mathrm{GL}(2r, \mathbb{Z}_\ell)$ the associated ℓ-adic representation and by $\overline{\rho} = \rho|\pi_1(U, u)$. Write ρ_ℓ and $\overline{\rho}_\ell$ respectively, for the mod-ℓ representations.

By the hard-Lefschetz theorem, (Theorem 4.2) we have $2r = 2g - \beta_1$ where β_1 is the first Betti number of X. By Theorem 4.5, we know that the sheaf $\mathcal{E}_{\mathbb{Z}_\ell}$ has big mod-ℓ monodromy, i.e., $\mathrm{im}(\overline{\rho}_\ell) = \mathrm{Sp}(2r, \mathbb{F}_\ell)$. We seek to apply Theorem 4.6 to this setup. 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 4.6 to C, we get

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

By Lemma 4.9 (since $\ell > 119r^2$), the first summand on the RHS is $\le 1/4$. From the calculation[11] of the étale cohomology of U (the projective line with $\#Z$ punctures), we deduce that $|\chi(U)| \le \#Z \le D^{N+1}$. For $q^w > 2D^{N+1}$, we have

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

In particular, if $Q = q^w > \Omega\left(D^{2N+17D^4}\right)$, we have

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

[11]see [Sta18, Tag 03RR]

which completes the proof. $\square$

Remark. Our methods yield a generalisation of the above theorem that enables one to compute the characteristic polynomial of Frobenius on $\mathrm{H}^{n-1}(X, \mathbb{Q}_\ell)$ for an n dimensional variety X from the action on $\mathrm{H}^{n-1}(Y, \mathbb{Q}_\ell)$ for hyperplane sections Y. In the case n is even, we still have big mod-ℓ symplectic monodromy and the proof proceeds similarly to the above. Remarks of Hall [Hal23] have led us to believe that the odd n case is not much harder, having big orthogonal mod-ℓ monodromy instead. This generalisation will be explored in future works.

3.4. **Protocol and algorithms for $P_1(T)$.** Let $X_0 \subset \mathbb{P}^N$ be a smooth projective variety of dimension $n > 1$ and degree D over $\mathbb{F}_q$. An AM$\cap$coAM protocol for certifying $P_1(X/\mathbb{F}_Q, T)$ for any field extension $\mathbb{F}_Q/\mathbb{F}_q$ with $Q > \Omega\left(D^{2N+17D^4}\right)$ is presented in Algorithm 4.

Algorithm 4 Verifying $P_1(T)$ of a *variety*

- **Input:** A smooth projective variety $X_0/\mathbb{F}_q$ of dimension $n > 1$ and degree D, presented as a system of m homogeneous polynomials $f_1, \ldots, f_m$ of degree $\leq d$ in the projective space $\mathbb{P}^N$.
- **Pre-processing:** We first move to a field extension $\mathbb{F}_Q/\mathbb{F}_q$ that affords enough smooth hyperplane sections as in Proposition 3.2 and satisfies the bound of Theorem 3.6. We may reduce to a surface Y by intersecting X with $n-2$ hyperplanes. Next, Y is fibred as a Lefschetz pencil of hyperplane sections following Algorithm 3. Denote by $U \subset \mathbb{P}^1$ the open subscheme parameterising the smooth fibres, and $Z := \mathbb{P}^1 \setminus U$ the finitely many singular ones.
- **Conditions:** Merlin provides a candidate $P(T)$ for $P_1(X/\mathbb{F}_Q, T)$ and Arthur engages in a protocol with Merlin to determine the veracity of the claim.

1: **Arthur:** Pick randomly distinct $u_i \in U(\mathbb{F}_Q)$, for $1 \leq i \leq 2$ following Theorem 3.6.
2: **Merlin:** Provide $P_1(Y_{u_i}/\mathbb{F}_Q, T)$, for $1 \leq i \leq 2$.
3: **Arthur:** Verify that the $P_1(Y_{u_i}/\mathbb{F}_Q, T)$ are as claimed by calling Algorithm 2. Compute their greatest common divisor $G(T)$, using e.g., Euclid's algorithm. Accept iff $G(T) = P(T)$.

