Bounding Picard numbers of surfaces using p-adic cohomology

Timothy G. Abbott, Kiran S. Kedlaya, and David Roe

January 17, 2006

Abstract

Motivated by an application to LDPC (low density parity check) algebraic geometry codes described by Voloch and Zarzar, we describe a computational procedure for establishing an upper bound on the arithmetic or geometric Picard number of a smooth projective surface over a finite field, by computing the Frobenius action on p-adic cohomology to a small degree of p-adic accuracy. We have implemented this procedure in Magma; using this implementation, we exhibit several examples, such as smooth quartics over $\mathbb{F}_2$ and $\mathbb{F}_3$ with arithmetic Picard number 1, and a smooth quintic over $\mathbb{F}_2$ with geometric Picard number 1. We also produce some examples of smooth quartics with geometric Picard number 2, which by a construction of van Luijk also have trivial geometric automorphism group.

Introduction

Much recent work has gone into the computational problem of computing the zeta function of a "random" curve over a finite field, in large part because the question of determining the order of the Jacobian group (class group) of such a curve stands in the way of using said group for public key cryptography. The history of this problem is not our present concern, and anyway it has been documented elsewhere; see for example [25] for an overview.

By contrast, relatively little work has gone into the analogous computational problem over higher dimensional varieties. Ongoing work of Bas Edixhoven and his collaborators, to give an efficient algorithm for computing the n-th Fourier coefficient of a fixed modular form when n is a large integer of known factorization, amounts to computing factors of zeta functions of higher-dimensional varieties over large prime fields using methods of ℓ-adic cohomology. Over fields of small characteristic, one also may use techniques of p-adic cohomology, which when applicable tend to yield more efficient algorithms. However, while a number of reasonable-looking algorithms for various higher-dimensional varieties have been described theoretically, e.g., by Gerkmann [12], Lauder [27, 28], and Lauder and Wan [30], until recently nothing had been attempted in practice. (For some very recent developments on this front, see Section 3.6.)

The purpose of this paper is to begin repairs on this gap in knowledge, by on one hand illustrating how even limited information about the action of Frobenius in p-adic cohomology can be used to address questions of some possibly practical import, and on the other hand to outline an algorithm which has been demonstrated in practice to be able to obtain this limited information. The potential import stems from the fact that one can use information about Frobenius, specifically bounds on Picard numbers obtained from performing linear algebra on a low-precision Frobenius matrix, to control the minimum distance of an algebraic geometry (Goppa) code derived from a surface. As observed by Voloch and Zarzar, such codes have the LDPC (low density parity check) property and so may be of special interest.

Besides this introduction, the paper is structured in four main sections. The first section is general, describing in detail what a Picard number is and how to use an approximately computed Frobenius matrix to bound it. The second part gathers some facts about algebraic de Rham cohomology and p-adic cohomology. The third part sketches a particular algorithm for producing an approximate Frobenius matrix on the cohomology of a smooth hypersurface, using p-adic cohomology and a description of the cohomology of a smooth hypersurface due to Griffiths [15]; we also mention some related proposals. The fourth part describes an implementation of our algorithm in Magma and tallies a few experimental results.

1 Picard numbers and Frobenius matrices

1.1 Picard groups

Definition 1.1.1. Let X be a variety over a field k. The *Picard group* $\mathrm{Pic}(X)$ is the group of isomorphism classes of line bundles (or invertible sheaves) on X. Note that for X smooth, isomorphism classes of line bundles are in natural bijection with rational equivalence classes of (Weil or Cartier) divisors on X.

Lemma 1.1.2. *Let X be a smooth proper irreducible variety over a field k, let k^{sep} denote the separable closure of k, and put $G = \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Then the natural map*

$$\mathrm{Pic}(X) \to \mathrm{Pic}(X \times_k k^{\mathrm{sep}})^G$$

(in which the superscripted G means take G-invariants) is always injective; moreover, if the Brauer group $\mathrm{Br}(k)$ is trivial (e.g., if k is finite), then the map is always surjective.

Proof. For any smooth X, the Hochschild-Serre spectral sequence in étale cohomology gives rise to an exact sequence

$$0 \to H^1(G, k^{\mathrm{sep}}[X]^*) \to \mathrm{Pic}(X) \to \mathrm{Pic}(X \times_k k^{\mathrm{sep}})^G \to H^2(G, k^{\mathrm{sep}}[X]^*)$$

where $k^{\mathrm{sep}}[X]^* = H^0(X \times_k k^{\mathrm{sep}}, \mathbb{G}_m)$ (see, e.g., [38, Lemme 6.3]). For X proper irreducible, $k^{\mathrm{sep}}[X]^* = (k^{\mathrm{sep}})^*$, and $H^1(G, (k^{\mathrm{sep}})^*) = 0$ by Hilbert's Theorem 90, while $H^2(G, (k^{\mathrm{sep}})^*) = \mathrm{Br}(k)$. This yields the desired results. □

Definition 1.1.3. For X smooth proper irreducible over a field k, we say that a divisor is *algebraically equivalent to zero* if it has the form

$$(D \cap (X \times \{p\})) - (D \cap (X \times \{q\}))$$

for some connected (but not necessarily smooth or irreducible) curve C, some pair of closed points p, q on C of the same degree, and some divisor D on $X \times C$ containing no fibres of the projection $X \times C \to C$. The set of divisors algebraically equivalent to zero is a subgroup closed under rational equivalence; let $\mathrm{Pic}^0(X)$ denote the image of this subgroup in $\mathrm{Pic}(X)$.

Remark 1.1.4. For k algebraically closed, the elements of $\mathrm{Pic}^0(X)$ can be thought of in a natural way as the k-valued points on a certain variety over k, the *Picard variety* associated to X; there is also a scheme-theoretic version of this fact that works over more general bases. We will not use this interpretation here.

Lemma 1.1.5. *Let X be a smooth irreducible complete intersection in $\mathbb{P}^r_k$, for k a perfect field and r a positive integer. Then $\mathrm{Pic}^0(X) = 0$, $\mathrm{Pic}(X)$ is torsion-free, and $\mathcal{O}(1)$ is indivisible in $\mathrm{Pic}(X)$.*

Proof. For k algebraically closed, this is [9, Théorème 1.8]; the general case follows from the algebraically closed case plus Lemma 1.1.2. Note that if $\dim(X) \geq 3$, one in fact has $\mathrm{Pic}(X) = \mathbb{Z} \cdot \mathcal{O}(1)$. □

1.2 Néron-Severi groups

Definition 1.2.1. For X smooth proper irreducible over a field k, the quotient $\mathrm{NS}(X) = \mathrm{Pic}(X)/\mathrm{Pic}^0(X)$ is called the *Néron-Severi group* of X.

Remark 1.2.2. For X projective, one may define the degree of a divisor with respect to any fixed ample divisor. The resulting map induces a homomorphism $\deg : \mathrm{NS}(X) \to \mathbb{Z}$ sending any ample divisor to a positive integer; in particular, $\mathrm{NS}(X)$ is nontrivial and any ample divisor represents a nonzero class in $\mathrm{NS}(X)$.

Remark 1.2.3. For $k = \mathbb{C}$, there is a natural map

$$\mathrm{NS}(X) \to H^2(X^{\mathrm{an}}, \mathbb{Z}) \cap H^{1,1}(X), \tag{1.2.3.1}$$

where X^{an} denotes the analytic space associated to X and $H^{1,1}(X) = H^1(X, \Omega^1_X)$ (which by GAGA may be computed either algebraically or analytically); the Lefschetz (1,1)-theorem [16, §1.2] asserts that the map (1.2.3.1) is a bijection.

Definition 1.2.4. Let X be a smooth proper irreducible variety over a field k. From the Lefschetz theorem, it follows that $\mathrm{NS}(X)$ is finitely generated in case $k = \mathbb{C}$. In fact, $\mathrm{NS}(X)$ is always finitely generated; this was first shown by Néron [36] (see also [19, 31]). The rank of $\mathrm{NS}(X)$ as a finitely generated abelian group is called the *Picard number* (or *arithmetic Picard number*) of X. The rank of $\mathrm{NS}(X \times_k \overline{k})$, for $\overline{k}$ the algebraic closure of k, is called the *geometric Picard number* of X.

Definition 1.2.5. Let X be a smooth projective surface over a field k. Then intersection theory [20, Chapter V] gives rise to a symmetric pairing on divisors of X, called the *intersection pairing*; this pairing respects algebraic equivalence, so it descends to $\mathrm{NS}(X)$. We say a divisor D is *numerically equivalent to zero* if $C \cdot D = 0$ for every projective curve C contained in X; this turns out to happen if and only if some multiple of D is algebraically equivalent to zero [33]. That is, the quotient of $\mathrm{NS}(X)$ by the classes of divisors numerically equivalent to zero is precisely $\mathrm{NS}(X)/\mathrm{NS}(X)_{\mathrm{tors}}$. This group is never zero because an ample divisor D satisfies $C \cdot D > 0$ for any C, and so is not numerically equivalent to zero. That is, the Picard number of a smooth projective surface is always positive.

Remark 1.2.6. Although we will only attempt to bound Picard numbers over finite fields, doing so also has consequences over number fields. That is because if $\mathfrak{p}$ is a prime ideal in the ring of integers $\mathfrak{o}_K$ of a number field K, $k = \mathfrak{o}_K/\mathfrak{p}$, and X is a smooth projective surface over the localization of $\mathfrak{o}_K$ at $\mathfrak{p}$, then the torsion-free quotient of $\mathrm{NS}(X_K)$ injects into the torsion-free quotient of $\mathrm{NS}(X_k)$, compatibly with the intersection pairing [45, §6]. We can thus control the size of $\mathrm{NS}(X_K)$ by controlling $\mathrm{NS}(X_k)$; in some cases, one can gain further control by reducing modulo more than one prime of good reduction [46].

1.3 Picard numbers and codes

We now recall briefly what Picard numbers have to do with error-correcting codes; the link lies in a higher-dimensional version of Goppa's construction [11] of algebraic geometry codes from curves over finite fields.

Definition 1.3.1. Let X be a smooth projective irreducible variety over a finite field $\mathbb{F}_q$. Let H be an ample divisor on X, let m be a positive integer such that the divisor mH is very ample, and let $\mathcal{L}(mH) = \Gamma(X, \mathcal{O}(mH))$ be the Riemann-Roch space of mH; we may identify elements of $\mathcal{L}(mH)$ with rational functions $f \in \mathbb{F}_q(X)$ such that the divisor $\mathrm{div}(f) + mH$ is effective. Let S be the set of $\mathbb{F}_q$-rational points of $X \setminus H$. Define the code $C(X, mH)$ to be the subspace of $\mathbb{F}_q^S$ of functions induced by elements of $\mathcal{L}(mH)$, viewed as a linear code over $\mathbb{F}_q$.

In Goppa's original construction, X is a curve, the rate of the code (the ratio between the dimensions of the code and of its ambient space) is determined by Riemann-Roch, and a good bound on the minimum distance (the smallest number of nonzero elements in a nonzero codeword) comes from the fact that a rational function cannot have more zeros than poles. In higher dimensions, one can still get rate information out of Riemann-Roch, but bounding the minimum distance is trickier. For surfaces, this question has been investigated by Voloch and Zarzar, with the idea of using the subcodes induced by curves on a surface to give an asynchronous decoding algorithm in the style of Luby-Mitzenmacher [32]. Voloch and Zarzar observe that a low Picard number gives rise to a good bound on the minimum distance; we limit ourselves here to mentioning two sample assertions, and defer to [48] for more information.

