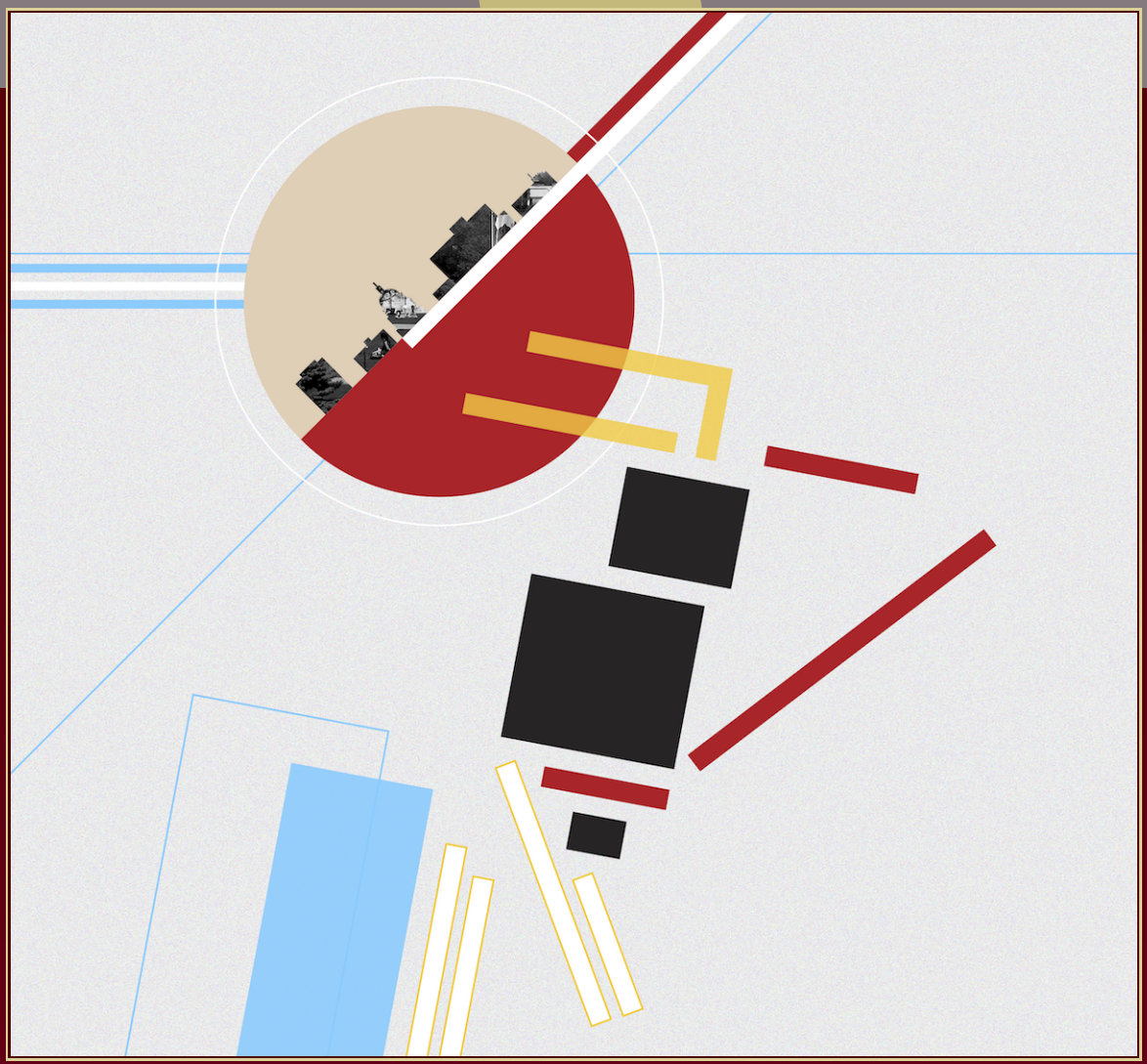
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

Zeta functions of nondegenerate hypersurfaces in toric varieties via controlled reduction in p-adic cohomology

Edgar Costa, David Harvey and Kiran S. Kedlaya



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.221

msp

Zeta functions of nondegenerate hypersurfaces in toric varieties via controlled reduction in p-adic cohomology

Edgar Costa, David Harvey and Kiran S. Kedlaya

We give an interim report on some improvements and generalizations of the Abbott–Kedlaya–Roe method to compute the zeta function of a nondegenerate ample hypersurface in a projectively normal toric variety over $\mathbb{F}_p$ in linear time in p. These are illustrated with a number of examples including K3 surfaces, Calabi–Yau threefolds, and a cubic fourfold. The latter example is a nonspecial cubic fourfold appearing in the Ranestad–Voisin coplanar divisor on moduli space; this verifies that the coplanar divisor is not a Noether–Lefschetz divisor in the sense of Hassett.

1. Introduction

We consider the problem of computing the zeta function $Z(\mathcal{X}, t)$ of an explicitly specified variety $\mathcal{X}$ over a finite field $\mathbb{F}_q$ of characteristic p. For curves and abelian varieties, Schoof's method and variants [Sch85; Pil90; GS04; GKS11; GS12] can compute $Z(\mathcal{X}, t)$ in time and space polynomial in $\log q$ and exponential in the genus/dimension; these have only been implemented for genus/dimension at most 2. Such methods may be characterized as *ℓ-adic*, as they access the ℓ-adic cohomology (for $\ell \neq p$ prime) of the variety via torsion points; there also exist *p-adic methods* which compute approximations of the Frobenius action on p-adic cohomology (Monsky–Washnitzer cohomology), and which have proven to be more viable in practice for large genus. Early examples include Kedlaya's algorithm [Ked01] for hyperelliptic curves, in which the time/space dependence is polynomial in the genus and quasilinear in p, and Harvey's algorithm [Har07], which improves the dependence on p to $p^{1/2+\epsilon}$. These methods have been subsequently generalized [GG01; DV06a; DV06b; Har12], notably by Tuitman's algorithm [Tui16; Tui17], which applies to (almost) all curves while keeping the quasilinear dependence on p. In another

Costa was partially supported by the Simons Collaboration Grant #550029. Harvey was supported by the Australian Research Council (grants DP150101689 and FT160100219). Kedlaya was supported by the National Science Foundation (grants DMS-1101343, DMS-1501214), UC San Diego (Warschawski Professorship), and a Guggenheim Fellowship. All three authors thank ICERM for its hospitality during the fall of 2015.
MSC2010: primary 11G25; secondary 11M38, 11Y16, 14G10.
Keywords: zeta function, toric varieties, Kedlaya's algorithm, p-adic methods.

direction, Harvey [Har14] has shown that when computing the zeta functions of reductions of a fixed hyperelliptic curve over a number field, p-adic methods can achieve *average* polynomial time in $\log p$ and the genus; this has been implemented in small genus [HS14; HS16].

One advantage of p-adic methods over ℓ-adic ones is that they scale much better to higher-dimensional varieties. For example, there are several p-adic constructions that apply to *arbitrary* varieties with reasonable asymptotic complexity [LW08; Har15], although we are not aware of any practical implementations. Various algorithms, and some implementations, have been given using Lauder's *deformation method* of computing the Frobenius action on the Gauss–Manin connection of a pencil [Lau04a; Lau04b; Ger07; Hub08; PT15; Tui19].

In this paper, we build on an algorithm of Abbott, Kedlaya and Roe [AKR10] which adapts the original approach of [Ked01] to smooth projective hypersurfaces. Here, we add two key improvements:

- We use *controlled reduction* in de Rham cohomology, as described in some lectures of Harvey [Har10a; Har10b; Har10c], to preserve sparsity of certain polynomials, thus reducing the time (respectively, space) dependence on p from polynomial to quasilinear (respectively, $O(\log p)$). The resulting *controlled AKR method* was implemented, with further improvements, in Costa's Ph.D. thesis [Cos15], with examples of generic surfaces and threefolds over $\mathbb{F}_p$ for $p \sim 10^6$ [Cos15, §1.6]; by contrast, the largest p used in [AKR10] is 29. Costa and Harvey are currently preparing a paper on this method; meanwhile, Costa's GPL-licensed code is available on GitHub [Cos] and is slated to be integrated into SageMath [Sag].
- We also generalize to toric hypersurfaces, subject to a standard genericity condition called *nondegeneracy*. This greatly increases the applicability of the method while preserving much of its efficiency. Some previous attempts have been made to compute zeta functions in this setting, such as work of Castryck, Denef and Vercauteren [CDV06] for curves and Sperber and Voight [SV13] in general; it is the combination with controlled reduction that makes our approach the most practical to date.