Proof of Theorem 1.1. Let $X_0 \subset \mathbb{P}^N$ be a smooth projective variety of dimension $n > 1$ and degree D, over the field $\mathbb{F}_q$ given by homogeneous forms $f_1, \ldots, f_m$, each of total degree $\leq d \in \mathbb{Z}_{>0}$. For any extension $\mathbb{F}_Q/\mathbb{F}_q$ such that $Q > \Omega\left(D^{2N+17D^4}\right)$ of poly-bounded degree, we may verify $P_1(X/\mathbb{F}_Q, T)$ using Algorithm 4. By the same technique as in Lemma 2.12, we can recover $P_1(X/\mathbb{F}_q, T)$ as well. $\square$

We now recall the following result to compute the zeta function of a smooth curve of fixed degree.

Theorem 3.7 (Pila, Huang-Ierardi)**.** *Let $C \subset \mathbb{P}^N$ be a smooth projective curve over $\mathbb{F}_q$, of fixed degree D. Then, there exists an algorithm that computes $P_1(C/\mathbb{F}_q, T)$ in time $O((\log q)^\Delta)$, where Δ is independent of q.*

Proof. Move to a plane nodal model C' of C via Lemma 2.2 and apply the main theorem of [HI98]. $\square$

Proof of Theorem 1.2. The proof proceeds as in the proof of Theorem 1.1. We replace Merlin and Algorithm 2, in Algorithm 4 for computing $P_1(Y_{u_i}/\mathbb{F}_Q, T)$, with the algorithm from Theorem 3.7.

Now, assume X_0 is a surface, which we have fibred as a Lefschetz pencil (parameterised by linear forms F and G) of hyperplane sections. We show how to compute β_2, i.e., the dimension of $\mathrm{H}^2(X, \mathbb{Q}_\ell)$. By [Mil80, V.3.12], we have

$$\beta_2 \;=\; \#Z + 2\beta_1 - 4g + 2\,,$$

where $\#Z$ is the number of critical fibres and g is the genus of a smooth hyperplane section. The latter can be computed by an effective Riemann-Roch algorithm (eg. Proposition 2.5), and $\#Z$ can be computed by hand as follows. Take a parametric hyperplane $\lambda F + \mu G$ in the family and intersect X with it. Using the Jacobian criterion for smoothness (on an affine piece), one recovers the finitely many $[\lambda : \mu]$ for which the associated hyperplane section is singular. The number β_1 can be read off from the degree of $P_1(X/\mathbb{F}_q, T)$; finally, giving β_2 as well. ☐

For Theorem 1.3, we recall a theorem of Kedlaya [Ked06] that enables efficient quantum computation of the zeta function of a curve.

Theorem 3.8 (Kedlaya)**.** *Let $C \subset \mathbb{P}^N$ be a smooth projective curve over $\mathbb{F}_q$, of degree D. Then, there exists a quantum algorithm that computes $P_1(C/\mathbb{F}_q, T)$ in time polynomial in $D \log q$.*

Proof of Theorem 1.3. Similar to the proof of Theorem 1.2; simply replace the algorithm of Huang-Ierardi for computing the zeta function of a curve (Theorem 3.7), by Kedlaya's quantum algorithm (Theorem 3.8). ☐

4. Vanishing cycles, monodromy, and equidistribution

4.1. **Vanishing cycles.** In this subsection, we give a brief overview of the theory of vanishing cycles associated to a surface fibred as a Lefschetz pencil over $\mathbb{P}^1$. Then, we discuss the 'hard-Lefschetz theorem' and some implications for the first étale cohomology. Finally, we wrap with a statement of Deligne's 'théorème du pgcd', which enables us to recover the characteristic polynomial of Frobenius, acting on the first cohomology, from its action on the cohomology of the fibres.

Let X_0 be a smooth, projective, geometrically irreducible surface over the finite field $\mathbb{F}_q$ of characteristic $p > 0$. Denote by X the base change to the algebraic closure. Assume we have a Lefschetz fibration $\pi : \tilde{X} \to \mathbb{P}^1$ following Algorithm 3. As usual, we let $Z \subset \mathbb{P}^1$ denote the set giving rise to singular fibres (nodal curves), and let U denote its complement. Let X_η be the generic fibre of π. It is a smooth curve of genus g over the function field of $\mathbb{P}^1$.