Lemma 1.3.2 (Voloch). *Let X be a smooth projective surface over a field k, and suppose $\mathrm{NS}(X)/\mathrm{NS}_{\mathrm{tors}}(X)$ is generated by the ample divisor H. Then for any positive integer m, the zero divisor of a nonzero element of $\mathcal{L}(mH)$ has at most m irreducible components.*

Proof. See [48, Lemma 2.2]. □

Lemma 1.3.3 (Zarzar). *Let X be a smooth surface of degree d in $\mathbb{P}^3$ over a perfect field k, and suppose that the Picard number of X is equal to 1. If Y is an irreducible surface in $\mathbb{P}^3$ of degree $m < d$, then $X \cap Y$ is also irreducible.*

Proof. First note that $\mathrm{Pic}(X)$ and $\mathrm{NS}(X)$ coincide and are torsion-free by Lemma 1.1.5. Then invoke [50, Lemma 2.1]. □

1.4 Zeta functions and Picard numbers

Definition 1.4.1. Let X be a smooth proper variety over a finite field $\mathbb{F}_q$. The *zeta function* of X is the power series

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

The Weil conjectures, proved by Dwork, Grothendieck, Deligne, et al. (see [20, Appendix C] for a fuller statement), assert that there exists a product decomposition

$$Z(X,T) = \prod_{i=0}^{2\dim(X)} P_i(T)^{(-1)^{i+1}},$$

where $P_i(T) \in \mathbb{Z}[T]$ and $P_i(0) = 1$, such that the roots of $P_i(T)$ in $\mathbb{C}$ all have absolute value $q^{-i/2}$. Moreover, the multiset of roots of P_i is invariant under the transformation $r \mapsto q^{-i}/r$.

The connection between zeta functions and Picard numbers was first articulated by Tate [41], who showed that

$$\operatorname{rank}\mathrm{NS}(X) \leq \operatorname{ord}_{T=1/q} P_2(T). \tag{1.4.1.1}$$

(Actually Tate's argument gives a bit more information than this; see Remark 1.5.2 below.) Tate conjectured further (by analogy with the conjecture of Birch and Swinnerton-Dyer) that equality always holds in (1.4.1.1); Tate himself showed this for abelian varieties, and it is also known in some other cases, e.g., for ordinary K3 surfaces [49]. Tate's conjecture in general is wide open; however, since our purpose here is merely to give upper bounds for Picard numbers, the unconditional inequality (1.4.1.1) will suffice. (See [42] for more context on Tate's conjecture.)

Note that (1.4.1.1) also gives a bound on the geometric Picard number:

$$\operatorname{rank}\mathrm{NS}(X \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}) \leq \sum_{\zeta} \operatorname{ord}_{T=\zeta/q} P_2(T), \tag{1.4.1.2}$$

where ζ runs over all roots of unity. Since $P_2(T)$ has integer coefficients, we can rewrite (1.4.1.2) as

$$\operatorname{rank} \mathrm{NS}(X \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}) \leq \sum_{n:\phi(n)\leq \deg(P_2)} \phi(n) \operatorname{ord}_{T=\zeta_n/q} P_2(T),$$

where ζ_n denotes any one primitive n-th root of unity. For computational purposes, we need an explicit bound on n; here is an easy such bound.

Lemma 1.4.2. *For any positive integer n, we have*

$$\phi(n) \geq \frac{n}{\lfloor \log_2(n) \rfloor + 1}.$$

Proof. We have

$$\frac{\phi(n)}{n} = \prod_p \left(1 - \frac{1}{p}\right),$$

the product running over the distinct prime divisors of n. There are at most $\lfloor \log_2(n) \rfloor$ such divisors, so

$$\frac{\phi(n)}{n} \geq \prod_{i=2}^{\lfloor \log_2(n) \rfloor + 1} \left(1 - \frac{1}{i}\right) = \frac{1}{\lfloor \log_2(n) \rfloor + 1},$$

as desired. □

Here is a standard parity consideration that arises in the context of Tate's conjecture.

Remark 1.4.3. Note that the right side of (1.4.1.2) has the same parity as $\operatorname{ord}_{T=1/q} P_2(T) + \operatorname{ord}_{T=-1/q} P_2(T)$. This in turn has the same parity as $\deg(P_2)$, since $\pm 1/q$ are the only real roots consistent with the restriction that each root has absolute value $1/q$. Under Tate's conjecture, equality would hold in (1.4.1.2), and would thus imply that if X is a smooth proper variety for which $\deg(P_2)$ is even, then the geometric Picard number of X is at least 2.

1.5 Weil cohomologies

Definition 1.5.1. Fix a finite field $\mathbb{F}_q$ of characteristic p, and let K be a field of characteristic zero. By a *(weak) Weil cohomology* over K, we will mean the following data.

- One must specify a collection of contravariant functors from smooth proper varieties X over $\mathbb{F}_q$ to finite dimensional K-vector spaces $H^i(X)$ equipped with endomorphisms F_i, such that

  $$P_i(T) = \det(1 - TF_i, H^i(X)) \qquad (i = 0, \ldots, 2\dim(X)).$$

  For $m \in \mathbb{Z}$, we write $H^i(X)(m)$ to mean the vector space $H^i(X)$ equipped with the endomorphism $q^{-m}F_i$.

- One must specify functorial, F-equivariant maps (for $d = \dim(X)$)

$$\mathrm{trace}_X : H^{2d}(X)(d) \to K$$

(where F acts as the identity on K) which should be isomorphisms when X is geometrically irreducible.

- One must specify associative, functorial, F-equivariant cup product pairings $\cup : H^i(X) \times H^j(X) \to H^{i+j}(X)$ such that (for $d = \dim(X)$) the pairings

$$H^i(X) \times H^{2d-i}(X)(d) \stackrel{\cup}{\to} H^{2d}(X)(d) \stackrel{\mathrm{trace}_X}{\to} K$$

are perfect (Poincaré duality).

- One must specify an injective K-linear homomorphism

$$\mathrm{NS}(X) \otimes_{\mathbb{Z}} K \to H^2(X)(1)^{F=1}$$

(the cycle class map).

For a more precise definition of the phrase "Weil cohomology" (which actually includes more structure than this, including a Künneth decomposition, cycle class maps for higher Chow groups, and a full Lefschetz hyperplane theorem, plus additional compatibilities), see [26].

Remark 1.5.2. By virtue of the cycle class map, the existence of a Weil cohomology yields the inequality (1.4.1.1), as the right side of (1.4.1.1) equals the dimension of the generalized eigenspace of $H^2(X)$ with eigenvalue q. In practice, we will use the resulting slightly stronger version of (1.4.1.1):

$$\mathrm{rank}\,\mathrm{NS}(X) \leq \mathrm{corank}(F_2 - q, H^2(X)) \tag{1.5.2.1}$$

and the corresponding version of (1.4.1.2):

$$\mathrm{rank}\,\mathrm{NS}(X \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}) \leq \sum_{n:\phi(n)\leq \deg(P_2)} \phi(n)\,\mathrm{corank}(F_2 - \zeta_n q, H^2(X)). \tag{1.5.2.2}$$

In theory, one expects that F_2 acts semisimply on $H^2(X)$; this would follow from the full conjecture of Tate, which is somewhat stronger than we have described here (as it makes predictions about $H^{2i}(X)$ for all i).

Remark 1.5.3. At the time [41] was written, the only Weil cohomologies that had been constructed were the ℓ-adic étale cohomologies for each $\ell \neq p$, which take values in $\mathbb{Q}_\ell$. Subsequently, it was shown that Berthelot's rigid cohomology is also a Weil cohomology; it takes values in the p-adic field $\mathbb{Q}_q$. (Here and throughout, for brevity we write $\mathbb{Z}_q$ for $W(\mathbb{F}_q)$ and $\mathbb{Q}_q$ for $\mathrm{Frac}\,\mathbb{Z}_q$.) For the essential properties of rigid cohomology, see [3, 4]; also see [22] for additional context on p-adic cohomology theories.

1.6 Approximate Gaussian elimination

Let us set some notation for this section.

Notation 1.6.1. Fix a finite field $\mathbb{F}_q$, and let K be a complete discretely valued field of characteristic zero and residual characteristic ℓ, which for now may or may not equal the characteristic of $\mathbb{F}_q$. Let $\mathfrak{o}_K$ be the ring of integers of K, fix a uniformizer π of $\mathfrak{o}_K$, and write $v(x)$ for the valuation of $x \in K$.

We are going to describe an algorithm for producing an upper bound on the corank of a matrix A over K, given only the information of the entries of A modulo π^m for some integer m. There is no harm in rescaling the matrix A (by multiplying by an appropriate power π^n of π, then replacing m by $m+n$) to ensure that A has entries in $\mathfrak{o}_K$.

Algorithm 1.6.2. *Given a matrix $\overline{A}$ with entries in $\mathfrak{o}_K/\pi^m\mathfrak{o}_K$ which is the reduction of a matrix A over $\mathfrak{o}_K$, the following algorithm returns an upper bound on* $\mathrm{corank}(A)$.

1. *Let r be the number of rows of $\overline{A}$, and let s be the number of columns of $\overline{A}$. If $\overline{A}$ has no nonzero entries (possibly because $\overline{A}$ is an empty matrix), return s and STOP.*
2. *Choose a nonzero entry $\overline{A}_{ij}$ of minimum valuation.*
3. *For $k = 1, \dots, r$ in succession, skipping over $k = i$, choose $c \in \mathfrak{o}_K/\pi^n\mathfrak{o}_K$ such that $c\overline{A}_{ij} = \overline{A}_{kj}$, and subtract c times the i-th row of $\overline{A}$ from the k-th row of $\overline{A}$.*
4. *For $\ell = 1, \dots, s$ in succession, skipping over $\ell = j$, choose $c \in \mathfrak{o}_K/\pi^n\mathfrak{o}_K$ such that $c\overline{A}_{ij} = \overline{A}_{i\ell}$, and subtract c times the j-th column of $\overline{A}$ from the ℓ-th column of $\overline{A}$.*
5. *Delete row i and column j from $\overline{A}$, then go to step 1.*

Proof. We prove the claim by induction on the number of rows plus columns of A. If $\overline{A}$ is the zero matrix, the claim is evident. Otherwise, we may assume without loss of generality that $i = j = 1$. By lifting each of the row and column operations from $\overline{A}$ to A appropriately, we may also assume that $A_{i1} = 0$ for $i = 2, \dots, m$ and that $A_{1j} = 0$ for $j = 2, \dots, n$. It is now clear that the corank of A is equal to that of its lower right $(m-1) \times (n-1)$ submatrix. □

One can also use Algorithm 1.6.2 to obtain information about the determinant of A.

Proposition 1.6.3. *Given an $n \times n$ matrix $\overline{A}$ with entries in $\mathfrak{o}_K/\pi^m\mathfrak{o}_K$ which is the reduction of a matrix A over $\mathfrak{o}_K$, suppose that Algorithm 1.6.2 returns the bound 0. For $h = 1, \dots, n$, with notation as in the h-th iteration of the algorithm, put $\overline{a_h} = \overline{A}_{ij} \in \mathfrak{o}_K/\pi^m\mathfrak{o}_K$ and $e_h = (-1)^{i+j} \in \mathfrak{o}_K$. Choose lifts $a_1, \dots, a_n$ of $\overline{a_1}, \dots, \overline{a_n}$ to A. Then*

$$v(\det(A) - a_1 e_1 \cdots a_n e_n) \geq \min_i \{m - v(a_i)\} + \sum_{i=1}^{n} v(a_i).$$

Proof. Perform the "shadow" computation of the proof of Algorithm 1.6.2 with the following change: at each step, instead of deleting row i and column j, move them to the far bottom and right. The final matrix has determinant $e_1 \cdots e_n \det(A)$; on the other hand, it is diagonal with entries congruent to $a_1, \dots, a_n$ modulo π^m. The desired estimate is now evident. □

Remark 1.6.4. Note that Proposition 1.6.3 may be used to obtain approximate characteristic polynomials, by applying it with the field K replaced by the completion of $K(t)$ for the Gauss valuation (i.e., the valuation which on a polynomial returns the minimum valuation of any coefficient) and approximating $\det(tI - A)$. If one knows that the matrix A is "nearly" divisible by some π^i, then one may obtain better information by approximating $\det(\pi^i tI - A)$; this often happens in the setting of p-adic cohomology. For example, suppose X is a smooth proper variety over $\mathbb{Z}_q$, where q is a power of a prime $p < \dim(X_{\mathbb{F}_q})$. Then if one writes down the Frobenius matrix on the j-th rigid cohomology with respect to an appropriate basis (namely, a basis of crystalline cohomology modulo torsion), the Hodge numbers

$$h^{i,j-i} = \dim_{\mathbb{Q}_q} H^{j-i}(X_{\mathbb{Q}_q}, \Omega^i_{X/\mathbb{Q}_q}) \qquad (i = 0, \dots, j)$$

give the multiplicities of p^i as elementary divisors of the matrix. See [22, Theorem 1.3.9] for a more general statement.