It may be possible to improve the dependence on p to square-root (as in [Har07]) or average polynomial time (as in [Har14]), but we do not attempt to do so here.

For reasons of space, we give only a summary of the algorithm, with further details to appear elsewhere. In lieu of these details, we present a number of worked examples in dimensions 2-4 that demonstrate the practicality of this algorithm in a wide range of cases. The results are based on an implementation in C++, using NTL [Sho] for the underlying arithmetic operations. Our examples in dimensions 2 and 3 were computed on one core of a desktop machine with an Intel Core i5-4590 3.30GHz processor; our sole example in dimension 4 was computed on one core of a server with an AMD Opteron 6378 1.6GHz processor. (We have not yet optimized our vector-matrix multiplications in any way; as a consequence, we observe a serious performance hit whenever the working moduli exceeds 2^{62}.)

In dimensions 2 and 3, our examples are *Calabi–Yau varieties*, i.e., smooth, proper, simply connected varieties with trivial canonical bundle. In dimension 1, these are simply elliptic curves. In dimension 2, they are *K3 surfaces*, whose zeta functions are of computational interest for various reasons. For instance,

these zeta functions can (potentially) be used to establish the infinitude of rational curves on a K3 surface (see the introduction to [CT14] for discussion); there has also been recent work on analogues of the Honda–Tate theorem, establishing conditions under which particular zeta functions are realized by K3 surfaces [Tae16; Ito16].

As for Calabi–Yau threefolds, much of the interest in their zeta functions can be traced back to *mirror symmetry* in mathematical physics. An early example is the work of Candelas, de la Ossa and Rodriguez Villegas [CdlORV03] on the Dwork pencil; a more recent example is [DKS+16], in which (using p-adic cohomology) certain mirror families of Calabi–Yau threefolds are shown to have related zeta functions.

Our four-dimensional example is a cubic projective fourfold. Such varieties occupy a boundary region between rational and irrational varieties; it is expected that a rational cubic fourfold is *special* in the sense of having a primitive cycle class in codimension 2. The geometry of special cubic fourfolds is in turn closely linked to that of K3 surfaces; in many cases, the Hodge structure of a K3 surface occurs (up to a twist) inside the Hodge structure of a special cubic fourfold, and (modulo standard conjectures) this implies a similar relationship between zeta functions. See [Has16] for further discussion.

The specific example we consider is related to the geometry of the moduli space of cubic fourfolds over $\mathbb{C}$. On this space, there exist various divisors consisting entirely of special cubic fourfolds; Hassett calls these *Noether–Lefschetz divisors* (by analogy with the case of surfaces). Recently, Ranestad and Voisin [RV17] exhibited four divisors which they believed not to be Noether–Lefschetz, but only checked this in one case. Addington and Auel [AA17] checked two more cases by finding in these divisors some cubic fourfolds over $\mathbb{Q}$ with good reduction at 2 such that the zeta functions over $\mathbb{F}_2$ show no primitive Tate classes in codimension 2. By replacing the brute-force point counts of Addington and Auel with p-adic methods, we are able to work modulo a larger prime to find an example showing that the fourth Ranestad–Voisin divisor is not Noether–Lefschetz.

To sum up, the overall goal of this project is to vastly enlarge the collection of varieties for which computing the zeta function is practical. It is our hope that doing so will lead to a rash of new insights, conjectures, and theorems of interest to a broad range of number theorists and algebraic geometers.

2. Toric hypersurfaces

We begin by reviewing the construction of a projective toric variety from a lattice polytope. For more details we recommend [CLS11].

Let $n \geq 1$ be an integer. For any commutative ring R, let $R[x^{\pm}]$ denote the Laurent polynomial ring in n variables $x_1, \ldots, x_n$ with coefficients in R. For $\alpha := (\alpha_i) \in \mathbb{Z}^n$, we write x^α for the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. We denote the R-torus by $\mathbb{T}_R^n := \operatorname{Spec}(R[x^{\pm}])$.

Let $\Delta \subset \mathbb{R}^n$ be the convex hull of a finite subset of $\mathbb{Z}^n$ that is not contained in any hyperplane, so that $\dim \Delta = n$. For $r \in \mathbb{R}$, let $r\Delta$ be the r-fold dilation of Δ. For an integer $d \geq 0$, let

$$P_d := \langle x^\alpha : \alpha \in d\Delta \cap \mathbb{Z}^n \rangle_R \quad \text{and} \quad P_d^{\mathrm{Int}} := \langle x^\alpha : \alpha \in \operatorname{Int}(d\Delta) \cap \mathbb{Z}^n \rangle_R$$

be the free R-modules on the sets of monomials with exponents in $d\Delta \cap \mathbb{Z}^n$ and $\mathrm{Int}(d\Delta) \cap \mathbb{Z}^n$ respectively. Define the R-graded algebras

$$P_\Delta := \bigoplus_{d=0}^{+\infty} P_d \quad \text{and} \quad P_\Delta^{\mathrm{Int}} := \bigoplus_{d=0}^{+\infty} P_d^{\mathrm{Int}}$$

with the usual multiplication in $R[x^{\pm}]$. We define the polarized toric variety associated to Δ as the pair $(\mathbb{P}_\Delta, \mathcal{O}_\Delta)$, where $\mathbb{P}_\Delta := \mathrm{Proj}\, P_\Delta$ and $\mathcal{O}_\Delta$ is the ample line bundle on $\mathbb{P}_\Delta$ associated to the graded P_Δ-module $P_\Delta(1)$. Note that P_Δ and P_Δ^{Int} admit n commuting degree-preserving differential operators $\partial_i := x_i(\partial/\partial x_i)$ for $i = 1, \dots, n$.

In order to suppress some expository and algorithmic complexity, we make the simplifying assumption that Δ is a *normal* polytope; that is, the map

$$(\Delta \cap \mathbb{Z}^n)^d \to d\Delta \cap \mathbb{Z}^n, \quad (x_1, \dots, x_d) \mapsto x_1 + \cdots + x_d,$$

is surjective for $d \geq 1$. This corresponds to the pair $(\mathbb{P}_\Delta, \mathcal{O}_\Delta)$ being *projectively normal*; this will be the case in our examples. As a consequence, we have that $\mathcal{O}_\Delta$ is indeed very ample.

Example 2.1. Let Δ be the regular n-simplex, the convex hull of $0, e_1, \dots, e_n$. We may then identify P_d with the set of homogeneous polynomials of degree d in $x_0, \dots, x_n$, by identifying $x^\alpha \in P_{\Delta,d}$ with the monomial $x_0^{d-\alpha_1-\cdots-\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$; then $(\mathbb{P}_\Delta, \mathcal{O}_\Delta)$ is isomorphic to $(\mathbb{P}_R^n, \mathcal{O}(1))$.

We obtain the weighted projective space $\mathbb{P}(w_0, \dots, w_n)$ by taking

$$\Delta = \left\{(x_0, \dots, x_n) \in \mathbb{R}^{n+1} : \textstyle\sum_{i=0}^n w_i x_i = w_0 \cdots w_n\right\};$$

see [Dol82, 1.2.5].

We obtain $\mathbb{P}_R^k \times_R \mathbb{P}_R^r$ by taking Δ to be the Cartesian product of the regular k-simplex by the regular r-simplex [CLS11, §2.4].

We now turn our attention to toric hypersurfaces over $R = \mathbb{F}_q$, the finite field with $q = p^a$ elements and characteristic p. Let $\mathcal{Y}$ be the hypersurface in $\mathbb{T}_{\mathbb{F}_q}^n$ defined by a Laurent polynomial $\bar{f} \in \mathbb{F}_q[x^{\pm}]$, $\mathcal{Y} := V(\bar{f}) \subset \mathbb{T}_{\mathbb{F}_q}^n$. Let

$$\mathrm{supp}\, \bar{f} = \{\alpha \in \mathbb{Z}^n : \bar{c}_\alpha \neq 0\}$$

be the support of $\bar{f}$ in $\mathbb{R}^n$; the convex hull of $\mathrm{supp}\, \bar{f}$ is the *Newton polytope* of $\bar{f}$, which we denote by Δ. We will work under the hypothesis that $\bar{f}$ is (Δ-)*nondegenerate*:[1] for all faces $\tau \subseteq \Delta$ (including Δ itself), the system of equations

$$\bar{f}_{\restriction \tau} = \partial_1 \bar{f}_{\restriction \tau} = \cdots = \partial_n \bar{f}_{\restriction \tau} = 0$$

has no solution in $\bar{\mathbb{F}}_q^{\times n}$, where $\bar{\mathbb{F}}_q$ denotes an algebraic closure of $\mathbb{F}_q$. Furthermore, nondegeneracy implies quasismoothness; see [BC94, Definition 3.1 and Proposition 4.15]. For fixed normal Δ over an

[1] This condition was introduced by Dwork [Dwo62] without a name; the term *nondegenerate* first appears in [Kou76; Var76]. Synonyms include Δ-*regular* [Bat93, § 4] and *schön* [Tev07].

infinite field, this condition holds for generic $\bar{f}$. Others have given point-counting algorithms under this assumption [CDV06; SV13].