Let ℓ be an odd prime, coprime to p. Consider the sheaf $\mathcal{F}^\ell := R^1\pi_\star\mu_\ell$ on $\mathbb{P}^1$. By the proper base-change theorem, we have that its stalk at a point $u \to \mathbb{P}^1$ is the group $\mathrm{H}^1(X_u, \mu_\ell) \simeq \mathrm{Pic}^0(X_u)[\ell]$. Further, we know that $\mathcal{F}^\ell|_U$ is a locally constant sheaf of rank $2g$ on U. We seek to understand the behaviour of $\mathcal{F}^\ell$ at points $z \in Z$. Let $X'_z \to X_z$ be the normalisation (which has genus $g-1$) of such a singular fibre, and denote by V_z, the kernel of the map $\mathcal{F}^\ell_z \to \mathrm{Pic}^0(X'_z)[\ell]$. We call V_z the group of *vanishing cycles* at z. We now recall a collection of results from [Mil80, V.3].

Proposition 4.1. *With the above setup, the following are true:*

- *For any $u \in \mathbb{P}^1$ there exists a cospecialisation map $\mathcal{F}_u^\ell \to \mathcal{F}_\eta^\ell$ which is an isomorphism if and only if $u \in U$.*
- *If $z \in Z$, the cospecialisation map $\mathcal{F}_z^\ell \to \mathcal{F}_\eta^\ell$ is an injection. In particular $\mathcal{F}_z^\ell \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g-1}$. Further, V_z is the exact annihilator of $\mathcal{F}_z^\ell$ under the Weil-pairing map*
$$\langle \cdot, \cdot \rangle : \mathcal{F}_\eta^\ell \times \mathcal{F}_\eta^\ell \longrightarrow \mu_\ell(\overline{\mathbb{F}}_q)\,.$$
- *$\mathcal{F}^\ell$ is tamely ramified at all $z \in Z$.*

In particular, for $z \in Z$, we have $V_z \simeq \mathbb{Z}/\ell\mathbb{Z}$ [12], and we denote by δ_z, the element that maps to 1. We may also identify δ_z with its image under the map $\mathcal{F}_z^\ell \to \mathcal{F}_\eta^\ell$, and call $\mathcal{E}^\ell(X_\eta)$ the subspace generated by all the δ_{z_i} in $\mathcal{F}_\eta^\ell$ for $z_i \in Z$. By the cospecialisation map, we refer to the corresponding subspace generated in $\mathcal{F}_u^\ell$ for $u \in U$ by $\mathcal{E}^\ell(X_u)$. By passage to the limit and tensoring, we also obtain the $\mathbb{Q}_\ell$-vector space of vanishing cycles $\mathcal{E}(X_u)$. Moreover, there exists a locally constant subsheaf $\mathcal{E} \subset R^1\pi_\star\mathbb{Q}_\ell|_U$, called the *sheaf of vanishing cycles* with stalk $\mathcal{E}_u = \mathcal{E}(X_u)$ for $u \in U$. We now recall the 'hard-Lefschetz' theorem for surfaces, which measures precisely the discrepancy between $\mathrm{H}^1(X_u, \mathbb{Q}_\ell)$ and $\mathrm{H}^1(X, \mathbb{Q}_\ell)$.

Theorem 4.2 (Hard-Lefschetz)**.** *We have the decomposition*
$$\mathrm{H}^1(X_u, \mathbb{Q}_\ell) \simeq \mathrm{H}^1(X, \mathbb{Q}_\ell) \oplus \mathcal{E}_u$$
with respect to the symplectic pairing. In particular, $\mathrm{H}^1(X, \mathbb{Q}_\ell) \simeq \mathcal{E}_u^\perp$ when viewed as a subspace of $\mathrm{H}^1(X_u, \mathbb{Q}_\ell)$ under the weak-Lefschetz map.

The general result is a deep theorem of Deligne [Del80, 4.3.9]. The surface case is easier to handle and is done in [Kle68, 2.A.10]. We conclude this subsection with a statement of Deligne's 'théorème du pgcd' [Del80, 4.5.1].

Let $X_0/\mathbb{F}_q$ now be a smooth, projective, geometrically irreducible variety of dimension n and let X be the base change to the algebraic closure.