Remark 1.6.5. It may be possible to obtain even better bounds on characteristic polynomials which are more adaptive (i.e., give individual bounds for each coefficient) by using more careful linear algebra plus p-adic floating point arithmetic. In particular, it would be interesting to give such bounds for the more general setting where the accuracy may vary from entry to entry; in our application to bounding Picard numbers, being able to work in this generality might lend some flexibility to the cohomological calculation. We will not consider the more general setting here.

2 A little p-adic cohomology

In this part, we set up a bit of the theory of p-adic cohomology for use later on; this involves some consideration of algebraic de Rham cohomology. Some of the calculations, particularly Theorem 2.2.5, may be of independent interest.

2.1 A homological calculation

We start with a brief excursion into homological algebra, following [10, Chapter 17].

Definition 2.1.1. Let R be a ring and choose $x = (x_1, \dots, x_n) \in R^n$. The *Koszul complex* $K(x)$ is the exterior algebra $\wedge^*_R(R^n)$ with differentials

$$d_x(z) = x \wedge z.$$

Let $K'(x)$ denote the dual complex, whose underlying R-module we also identify with $\wedge^*_R(R^n)$; let ∂_x denote the differentials in $K'(x)$.

Lemma 2.1.2. *Let R be a ring. For any $x, y \in R^n$ and any $z \in \wedge_R^*(R^n)$,*

$$(d_x\partial_y + \partial_y d_x)(z) = (x_1y_1 + \cdots + x_ny_n)z.$$

Proof. An easy calculation: see [10, Lemma 17.13]. □

Proposition 2.1.3. *Let R be a ring generated over $\mathbb{Z}$ by elements $x_1, \ldots, x_n$. Let C be a complex of R-modules (with R-linear differentials). Then the homology of the product complex $K(x) \otimes C$ is annihilated by any element of the ideal $(x_1, \ldots, x_n)$.*

Proof. Given $r \in (x_1, \ldots, x_n)$, choose $y_1, \ldots, y_n \in R$ such that $x_1y_1 + \cdots + x_ny_n = r$. Then Lemma 2.1.2 shows that multiplication by r is homotopic to zero on $K(x)$, with the homotopy given by ∂_y. Tensoring that homotopy with the identity map on C yields the same assertion on $K(x) \otimes C$, proving the claim. □

2.2 Algebraic de Rham cohomology

Algebraic de Rham cohomology is usually considered over a field of characteristic zero, but for p-adic cohomological calculations, we also need to work with it over arithmetically interesting base schemes.

Definition 2.2.1. By a *smooth pair* (resp. *smooth proper pair*) of relative dimension n over a scheme S, we mean a pair (X, Z) in which X is a smooth (resp. smooth proper) S-scheme of relative dimension n, and Z is a relative reduced normal crossings divisor on X. That is (in the smooth-only case), étale locally on X, we can find an S-isomorphism of X with a Zariski open subset of $\mathbb{A}^n_S$ under which Z is carried to an open subset of a union of some (or all, or none) of the coordinate hyperplanes. We think of Z as defining a logarithmic structure on X in the sense of Kato [23], and write (X, Z) also for the resulting log scheme. If $Z = \emptyset$, we abbreviate (X, Z) to simply X.

Definition 2.2.2. Let (X, Z) be a smooth pair of relative dimension n over a scheme S. Let $\Omega_{(X,Z)/S}$ be the sheaf of differentials on X with logarithmic singularities along Z, relative to S; then $\Omega_{(X,Z)/S}$ is a locally free coherent $\mathcal{O}_X$-module of rank n. Put $\Omega^i_{(X,Z)/S} = \wedge^i_{\mathcal{O}_X}\Omega_{(X,Z)/S}$; then exterior differentiation induces maps $d_i : \Omega^i_{(X,Z)/S} \to \Omega^{i+1}_{(X,Z)/S}$ such that $d_{i+1} \circ d_i = 0$. The resulting complex is called the *de Rham complex* of (X, Z) over S, and its j-th hypercohomology

$$H^j_{\mathrm{dR}}((X, Z)/S) = \mathbb{H}^j(X, \Omega_{(X,Z)/S})$$

is called the j-th *algebraic de Rham cohomology* group of (X, Z) over S.

Remark 2.2.3. Since the Ω^i are quasi-coherent, we may calculate algebraic de Rham cohomology on the étale site instead of the Zariski site [34, Proposition 3.7]. This allows us to use étale localization arguments.

Let (X, Z) be a smooth pair over $\mathbb{C}$, and put $U = X \setminus Z$; one then has an isomorphism

$$H^j_{\mathrm{dR}}((X, Z)/\mathbb{C}) \cong H^j_{\mathrm{dR}}(U). \tag{2.2.3.1}$$

Namely, by Serre's GAGA theorem [39] on the left side and Grothendieck's comparison theorem [18] on the right side (which also uses GAGA, together with resolution of singularities), this may be checked for *analytic* de Rham cohomology, where it amounts to the Poincaré lemma (see [9] for variations on this theme).

However, it was pointed out to us by Johan de Jong that one can also establish (2.2.3.1) algebraically, using étale localization. In so doing, one can also prove an integral variant where one compares cohomology of the complex of differentials with logarithmic poles with the complex of differentials where the poles are made somewhat worse. Here is the result; in its relevance to computing p-adic cohomology, it should be viewed as a generalization of [24, Lemma 2].

Definition 2.2.4. Let (X, Z) be a smooth pair over a scheme S, and put $U = X \setminus Z$. For m a nonnegative integer, write (as usual) $\Omega^j_{(X,Z)/S}(mZ)$ for the twist $\Omega^j_{(X,Z)/S} \otimes_{\mathcal{O}_X} \mathcal{O}_X(mZ)$; note that $\Omega^j_{U/S}$ is the direct limit of the $\Omega^j_{(X,Z)/S}(mZ)$ as m increases.

Theorem 2.2.5. *Let (X, Z) be a smooth pair over a scheme S. For each nonnegative integer m, the cokernels of the maps on cohomology sheaves induced by the natural map of complexes of sheaves*

$$\Omega^{\cdot}_{(X,Z)/S} \to \Omega^{\cdot}_{(X,Z)/S}(mZ)$$

on the small étale site of X are killed by $\mathrm{lcm}(1, \dots, m)$.

Proof. The claim may be verified stalkwise on S, so we may assume $S = \operatorname{Spec} A$ is affine and local. The claim may also be verified étale locally on X; it only bears content in a neighborhood of a point on Z. Starting with such a point lying on h different components of Z, we may perform an étale localization to reduce to the case where $X = \operatorname{Spec} R$ is Zariski open in $\mathbb{A}^n_S = \operatorname{Spec} A[x_1, \dots, x_n]$, $Z = V(x_1 \cdots x_h)$, and our chosen point lies on $V(x_1, \dots, x_h)$. For each $T \subseteq \{1, \dots, h\}$, let I_T be the ideal generated by x_i for each $i \in T$, and put $R_T = R/I_T$. By a further Zariski localization, we may also assume that R contains a copy of each R_T.

Define

$$\tilde{d}x_i = \begin{cases} \frac{dx_i}{x_i} & 1 \leq i \leq h \\ dx_i & i > h \end{cases} \qquad \tilde{\partial}_i = \begin{cases} x_i \frac{\partial}{\partial x_i} & 1 \leq i \leq h \\ \frac{\partial}{\partial x_i} & i > h. \end{cases}$$

For each subset $U = \{i_1, \dots, i_r\}$ of $\{1, \dots, n\}$ with $i_1 < \cdots < i_r$, put

$$\tilde{d}x_U = \tilde{d}x_{i_1} \wedge \cdots \wedge \tilde{d}x_{i_r}.$$

Let M be the set of monomials $x_1^{j_1} \cdots x_h^{j_h}$ with $j_1, \dots, j_h \in \{0, \dots, m\}$, viewed as a partially ordered set under divisibility. For D a nonempty down-closed subset of M (i.e.,

one in which inclusion of μ implies inclusion of any divisor of μ, so that in particular $1 \in D$), define

$$Q_D = \bigcup_{\mu \in D} \mu^{-1} R;$$

note that each $\tilde{\partial}_i$ sends Q_D into itself.

Let D be a down-closed subset of M strictly bigger than $\{1\}$. Choose $\mu = x_1^{j_1} \cdots x_h^{j_h}$ maximal in D; then $D' = D \setminus \{\mu\}$ is also down-closed. Let T be the set of $i \in \{1, \dots, h\}$ for which $j_i \neq 0$, which is necessarily nonempty since we cannot have $\mu = 1$; then we have an isomorphism of additive groups

$$Q_D / Q_{D'} \cong \mu^{-1} R_T.$$

Note that this isomorphism is equivariant for the action of each $\tilde{\partial}_i$; in particular, for each $i \in T$, $\tilde{\partial}_i$ acts on the right side by multiplication by $-j_i$. If we use these to form a de Rham complex, the result is the tensor product over $\mathbb{Z}$ of the Koszul complex $\mathbb{Z}(j_i : i \in T)$ with another complex; its cohomology is thus killed by $\gcd(j_i : i \in T)$ by Proposition 2.1.3.

Now suppose $\omega \in Q_D \otimes_R \Omega^r_{(X,Z)/S}$ satisfies $d\omega = 0$. Write $\omega = \sum_U g_U \tilde{dx}_U$, where U runs over r-element subsets of $\{1, \dots, n\}$. Let $h_U \in \mu^{-1} R_T$ be the image of g_U under the map $Q_D / Q_{D'} \to \mu^{-1} R_T$; then $d(\sum_U h_U \tilde{dx}_U) = 0$ as well. By the previous paragraph, $\sum_U h_U \tilde{dx}_U$ times $\gcd(j_i : i \in T)$ is a coboundary. Since $1 \leq \gcd(j_1 : i \in T) \leq m$, ω is thus equal to a differential whose image in the cokernel of the map on cohomology is killed by $\mathrm{lcm}(1, \dots, m)$ plus an exact differential in $Q_{D'} \otimes_R \Omega^r_{(X,Z)/S}$. This yields the claim by induction on the cardinality of D. □

Corollary 2.2.6. *Let (X, Z) be a smooth pair over a field K of characteristic 0, and put $U = X \setminus Z$. Then for each i, the map $H^i_{\mathrm{dR}}((X, Z)/K) \to H^i_{\mathrm{dR}}(U/K)$ is an isomorphism of K-vector spaces.*

Proof. Apply Theorem 2.2.5 and note that formation of cohomology commutes with direct limits. □

Remark 2.2.7. Note that if Z is smooth, then the proof of Theorem 2.2.5 actually gives something slightly stronger: any exact r-form with poles of order $m+1$ can locally be written as an exact logarithmic r-form plus a form which when multiplied by $\mathrm{lcm}(1, \dots, m)$ becomes the differential of an $(r-1)$-form with poles of order $\leq m$. This is crucial for our application: see Proposition 3.4.6.