Let $\mathcal{X} := \operatorname{Proj} P_\Delta/(\bar{f})$ denote the closure of $\mathcal{Y}$ in $\mathbb{P}_\Delta$ (placing $\bar{f}$ in degree 1) and set $\mathcal{U} := \mathbb{T}^n \backslash \mathcal{Y}$. Let H^i_{rig} denote the i-th rigid cohomology group in the sense of Berthelot [Ber97]. The Lefschetz hyperplane theorem, combined with Poincaré duality, shows that the map

$$H^i_{\mathrm{rig}}(\mathbb{P}_\Delta) \to H^i_{\mathrm{rig}}(\mathcal{X})$$

induced by the inclusion $\mathcal{X} \hookrightarrow \mathbb{P}_\Delta$ is an isomorphism for $i \neq n-1$ [BC94, Proposition 10.8]. This implies that the "interesting" part of the cohomology of $\mathcal{X}$ occurs in dimension $n-1$ and consists of those classes that do not come from P_Δ. Denote by $PH^{n-1}_{\mathrm{rig}}(\mathcal{X})$ the primitive cohomology group of X, defined by the (Frobenius-equivariant) exact sequence

$$0 \to H^{n-1}_{\mathrm{rig}}(\mathbb{P}_\Delta) \to H^{n-1}_{\mathrm{rig}}(\mathcal{X}) \to PH^{n-1}_{\mathrm{rig}}(\mathcal{X}) \to 0.$$

With this notation, we may write

$$Z(\mathcal{X}, t) = Z(\mathbb{P}_\Delta, t) Q(t)^{(-1)^n},$$

where

$$Q(t) := \det(1 - t \operatorname{Frob}_q \mid PH^{n-1}_{\mathrm{rig}}(\mathcal{X})).$$

Thus given $\bar{f}$, we would like to compute $Q(t)$.

The cohomology group $PH^{n-1}_{\mathrm{rig}}(\mathcal{X})$ is closely related to $H^n_{\mathrm{rig}}(\mathbb{P}_\Delta \backslash \mathcal{X})$. For example, if $\mathbb{P}_\Delta$ is a (weighted) projective space, as in [AKR10; Cos15], the two cohomology groups are isomorphic; see [BC94, Proposition 10.11].

3. de Rham cohomology of toric hypersurfaces

In preparation for our use of p-adic cohomology to compute $Q(t)$, we give an explicit description of the algebraic de Rham cohomology of a nondegenerate toric hypersurface in characteristic zero. We take R to be the ring $\mathbb{Z}_q$, that is, the ring of integers of $\mathbb{Q}_q$, which is the unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$.

Let $f \in \mathbb{Z}_q[x^{\pm}]$ be a lift of $\bar{f}$ to characteristic zero with the same support as f (it will also be nondegenerate). Consider $Y := V(f) \subset \mathbb{T} := \mathbb{T}_{\mathbb{Q}_q}$ and X, the closure of Y in $\mathbb{P}_\Delta$. Write $U := \mathbb{T} \backslash Y$, and $V := \mathbb{P}_\Delta \backslash X \simeq \operatorname{Spec}(A)$, where A is the coordinate ring of V; explicitly,

$$A \simeq \bigcup_{d=0}^{+\infty} f^{-d} P_d.$$

Let I_f be the ideal in P_Δ generated by $f, \partial_1 f, \ldots, \partial_n f$. We call I_f the *toric Jacobian ideal* and the quotient ring $J_f := P_\Delta / I_f$ the *toric Jacobian ring*. Since f is nondegenerate, the ideal I_f is irrelevant in P_Δ and $\operatorname{rank}_{\mathbb{Z}_q} J_f = n! \operatorname{Vol}(\Delta)$; furthermore, $(J_f)_d = 0$ for $d > n$ [Bat93, §4]. If $\mathcal{O}_\Delta$ is not very ample, then I_f might not be generated in degree 1 and we might have $(J_f)_d = 0$ only for $d \gg n$.

Let $\Omega^\bullet$ denote the logarithmic de Rham complex of V with poles along $\mathbb{P}_\Delta \backslash \mathbb{T}$. Let $H^\bullet$ be the cohomology groups of $\Omega^\bullet$; these are naturally isomorphic to $H^\bullet_{\mathrm{dR}}(V \cap \mathbb{T} = \mathbb{T} \backslash Y = U)$ and $H^\bullet_{\mathrm{rig}}(\mathbb{T}_{\mathbb{F}_q} \backslash \mathcal{Y} = \mathcal{U})$ [Kat89].

We now provide an explicit description of the group H^n, as in [Bat93, §§6 and 7], in which we will compute $Q(t)$. Set

$$\omega := \frac{\mathrm{d}x_1}{x_1} \wedge \cdots \wedge \frac{\mathrm{d}x_n}{x_n} \in \Omega^n,$$

and define the ascending filtration in Ω^n by

$$\mathrm{Fil}^d\, \Omega^n := \{g f^{-d} \omega : g \in P_d\}.$$

The associated graded ring

$$\Omega^n := \bigoplus_{d=0}^{\infty} \mathrm{Gr}^d\, \Omega^n, \quad \mathrm{Gr}^d\, \Omega^n := \mathrm{Fil}^d\, \Omega^n / \mathrm{Fil}^{d-1}\, \Omega^n,$$

is then isomorphic to $P_\Delta/(f)$ (again placing f in degree 1).

Equip H^n with the filtration induced from Ω^n, and view H^n as the quotient of Ω^n by the $\mathbb{Q}_q$-submodule generated by the relations

$$\frac{g}{f^d}\omega - \frac{gf}{f^{d+1}}\omega \quad \text{and} \quad \frac{\partial_i(g)}{f^d}\omega - \frac{dg\partial_i(f)}{f^{d+1}}\omega \tag{3-1}$$

for each $i = 1, \ldots, n$, each nonnegative integer d, and each $g \in P_d$. From these relations, we see that

$$\mathrm{Gr}^1\, H^n \simeq P_1/(f) \quad \text{and} \quad \mathrm{Gr}^d\, H^n \simeq (J_f)_d \quad (d > 1).$$

This gives a way to compute explicitly in H^n: for any $h \in (J_f)_{d+1}$ with $d > n$, we can find a relation of the form

$$d\frac{h}{f^{d+1}}\omega = d\frac{g_0 f + \sum_{i=1}^n g_i \partial_i f}{f^{d+1}}\omega \equiv \frac{dg_0 + \sum_{i=1}^n \partial_i g_i}{f^d}\omega \tag{3-2}$$

because $P_d \subset (I_f)_d$, so in H^n we can reduce the pole order of any form to at most n. This process was introduced for smooth projective hypersurfaces in [Gri69a; Gri69b] and attributed to Dwork; it is commonly known as *Griffiths–Dwork reduction*.

With the above representation of H^n, we may also identify $PH^{n-1}_{\mathrm{dR}}(X)$ with $(P_\Delta^{\mathrm{Int}} + I_f)/I_f \subset H^n$, where the filtration by pole order is the Hodge filtration; see [Bat93; BC94, §§9 and 11].

We now introduce a variation of Griffiths–Dwork reduction, called *controlled reduction*. This will be crucial for our application to p-adic cohomology, as careless application of Griffiths–Dwork reduction to a sparse form will easily lead to a dense form. For $d = 1, \ldots, n+1$, choose a $\mathbb{Z}_q$-linear splitting $P_d \approx (J'_f)_d \oplus C_d$, where $(J'_f)_d$ is a lift of $(J_f)_d$ into P_d. Let $\rho_d \colon P_d \to (J'_f)_d$ and $\pi_{d,0}, \ldots, \pi_{d,n} \colon P_d \to P_{d-1}$ be $\mathbb{Z}_q$-linear maps such that

$$g = \rho_d(g) + \pi_{d,0}(g) \cdot f + \sum_{i=1}^n \pi_{d,i}(g) \cdot \partial_i f, \quad g \in P_d.$$

These maps may be constructed one monomial at a time.