Theorem 4.3 (Le théorème du pgcd)**.** *Let $(X_t)_{t \in \mathbb{P}^1}$ be a Lefschetz pencil of hypersurface sections of degree $d \geq 2$ on X. Then $P_{n-1}(X/\mathbb{F}_q, T)$ can be constructed as the least common multiple of polynomials $f(T) \in \mathbb{C}[T]$, satisfying the condition that for any $t \in \mathbb{F}_{q^r}$ such that X_t is smooth, the polynomial* [13] *$f(T)^{(r)}$ divides $P_{n-1}(X_t/\mathbb{F}_{q^r}, T)$.*

Deligne derived the above as a consequence of his proof of the Weil-Riemann hypothesis and hard-Lefschetz theorem for ℓ-adic cohomology. Theorem 4.3 has been used by Katz-Messing in [KM74] to deduce the same facts for any Weil cohomology theory. The theorem was also used by Gabber in [Gab83] to show torsion-freeness of the integral ℓ-adic cohomology for smooth projective varieties for 'almost all' ℓ.

4.2. **Monodromy and equidistribution.** In this subsection, we introduce the notion of monodromy in a Lefschetz pencil. We then recall a big mod-ℓ monodromy result, obtained by an adaptation of work of Hall. Finally, we state a version of Deligne's equidistribution theorem [Del80, 3.5.3] due to Katz. As before, let $\pi : \tilde{X} \to \mathbb{P}^1$ be a Lefschetz pencil of curves on a smooth, projective surface X. We denote by $U_0 \subset \mathbb{P}^1$ the locus parameterising smooth fibres (of genus g) and by $U = U_0 \times \overline{\mathbb{F}}_q$. Let $Z = \mathbb{P}^1 \setminus U$ be the finite set parameterising the critical fibres. Write $\mathcal{F} = R^1\pi_\star\mathbb{Q}_\ell$ and $\mathcal{F}^\ell = R^1\pi_\star\mu_\ell$ for the respective direct-image sheaves.

Let $u \in U$ be a geometric point. The *arithmetic étale fundamental group* (see [Mur67] for the definition) $\pi_1(U_0, u)$ acts on $\mathcal{F}_u^\ell$ and by passage to the limit, on $\mathcal{F}_u$. This latter

[12] we omit Tate-twists by fixing an isomorphism $\mathbb{Z}/\ell\mathbb{Z} \simeq \mu_\ell(\overline{\mathbb{F}}_q)$.

[13] if $f(T) = \prod_j (1 - \alpha_j T)$, then $f(T)^{(r)} := \prod_j (1 - \alpha_j^r T)$.

representation restricted to the *geometric étale fundamental group* $\pi_1(U,u)$ is called the *monodromy* of the pencil. Since $\mathcal{F}$ is tamely ramified, the action of $\pi_1(U,u)$ factors through the *tame fundamental group*[14] $\pi_1^t(U,u)$. By a theorem of Grothendieck [Gro57, 182-27], $\pi_1^t(U,u)$ is generated topologically by $\#Z$ elements σ_i for each $z_i \in Z$, satisfying the relation $\Pi_{i=1}^{\#Z}\sigma_i = 1$. The Picard-Lefschetz formulas make this action explicit. See [Mil80, Theorem 3.14] or [FK13, III.4.3] for a proof.

Proposition 4.4 (Picard-Lefschetz formulas)**.** *For any* $\gamma \in \mathcal{F}_u^\ell$*, we have*

$$\sigma_i(\gamma) \ = \ \gamma - \epsilon_i \cdot \langle \gamma, \delta_{z_i} \rangle \cdot \delta_{z_i} \ ,$$

where for a uniformising parameter θ_i at z_i, we have $\sigma_i(\theta_i^{1/\ell}) = \epsilon_i \cdot \theta_i^{1/\ell}$. Clearly, the monodromy action respects the symplectic pairing.

By the hard-Lefschetz theorem, we know that $\mathrm{H}^1(X_u,\mathbb{Q}_\ell) \simeq \mathrm{H}^1(X,\mathbb{Q}_\ell) \oplus \mathcal{E}_u$, with $\mathrm{H}^1(X,\mathbb{Q}_\ell) = \mathcal{E}_u^\perp$. In particular, $\pi_1(U,u)$ acts trivially on $\mathrm{H}^1(X,\mathbb{Q}_\ell)$, implying that the monodromy action factors through $\mathrm{Sp}(\mathcal{E}_u)$. We know [Del74, 5.10] that the image of $\pi_1(U,u)$ is open and Zariski-dense in $\mathrm{Sp}(\mathcal{E}_u)$. Further, by the conjugacy of vanishing cycles, we also know $\pi_1(U,u)$ acts absolutely irreducibly on $\mathcal{E}_u$.