Proposition 2.2.8. *Let (X, Z) be a smooth pair over a scheme S, with Z also smooth; let j denote the inclusion $Z \hookrightarrow X$. Then there is an exact sequence of complexes of coherent sheaves on X:*

$$0 \to \Omega^{\cdot}_{X/S} \to \Omega^{\cdot}_{(X,Z)/S} \xrightarrow{\mathrm{Res}} j_* \Omega^{\cdot}_{Z/S}[+1] \to 0,$$

yielding an exact sequence in cohomology

$$\cdots \to H^i_{\mathrm{dR}}(X/S) \to H^i_{\mathrm{dR}}((X, Z)/S) \to H^{i-1}_{\mathrm{dR}}(Z/S) \to H^{i+1}_{\mathrm{dR}}(X/S) \to \cdots.$$

Proof. In an étale neighborhood where X looks like an open subscheme of $\operatorname{Spec} \mathbb{A}^n_S$, we can choose coordinates so that $Z = V(x_n)$. Then locally each section of the quotient $\Omega^r_{(X,Z)/S}/\Omega^r_{(X,Z)/S}$ admits a representative of the form $dx_n/x_n \wedge \omega$ for some ω, and the residue map carries this section to the reduction of ω modulo x_n. To see that this is well-defined globally, we must simply observe that the map is not changed by changing the choice of the parameter x_n: if u is a unit on X, then $d(x_n u)/(x_n u) = dx_n/x_n + du/u$, so $dx_n/x_n \wedge \omega$ and $d(x_n u)/(x_n u) \wedge \omega$ represent the same element of the quotient. □

2.3 p-adic cohomology in general

We suggest [22] as a useful survey for the material underlying this section.

Notation 2.3.1. Throughout this section, let k be a perfect field of characteristic p, and write K for $\operatorname{Frac} W(k)$ and $\mathfrak{o}_K$ for $W(k)$. Let $\sigma : \mathfrak{o}_K \to \mathfrak{o}_K$ denote the Witt vector Frobenius, which is the unique lift to $\mathfrak{o}_K$ of the absolute Frobenius on k.

Definition 2.3.2. Let (X, Z) be a smooth proper pair over k. Let $H^i_{\mathrm{crys}}(X, Z)$ denote the i-th *(log-)crystalline cohomology* of (X, Z); this is a $\mathfrak{o}_K$-module whose construction is contravariantly functorial in the pair (X, Z). Moreover, the absolute Frobenius on k acts σ-semilinearly on $H^i_{\mathrm{crys}}(X, Z)$. For the general construction, see for instance [40, Chapter 2].

To make the Frobenius action on de Rham cohomology explicit, we need to pass to rigid cohomology, so we can use the Monsky-Washnitzer interpretation of p-adic cohomology.

Definition 2.3.3. Let X be a smooth k-scheme. Let $H^i_{\mathrm{rig}}(X)$ denote the i-th *rigid cohomology* of X in the sense of Berthelot [3]; it is a finite-dimensional K-vector space whose construction is contravariantly functorial in the k-scheme X. Moreover, the absolute Frobenius on k acts σ-semilinearly on $H^i_{\mathrm{crys}}(X, Z)$. For X proper, Berthelot [3, Proposition 1.9] constructs a functorial isomorphism

$$H^i_{\mathrm{crys}}(X) \otimes_{\mathfrak{o}_K} K \cong H^i_{\mathrm{rig}}(X).$$

For (X, Z) a smooth pair over k, Shiho [40, §2.4] (using crucially a result of Baldassarri and Chiarellotto [2]) constructs a functorial, Frobenius-equivariant isomorphism

$$H^i_{\mathrm{crys}}(X, Z) \otimes_{\mathfrak{o}_K} K \cong H^i_{\mathrm{rig}}(X \setminus Z).$$

2.4 p-adic cohomology in the liftable case

When things can be lifted nicely to characteristic zero, the construction of p-adic cohomology becomes much simpler.

Proposition 2.4.1. *Let $(\mathfrak{X}, \mathfrak{Z})$ be a smooth proper pair over $\mathfrak{o}_K$. Put $X = \mathfrak{X}_k$, $Z = \mathfrak{Z}_k$, and $U = X \setminus Z$.*

(a) There are isomorphisms

$$H^i_{\mathrm{crys}}(X, Z) \cong H^i_{\mathrm{dR}}((\mathfrak{X}, \mathfrak{Z})/\mathfrak{o}_K)$$

which are functorial in smooth pairs over $\mathfrak{o}_K$. In particular, the right side inherits an action of Frobenius.

(b) Suppose that $\mathfrak{Z}$ is also smooth, and use Proposition 2.2.8 and (a) to obtain an exact sequence

$$\cdots \to H^i_{\mathrm{rig}}(X) \to H^i_{\mathrm{rig}}(U) \to H^{i-1}_{\mathrm{rig}}(Z) \to H^{i+1}_{\mathrm{rig}}(X) \to \cdots.$$

These maps are then Frobenius-equivariant for the following twists:

$$\begin{aligned} H^i_{\mathrm{rig}}(X) &\to H^i_{\mathrm{rig}}(U) \\ H^i_{\mathrm{rig}}(U) &\to H^{i-1}_{\mathrm{rig}}(Z)(-1) \\ H^{i-1}_{\mathrm{rig}}(Z) &\to H^{i+1}_{\mathrm{rig}}(X)(1), \end{aligned}$$

where again $M(n)$ denotes M with its absolute Frobenius action multiplied by p^{-n}.

Proof. For (a), see [23, Theorem 6.4]. For (b), we may invoke rigid analytic GAGA to argue that algebraic de Rham cohomology of a proper smooth pair over K with X proper coincides with rigid analytic de Rham cohomology of the analytification. The Frobenius equivariance may now be checked at the level of complexes by following the construction of the Gysin isomorphism in rigid cohomology [3, §5], [43]. □

One also has a nice description of the Frobenius action on the rigid cohomology of a smooth affine scheme in terms of a lifting.

Definition 2.4.2. Let X be a smooth affine k-scheme, suppose $\mathfrak{X}$ is a smooth affine $\mathfrak{o}_K$-scheme lifting X, write $\mathfrak{X} = \operatorname{Spec} A$, and choose a presentation $A \cong \mathfrak{o}_K[x_1, \dots, x_n]/I$. Let $\mathfrak{o}_K\langle x_1, \dots, x_n\rangle^\dagger$ be the ring of power series in $\mathfrak{o}_K[\![x_1, \dots, x_n]\!]$ which converge on some polydisc of radius greater than 1, and put

$$A^\dagger = \mathfrak{o}_K\langle x_1, \dots, x_n\rangle^\dagger / I\mathfrak{o}_K\langle x_1, \dots, x_n\rangle^\dagger.$$

Then Berthelot [3, Proposition 1.10] constructs an isomorphism between $H^i_{\mathrm{rig}}(X)$ and the cohomology of the complex

$$\Omega^\cdot_{A/\mathfrak{o}_K} \otimes_A A^\dagger \otimes_{\mathfrak{o}_K} K;$$

the latter is the complex computing Monsky-Washnitzer's "formal cohomology" [44]. Moreover, if $F : A^\dagger \to A^\dagger$ is any ring homomorphism extending σ on $\mathfrak{o}_K$ and lifting the absolute Frobenius, then pullback by F induces the Frobenius action on rigid cohomology.

Remark 2.4.3. For example, one can compute from the above description that the q-power Frobenius action on $H^{2i}_{\mathrm{rig}}(\mathbb{P}^n_{\mathbb{F}_q})$ consists of multiplication by q^i. This also follows from the fact that the cohomology of projective space is generated by cycle clasess.

3 The case of smooth hypersurfaces

From the first part of this paper, we obtain a procedure for bounding from above the Picard number and the geometric Picard number of a smooth proper variety X over a finite field $\mathbb{F}_q$: compute an approximation modulo p^m, for some m, to the matrix via which Frobenius acts on the rigid cohomology space $H^2(X)$ over $\mathbb{Q}_q$ (i.e., a "higher Cartier matrix"), then use Algorithm 1.6.2 to bound the right-hand side of (1.5.2.1) or (1.5.2.2), respectively. What remains to be done, for any particular class of varieties, is to describe how to compute the approximate Frobenius matrix for varieties in that class, by realizing the constructions described in the second part of the paper. Here, we describe one such procedure for smooth hypersurfaces in a projective space, based on work of Griffiths [15], and give a few details of an implementation of this procedure which we have constructed. We also mention some alternate approaches that we have not (yet) experimented with.

It is worth noting that much of what is described below generalizes relatively easily to smooth hypersurfaces, or even smooth complete intersections, in toric varieties. We have restricted to hypersurfaces in projective space, and ultimately to surfaces in $\mathbb{P}^3$, for simplicity of exposition and because that is all that we have attempted to implement so far.

3.1 A calculation on projective space

We pause for a brief excursion into the cohomology of sheaves of differentials on projective space.

Lemma 3.1.1. *Let S be a scheme. For any positive integer n, there is an exact sequence of sheaves on $X = \mathbb{P}^n_S$:*

$$0 \to \Omega^1_{X/S} \to \mathcal{O}_X(-1)^{n+1} \to \mathcal{O}_X \to 0.$$

Proof. A standard calculation: see [19, Theorem II.8.13]. □

The following is due to Bott [6] over $\mathbb{C}$ (and can be deduced over any field of characteristic zero); we were unable to find a reference for the general version, so we include the easy calculation. One might like to think of it as a special case of the Kodaira-Nakano vanishing theorem, but the latter is not valid over a general base; Raynaud [37] exhibited a counterexample over a field of positive characteristic.

Proposition 3.1.2. *Let $S = \operatorname{Spec} A$ be an affine scheme. For n a positive integer, put $X = \mathbb{P}^n_S$. Let k, p, q be integers with $0 \leq p, q \leq n$. Then $H^p(X, \Omega^q_{X/S}(k)) = 0$ unless one of the following conditions holds:*

(a) $p = q$ and $k = 0$, in which case $H^p(X, \Omega^p_{X/S}(k))$ is free of rank 1 over A;

(b) $p = 0$ and $k > q$;

(c) $p = n$ and $k < q - n$.

Proof. We will use without comment Serre's calculation of the cohomology of $\mathcal{O}_X(k)$, in the form of the statement of the lemma in all cases where $q = 0$; for this, see [19, Theorem III.5.1] (and suppress the superfluous noetherian hypothesis) or [17, Proposition 2.1.12].

Take the q-th exterior power of the exact sequence in Lemma 3.1.1, then twist by k, to obtain

$$0 \to \Omega^q_{X/S}(k) \to \left(\wedge^q(\mathcal{O}_X(-1)^{n+1})\right)(k) \to \Omega^{q-1}_{X/S}(k) \to 0,$$

which we may rewrite as

$$0 \to \Omega^q_{X/S}(k) \to \mathcal{O}_X(-q+k)^{\binom{n+1}{q}} \to \Omega^{q-1}_{X/S}(k) \to 0. \tag{3.1.2.1}$$

We now proceed by inspecting various parts of the long exact sequence in cohomology of (3.1.2.1), such as

$$H^{p-1}(X, \mathcal{O}_X(-q+k))^{\binom{n+1}{q}} \to H^{p-1}(X, \Omega^{q-1}_{X/S}(k)) \to H^p(X, \Omega^q_{X/S}(k)) \to H^p(X, \mathcal{O}_X(-q+k))^{\binom{n+1}{q}}. \tag{3.1.2.2}$$

In case $k < q-p$ and $0 \leq p < n$, then the outside terms of (3.1.2.2) vanish, so $H^{p-1}(X, \Omega^{q-1}_{X/S}(k))$ and $H^p(X, \Omega^q_{X/S}(k))$ are isomorphic. We obtain the vanishing of $H^p(X, \Omega^q_{X/S}(k))$ in this case by successively decreasing both p and q until the step when at least one of them goes negative, at which moment the correct formal interpretation of (3.1.2.2) yields the desired vanishing. Similarly, in case $k > q - p$ and $0 < p \leq n$, we obtain vanishing of $H^p(X, \Omega^q_{X/S}(k))$ by successively increasing both p and q until the step when at least one of them exceeds n.