Proposition 3.1 (controlled reduction). *Let $x^\nu \in P_1$ and $x^\mu \in P_d$ be two monomials and define the $\mathbb{Z}_q$-linear maps*

$$R_{\mu,\nu}(g) := (d+n)\pi_{n+1,0}(x^\nu g) + \sum_{i=1}^{n} (\partial_i + \mu_i)(\pi_{n+1,i}(x^\nu g)),$$

$$S_\nu(g) := \pi_{n+1,0}(x^\nu g) + \sum_{i=1}^{n} \nu_i \pi_{n+1,i}(x^\nu g).$$

Then for any $g \in P_n$ and any nonnegative integer j, in H^n we have

$$g\frac{x^{(j+1)\nu+\mu}}{f^{d+n+j+1}}\omega \equiv (d+n+j)^{-1}(R_{\mu,\nu}(g) + jS_\nu(g))\frac{x^{j\nu+\mu}}{f^{d+n+j}}\omega.$$

Proof. This is straightforward from (3-1) and (3-2). □

Note that Proposition 3.1 enables us to reduce the pole order of a differential form from $d+n+j+1$ to $d+n+j$ without increasing its total number of monomials; we can thus reduce the pole order of a sparse form without making it dense.

Corollary 3.2. *With notation as in Proposition 3.1, let k be a positive integer. Then for any $g \in P_n$,*

$$g\frac{x^{\mu+k\nu}}{f^{d+n+k}}\omega \equiv \frac{\prod_{j=0}^{k-1}(R_{\mu,\nu} + jS_\nu)(g)}{\prod_{j=0}^{k-1}(d+n+j)}\frac{x^\mu}{f^{d+n}}\omega,$$

forming the composition product from left to right.

Using Proposition 3.1 amounts to performing linear algebra on matrices of size $\#(n\Delta \cap \mathbb{Z}^n) \sim n^n \operatorname{Vol}(\Delta)$. One can reduce this by a factor of $n^n/n! \sim e^n$ at the expense of making the expression for the reduction matrix more convoluted; compare [Cos15, Remark 1.17 and Proposition 1.18].

4. Monsky–Washnitzer cohomology

We now indicate how Monsky–Washnitzer cohomology, as introduced in [MW68; Mon68; Mon71], provides a crucial link between algebraic de Rham cohomology and p-adic rigid cohomology, by transferring to the former the canonical Frobenius action on the latter; see also [vdP86]. To simplify, we assume $p > \max\{n, 2\}$.

Let $A^\dagger$ denote the *weak p-adic completion* of A, the ring consisting of formal sums $\sum_{d=0}^{+\infty} g_d f^{-d}$ such that for some $a, b > 0$, $g_d \in p^{\max\{0, \lfloor ad-b \rfloor\}} P_d$ for all $d \geq 0$. We define the associated logarithmic de Rham complex $\Omega^{\dagger,\bullet}$ by $\Omega^{\dagger,i} := \Omega^i \otimes_A A^\dagger$; denote the cohomology groups of this complex by $H^{\dagger,\bullet}$. We may then obtain p-adic Monsky–Washnitzer cohomology groups $H^{\dagger,\bullet} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$. The map $\Omega^\bullet \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \to \Omega^{\dagger,\bullet} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ is a quasi-isomorphism [Mon70; vdP86; Kat89]; that is, the induced maps $H^i \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \to H^{\dagger,i} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ are isomorphisms. We can thus identify the algebraic de Rham cohomology of U with the Monsky–Washnitzer cohomology of $\mathcal{U}$.

On the other hand, we also have $H^{\dagger,\bullet} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \simeq H^\bullet_{\mathrm{rig}}(\mathcal{U})$ and the latter object is functorial with respect to geometry in characteristic p [Ber97]. In this way, $H^{\dagger,i}$ receives an action of the Frobenius automorphism,

which we can make explicit by constructing a lift σ of the p-th power Frobenius on $\mathbb{F}_q$ to $A^\dagger$. To do so, we take the Witt vector Frobenius on $\mathbb{Z}_q$ and set $\sigma(\mu) = \mu^p$ for any monomial $\mu \in P_\Delta$. We then extend σ to $A^\dagger$ by the formula

$$\sigma\left(\frac{g}{f^d}\right) := \sigma(g)\sigma(f)^{-d} = \sigma(g)\sum_{i\geq 0}\binom{-d}{i}\frac{(\sigma(f)-f^p)^i}{f^{p(d+i)}}. \tag{4-1}$$

The above series converges (because p divides $\sigma(f) - f^p$) and the definitions ensure that σ is a semilinear (with respect to the Witt vector Frobenius) endomorphism of $A^\dagger$. We finally extend σ to $\Omega^{\dagger,\bullet}$ by $\sigma(g\,\mathrm{d}h) := \sigma(g)\,\mathrm{d}(\sigma(h))$.

5. Sketch of the algorithm

We now indicate briefly how to use controlled reduction to compute the Frobenius action on the cohomology of nondegenerate toric hypersurfaces. We start as in [Har07, Proposition 4.1], by rewriting the Frobenius action in a sparser form.

Lemma 5.1. *For any positive integers d, N and $g \in P_d$, in $A^\dagger$ we have*

$$\sigma\left(\frac{g}{f^d}\right) \equiv \sum_{j=0}^{N-1}\binom{-d}{j}\binom{d+N-1}{d+j}\sigma(gf^j)f^{-p(d+j)} \pmod{p^N}.$$

Proof. This follows from (4-1) by truncating the sum and then rewriting it formally; see [Cos15, Lemma 1.10]. □

In order to compute a p-adic approximation of the Frobenius action on $PH^{n-1}(\mathcal{X})$, we must first fix a basis of the latter; we do this by constructing a monomial basis for $PH^{n-1}_{\mathrm{dR}}(X)$ via explicit linear algebra. We then apply Frobenius to each basis element in the sparse truncated form given by Lemma 5.1, recursively reduce the pole order using Corollary 3.2 (using $k = p$ as much as possible), and project to the chosen monomial basis. The dominant step is controlled reduction, which amounts to $O(pn^N \operatorname{Vol}(\Delta))$ matrix multiplications of size $n!\operatorname{Vol}(\Delta)$ per basis element.

We will not address precision estimates in this report, except to note that the machinery of [AKR10, §3.4] applies. In general, if we want N digits of p-adic accuracy, we must apply Lemma 5.1 with N replaced by $N' = N + O(n + \log N)$ and work modulo $p^{O(N')}$. Hence, with respect to p alone, we expect our algorithm to run in quasilinear time in p and use $O(\log p)$ space.

6. K3 surfaces

We now turn our attention to examples, starting with K3 surfaces. For X a K3 surface, $\dim H^2(X) = 22$ and the Hodge numbers are $(1, 20, 1)$. A common example of a K3 surface is a smooth quartic surface in $\mathbb{P}^3$; but they also occur in other ways, such as hypersurfaces in weighted projective spaces. Using a criterion of Miles Reid [Rei80], Yonemura [Yon90] found the complete list of (polarized) weighted projective spaces in which a generic hypersurface is a K3 surface; there are 95 of these. For toric varieties, the corresponding classification is that of reflexive 3-dimensional polytopes, of which there are 4,319 in all [KS98].

In the following examples, we worked modulo p^4 in order to obtain $Q(t)$ with two p-adic significant digits. As a result, we observe a performance hit for $p > 2^{16}$.

Example 6.1. Consider the projective quartic surface $\mathcal{X} \subset \mathbb{P}^3_{\mathbb{F}_p}$ defined by

$$x^4 + y^4 + z^4 + w^4 + \lambda xyzw = 0;$$

it is a member of the Dwork pencil. For $p = 2^{20} - 3$ and $\lambda = 1$, using the *controlled AKR algorithm* in 22h 7m we compute that

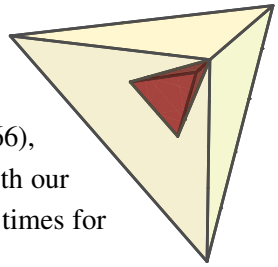
$$Z(\mathcal{X}, t)^{-1} = (1-t)(1-pt)^{16}(1+pt)^3(1-p^2t)Q(t),$$

where the "interesting" factor is

$$Q(t) = (1+pt)(1-1688538t+p^2t^2).$$

For this family, the remaining factors, apart from $Q(t)$, could have also been deduced by a p-adic formula of de la Ossa and Kadir [Kad04, Chapter 6]. In this context, the Hodge numbers of $PH^2(\mathcal{X})$ are (1, 19, 1).