One seeks a version of the above to compute the mod-ℓ geometric monodromy for certain equidistribution estimates coming from Theorem 4.6. Consider the torsion-free sheaf $R^1\pi_\star\mathbb{Z}_\ell$ of rank $2g$ on U. It has as subsheaf, the sheaf of integral ℓ-adic vanishing cycles $\mathcal{E}_{\mathbb{Z}_\ell} \subset R^1\pi_\star\mathbb{Z}_\ell$ of rank, say, $2r$. This in turn, corresponds to representations $\rho : \pi_1(U_0,u) \to \mathrm{GL}(2r,\mathbb{Z}_\ell)$ and $\overline{\rho} = \rho|\pi_1(U,u)$. Let $\mathcal{V} := \mathcal{E}_{\mathbb{Z}_\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell$ be the lisse $\mathbb{F}_\ell$-sheaf giving rise to, respectively, the mod-ℓ representations ρ_ℓ and $\overline{\rho}_\ell$. There are multiple ways to show big mod-ℓ monodromy for 'almost all primes ℓ' (all but finitely many), but [Hal08, §4-6] gives a method that works for *every* prime $\ell \geq 5$ invertible on the characteristic. The following result appears to be known to Hall and Katz ([Hal08, pg 5] and [Hal23]); for completeness, we provide a brief sketch below.

Theorem 4.5 (Big mod-ℓ monodromy)**.** *We have* $G := \overline{\rho}_\ell\left(\pi_1(U,u)\right) = \mathrm{Sp}(2r,\mathbb{F}_\ell)$.

Proof sketch. It is enough to show that the representation is irreducible and contains a transvection. Indeed, by [Hal08, Theorem 3.1], this implies that $G = \mathrm{Sp}(2r,\mathbb{F}_\ell)$. The proof of [Hal08, Theorem 5.1] can be adapted to work in our case by considering the tame local system $\mathcal{V}$ on U instead. The essential ingredient is Katz's [Kat96, Ch 6] *middle convolution algorithm* [Sim09, DR00] to relate the $\mathbb{F}_\ell$-sheaf $\mathcal{V}$ to a middle convolution sheaf $\mathcal{M}$ (see below), which is known to be irreducible.

We notice firstly, that the representation corresponding to $\mathcal{V}$ satisfies the conditions of [DR00, Corollary 3.6]. Next, let $j : U \hookrightarrow \mathbb{P}^1$ be the open immersion. For $t \in \mathbb{P}^1 \setminus \{\infty\}$, denote by τ_t the involution on $\mathbb{P}^1$ associated to $x \mapsto t - x$ and by $\iota : U \setminus \{t\} \to \mathbb{P}^1$, the inclusion.

We consider the cohomology groups $\mathrm{H}^1(\mathbb{P}^1, \iota_\star\iota^\star(j_\star\mathcal{V} \otimes \tau_t^\star\mathcal{L}_\lambda))$, where the $\mathbb{F}_\ell$-sheaf $\mathcal{L}_\lambda$ is a Kummer sheaf [15] adapted from [Hal08, §4]. We call $\mathcal{M}$ the sheaf whose stalk at any $t \in \mathbb{P}^1$ is the above group. Its rank is constant for $t \in U$.

Using [Hal08, Lemma 4.1] and an analysis of the stalks $\mathcal{M}_z$ for $z \in Z$, it can be shown that the local monodromy around z contains a transvection, in particular an irreducible rank 2 Jordan block (essentially coming from the Picard-Lefschetz formulas). This, then, combined with [DR00, Corollary 3.6] gives the result. □

[14] essentially classifying finite étale covers of U tamely ramified over Z.

[15] chosen according to [Kat96, 5.2.1]

Remark. There is a simpler proof of the above, if we know that $\mathrm{H}^2(X, \mathbb{Z}_\ell)$ is free of torsion. In that case, one has a 'mod-ℓ hard-Lefschetz theorem', which, combined with the conjugacy of the mod-ℓ vanishing cycles, gives the irreducibility. However, we only have torsion-freeness for all but finitely many ℓ [Gab83], with no known effective bounds in general.

We close this subsection with the statement of a powerful Chebotarev-type equidistribution theorem 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. 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. The following is [Cha97, Theorem 4.1].

Theorem 4.6 (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.