In case $k = q - p$, the outside terms of (3.1.2.2) still vanish as long as $1 \leq p \leq n$. If $k \neq 0$, then successively decreasing p and q still eventually manages to send one of them below zero, so we get the desired vanishing. If $k = 0$, we instead hit $H^0(X, \mathcal{O}_X)$ which is free of rank 1. This plus Serre's calculation yields all the desired results. □

Corollary 3.1.3. *Let $S = \operatorname{Spec} A$ be an affine scheme, let n be a positive integer, and put $X = \mathbb{P}^n_S$. Let k be a nonnegative integer, let Z be a smooth hypersurface in X, and define the complex $C^p = \Omega^p_{X/S}((k+p)Z)$ with the evident differentials d. Then the hypercohomology of $C^\cdot$ coincides with the homology of the complex $H^0(X, C^\cdot)$. In particular,*

$$\mathbb{H}^n(X, C^\cdot) = H^0(X, C^n)/dH^0(X, C^{n-1}).$$

Proof. We compute $\mathbb{H}^n(X, C^\cdot)$ using a spectral sequence with $E_1^{pq} = H^q(X, C^p)$. By Proposition 3.1.2 and the fact that $C^p \cong \Omega^p_{X/S}((k+p)\deg(Z))$, we have $E_1^{pq} = 0$ for $q > 0$. Hence the sequence degenerates at E_2 and yields the claim. □

Corollary 3.1.4. *For any affine scheme $S = \operatorname{Spec} A$,*

$$H^i_{\mathrm{dR}}(\mathbb{P}^n_S) \cong \begin{cases} A & i = 0, 2, \ldots, 2n \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Proposition 3.1.2, $H^p(\mathbb{P}^n_S, \Omega^q_{\mathbb{P}^n_S/S})$ is free of rank 1 over A if $p = q \in \{0, \ldots, n\}$ and is otherwise zero. Hence the spectral sequence computing hypercohomology degenerates at E_1, yielding the desired result. □

3.2 Cohomology of smooth hypersurfaces (after Griffiths)

The middle cohomology of a smooth hypersurface in a projective space was described by Griffiths [15] using mostly analytic arguments (i.e., working over $\mathbb{C}$ and invoking GAGA). One can reconstruct these results algebraically; we will not do so explicitly, but we will use algebraic techniques later to extract arithmetic information.

Notation 3.2.1. Throughout this section, let K be a field of characteristic zero, put $X = \mathbb{P}^n_K$, let Z be a smooth hypersurface of degree d in X, defined by the homogeneous polynomial $P \in K[x_0, \dots, x_n]$, and put $U = X \setminus Z$. By the Lefschetz hyperplane theorem, the map $H^i_{\mathrm{dR}}(X/K) \to H^i_{\mathrm{dR}}(Z/K)$ induced by the inclusion $Z \hookrightarrow X$ is bijective for $i \leq n-2$ and injective for $i = n-1$. By Corollary 3.1.4 and Poincaré duality, we thus conclude that for $0 \leq i \leq 2n-2$ with $i \neq n-1$, we have

$$\dim_K H^i_{\mathrm{dR}}(Z/K) = \begin{cases} 1 & i \text{ even} \\ 0 & i \text{ odd.} \end{cases}$$

In particular, the only cohomology group of Z requiring further inspection is the middle cohomology $H^{n-1}_{\mathrm{dR}}(Z/K)$.

The following result lets us shift attention from Z to the ambient projective space X, where it is easier to make calculations. Remember that $H^n_{\mathrm{dR}}((X,Z)/K) \cong H^n_{\mathrm{dR}}(U/K)$ by Corollary 2.2.6.

Proposition 3.2.2. *The exact sequence of Proposition 2.2.8 induces exact sequences as follows: if n is even, then*

$$0 \to H^n_{\mathrm{dR}}(U/K) \to H^{n-1}_{\mathrm{dR}}(Z/K) \to 0$$

is exact; if n is odd, then

$$0 \to H^n_{\mathrm{dR}}(U/K) \to H^{n-1}_{\mathrm{dR}}(Z/K) \to H^{n+1}_{\mathrm{dR}}(X/K) \to 0$$

is exact.

Proof. See [15, (10.16)]. □

Definition 3.2.3. Put

$$\Omega = \sum_{i=0}^{n} (-1)^i x_i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_n,$$

where the hat denotes omission. One then calculates as in [15, §4] that $H^n_{\mathrm{dR}}((X,Z)/K)$ is isomorphic to the quotient of the group of n-forms $A\Omega/P^m$, where m is a positive integer and $A \in K[x_0, \dots, x_n]$ is homogeneous of degree $md - n - 1$, by the subgroup generated by

$$\frac{(\partial_i A)\Omega}{P^m} - m\frac{A(\partial_i P)\Omega}{P^{m+1}}$$

for all nonnegative integers m, all $i \in \{0, \dots, n+1\}$, and all homogeneous polynomials $A \in K[x_0, \dots, x_n]$ of degree $md - n$. (Here ∂_i is shorthand for $\frac{\partial}{\partial x_i}$.)

Remark 3.2.4. Note that $H^n_{\mathrm{dR}}(U/K)$ admits a natural filtration whose i-th step consists of those classes represented by forms $A\Omega/P^m$ for some integer $m \leq i+1$. In fact, this filtration is induced by the Hodge filtration on $H^{n-1}_{\mathrm{dR}}(Z/K)$ [15, §10].

Remark 3.2.5. The description in Definition 3.2.3 gives rise to a natural "reduction of poles" procedure for computing in $H^n_{\mathrm{dR}}(U)$, sometimes referred to as the Griffiths-Dwork method. First, one writes down a basis: for $h = 1, \dots, n$, one finds monomials of degree $hd - n - 1$ which generate the quotient of the space of all such monomials by the multiples of $\partial_0 P, \dots, \partial_n P$. Then, to write the class of a given form $A\Omega/P^m$ in terms of these, one uses a Gröbner basis division procedure to write A as a linear combination of $\partial_0 P, \dots, \partial_n P$ (plus basis elements if $m \leq n$), then reduces the pole order. The fact that it is always possible to perform this reduction follows from a theorem of Macaulay [15, §4] or from a sheaf-theoretic reinterpretation [15, §10].

3.3 The p-adic cohomology interpretation

We now use the previous section to describe the p-adic cohomology of a smooth hypersurface in $\mathbb{P}^n_{\mathbb{F}_q}$. Note that while the p-power Frobenius action on rigid cohomology of a variety over $\mathbb{F}_q$ will only be semilinear, the q-power Frobenius action will be linear over $\mathbb{Q}_q$.

We start by setting notation for the rest of the chapter.

Notation 3.3.1. Let Z be a smooth hypersurface of degree d in $X = \mathbb{P}^n_{\mathbb{F}_q}$, for $\mathbb{F}_q$ a finite field of characteristic $p > 0$, defined by the homogeneous polynomial $P(x_0, \dots, x_n) \in \mathbb{F}_q[x_0, \dots, x_n]$. Choose a lift $\mathfrak{P}(x_0, \dots, x_n) \in \mathbb{Z}_q[x_0, \dots, x_n]$ of P to a homogeneous polynomial of the same degree d, let $\mathfrak{Z}$ be the zero locus of $\mathfrak{P}$ in $\mathfrak{X} = \mathbb{P}^n_{\mathbb{Z}_q}$, and put $\mathfrak{U} = \mathfrak{X} \setminus \mathfrak{Z}$. Put $\tilde{X} = \mathfrak{X}_{\mathbb{Q}_q}$, $\tilde{Z} = \mathfrak{Z}_{\mathbb{Q}_q}$, and $\tilde{U} = \mathfrak{U}_{\mathbb{Q}_q}$; also write $\tilde{P}$ for $\mathfrak{P}$ as an element of $\mathbb{Q}_q[x_0, \dots, x_n]$.

By Proposition 2.4.1, we have $H^i_{\mathrm{rig}}(Z) \cong H^i_{\mathrm{dR}}(\tilde{Z}/\mathbb{Q}_q)$, and $H^i_{\mathrm{rig}}(Z) \cong H^i_{\mathrm{rig}}(X)$ for $i \leq n-2$. Adding Poincaré duality, we see that for $0 \leq i \leq 2n-2$ with $i \neq n-1$, if i is odd, then $H^i_{\mathrm{rig}}(Z) = 0$, while if i is even, then $H^i_{\mathrm{rig}}(Z)$ is one-dimensional and the q-power Frobenius acts by multiplication by q. Moreover, by Proposition 3.2.2, we have Frobenius-equivariant exact sequences

$$0 \to H^n_{\mathrm{rig}}(U) \to H^{n-1}_{\mathrm{rig}}(Z)(-1) \to 0$$

if n is even and

$$0 \to H^n_{\mathrm{rig}}(U) \to H^{n-1}_{\mathrm{rig}}(Z)(-1) \to H^{n+1}_{\mathrm{rig}}(X) \to 0$$

if n is odd. That is, $H^n_{\mathrm{rig}}(U)(1)$ coincides with $H^{n-1}_{\mathrm{rig}}(Z)$ except that if n is odd, its generalized eigenspace for Frobenius of eigenvalue $q^{(n-1)/2}$ has dimension one less.

Thanks to Berthelot's comparison theorems (see Definition 2.4.2), we can describe the Frobenius action on $H^n_{\mathrm{rig}}(U)$ as follows.

Definition 3.3.2. Let v denote the Gauss valuations on polynomials over $\mathbb{Q}_q$; that is, $v(\sum c_I x^I) = \min_I\{v_p(c_I)\}$, where v_p denotes the p-adic valuation on $\mathbb{Q}_q$ normalized by $v_p(p) = 1$.

Definition 3.3.3. Let R denote the ring of formal sums $\sum_{i=0}^{\infty} A_i \tilde{P}^{-i}$, where $A_i \in \mathbb{Q}_q[x_0, \dots, x_n]$ is homogeneous of degree di, and

$$\liminf_{i \to \infty} \frac{v(A_i)}{i} > 0.$$

That is, the valuations of the A_i grow linearly in i. Define the ring map $F : R \to R$ by formally setting $F(x_i) = x_i^q$ for $i = 0, \dots, n$, and

$$F(\tilde{P}^{-1}) = \tilde{P}^{-q} \left(1 + p \frac{F(\tilde{P}) - \tilde{P}^q}{p\tilde{P}^q}\right)^{-1},$$

expanding the parenthesized expression as a binomial series. Formally extend F to n-forms by setting

$$F(A\Omega) = F(Ax_0 \cdots x_n) F(x_0^{-1} \cdots x_n^{-1} \Omega),$$

where $F(dx_0/x_0) = q\, dx_0/x_0$ and so forth. As noted in Definition 2.4.2, this ring map induces the q-power Frobenius in rigid cohomology on $H^n_{\mathrm{rig}}(U) \cong H^n_{\mathrm{dR}}((\tilde{X}, \tilde{Z})/\mathbb{Q}_q) \cong H^n_{\mathrm{dR}}(\tilde{U}/\mathbb{Q}_q)$.

3.4 Precision estimates

The plan now is to compute an approximation to the Frobenius action on $H^n_{\mathrm{rig}}(U)$ by applying a truncation of F to a basis of $H^n_{\mathrm{dR}}(\tilde{U})$ and using the "reduction of poles" process (Remark 3.2.5) to put the results back in terms of the basis. To do this, we must produce *effective* bounds on the amount of p-adic precision needed to keep the error introduced by the truncation to a particular amount. One can derive general bounds easily from the theory of p-adic cohomology, but for effective bounds we must work a bit harder. This is analogous to the precision analysis in [24], but the higher-dimensional situation we are in makes things a bit more technical.

Our first order of business is to relate a basis, which is natural from the point of view of reduction of poles, to the integral structure on de Rham cohomology.