A similar runtime would be expected if we used our current implementation to compute $Z(\mathcal{X}, t)$ with Δ being the 3-simplex (tetrahedron), as indicated by the outer polytope at right. Instead, we observe that the monomials defining $\mathcal{X}$ generate a sublattice of index 4^2 in $\mathbb{Z}^3$; hence, we can instead run our algorithm with a polytope of significantly smaller volume ($32/3 \approx 10.66$ versus $2/3 \approx 0.66$), as indicated by the inner polytope at right. This leads to a dramatic speedup: with our current implementation, we computed $Q(t)$ in 1m 33s. We present the running times for other p in Table 1; memory usage was about 16MB.



In the new framework, $\mathcal{X}$ is given by the closure (in $\mathbb{P}_\Delta$) of the affine surface defined by the Laurent polynomial

$$x^4y^{-1}z^{-1} + \lambda x + y + z + 1,$$

p	CHK time	PT time	p	CHK time
$2^8 - 5$	0.03s	1.65s	$2^{17} - 1$	11.9s
$2^9 - 3$	0.04s	3.64s	$2^{18} - 5$	23.4s
$2^{10} - 3$	0.04s	7.39s	$2^{19} - 1$	46.9s
$2^{11} - 9$	0.06s	14.65s	$2^{20} - 3$	1m 33s
$2^{12} - 3$	0.08s	34.80s	$2^{21} - 9$	3m 6s
$2^{13} - 1$	0.13s	34.80s	$2^{22} - 3$	6m 15s
$2^{14} - 3$	0.22s	2m 33s		
$2^{15} - 19$	0.41s	6m 43s		
$2^{16} - 15$	5.72s	14m 14s		

Table 1. The second and fifth columns use our current implementation to compute $Q(t)$. The third column uses the Pancratz–Tuitman implementation [PT15] to compute $Z(\mathcal{X}, t)$.

and the Hodge numbers of $PH^2(\mathcal{X})$ are $(1, 1, 1)$, which explains why $\deg Q(t) = 3$.

Since the Dwork pencil is a "small" deformation of the Fermat quartic, we may also use the Pancratz–Tuitman implementation of the *deformation method* [PT15] to compute $Z(\mathcal{X}, t)$. We did this and verified that our results agree; we compare running times in Table 1. To interpret these fairly, note that Pancratz and Tuitman work in $\mathbb{P}^3$ and so compute the whole numerator of $Z(\mathcal{X}, t)$ rather than just $Q(t)$. (Note that the algorithm of [Tui19] has a square-root dependence on p, as in [Har07].)

Example 6.2. Consider the projective quartic surface $\mathcal{X} \subset \mathbb{P}^3_{\mathbb{F}_p}$ defined by

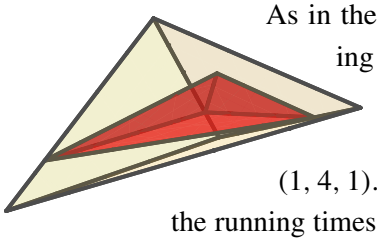
$$x^3y + y^4 + z^4 + w^4 - 12xyzw,$$

which contains a hypergeometric motive; see [DKS+16, §5]. For $p = 2^{15} - 19$, using the *controlled AKR algorithm*, in 27m 12s we compute that

$$Z(\mathcal{X}, t)^{-1} = (1-t)(1-pt)^2(1+pt)^2(1-pt+p^2t^2)^2(1-p^2t^2+p^4t^4)^2(1-p^2t)\,Q(t),$$

where the "interesting" factor is (up to rescaling)

$$p\,Q(t/p) = p + 20508t^1 - 18468t^2 - 26378t^3 - 18468t^4 + 20508t^5 + pt^6.$$



As in the previous example, the Newton polytope has volume 8, but the defining monomials generate a sublattice of index 4 in $\mathbb{Z}^3$; we may thus work instead with a polytope of volume 2 (depicted at left) and observe a significant speedup. In this setting, the Hodge numbers of $PH^2(\mathcal{X})$ are $(1, 4, 1)$. With our current implementation we computed $Q(t)$ in 4s. We present the running times for other p in Table 2, where the memory footprint was about 52MB.

Alternatively, one could try to use Magma [BCP97] to confirm $Q(t)$. Unfortunately, Magma is only able to confirm the linear coefficient:

```
> C2F2 := HypergeometricData([6,12], [1,1,1,2,3]);
> EulerFactor(C2F2, 2^10 * 3^6, 2^15 - 19: Degree:=1);
1 + 20508*$.1 + O($.1^2)
```

p	time	p	time	p	time
$2^8 - 5$	0.20s	$2^{13} - 1$	1.12s	$2^{18} - 5$	4m 54s
$2^9 - 3$	0.23s	$2^{14} - 3$	2.08s	$2^{19} - 1$	9m 46s
$2^{10} - 3$	0.29s	$2^{15} - 19$	4.00s	$2^{20} - 3$	19m 32s
$2^{11} - 9$	0.41s	$2^{16} - 15$	1m 11s	$2^{21} - 9$	38m 58s
$2^{12} - 3$	0.64s	$2^{17} - 1$	2m 30s	$2^{22} - 3$	1h 18m

Table 2. Running times for Example 6.2.

p	time	p	time	p	time
2^7-1	6.46s	$2^{10}-3$	18.93s	$2^{13}-1$	1m 46s
2^8-5	9.50s	$2^{11}-9$	31.34s	$2^{14}-3$	3m 24s
2^9-3	12.64s	$2^{12}-3$	56.23s	$2^{15}-19$	6m 20s

Table 3. Running times for Example 6.3.

Example 6.3. Consider the closure $\mathcal{X}$ in $\mathbb{P}_\Delta$ (which in this case is not a weighted projective space) of the affine surface defined by the Laurent polynomial

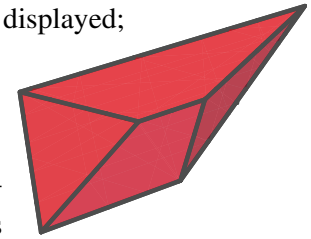
$$3x+y+z+x^{-2}y^2z+x^3y^{-6}z^{-2}+3x^{-2}y^{-1}z^{-2}-2-x^{-1}y-y^{-1}z^{-1}-x^2y^{-4}z^{-1}-xy^{-3}z^{-1};$$

it is a K3 surface of geometric Picard rank 6, and the Hodge numbers of $PH^2(\mathcal{X})$ are (1, 14, 1). For $p=2^{15}-19$, using our current implementation, in 6m 20s we obtain the "interesting" factor of $Z(\mathcal{X},t)$

$$\begin{aligned} pQ(t/p) = (1-t)(1+t)\big(p &+ 33305t^1 + 1564t^2 - 14296t^3 - 11865t^4 \\ &+ 5107t^5 + 27955t^6 + 25963t^7 + 27955t^8 + 5107t^9 \\ &- 11865t^{10} - 14296t^{11} + 1564t^{12} + 33305t^{13} + pt^{14}\big). \end{aligned}$$

We present the running times for other p in Table 3, where the peak memory usage was about 144MB.

The vertices of the associated polytope correspond to the first six terms displayed; the remaining terms are interior points. We depict this polytope of volume 8 at right.



We know of no previous algorithm that can compute $Z(\mathcal{X},t)$ for p in this range. The defining polynomial is "dense" from the point of the Sperber–Voight algorithm [SV13], which is based on Dwork cohomology and scales with the number of monomials away from the vertices of the Newton polytope.