4.3. **Symplectic groups over finite fields.** 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 4.7. The group of *symplectic similitudes*, $\mathrm{GSp}(2r, \mathbb{F}_\ell)$ is defined as

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

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

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

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 4.8. *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 $W \subset \mathbb{A}^r_{\mathbb{F}}$ 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 $\#W(\mathbb{F}_\ell) \le 4r\ell^{r-1}$. Further, recalling the order formula for the symplectic group, we have

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

Therefore, combining with Lemma 4.8, 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 4.9 (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 $\ell > 119r^2$,*

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

5. Conclusion

We have presented randomised methods to efficiently certify and compute the characteristic polynomial of the geometric Frobenius on the first ℓ-adic étale cohomology of smooth varieties. The immediate question is for cohomology in higher degrees: to begin with, how do we compute $P_2(T)$ for a smooth projective surface over $\mathbb{F}_q$ in time polynomial in $\log q$? It is conceivable to do this using the method of vanishing cycles, combined with lifting techniques; these possibilities will be the subject of a future work.

In another direction, one may ask for *deterministic* verification, i.e., an $\mathrm{NP} \cap \mathrm{coNP}$ protocol for $P_1(T)$ and more generally for $P_i(T)$.

Finally, one seeks an effective gcd theorem[16] for Lefschetz pencils of any fibre dimension, with a view towards effective bounds for Gabber's theorem [Gab83, Gab22] on the torsion-freeness of integral ℓ-adic cohomology. These issues will be addressed in forthcoming works.

[16] see the remark following Theorem 3.6

Acknowledgements

V.M. is supported by a C3iHub research fellowship. N.S. thanks the funding support from DST-SERB (CRG/2020/45 + JCB/2022/57) and N. Rama Rao Chair. V.M. thanks Chris Hall, Donu Arapura and Jeff Achter for email conversations. We thank Vasudevan Srinivas, Kiran Kedlaya and Partha Mukhopadhyay for enthusiastic discussions about the related problems.

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach.* Cambridge University Press, 2009. 2, 8, 9

[ABCL02] Simon Abelard, Elena Berardini, Alain Couvreur, and Grégoire Lecerf. Computing Riemann–Roch spaces via Puiseux expansions. *Journal of Complexity*, 73, 2002. 6

[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. 3

[Bal03] Edoardo Ballico. An effective Bertini theorem over finite fields. *Advances in Geometry*, 3(4):361–363, 2003. 11

[Ber86] Pierre Berthelot. Géométrie rigide et cohomologie des variétés algébriques de caractéristique p. *Groupe de travail d'analyse ultramétrique*, 9(3):J1–J18, 1986. 2

[BS86] Zenon Ivanovich Borevich and Igor Rostislavovich Shafarevich. *Number theory.* Academic press, 1986. 20

[CDV06] Wouter Castryck, Jan Denef, and Frederik Vercauteren. Computing zeta functions of nondegenerate curves. *International Mathematics Research Papers*, 2006:72017, 2006. 3

[CFA+05] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography.* CRC press, 2005. 2

[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. 14, 19

[Del74] Pierre Deligne. La conjecture de Weil : I. *Publications Mathématiques de l'IHÉS*, 43:273–307, 1974. 1, 14, 18

[Del80] Pierre Deligne. La conjecture de Weil : II. *Publications Mathématiques de l'IHÉS*, 52:137–252, 1980. 3, 5, 13, 17

[DR00] Michael Dettweiler and Stefan Reiter. An algorithm of Katz and its application to the inverse Galois problem. *Journal of Symbolic Computation*, 30(6):761–798, 2000. 18

[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. 3

[Dwo60] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math*, 82:631–648, 1960. 3

[FK13] Eberhard Freitag and Reinhardt Kiehl. *Étale cohomology and the Weil Conjecture*, volume 13. Springer Science & Business Media, 2013. 18

[FR94] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of computation*, 62(206):865–874, 1994. 3

[Fu11] Lei Fu. *Etale cohomology theory*, volume 13. World Scientific, 2011. 11

[G+77] Alexander Grothendieck et al. Cohomologie ℓ-adique et fonctions L (SGA V). *Lecture Notes in Math*, 589, 1977. 1, 2

[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. 17, 19, 20

[Gab22] Ofer Gabber. Bounding the torsion in the ℓ-adic cohomology of smooth projective varieties without unbounded searches. ICM talk, 2022. 20