Definition 3.4.1. Let H be the image of $H^n_{\mathrm{dR}}((\mathfrak{X}, \mathfrak{Z})/\mathbb{Z}_q)$ in $H^n_{\mathrm{dR}}((\tilde{X}, \tilde{Z})/\mathbb{Q}_q)$; we refer to elements of H as *integral* elements of $H^n_{\mathrm{dR}}((\tilde{X}, \tilde{Z})/\mathbb{Q}_q)$, or of $H^n_{\mathrm{dR}}(\tilde{U}/\mathbb{Q}_q)$, or of $H^n_{\mathrm{rig}}(U)$.

Definition 3.4.2. Let B denote a basis of $H^n_{\mathrm{dR}}(\tilde{U}/\mathbb{Q}_q)$ obtained as follows: for $h = 1, \dots, n$, form the quotient of the space of homogeneous polynomials in $\mathbb{F}_q[x_0, \dots, x_n]$ of degree $hd - n - 1$ by the multiples of $\partial_0 P, \dots, \partial_n P$. Find monomials in $\mathbb{F}_q[x_0, \dots, x_n]$ which project onto a basis of this quotient, then lift these monomials to monomials in $\mathbb{Z}_q[x_0, \dots, x_n]$.

Lemma 3.4.3. *Let V be the $\mathbb{Z}_q$-span of the image of B in $H^n_{\mathrm{dR}}(\tilde{U}/\mathbb{Q}_q)$. Then*

$$H \subseteq V.$$

Proof. Map the complex $\Omega^{\cdot}_{(\mathfrak{X},\mathfrak{Z})/\mathbb{Z}_q}$ into the complex $C^{\cdot}$ with

$$C^i = \Omega^i_{\mathfrak{X}/\mathbb{Z}_q}(i\mathfrak{Z}),$$

then invoke Corollary 3.1.3. □

Remark 3.4.4. In the case $p \geq n$, Lemma 3.4.3 yields $H = V$. In this case, we also know that $H^{n-1}_{\mathrm{dR}}(\mathfrak{Z}/\mathbb{Z}_q)$ is torsion-free because of the degeneration of the Hodge-de Rham spectral sequence. See [22] for further discussion.

We next consider the loss of p-adic precision incurred when one reduces a given differential into standard form.

Definition 3.4.5. For m a positive integer, let $f(m)$ be the smallest integer t with the following property: for each form $\omega = A\Omega/\tilde{P}^m$, we have $p^t\omega \in H$. The following relations are evident (using the relations in cohomology):

$$\begin{aligned} f(1) &= 0 \\ f(m) &\leq f(m+1) \\ f(m) &= f(p\lceil m/p \rceil) \qquad (m \geq n). \end{aligned}$$

Proposition 3.4.6. *For each $m > 0$,*

$$f(m) \leq \sum_{i=1}^{n} \lfloor \log_p \max\{1, m-i\} \rfloor.$$

Proof. Apply Theorem 2.2.5; we get the n terms of the sum by feeding the cohomology sheaves into the spectral sequence computing hypercohomology, keeping in mind Remark 2.2.7. (We don't get an $(n+1)$-st term because the map of Theorem 2.2.5 on zero-th cohomology sheaves is an isomorphism, so those do not contribute.) □

Corollary 3.4.7. *We have $f(m) \leq v_p((m-1)!)$ for all $m \geq 0$. In particular, in the notation of Lemma 3.4.3, we have $(n-1)!V \subseteq H$.*

This bound is asymptotically $n \log_p(m)$, which for our application to surfaces will be a bit too large to be practical. Fortunately we can shave it down a bit.

Definition 3.4.8. For m, i integers with $i \geq 0$, let $g(m,i)$ be the p-adic valuation of $\binom{-m}{i}$. By a standard argument attributed to Kummer, $g(m,i)$ equals the number of carries in the base p addition of i and $-m-i$.

Proposition 3.4.9. *Let m be a positive integer. Put*

$$N = \max_{\ell > 0}\{f((m+\ell)p) - \ell - g(m,\ell)\}.$$

Then

$$f(mp) \leq \max\{N, n-1+f(m)\}.$$

Proof. Given a form $A\Omega/\tilde{P}^{mp}$ with $A \in \mathbb{Z}_q[x_0, \dots, x_n]$, separate the monomials of A depending on the reductions modulo p of their exponents. Let B be the sum of the monomials whose exponents are all congruent to $p-1$ modulo p, and put $C = A - B$. Then $C\Omega/\tilde{P}^{mp}$ is cohomologous to a form $mpD\Omega/\tilde{P}^{mp+1}$ with $D \in \mathbb{Z}_q[x_0, \dots, x_n]$, because

$$\frac{x_i^j \Omega}{\tilde{P}^{mp}} \equiv \frac{mp}{j+1} \frac{x_i^{j+1}(\partial_i \tilde{P})\Omega}{\tilde{P}^{mp+1}}$$

in cohomology. On the other hand, B is equal to an element of the image of $p^{-n}F$ plus a series of the form $\sum_{\ell>0} p^\ell \binom{-m}{\ell} B_\ell \Omega/\tilde{P}^{(m+\ell)p}$. Since $p^{-1}F$ acts on H (by comparison with $H^{n-1}_{\mathrm{dR}}(\mathfrak{Z}/\mathbb{Z}_q)$ via Proposition 2.4.1), this yields the claim. □

Proposition 3.4.9 plus any sublinear bound on f suffices to give an upper bound of the form $(n-1)\log_p(m)$ plus a constant. However, for implementation purposes, it is important to control that additive constant as much as possible; this can be done using an iterative algorithm as follows.

Algorithm 3.4.10. *Define the function*

$$f_0(m) = \sum_{i=1}^{n} \lfloor \log_p \max\{1, m-i\} \rfloor.$$

Given an input positive integer m and an input array A_0 such that $f(j) \leq A_0(j)$ for each j for which $A_0(j)$ exists, the following algorithm, if it terminates, returns an array A of length at least m, such that $f(j) \leq A(j)$ for each j for which $A(j)$ exists, and $A(j) \leq A_0(j)$ for each j for which $A(j)$ and $A_0(j)$ both exist.

1. *Create an array*

$$A(j) = \begin{cases} A_0(j) & A_0(j) \text{ exists} \\ f_0(j) & \text{otherwise} \end{cases} \qquad (j = 1, \dots, \min\{n, m\}).$$

2. *Make a copy A' of A. Put $j = n+1$.*

3. *If $A(j)$ is not defined, check whether A and A' are identical (of the same length). If so, return $A(m)$ and STOP. Otherwise, go to step 2. (If $A(j)$ is defined, continue to step 4.)*

4. *Put $j_1 = p\lceil j/p \rceil$, $N = n - 1 + A(j_1/p)$, and $\ell = 1$.*

5. *If $np < j_1 + \ell p$ and $n\log_p(j_1 + \ell p) - \ell \leq N$, then set*

$$A(j) = A(j+1) = \cdots = A(j_1) = \min\{N, f_0(j_1)\},$$

replace j by $j_1 + 1$, and go to step 3.

6. *If $f_0(j_1 + \ell p) - \ell - g(j_1, \ell) \leq N$, then replace ℓ by $\ell + 1$ and go to step 5.*

7. *Extend A using the formula $A(i) = f_0(i)$ if needed to ensure that $A(j_1 + \ell p)$ exists. Replace N by $\max\{A(j_1 + \ell p) - \ell - g(j_1, \ell), N\}$, replace ℓ by $\ell + 1$, and go to step 5.*

Proof. What we show is that at every stage, whenever some $A(j)$ is defined, we have $f(j) \leq A(j)$. This holds whenever an $A(j)$ is instantiated by Proposition 3.4.6. In step 5, the quantity $n \log_p(j_1 + \ell p) - \ell$ is a decreasing function of ℓ for $np < j_1 + \ell p$; it is also an upper bound for $f(j_1 + \ell p) - \ell - g(j_1, \ell)$ by Proposition 3.4.6 again. The property that $f(j) \leq A(j)$ is preserved in step 5 thanks to Proposition 3.4.9. □

Remark 3.4.11. One can prove termination of Algorithm 3.4.10 and control its runtime with a bit of effort, but in practice it suffices to simply let it run until either the process terminates, or one goes through a set number of iterations of step 3 (we used 20 iterations in our examples).

3.5 Summary of the algorithm

To summarize, we describe how to assemble an algorithm for computing an approximate Frobenius matrix on $H^n_{\mathrm{rig}}(U)(-1)$.

To start with, write down a basis B of rigid cohomology as in Definition 3.4.2. Say we want to compute the Frobenius matrix on this basis modulo p^r. Choose the integer s using the following algorithm:

1. Put $s = r$. Create an empty array A.

2. Put $j = s - n + 1$.

3. If $j > 0$ and $n \log_p(p(n + j) - 1) \leq n - 1 + j - r$, then return s and STOP.

4. Replace A by the result of Algorithm 3.4.10 applied with inputs $p(n + j)$ and A. If $A(p(n + j)) > n - 1 + j - r$, then replace s by $s + 1$ and go to step 2. Otherwise, replace j by $j + 1$ and go to step 3.

For each basis element, compute the image of Frobenius truncating all terms which vanish modulo p^s, then use reduction of poles (Remark 3.2.5; see also Remark 3.5.2 below) to express the result in terms of the basis elements. The verification that this gives enough precision is analogous to the analysis of Algorithm 3.4.10.

Remark 3.5.1. This algorithm readily admits some parallelization, as one can compute the reductions of the Frobenius images of different basis elements independently. The experimental results we describe later do not depend on this capability, but it may be useful for larger examples.

Remark 3.5.2. There are at least four distinct ways to carry out the reduction of poles implied by Remark 3.2.5.

- One can simply perform the entire calculation over $\mathbb{Q}$, then interpret the final result modulo the appropriate power of p. This was our first choice, implemented in SINGULAR, but it leads to undesirable intermediate coefficient blowup.

- One can perform the calculation over $\mathbb{Z}/p^s\mathbb{Z}$ by using integral analogues of Gröbner basis arithmetic as implemented in MAGMA: to do this, one must postpone the division by $m-1$ implied in reducing the pole order from m to $m-1$ until the end of the calculation. One must also remember to use the trivial relation $A\Omega/\tilde{P}^m = A\tilde{P}\Omega/\tilde{P}^{m+1}$, as P may not be generated by its partial derivatives (in case p divides $\deg(P)$). This was our second choice, and is used in our current implementation.

- One can perform the calculation over $\mathbb{F}_\ell$ for any prime ℓ of good reduction of the lifted hypersurface. This would allow the use of the more efficient polynomial arithmetic of SINGULAR over MAGMA; however, in order to recover the desired answer (by working modulo many small ℓ and using the Chinese remainder theorem) one would need a bound on the heights of the entries of the resulting matrix. We have not attempted this method.

- One can perform the calculation over $\mathbb{C}$ by going through the Betti-de Rham comparison as in [15]: numerically integrate each truncated Frobenius image against a basis of homology, then perform a lattice reduction to express these in terms of the integrals of a basis of cohomology. Again, this requires height bounds, and again we have not attempted this method.

The last two methods share ideas with the method Edixhoven uses to compute the Δ modular form (and by extension with the Schoof-Elkies-Atkin method for computing zeta functions of elliptic curves).

3.6 Alternate algorithms

As the experimental data in the final part of the paper suggests, computing approximate Frobenius matrices in p-adic cohomology in the manner we have suggested is rather laborious. There are several other ways one might perform this computation; we mention some of these in passing, noting that any of them can be used together with the first part of the paper to give a test for low Picard number. (The arguments in the second part of the paper, notably Theorem 2.2.5, may help in the analysis of precision loss in such algorithms.)