Example 6.4. Let $\mathcal{X}$ be the smooth projective surface in $\mathbb{P}^3$ defined by the fully dense, randomly chosen quartic polynomial

$$\begin{aligned} -9x^4 - 10x^3y - 9x^2y^2 + 2xy^3 - 7y^4 + 6x^3z + 9x^2yz - 2xy^2z + 3y^3z \\ +8x^2z^2 + 6y^2z^2 + 2xz^3 + 7yz^3 + 9z^4 + 8x^3w + x^2yw - 8xy^2w \\ -7y^3w + 9x^2zw - 9xyzw + 3y^2zw - xz^2w - 3yz^2w + z^3w - x^2w^2 \\ -4xyw^2 - 3xzw^2 + 8yzw^2 - 6z^2w^2 + 4xw^3 + 3yw^3 + 4zw^3 - 5w^4; \end{aligned}$$

then Δ is the 3-simplex (tetrahedron) of volume $32/3 \approx 10.66$. For this example, we have $PH^2(\mathcal{X}) \simeq H^3(\mathbb{P}^3 \backslash \mathcal{X})$, the Hodge numbers are (1, 19, 1), and

$$Z(\mathcal{X},t)^{-1} = (1-t)(1-pt)(1-p^2t)Q(t),$$

p	time	p	time	p	time
2^7-1	25.41s	$2^{10}-3$	1m 30s	$2^{13}-1$	9m 26s
2^8-17	37.73s	$2^{11}-9$	2m 37s	$2^{14}-3$	18m 42s
2^9-3	55.82s	$2^{12}-3$	4m 50s	$2^{15}-19$	36m 29s

Table 4. Running times for Example 6.4.

where $\deg Q(t)=21$. For $p=2^{15}-19$, we obtain

$$\begin{aligned} pQ(t/p) = (1+t)\big(p &- 53159t^1 + 10023t^2 - 3204t^3 + 49736t^4 - 56338t^5 + 43086t^6 \\ &- 48180t^7 + 44512t^8 - 42681t^9 + 47794t^{10} - 42681t^{11} + 44512t^{12} - 48180t^{13} \\ &+ 43086t^{14} - 56338t^{15} + 49736t^{16} - 3204t^{17} + 10023t^{18} - 53159t^{19} + pt^{20}\big) \end{aligned}$$

using the *controlled AKR algorithm* in 38m 27s; our current implementation takes roughly the same time. We present the running times for other p in Table 4. The memory footprint was about 230MB.

Unfortunately, the *deformation method* is not suitable for dense quartics with p in this range. For example, for $p=31$ the running time was 2h 8m and its memory footprint was around 7GB, and both time and space should scale linearly with p.

7. Calabi–Yau threefolds

We next consider Calabi–Yau threefolds. Unlike for K3 surfaces, the middle Betti numbers of Calabi–Yau threefolds are not a priori bounded; the largest value of which we are aware is 984 (found in [KS00]).

A common example is a smooth quintic surface in $\mathbb{P}^4$. Again, additional constructions arise from generic hypersurfaces in weighted projective spaces, of which there are 7,555 in all, or more generally from toric varieties corresponding to reflexive 4-dimensional polytopes, of which there are 473,800,776 in all [KS00].

In all of the following examples, we worked modulo p^6 in order to obtain $Q(t)$ and our memory footprint ranged between 100MB and 270MB.

Example 7.1. Consider the projective quintic threefold $\mathcal{X} \subset \mathbb{P}^3_{\mathbb{F}_p}$ defined by

$$x_0^5 + x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_0x_1x_2x_3x_4 = 0;$$

it is a member of the Dwork pencil. We have

$$Z(\mathcal{X},t) = \frac{R_1(pt)^{20}R_2(pt)^{30}Q(t)}{(1-t)(1-pt)(1-p^2t)(1-p^3t)},$$

where R_1 and R_2 are the numerators of the zeta functions of certain curves given by a formula of Candelas, de la Ossa and Rodriguez Villegas [CdlORV03].

As it is presented, we would work with $\mathbb{P}_\Delta = \mathbb{P}^4$, where Δ is the 4-simplex of volume $625/24$. As in Example 6.1, the monomials of the equation generate a sublattice of index 5^3 in $\mathbb{Z}^4$, so we may instead

p	time	p	time	p	time
2^8-5	0.73s	$2^{13}-1$	6.41s	$2^{18}-5$	2m 50s
2^9-3	0.77s	$2^{14}-3$	11.61s	$2^{19}-1$	5m 38s
$2^{10}-3$	0.80s	$2^{15}-19$	21.98s	$2^{20}-3$	11m 18s
$2^{11}-9$	2.54s	$2^{16}-15$	43.07s	$2^{21}-9$	22m 41s
$2^{12}-3$	3.80s	$2^{17}-1$	1m 25s	$2^{22}-3$	52m 37s

Table 5. Running times for Example 7.1.

work with a polytope whose volume is smaller by a factor of 5^3. For $p = 2^{20} - 3$, we compute the "interesting" factor

$$Q(t) = 1 - 1576492860t^1 + 2672053179370pt^2 - 1576492860p^3t^3 + p^6t^4$$

in 11m 18s; if we instead had tried to apply the *controlled AKR algorithm* to compute $Q(t)$ (and not the other factors) we extrapolate that it would take us at least 120 days. We present the running times for other p in Table 5.

Since this is a "small" perturbation of the Fermat threefold, we again attempted to confirm these results using the *deformation method*; however, this was again hampered by the fact that the Pancratz–Tuitman implementation works in $\mathbb{P}_\Delta$ instead of $\mathbb{P}^3$. For $p = 7$, it took 5h 4m and its memory footprint was around 12GB.

Example 7.2. Let $\mathcal{X}$ be the threefold defined by

$$x_0^8 + x_1^5x_2 + x_0^2x_1^2x_2x_3 + x_1x_2^3x_3 + x_1^2x_3^3 + x_0x_1x_2x_3x_4 + x_2x_3x_4^2$$

in the weighted projective space $\mathbb{P}(1, 14, 18, 20, 25)$. The Newton polytope has volume $11/3 \approx 3.67$; by changing the lattice we may instead work with a polytope of volume $1/3 \approx 0.33$. In this setting, the Hodge numbers of $PH^3(\mathcal{X})$ are $(1, 1, 1, 1)$.

For $p = 2^{20} - 3$, we compute the "interesting" factor of $Z(\mathcal{X}, t)$

$$1 - 618297672t^1 + 390956360946pt^2 - 618297672p^3t^3 + p^6t^4$$

in 32m 33s. We present the running times for other p in Table 6.

p	time	p	time	p	time
2^8-5	1.90s	$2^{13}-1$	18.2s	$2^{18}-5$	8m 0s
2^9-3	1.96s	$2^{14}-3$	32.9s	$2^{19}-1$	16m 8s
$2^{10}-3$	2.06s	$2^{15}-19$	1m 6s	$2^{20}-3$	32m 33s
$2^{11}-9$	7.48s	$2^{16}-15$	2m 4s	$2^{21}-9$	1h 5m
$2^{12}-3$	10.9s	$2^{17}-1$	4m 3s	$2^{22}-3$	2h 23m

Table 6. Running times for Example 7.2.

p	time	p	time	p	time
2^8-5	4.47s	$2^{13}-1$	1m 8s	$2^{18}-5$	32m 25s
2^9-3	4.60s	$2^{14}-3$	2m 8s	$2^{19}-1$	1h 5m
$2^{10}-3$	4.96s	$2^{15}-19$	4m 6s	$2^{20}-3$	2h 10m
$2^{11}-9$	25.8s	$2^{16}-15$	8m 18s	$2^{21}-9$	4h 17m
$2^{12}-3$	39.1s	$2^{17}-1$	16m 31s	$2^{22}-3$	9h 33m

Table 7. Running times for Example 7.3.

Example 7.3. Let $\mathcal{X}$ be the threefold defined by

$$x_1^7 + x_0^5x_1x_2 + x_0^2x_1^2x_2x_3 + x_0^4x_2x_4 + x_0x_2^3x_3 + x_0^2x_3^3 + x_0x_1x_2x_3x_4 + x_2x_3x_4^2$$

in the weighted projective space $\mathbb{P}(10, 11, 16, 19, 21)$. Again, by choosing the right lattice, we reduce the volume of the Newton polytope from $55/12 \approx 4.58$ to $11/24 \approx 0.46$, and the Hodge numbers of $PH^3(\mathcal{X})$ are $(1, 2, 2, 1)$. For $p = 2^{20} - 3$, we computed the "interesting" factor of $Z(\mathcal{X}, t)$

$$1 - 2068001468t^1 + 3449674041773pt^2 - 3772715295733197p^2t^3 + 3449674041773p^4t^4 - 2068001468p^6t^5 + p^9t^6$$

in 2h 10m. We present the running times for other p in Table 7.