[GLP83] Laurent Gruson, Robert Lazarsfeld, and Christian Peskine. On a theorem of Castelnuovo, and the equations defining space curves. *Inventiones mathematicae*, 72:491–506, 1983. 13

[Gro57] Alexander Grothendieck. Fondements de la géométrie algébrique. Commentaires. *Séminaire Bourbaki*, 7:297–298, 1957. 18

[GS86] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 59–68, 1986. 4

[Hal08] Chris Hall. Big symplectic or orthogonal monodromy modulo ℓ. *Duke Mathematical Journal*, 141(1):179 – 203, 2008. 5, 14, 18

[Hal23] Chris Hall. personal communication. 2023. 15, 18

[Har05] Gilbert Harman. On the greatest prime factor of $p-1$ with effective constants. *Mathematics of Computation*, 74(252):2035–2041, 2005. 10

[Har13] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013. 6

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

[Has36] Helmut Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. 1936. 7

[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. 6, 7

[HI98] Ming-Deh Huang and Doug Ierardi. Counting points on curves over finite fields. *Journal of Symbolic Computation*, 25(1):1–21, 1998. 3, 15

[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. 12

[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. 12

[Kat96] Nicholas M Katz. *Rigid local systems.* Number 139. Princeton University Press, 1996. 18

[Ked01] Kiran S Kedlaya. Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology. *J. Ramanujan Math. Soc.*, 2001. 3

[Ked06] Kiran S Kedlaya. Quantum computation of zeta functions of curves. *computational complexity*, 15:1–19, 2006. 2, 4, 7, 10, 16

[Kle68] Steven L Kleiman. Algebraic cycles and the Weil conjectures. *Dix Exposes sur la Cohomologie des Schemas, Masson et Cie*, 1968. 17

[KM74] Nicholas M Katz and William Messing. Some consequences of the Riemann hypothesis for varieties over finite fields. *Inventiones mathematicae*, 23(1):73–77, 1974. 17

[Koz94] Dexter Kozen. Efficient Resolution of Singularities of Plane Curves. *Foundation of Software Technology and Theoretical Computer Science*, 141:1 – 11, 1994. 7

[KS99] Nicholas M Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45. American Mathematical Soc., 1999. 14, 19

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

[Lev22] Christophe Levrat. Calcul effectif de la cohomologie des faisceaux constructibles sur le site étale d'une courbe. *arXiv preprint arXiv:2209.10221*, 2022. 4

[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. 6, 8

[LPP03] Hendrik Lenstra, Jonathan Pila, and Carl Pomerance. Future directions in algorithmic number theory. Available on-line at `http://www.aimath.org/WWN/primesinp/articles/html/38a`, 2003. 2

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

[Mac19] Eoin Mackall. A degree-bound on the genus of a projective curve. Available on author's webpage: `https://www.eoinmackall.com/s/deggen2.pdf`, 2019. 13

[Mil80] James S Milne. *Etale cohomology (PMS-33)*. Princeton University Press, 1980. 13, 16, 18

[Mil98] James S Milne. Lectures on étale cohomology. Available on-line at `http://www.jmilne.org/math/CourseNotes/LEC.pdf`, 1998. 12, 13

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

[Mur67] Jacob P Murre. *Lectures on an introduction to Grothendieck's theory of the fundamental group*. Tata Institute of Fundamental Research Bombay, 1967. 17

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

[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. 3

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

[Ser88] Jean-Pierre Serre. *Algebraic groups and class fields*. Springer, 1988. 7

[Sim09] Carlos Simpson. Katz's Middle Convolution Algorithm. *Pure and Applied Mathematics Quarterly*, 5(2):781–852, 2009. 18

[Sta18] The Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`, 2018. 14

[Vol00] José Felipe Voloch. Jacobians of curves over finite fields. *The Rocky Mountain Journal of Mathematics*, 30(2):755–759, 2000. 7

[Wei48a] André Weil. *Sur les courbes algébriques et les variétés qui s' en déduisent*. Number 1041. Actualités Sci. Ind, 1948. 6, 7

[Wei48b] André Weil. *Variétés abéliennes et courbes algébriques*, volume 32. Paris, 1948. 6

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

Email address: diptajit@cse.iitk.ac.in

Current address: https://www.cse.iitk.ac.in/users/nitin/
Email address: nitin@cse.iitk.ac.in