The shift from a hypersurface to its affine complement amounts to an increase by one in the dimensions of the varieties under consideration, and in the number of variables in the polynomial rings in which the calculations take place. That shift turns out to be costly, so one would ideally like to avoid it. This appears to be possible for so-called nondegenerate hypersurfaces, those which together with the coordinate hyperplanes and the hyperplane at infinity form a normal crossings divisor. For curves, this has been proposed by Castryck, Denef, and Vercauteren [7], but the method extends readily to higher dimensions. We made a cursory attempt to implement this method for surfaces in $\mathbb{P}^3$, but our results were

inconclusive: the additional complexity in the method (especially in lifting Frobenius, which would now be done on an affine piece of the original hypersurface rather than on an affine complement) seemed to introduce large constant factors that interfered with the asymptotic improvements at the scale at which our calculations took place. Nonetheless, we think the method deserves further study.

A better approach may be to use dévissage: write your surface as a fibration of curves, compute the higher direct images of the constant sheaf, then compute the cohomology of these. This has been suggested by Lauder, who has implemented this in some examples with good results [29].

Yet another approach is to avoid directly computing the cohomology of the particular hypersurface of interest, by instead putting it into a pencil with one member chosen to be smooth with extra automorphisms. One can then compute its Frobenius matrix more easily, then use that data as the "initial condition" in the differential equation relating the Gauss-Manin connection of the pencil with its global Frobenius action. This is the "deformation" method of Lauder [27, 28]; it has been tested experimentally for families of elliptic curves by Gerkmann [13] and has been theoretically analyzed for hyperelliptic curves by Hubrechts [21] (where it already gives some improvement over the direct method), but we are not aware of any work in higher dimensions besides Lauder's original papers.

4 Implementation details

In this section, we describe an implementation that implements a special case of the algorithm we have described, and give some experimental results. One glaring omission is that we do not make a complexity analysis; this is only partly out of laziness. The other reason is that Gröbner basis calculations in general have extremely bad worst-case performance; we are not in the worst case here, but we would have to look closely at what we are using to obtain complexity estimates. Since the purpose of this paper is more about demonstrating the practicality of these methods, we do not carry out such intricate analysis here.

4.1 Implementation notes

Using the Magma algebra system [5], we have developed an implementation of the methods of this paper, to obtain an algorithm for computing approximate Frobenius matrices in rigid cohomology for smooth surfaces in projective 3-space over a prime finite field [1].

We have tested this implementation on the computer `dwork.mit.edu`, a Sun workstation with dual Opteron 246 CPUs running at 2 GHz, with access to 2GB of RAM. Although these CPUs are 64-bit processors, these experiments were conducted in 32-bit mode under Red Hat Enterprise Linux 4. Each individual surface was run on a single CPU with no use of parallelism (see Remark 3.5.1), and timings are reported in CPU seconds; memory usages are reported in megabytes. Beware that these should only be taken as order-of-magnitude indications: there are slight variations from run to run of a single example, and there are

much bigger variations within classes of examples, probably arising from the vagaries of Gröbner basis arithmetic.

Some initial experiments were also conducted using the SINGULAR algebra system [14]. The main downside with using SINGULAR for this calculation is that it only treats polynomials over a field; while one obtains correct answers by reducing poles over $\mathbb{Q}$ and then reducing modulo a power of p, the resulting calculations experience unacceptable intermediate coefficient blowup. By contrast, the MAGMA implementation uses a Gröbner basis implementation over $\mathbb{Z}/p^m\mathbb{Z}$, which avoids the coefficient blowup. (Compare Remark 3.5.2.)

In the subsequent sections, we describe some examples computed using this implementation. These examples were chosen to be "generic", without special geometric properties: their coefficients were chosen at random with a bias towards zero coefficients. The bias somewhat simplifies the Gröbner basis calculations.

It is worth noting that one can use a "prescreening" strategy to find such examples: deliberately compute approximations with *not enough* initial precision, then revisit the examples that appear to work with a provably sufficient amount of precision. We suspect that this works because our precision estimates do not give a complete picture of how quickly the p-adic approximations are converging; see Remark 4.2.3 for an instance of this.

4.2 Example: degree 4 over $\mathbb{F}_3$

We start with a careful analysis of an example in what is possibly the simplest nontrivial case. Namely, surfaces of degree 1 and 2 over a finite field $\mathbb{F}_p$ are isomorphic to $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$, whose zeta functions are known, while surfaces of degree 3 have all cohomology generated by the classes of the 27 lines on the surface over $\overline{\mathbb{F}_p}$, so the zeta function can be computed from the Galois action on these lines. (Note that while a smooth cubic surface over $\mathbb{F}_p$ has geometric Picard number 7, its arithmetic Picard number can equal 1; see [50] for an example.)

A smooth surface in $\mathbb{P}^3$ of degree 4 is a K3 surface, whose middle cohomology has dimension 22 and Hodge numbers 1, 20, 1. (Remember that we compute using *primitive* middle cohomology, in which the dimension and the central Hodge number are both decreased by 1.) We will exhibit an example of provable arithmetic Picard number 1 over $\mathbb{F}_3$; the more natural first choice $\mathbb{F}_2$ actually turns out to be somewhat trickier (see Section 4.4).

Example 4.2.1. The smooth quartic surface over $\mathbb{F}_3$ defined by the polynomial

$$x^4 - xy^3 + xy^2w + xyzw + xyw^2 - xzw^2 + y^4 + y^3w - y^2zw + z^4 + w^4$$

was found to have Picard number 1 by computing a Frobenius matrix modulo 3^3. To carry out this calculation provably using the optimal bound extracted from Algorithm 3.4.10, it was necessary to truncate differentials modulo 3^7; using only Proposition 3.4.6 would have required working modulo 3^{12}.

Remark 4.2.2. For comparison, Table 1 gives some timings and memory usages for various levels of initial and final precision in Example 4.2.1. When a final precision is specified,

that means the initial precision in that row is the minimum needed to guarantee that final precision in the Frobenius matrix under Algorithm 3.4.10; however, see Remark 4.2.3.

Table 1: Timings for a smooth quadric over $\mathbb{F}_3$.

Final precision	Initial precision	CPU sec	MB
3^2	3^6	227	37
3^3	3^7	731	53
—	3^8	907	64
—	3^9	4705	124
3^4	3^{10}	13844	906
3^5	3^{11}	15040	1103
3^6	3^{12}	40144	1795

Remark 4.2.3. One reality check on Example 4.2.1 is to verify the implied compatibilities between the answers computed to various p-adic precisions; that is, the computed Frobenius matrices for any two rows in Table 1 should agree modulo the final precision of the earlier row. This turns out to be true in a strong fashion: some of the calculations are even more accurate than predicted. Namely, we obtain the correct Frobenius matrices modulo $3^3, 3^4, 3^5, 3^6$ using initial precisions $3^6, 3^7, 3^9, 3^{10}$, respectively.

Remark 4.2.4. Another reality check on Example 4.2.1 is a comparison of initial coefficients of the predicted zeta functions against those coefficients determined exactly by actually enumerating rational points. Over $\mathbb{F}_{3^i}$ for $i = 1, 2, 3, 4, 5$, the respective numbers of rational points on the surface are

$$8, 80, 713, 6836, 58868;$$

this counting took several hours on a laptop computer using a simple-minded Magma program. From the formula for the zeta function (Definition 1.4.1), and the fact that it has the form $(Q(T)(1-T)(1-3T)(1-9T))^{-1}$ where $Q(T)$ has degree 21, we deduce that the characteristic polynomial of $3^{-1}F$ on primitive middle cohomology begins

$$\frac{1}{3}(3T^{21} + 5T^{20} + 6T^{19} + 7T^{18} + 5T^{17} + 4T^{16} + \cdots).$$

On the other hand, applying Remark 1.6.4 to the Frobenius matrix computed with final precision 3^6, we determine that the same characteristic polynomial is congruent modulo 3^4 to

$$\frac{1}{3}(3T^{21} + 5T^{20} + 6T^{19} + 7T^{18} + 5T^{17} + 4T^{16} + 2T^{15} - T^{14} - 3T^{13} - 5T^{12} - 5T^{11}$$
$$-5T^{10} - 5T^9 - 3T^8 - T^7 + 2T^6 + 4T^5 + 5T^4 + 7T^3 + 6T^2 + 5T + 3).$$

Not only are the two assertions consistent, but the characteristic polynomial computed from p-adic cohomology demonstrates the symmetry forced by the functional equation of the zeta function, i.e., by Poincaré duality on cohomology. (The geometric Picard number in this instance appears to be 4, as the characteristic polynomial appears to be divisible not only by $T+1$ but also by T^2+1, so Tate's conjecture predicts extra cycle classes over $\mathbb{F}_{3^2}$ and again over $\mathbb{F}_{3^4}$.)

Remark 4.2.5. It seems an interesting question to explore to what extent one can recover a zeta function from the various pieces of data we have in the above situation:

- the symmetry and location of roots, from the Weil conjectures;
- the initial point counts;
- divisibilities implied by the relationship between the Newton and Hodge polygons (see Remark 1.6.4);
- congruences derived from computing p-adic cohomology to low precision.

In particular, in many cases it may be possible to combine information to recover zeta functions using p-adic cohomology calculations at much less precision than would be predicted by a straightforward application of the Weil conjectures plus taking into account the Hodge polygon. We are currently investigating this experimentally; we defer reporting on the results to another occasion.

4.3 Examples: degree 4 over $\mathbb{F}_p$ ($p = 5, \dots, 19$)

We next exhibit some examples where we can compute the geometric Picard number. These examples appear in a construction of van Luijk [47]; for context, we first state [47, Proposition 4.1].

Proposition 4.3.1 (van Luijk). *Let k be a field, and suppose $\alpha, \beta \in k$ satisfy $\alpha^3\beta \neq \alpha\beta^3$. Let $f \in k[w,x,y,z]$ be a homogeneous polynomial of degree 3, such that either the coefficients of y^3 and z^3 in f differ, or the coefficients of x^2y and x^2z in f differ. Suppose that the surface X in $\mathbb{P}^3_k$ defined by*

$$wf - (xy + xz + \alpha yz)(xy + xz + \beta yz) \tag{4.3.1.1}$$

is smooth with geometric Picard number 2, and put $\overline{X} = X \times_k \overline{k}$. Then the group $\mathrm{Aut}(\overline{X})$ is trivial.

Note that the surface in (4.3.1.1), if smooth, has arithmetic Picard number at least 2, as the hyperplane section $w = 0$ splits into two conics.

Example 4.3.2. Over $\mathbb{F}_5$, we verify the instance of Proposition 4.3.1 with $\alpha = 1$, $\beta = 3$, and

$$f = 3x^3 + 3xy^2 - xyw + 3xzw - xw^2 + y^3 - y^2w + 2z^3 + w^3;$$

[47, Proposition 5.1] relies on the fact that this surface has geometric Picard number at most 2 (and hence has Picard number and geometric Picard number exactly 2). This we verify in turn by computing the matrix modulo 5^3, which requires initial precision 5^7, 5482 CPU seconds, and 514 MB of memory; applying Algorithm 1.6.2 to bound the contributions to the right side of (1.5.2.2) shows that the geometric Picard number is indeed at most 2.

For $p > 5$, there are relatively few values of n that can contribute to (1.5.2.2) for which ζ_n is p-adically close to 1, so one might expect that less final precision is needed to bound the geometric Picard number. This expectation is confirmed by the following set of examples.

Example 4.3.3. Table 2 lists some further instances in which the geometric Picard number condition in Proposition 4.3.1 can be verified (for $p = 7, 11, 13, 17, 19$), and two cases where it appears to hold but we were unable to verify it definitively (for $p = 23, 29$). In all cases, we took $\alpha = 1$, $\beta = 3$, and final precision p^2; the initial precision required was always p^4, and for $p \leq 19$, the upper bound in (1.5.2.2) was found to be 2. The examples for $p = 11, 13, 17, 19$ were found by prescreening with initial precision p^3; the examples for $p = 23, 29$ were obtained by prescreening but we did not complete the calculation at initial precision p^4.

Table 2: Further instances and presumed instances of Proposition 4.3.1 over $\mathbb{F}_p$.

p	f	CPU sec	MB
7	$-2x^3 + 2x^2y + 2x^2w + y^3 + 3y^2w + yzw - yw^2 + 2z^3$	697	63
11	$-5x^3 - 2x^2y - 5xy^2 - 2xz^2 + y^3 - yz^2 + 2z^3 - 4w^3$	5320	106
13	$3x^3 - 6x^2z + y^3 - 6yw^2 + 2z^3$	14997	158
17	$-x^3 + 8x^2y - xyw + y^3 - y^2w + 2z^3 + 5z^2w - 5zw^2$	61996	306
19	$6x^3 + 3x^2z + 7xyw - 7xz^2 + 8xzw - 9xw^2 + y^3$ $-y^2w - 5yz^2 + 5yw^2 + 2z^3 - 4z^2w - 2zw^2$	116323	459
23	$-11x^3 - 9x^2y - 2x^2z - 5x^2w - 3xyz$ $-10xyw + y^3 + 11yw^2 + 2z^3 - 4w^3$	?	?
29	$4x^3 + 4x^2w - 5xy^2 - 14xyw + y^3$ $+7y^2z - 3yz^2 + 3yw^2 + 2z^3 - w^3$	?	?

4.4 Examples: degrees 4, 5 over $\mathbb{F}_2$

To conclude, we edge towards the realm of coding theory proper, by considering examples over $\mathbb{F}_2$. Frustratingly, the asymptotic advantage obtained in the p-adic algorithms by taking $p = 2$ (which occur because the degree of the truncated Frobenius lift is a linear function of p) is somewhat counterbalanced by the need for additional precision to fight the unfortunate propensity of small integer denominators to be divisible by large powers of 2. Nonetheless, one can still say something.

Example 4.4.1. The smooth quartic surface over $\mathbb{F}_2$ defined by the polynomial

$$x^4 + x^3z + x^2y^2 + x^2yw + x^2z^2 + x^2zw + xy^3 + y^4 + y^3w + yz^3 + z^4 + z^2w^2 + w^4$$

was found to have Picard number 1 by computing a Frobenius matrix modulo 2^4; this required initial precision 2^{13}, 7182 CPU seconds, and 472 MB of memory. This example was found by prescreening using initial precision 2^8, which required a mere 88 CPU seconds and 52 MB of memory.

If we pass from quartics to quintics, then middle cohomology becomes 53-dimensional, with Hodge numbers 4, 45, 4. (Again, the space we compute in is only 52-dimensional because passing from $\tilde{X}$ to $\tilde{U}$ removes one cycle class.) This removes the parity obstruction to having *geometric* Picard number 1, and one would expect to be able to find examples of such. Moreover, since in this case one is not forced to include the eigenvalue -2, which is indistinguishable from $+2$ modulo 2^2, one might even expect to be able to work with less precision. The following example fulfills these expectations.

Example 4.4.2. The smooth quintic surface over $\mathbb{F}_2$ defined by the polynomial

$$\begin{gathered} x^5 + x^3yz + x^2y^2w + x^2yz^2 + x^2z^3 + xz^2w^2 \\ +y^5 + y^3zw + y^2zw^2 + yzw^3 + z^5 + z^2w^3 + w^5 \end{gathered}$$

was found to have geometric Picard number 1 by computing a Frobenius matrix modulo 2^3; this required initial precision 2^{12}, 22685 CPU seconds, and 179 MB of memory. Note that in this case screening for the geometric Picard number is a nontrivial calculation, because we must check up to $n = 210$, which entails working in some large extensions of $\mathbb{Q}_2$.

The example was found by prescreening with initial precision 2^6. If we had needed final precision 2^4, we would have required initial precision 2^{13}; we project that in our implementation, such a calculation would require roughly 100000 CPU seconds, and would have to be done in batches (or parallelized) to avoid memory overrun.

Acknowledgments

Kedlaya wishes to thank Felipe Voloch, whose discussions about his work with Zarzar initiated this project, Ronald van Luijk for helpful discussions about [47], and Johan de Jong and Bas Edixhoven for additional discussions. Some of these discussions took place at the Oberwolfach workshop "Explicit methods in number theory" in July 2005, where some of this material was presented in early form. Abbott and Roe were supported by MIT's Undergraduate Research Opportunities Program. Kedlaya was supported by NSF grant DMS-0400747.

References

[1] T.G. Abbott, K.S. Kedlaya, and D. Roe, Magma packages available at `http://math.mit.edu/~kedlaya/papers/`.

[2] F. Baldassarri and B. Chiarellotto, Algebraic versus rigid cohomology with logarithmic coefficients, in *Barsotti symposium in algebraic geometry (Abano Terme, 1991)*, Perspect. Math. 15, Academic Press, San Diego, 1994, 11–50.

[3] P. Berthelot, Finitude et pureté cohomologique en cohomologie rigide (with an appendix in English by A.J. de Jong), *Invent. Math.* **128** (1997), 329–377.

[4] P. Berthelot, Dualité de Poincaré et formule de Künneth en cohomologie rigide, *C.R. Acad. Sci. Paris* **325** (1997), 493–498.

[5] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comp.* **24** (1997), 235–265; home page for MAGMA version 2.12-12 (2005) at `http://magma.maths.usyd.edu.au`.

[6] R. Bott, Homogeneous vector bundles, *Annals of Math.* **66** (1957), 203–248.

[7] W. Castryck, J. Denef, and F. Vercauteren, Computing zeta functions of nondegenerate curves, preprint.

[8] P. Deligne, Équations différentielles à points singuliers réguliers, Lecture Notes in Math. 163, Springer, Berlin, 1970.

[9] P. Deligne, Cohomologie des intersections complètes, Exposé XI in *Groupes de monodromie en géométrie algébrique (SGA 7 II)*, Lecture Notes in Math. 340, Springer, Berlin, 1973.

[10] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Math. 150, Springer, New York, 1995.

[11] V.D. Goppa, Codes on algebraic curves, *Soviet Math. Dokl.* **24** (1981), 170–172.

[12] R. Gerkmann, The p-adic cohomology of varieties over finite fields and applications to the computation of zeta functions, thesis, Universität Duisburg-Essen, 2003.

[13] R. Gerkmann, Relative rigid cohomology and point counting on families of elliptic curves, preprint and associated MAGMA code available at `http://www.mathematik.uni-mainz.de/~gerkmann/`.

[14] G.-M. Greuel, G. Pfister, and H. Schönemann, SINGULAR version 3.0.0, 2005; home page at `http://www.singular.uni-kl.de`.

[15] P. Griffiths, On the periods of certain rational integrals. I, II, *Ann. of Math.* **90** (1969), 460–495; *ibid.* **90** (1969), 496–541.

[16] P. Griffiths and J. Harris, *Principles of algebraic geometry*, Wiley-Interscience, New York, 1978.

[17] A. Grothendieck, Éléments de géométrie algébrique (rédigés avec la collaboration de Jean Dieudonné): III. Étude cohomologique des faisceaux cohérents, Première partie, *Publ. Math. IHÉS* **11** (1961), 5–167.

[18] A. Grothendieck, On the de Rham cohomology of algebraic varieties, *Publ. Math. IHÉS* **29** (1966), 95–103.

[19] R. Hartshorne, Equivalence relations on algebraic cycles and subvarieties of small codimension, in *Algebraic geometry (Arcata, 1974)*, Proc. Sympos. Pure Math. 29, Amer. Math. Soc., Providence, 1973, 129–164.

[20] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math. 52, Springer, New York, 1977.

[21] H. Hubrechts, Point counting in families of hyperelliptic curves, preprint.

[22] L. Illusie, Crystalline cohomology, in *Motives*, part 1, Proc. Sympos. Pure Math. 55, Amer. Math. Soc., Providence, 1994, 43–70.

[23] K. Kato, Logarithmic structures of Fontaine-Illusie, in *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, Johns Hopkins Univ. Press, Baltimore, 1989, 191–224.

[24] K.S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, *J. Ramanujan Math. Soc.* **16** (2001), 323–338.

[25] K.S. Kedlaya, Computing zeta functions via p-adic cohomology, in *ANTS-VI*, Lecture Notes in Math. 3076, Springer, New York, 2004, 1–17.

[26] S. Kleiman, Algebraic cycles and the Weil conjectures, in *Dix exposés sur la cohomologie des schémas*, North-Holland, 1968, 359–386.

[27] A.G.B. Lauder, Deformation theory and the computation of zeta functions, *Proc. London Math. Soc.* **88** (2004), 565–602.

[28] A.G.B. Lauder, Counting solutions to equations in many variables over finite fields, *Found. Comp. Math.* **4** (2004), 221–267.

[29] A.G.B. Lauder, A recursive method for computing zeta functions of varieties, preprint.

[30] A.G.B. Lauder and D. Wan, Counting rational points on varieties over finite fields of small characteristic, preprint available at `http://www.math.uci.edu/~dwan/`.

[31] S. Lang and A. Néron, Rational points of abelian varieties over function fields, *Amer. J. Math.* **81** (1959), 95–118.

[32] M.G. Luby and M. Mitzenmacher, Verification-based decoding for packet-based low-density parity-check codes, *IEEE Trans. Information Theory* **51** (2005), 120–127.

[33] T. Matsusaka, The criteria for algebraic equivalence and the torsion group, *Amer. J. Math.* **79** (1957), 53–66.

[34] J.S. Milne, *Étale cohomology*, Princeton Math. Series 33, Princeton Univ. Press, Princeton, 1980.

[35] D. Mumford, *Lectures on curves on an algebraic surface*, Annals of Math. Studies 59, Princeton Univ. Press, Princeton, 1966.

[36] A. Néron, Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps, *Bull. Soc. Math. France* **80** (1952), 101–166.

[37] M. Raynaud, Contre-exemple au "Vanishing Theorem" en caractéristique $p > 0$, in *C.P. Ramanujam—a tribute*, Studies in Math. 8, Tata Institute of Fundamental Research, Bombay, 1978, 273–278.

[38] J.-J. Sansuc, Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres, *J. reine angew. Math.* **327** (1981), 12–80.

[39] J.-P. Serre, Géométrie algébrique et géométrie analytique, *Ann. Inst. Fourier (Grenoble)* **6** (1965–1966), 1–42.

[40] A. Shiho, Crystalline fundamental groups. II. Log convergent cohomology and rigid cohomology, *J. Math. Sci. Univ. Tokyo* **9** (2002), 1–163.

[41] J. Tate, Algebraic cycles and poles of zeta functions, in *Arithmetical algebraic geometry (Purdue, 1963)*, Harper & Row, New York, 1965, 93–110.

[42] J. Tate, Conjectures on algebraic cycles in ℓ-adic cohomology, in *Motives*, part 1, Proc. Sympos. Pure Math. 55, Amer. Math. Soc., Providence, 1994, 71–83.

[43] N. Tsuzuki, On the Gysin isomorphism of rigid cohomology, *Hiroshima Math. J.* **29** (1999), 479–527.

[44] M. van der Put, The cohomology of Monsky and Washnitzer, in Introductions aux cohomologies p-adiques (Luminy, 1984), *Mém. Soc. Math. France* **23** (1986), 33–59.

[45] R. van Luijk, An elliptic K3 surface associated to Heron triangles, arXiv preprint `math.AG/0411606`.

[46] R. van Luijk, K3 surfaces with Picard number one and infinitely many rational points, arXiv preprint `math.AG/0506416`.

[47] R. van Luijk, Quartic K3 surfaces without nontrivial automorphisms, *Math. Res. Lett.*, to appear; arXiv preprint `math.AG/0511542`.

[48] J.F. Voloch and M. Zarzar, Algebraic geometric codes on surfaces, preprint.

[49] Yu. G. Zarhin, Transcendental cycles on ordinary $K3$ surfaces over finite fields, *Duke Math. J.* **72** (1993), 65–83.

[50] M. Zarzar, Error-correcting codes on low rank surfaces, preprint available at `http://www.math.utexas.edu/~zarzar/`.