Example 7.4. Let $\mathcal{X}$ be the closure in $\mathbb{P}_\Delta$ (which is not a weighted projective space) of the threefold defined by the Laurent polynomial

$$xyz^2w^3 + x + y + z - 1 + y^{-1}z^{-1} + x^{-2}y^{-1}z^{-2}w^{-3} = 0.$$

Choosing the correct lattice reduces the volume of the Newton polytope from $9/8 \approx 1.12$ to $3/8 \approx 0.38$, and the Hodge numbers of $PH^3(\mathcal{X})$ are $(1, 2, 2, 1)$. For $p = 2^{20} - 3$, we computed the "interesting" factor of $Z(\mathcal{X}, t)$

$$(1 + 718pt + p^3t^2)(1 + 1188466826t^1 + 1915150034310pt^2 + 1188466826p^3t^3 + p^6t^4)$$

in 1h 15m. We present the running times for other p in Table 8.

p	time	p	time	p	time
2^8-5	2.74s	$2^{13}-1$	39.28s	$2^{18}-5$	18m 34s
2^9-3	2.80s	$2^{14}-3$	1m 13s	$2^{19}-1$	38m 8s
$2^{10}-3$	3.00s	$2^{15}-19$	1m 21s	$2^{20}-3$	1h 15m
$2^{11}-9$	14.86s	$2^{16}-15$	4m 45s	$2^{21}-9$	2h 32m
$2^{12}-3$	22.32s	$2^{17}-1$	9m 12s	$2^{22}-3$	5h 39m

Table 8. Running times for Example 7.4.

8. Cubic fourfolds

For our final example, we consider a cubic fourfold. For X a smooth cubic fourfold in $\mathbb{P}^5$, $\dim H^4(X) = 23$ and the Hodge numbers are $(0, 1, 21, 1, 0)$.

In this example, we worked modulo p^6 in order to obtain $Q(t)$.

Example 8.1. Let $\mathcal{X}$ be the smooth projective cubic fourfold in $\mathbb{P}^5_{\mathbb{F}_p}$ defined by

$$x_0^3 + x_1^3 + x_2^3 + (x_0 + x_1 + 2x_2)^3 + x_3^3 + x_4^3 + x_5^3 + 2(x_0 + x_3)^3 + 3(x_1 + x_4)^3 + (x_2 + x_5)^3;$$

it is nondegenerate in $\mathbb{P}^5$. For $p = 31$, in 21h 31m we computed

$$Z(\mathcal{X}, t)^{-1} = (1-t)(1-pt)(1-p^2t)(1-p^3t)(1-p^4t)Q(t),$$

where the "interesting" factor is an irreducible Weil polynomial given by

$$\begin{aligned} pQ(t/p^2) = p - 7t^1 + 21t^2 - 52t^3 - 8t^4 - 28t^5 + 21t^6 + 35t^7 + 39t^9 + 62t^{10} + 23t^{11} \\ + 62t^{12} + 39t^{13} + 35t^{15} + 21t^{16} - 28t^{17} - 8t^{18} - 52t^{19} + 21t^{20} - 7t^{21} + pt^{22}; \end{aligned}$$

the coefficient of t^1 may be confirmed independently by counting $\mathcal{X}(\mathbb{F}_p)$ using the Sage function `count_points`. For $p = 127$ the running time was 23h 15m and for $p = 499$ it was 24h 55m; in both cases, the "interesting" factor is an irreducible Weil polynomial. In these computations, the memory footprint was around 36.5GB.

In dimension 4, the bottleneck seems to be the linear algebra required to set up controlled reduction. For $p = 31$, more than half of the running time (15h 32m) is spent solving a linear problem of size $15{,}504 \times 37{,}128$ modulo p^6. With careful handling of this step (e.g., avoiding Hensel lifts) we would expect a significant speedup.

Note that the defining equation for $\mathcal{X}$ is quite sparse. To assess the effect of this sparsity, as well as to cross-check the answer, we recomputed $Z(\mathcal{X}, t)$ after applying a random linear change of variables to obtain a dense defining equation. For $p = 31$, in 27h 55m and using about 41GB we obtained the same value for $Z(\mathcal{X}, t)$ as above.

Recall from the Introduction that a cubic fourfold is *coplanar* if it is defined by an expression $\sum_{i=1}^{10} a_i^3$ in which each a_i is a linear form and some four of the a_i are linearly dependent. Ranestad and Voisin [RV17] showed that the Zariski closure D_{copl} of the coplanar locus is a divisor on the moduli space of cubic fourfolds. Example 8.1 is a nonspecial coplanar cubic fourfold: the existence of a primitive codimension-2 cycle class would imply[2] that $pQ(t/p^2)$ has a cyclotomic factor. This shows (modulo detailed analysis of the algorithm) that D_{copl} is not a Noether–Lefschetz divisor.

References

[AA17] Nicolas Addington and Asher Auel, *Some non-special cubic fourfolds*, preprint, 2017. arXiv 1703.05923

[2]While it is not needed here, the Tate conjecture for ordinary cubic fourfolds is known [Lev01].

[AKR10] Timothy G. Abbott, Kiran S. Kedlaya, and David Roe, *Bounding Picard numbers of surfaces using p-adic cohomology*, Arithmetics, geometry, and coding theory (AGCT 2005), Sémin. Congr., no. 21, Soc. Math. France, Paris, 2010, pp. 125–159. MR 2856564

[Bat93] Victor V. Batyrev, *Variations of the mixed Hodge structure of affine hypersurfaces in algebraic tori*, Duke Math. J. **69** (1993), no. 2, 349–409. MR 1203231

[BC94] Victor V. Batyrev and David A. Cox, *On the Hodge structure of projective hypersurfaces in toric varieties*, Duke Math. J. **75** (1994), no. 2, 293–338. MR 1290195

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR 1484478

[Ber97] Pierre Berthelot, *Finitude et pureté cohomologique en cohomologie rigide*, Invent. Math. **128** (1997), no. 2, 329–377. MR 1440308

[CdlORV03] Philip Candelas, Xenia de la Ossa, and Fernando Rodriguez-Villegas, *Calabi–Yau manifolds over finite fields, II*, Calabi–Yau varieties and mirror symmetry, Fields Inst. Commun., no. 38, Amer. Math. Soc., 2003, pp. 121–157. MR 2019149

[CDV06] W. Castryck, J. Denef, and F. Vercauteren, *Computing zeta functions of nondegenerate curves*, IMRP Int. Math. Res. Pap. (2006), art. id. 72017. MR 2268492

[CLS11] David A. Cox, John B. Little, and Henry K. Schenck, *Toric varieties*, Graduate Studies in Mathematics, no. 124, Amer. Math. Soc., Providence, RI, 2011. MR 2810322

[Cos] Edgar Costa, *controlledreduction: C++ implementation of the controlled reduction method to compute Hasse–Weil zeta functions of smooth projective hypersurfaces over finite fields*.

[Cos15] Edgar Costa, *Effective computations of Hasse–Weil zeta functions*, Ph.D. thesis, New York University, 2015, p. 78. MR 3419250

[CT14] Edgar Costa and Yuri Tschinkel, *Variation of Néron–Severi ranks of reductions of K3 surfaces*, Exp. Math. **23** (2014), no. 4, 475–481. MR 3277943

[DKS+16] Charles F. Doran, Tyler L. Kelly, Adriana Salerno, Steven Sperber, John Voight, and Ursula Whitcher, *Zeta functions of alternate mirror Calabi–Yau families*, preprint, 2016. arXiv 1612.09249

[Dol82] Igor Dolgachev, *Weighted projective varieties*, Group actions and vector fields, Lecture Notes in Math., no. 956, Springer, 1982, pp. 34–71. MR 704986

[DV06a] Jan Denef and Frederik Vercauteren, *Counting points on C_{ab} curves using Monsky–Washnitzer cohomology*, Finite Fields Appl. **12** (2006), no. 1, 78–102. MR 2190188

[DV06b] ———, *An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2*, J. Cryptology **19** (2006), no. 1, 1–25. MR 2210897

[Dwo62] Bernard Dwork, *On the zeta function of a hypersurface*, Inst. Hautes Études Sci. Publ. Math. **12** (1962), 5–68. MR 0159823

[Ger07] Ralf Gerkmann, *Relative rigid cohomology and deformation of hypersurfaces*, Int. Math. Res. Pap. IMRP (2007), no. 1, art. id. rpm003. MR 2334009

[GG01] Pierrick Gaudry and Nicolas Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in cryptology—ASIACRYPT 2001, Lecture Notes in Comput. Sci., no. 2248, Springer, 2001, pp. 480–494. MR 1934859

[GKS11] Pierrick Gaudry, David Kohel, and Benjamin Smith, *Counting points on genus 2 curves with real multiplication*, Advances in cryptology—ASIACRYPT 2011, Lecture Notes in Comput. Sci., no. 7073, Springer, 2011, pp. 504–519. MR 2935020

[Gri69a] Phillip A. Griffiths, *On the periods of certain rational integrals, I*, Ann. of Math. **90** (1969), no. 3, 460–495. MR 0260733

[Gri69b] ———, *On the periods of certain rational integrals, II*, Ann. of Math. **90** (1969), no. 3, 496–541. MR 0260733

[GS04] Pierrick Gaudry and Éric Schost, *Construction of secure random curves of genus 2 over prime fields*, Advances in cryptology—EUROCRYPT 2004, Lecture Notes in Comput. Sci., no. 3027, Springer, 2004, pp. 239–256. MR 2153176

[GS12] ———, *Genus 2 point counting over prime fields*, J. Symbolic Comput. **47** (2012), no. 4, 368–400. MR 2890878

[Har07] David Harvey, *Kedlaya's algorithm in larger characteristic*, Int. Math. Res. Not. **2007** (2007), no. 22, art. id. rnm095. MR 2376210

[Har10a] D. Harvey, *Computing zeta functions of certain varieties in larger characteristic*, lecture slides, 2010.

[Har10b] ———, *Computing zeta functions of projective surfaces in large characteristic*, lecture slides, 2010.

[Har10c] ———, *Counting points on projective hypersurfaces*, lecture slides, 2010.

[Har12] Michael C. Harrison, *An extension of Kedlaya's algorithm for hyperelliptic curves*, J. Symbolic Comput. **47** (2012), no. 1, 89–101. MR 2854849

[Har14] David Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Ann. of Math. **179** (2014), no. 2, 783–803. MR 3152945

[Har15] ———, *Computing zeta functions of arithmetic schemes*, Proc. Lond. Math. Soc. **111** (2015), no. 6, 1379–1401. MR 3447797

[Has16] Brendan Hassett, *Cubic fourfolds, K3 surfaces, and rationality questions*, Rationality problems in algebraic geometry, Lecture Notes in Math., no. 2172, Springer, 2016, pp. 29–66. MR 3618665

[HS14] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 257–273. MR 3240808

[HS16] ———, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, Contemp. Math., no. 663, Amer. Math. Soc., 2016, pp. 127–147. MR 3502941

[Hub08] Hendrik Hubrechts, *Point counting in families of hyperelliptic curves*, Found. Comput. Math. **8** (2008), no. 1, 137–169. MR 2403533

[Ito16] Kazuhiro Ito, *Unconditional construction of k3 surfaces over finite fields with given L-function in large characteristic*, preprint, 2016. arXiv 1612.05382

[Kad04] Shabnam N. Kadir, *The arithmetic of Calabi–Yau manifolds and mirror symmetry*, Ph.D. thesis, University of Oxford, 2004.

[Kat89] Kazuya Kato, *Logarithmic structures of Fontaine–Illusie*, Algebraic analysis, geometry, and number theory, Johns Hopkins Univ. Press, Baltimore, MD, 1989, pp. 191–224. MR 1463703

[Ked01] Kiran S. Kedlaya, *Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338. MR 1877805

[Kou76] A. G. Kouchnirenko, *Polyèdres de Newton et nombres de Milnor*, Invent. Math. **32** (1976), no. 1, 1–31. MR 0419433

[KS98] Maximilian Kreuzer and Harald Skarke, *Classification of reflexive polyhedra in three dimensions*, Adv. Theor. Math. Phys. **2** (1998), no. 4, 853–871. MR 1663339

[KS00] ———, *Complete classification of reflexive polyhedra in four dimensions*, Adv. Theor. Math. Phys. **4** (2000), no. 6, 1209–1230. MR 1894855

[Lau04a] Alan G. B. Lauder, *Counting solutions to equations in many variables over finite fields*, Found. Comput. Math. **4** (2004), no. 3, 221–267. MR 2078663

[Lau04b] ———, *Deformation theory and the computation of zeta functions*, Proc. London Math. Soc. **88** (2004), no. 3, 565–602. MR 2044050

[Lev01] Norman Levin, *The Tate conjecture for cubic fourfolds over a finite field*, Compositio Math. **127** (2001), no. 1, 1–21. MR 1832984

[LW08] 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, Math. Sci. Res. Inst. Publ., no. 44, Cambridge Univ. Press, 2008, pp. 579–612. MR 2467558

[Mon68] P. Monsky, *Formal cohomology, II: The cohomology sequence of a pair*, Ann. of Math. **88** (1968), 218–238. MR 0244272

[Mon70] Paul Monsky, *p-adic analysis and zeta functions*, Lectures in Mathematics, Department of Mathematics, Kyoto University, no. 4, Kinokuniya, Tokyo, 1970. MR 0282981

[Mon71] ———, *Formal cohomology, III: Fixed point theorems*, Ann. of Math. **93** (1971), 315–343. MR 0321931

[MW68] P. Monsky and G. Washnitzer, *Formal cohomology, I*, Ann. of Math. **88** (1968), 181–217. MR 0248141

[Pil90] J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), no. 192, 745–763. MR 1035941

[PT15] Sebastian Pancratz and Jan Tuitman, *Improvements to the deformation method for counting points on smooth projective hypersurfaces*, Found. Comput. Math. **15** (2015), no. 6, 1413–1464. MR 3413626

[Rei80] Miles Reid, *Canonical 3-folds*, Journées de Géometrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Sijthoff & Noordhoff, Alphen aan den Rijn—Germantown, Md., 1980, pp. 273–310. MR 605348

[RV17] Kristian Ranestad and Claire Voisin, *Variety of power sums and divisors in the moduli space of cubic fourfolds*, Doc. Math. **22** (2017), 455–504. MR 3628789

[Sag] The Sage developers, *Sagemath, the Sage mathematics software system*, http://www.sagemath.org.

[Sch85] René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494. MR 777280

[Sho] Victor Shoup, *NTL: number theory library*, http://www.shoup.net/ntl/.

[SV13] Steven Sperber and John Voight, *Computing zeta functions of nondegenerate hypersurfaces with few monomials*, LMS J. Comput. Math. **16** (2013), 9–44. MR 3033943

[Tae16] Lenny Taelman, *K3 surfaces over finite fields with given L–function*, Algebra Number Theory **10** (2016), no. 5, 1133–1146. MR 3531364

[Tev07] Jenia Tevelev, *Compactifications of subvarieties of tori*, Amer. J. Math. **129** (2007), no. 4, 1087–1104. MR 2343384

[Tui16] Jan Tuitman, *Counting points on curves using a map to* $\mathbb{P}^1$, Math. Comp. **85** (2016), no. 298, 961–981. MR 3434890

[Tui17] ———, *Counting points on curves using a map to* $\mathbb{P}^1$*, II*, Finite Fields Appl. **45** (2017), 301–322. MR 3631366

[Tui19] ———, *Computing zeta functions of generic projective hypersurfaces in larger characteristic*, Math. Comp. **88** (2019), no. 315, 439–451. MR 3854065

[Var76] A. N. Varchenko, *Zeta-function of monodromy and Newton's diagram*, Invent. Math. **37** (1976), no. 3, 253–262. MR 0424806

[vdP86] Marius van der Put, *The cohomology of Monsky and Washnitzer*, Introductions aux cohomologies p–adiques, Mém. Soc. Math. France, no. 23, Soc. Math. France, Paris, 1986, pp. 4, 33–59. MR 865811

[Yon90] Takashi Yonemura, *Hypersurface simple K3 singularities*, Tohoku Math. J. **42** (1990), no. 3, 351–380. MR 1066667

Received 1 Mar 2018. Revised 24 Aug 2018.

EDGAR COSTA: edgarc@mit.edu
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, United States

DAVID HARVEY: d.harvey@unsw.edu.au
School of Mathematics and Statistics, University of New South Wales, Sydney, Australia

KIRAN S. KEDLAYA: kedlaya@ucsd.edu
Department of Mathematics, University of California, San Diego, La Jolla, CA, United States

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine