SOME NON-SPECIAL CUBIC FOURFOLDS

NICOLAS ADDINGTON AND ASHER AUEL

Abstract. In [20], Ranestad and Voisin showed, quite surprisingly, that the divisor in the moduli space of cubic fourfolds consisting of cubics "apolar to a Veronese surface" is not a Noether–Lefschetz divisor. We give an independent proof of this by exhibiting an explicit cubic fourfold X in the divisor and using point counting methods over finite fields to show X is Noether–Lefschetz general. We also show that two other divisors considered in [20] are not Noether–Lefschetz divisors.

1. Introduction

In [20], Ranestad and Voisin introduced some new divisors in the moduli space of smooth complex cubic fourfolds, quite different from Hassett's Noether–Lefschetz divisors [15]. A cubic $X \subset \mathbb{P}^5$ is called *special* if

$$H^{2,2}_{\text{prim}}(X,\mathbb{Z}) := H^4_{\text{prim}}(X,\mathbb{Z}) \cap H^{2,2}(X)$$

is non-zero, or equivalently if X contains a surface not homologous to a complete intersection. The locus of special cubic fourfolds is a countable union of irreducible divisors in the moduli space, called Noether–Lefschetz divisors. Special cubic fourfolds often have rich connections to K3 surfaces, and it is expected that all rational cubic fourfolds are special; see [14] for a recent survey of the topic.

Ranestad and Voisin's divisors are constructed in a much more algebraic way, using apolarity. Briefly, a cubic fourfold X cut out by a polynomial $f(y_0, \ldots, y_5)$ is said to be *apolar* to an ideal generated by quadrics,

$$I = \langle q_1, \ldots, q_m \rangle \subset \mathbb{C}[y_0, \ldots, y_5],$$

if, writing $q_i = \sum a_{ijk}\, y_j y_k$, we have

$$\sum a_{i,jk}\, \partial_j \partial_k f = 0 \text{ for all } i.$$

Ranestad and Voisin showed that the following loci are irreducible divisors in the moduli space of cubic fourfolds: $D_{V\text{-}ap}$, the set of cubics apolar to a Veronese surface; D_{IR}, the set of cubics apolar to a quartic scroll; and D_{rk3}, the closure of the set of cubics apolar to the union of a plane and a disjoint hyperplane. (They also studied a fourth divisor D_{copl}, not defined using apolarity, which we do not address.) They showed that $D_{V\text{-}ap}$ is *not* a Noether–Lefschetz divisor, by carefully analyzing its singularities. From this they deduced that for a generic cubic X, the "varieties of sums of powers" of the polynomial f, which is a hyperkähler fourfold, is not Hodge-theoretically related to the Fano variety of lines on X, a better-known hyperkähler fourfold. They remarked that D_{rk3} is "presumably" not a Noether–Lefschetz divisor, and that if one could prove that D_{IR} is not a Noether–Lefschetz divisor then it would give another approach to proving their main theorem.

We were very surprised to learn that $D_{V\text{-}ap}$ is not a Noether–Lefschetz divisor: we would have guessed that it was Hassett's divisor $\mathcal{C}_{38}$, for the following reason. Cubic fourfolds in $\mathcal{C}_{38}$, which are conjectured to be rational, have associated K3 surfaces of degree 38. Mukai [17] observed that the generic such K3 surface S can be described as the variety of sums of powers of a plane sextic $g(x_0, x_1, x_2)$; see [19, Thm. 1.7(iii)] for a more detailed account. A natural way to construct a cubic fourfold from g is to consider the multiplication map

$$m\colon \operatorname{Sym}^3 \operatorname{Sym}^2 \mathbb{C}^3 \to \operatorname{Sym}^6 \mathbb{C}^3$$

and its transpose

$$m^\vee\colon \operatorname{Sym}^6 \mathbb{C}^{3\vee} \to \operatorname{Sym}^3 \operatorname{Sym}^2 \mathbb{C}^{3\vee}.$$

Then $m^\vee(g)$ cuts out a cubic $X \subset \mathbb{P}(\operatorname{Sym}^2 \mathbb{C}^{3\vee}) = \mathbb{P}^5$, typically smooth. By [20, Lem. 1.7], the cubics obtained this way are exactly those in $D_{V\text{-}ap}$. It seemed reasonable to expect that the cubic X would be Hodge-theoretically associated with the K3 surface S, but by Ranestad and Voisin's result, it cannot be.

Since the result is so surprising, and the proof quite difficult, at least to our eyes, we thought it worthwhile to seek experimental confirmation. In this note, we give a computer-aided proof of the following result, and in particular a more direct proof of Ranestad and Voisin's result:

Theorem 1. *There is an explicit sextic polynomial g, defined over $\mathbb{Q}$, such that the cubic fourfold X cut out by $m^\vee(g)$ is smooth and satisfies $H^{2,2}_{\text{prim}}(X, \mathbb{Z}) = 0$. In particular, $X \in D_{V\text{-}ap}$, but X is not in any Noether–Lefschetz divisor.*

We also confirm Ranestad and Voisin's expectations for the other two divisors mentioned above:

Theorem 2. *There is an explicit cubic fourfold $X \in D_{IR}$, defined over $\mathbb{Q}$, with $H^{2,2}_{\text{prim}}(X, \mathbb{Z}) = 0$. In particular, D_{IR} is not a Noether–Lefschetz divisor.*

Theorem 3. *There is an explicit cubic fourfold $X \in D_{rk3}$, defined over $\mathbb{Q}$, with $H^{2,2}_{\text{prim}}(X, \mathbb{Z}) = 0$. In particular, D_{rk3} is not a Noether–Lefschetz divisor.*

Thus it seems that apolarity produces cubic fourfolds of a different character than those considered in [15]. It would be very interesting to know if there is any connection with rationality.

We follow a strategy developed by van Luijk [23] and refined by Elsenhans and Jahnel [9, 10], for producing explicit K3 surfaces of Picard rank 1. We find an explicit cubic fourfold with good reduction modulo 2, then count points over $\mathbb{F}_{2^m}$ for $m = 1, 2, \ldots, 11$ to determine the eigenvalues of Frobenius acting on $H^4_{\mathrm{prim}}(X_{\overline{\mathbb{F}}_2}, \mathbb{Q}_\ell(2))$, which give a bound on the rank of $H^{2,2}_{\mathrm{prim}}(X, \mathbb{Z})$. In §2, we give the details of adapting van Luijk's method to cubic fourfolds.

On the one hand, our task is simpler than van Luijk's: since the geometric Picard rank of a K3 surface over a finite field is necessarily even, to show that a K3 surface has Picard rank 1 one has to work modulo two different primes and compare intersection forms; but here we need only work modulo one prime. On the other hand, a fourfold is much bigger than a surface, and it is infeasible to count points naively by iterating over $\mathbb{P}^5$. Nor can we control the cohomology of X by counting points on an associated K3 surface as in [2] or [16], since there is none. In §3 we explain how to exploit the conic bundle structure on the blow-up of X along a line, so that we only need to iterate over $\mathbb{P}^3$, and with a little more work, only over $\mathbb{P}^2$. The same idea was used to count points on cubic threefolds by Debarre, Laface, and Roulleau [7, §4.3], who trace it back to Bombieri and Swinnerton–Dyer [3]. Whereas those papers restrict to odd characteristic, we find that the hassle of working with conics in characteristic 2 is more than repaid by the fact that computation in $\mathbb{F}_{2^m}$ is so fast.

We do not use the p-adic cohomology methods of Kedlaya, Harvey, and others [1, 13, 6]. While these methods are surely the way of the future, they are much harder to implement than our algorithm, and the available implementations are not quite ready to handle cubic fourfolds.

In §4, we give the explicit polynomials and the point counts needed to prove Theorems 1, 2, and 3. In §5, we conclude with some remarks about computer implementation and verification.

The existence of Noether–Lefschetz general cubic fourfolds (and other complete intersections) defined over $\mathbb{Q}$ was first proved by Terasoma [21], although his proof is not constructive. Elsenhans and Jahnel gave an explicit example in [10, Example 3.15], also using point-counting methods. But the existence of Noether–Lefschetz general cubic fourfolds with specified algebraic properties is far from clear *a priori*.

Acknowledgements. We thank J.-L. Colliot-Thélène, E. Costa, D. Harvey, B. Hassett, A. Kuznetsov, K. Ranestad, R.P. Thomas, A. Várilly-Alvarado, and B. Viray for helpful conversations, and the organizers of the Fall 2016 AGNES workshop at UMass Amherst for their hospitality. In the course of this project we used the computer algebra system Macaulay2 [12] extensively, and Magma [4] to a lesser extent. The second author was partially supported by NSA Young Investigator Grant H98230-16-1-0321.

2. Adaptation of van Luijk's method

In this section we adapt the method developed in [23] from K3 surfaces to cubic fourfolds. We begin with the following proposition, which is similar to [22, Cor. 6.3]. Note that due to our choice of Tate twist, our Frobenius eigenvalues have absolute value 1 rather than q^i.

Proposition 2.1. *Let R be a discrete valuation ring of a number field L with residue field $k \cong \mathbb{F}_q$ for $q = p^r$, and let X be a smooth projective scheme over R. Let X^{an} denote the complex manifold associated to the complex variety $X_{\mathbb{C}}$. Let $\Phi\colon X_k \to X_k$ be the r-th power absolute Frobenius, let ℓ be a prime different from p, and let Φ^* be the automorphism of*

$$H^{2i}_{\text{ét}}(X_{\bar{k}}, \mathbb{Q}_\ell(i))$$

induced by $\Phi \times 1$ on $X_k \times \bar{k}$.

Then the rank of the image of the cycle class map

$$\mathrm{CH}^i(X_{\mathbb{C}}) \xrightarrow{\mathrm{cl}} H^{2i}(X^{\mathrm{an}}, \mathbb{Z}(i)) \tag{1}$$

is less than or equal to the number of eigenvalues of Φ^*, counted with multiplicity, that are roots of unity.

In particular, if the Hodge conjecture holds for codimension-i cycles on X, then the rank of $H^{2i}(X^{\mathrm{an}}, \mathbb{Z}) \cap H^{i,i}(X^{\mathrm{an}})$ is bounded above by the number of such eigenvalues.

Proof. The rank of the image of (1) agrees with the rank of the image of

$$\mathrm{CH}^i(X_{\mathbb{C}}) \xrightarrow{\mathrm{cl}} H^{2i}(X^{\mathrm{an}}, \mathbb{Z}_\ell(i)).$$

By the comparison theorem between singular and ℓ-adic cohomology, this agrees with the rank of the image of

$$\mathrm{CH}^i(X_{\mathbb{C}}) \xrightarrow{\mathrm{cl}} H^{2i}_{\text{ét}}(X_{\mathbb{C}}, \mathbb{Z}_\ell(i)).$$

Now let K be the field of fractions of the completion $\widehat{R}$, and consider the commutative diagram

$$\begin{array}{ccc}
\mathrm{CH}^i(X_{\mathbb{C}}) & \xrightarrow{\mathrm{cl}} & H^{2i}_{\text{ét}}(X_{\mathbb{C}}, \mathbb{Z}_\ell(i)) \\
\uparrow & & \uparrow \cong \\
\mathrm{CH}^i(X_{\bar{L}}) & \xrightarrow{\mathrm{cl}} & H^{2i}_{\text{ét}}(X_{\bar{L}}, \mathbb{Z}_\ell(i)) \\
\downarrow & & \downarrow \cong \\
\mathrm{CH}^i(X_{\bar{K}}) & \xrightarrow{\mathrm{cl}} & H^{2i}_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}_\ell(i)).
\end{array}$$

The right-hand vertical maps are isomorphisms by smooth base change, and while the left-hand vertical maps are typically not isomorphisms, the images of the three horizontal maps agree thanks to the existence of Hilbert schemes, as remarked in [5, Rem. 46].[1]

[1]Alternatively we could have embedded $\bar{K} \hookrightarrow \mathbb{C}$, but we preferred to use the more natural embeddings $\mathbb{C} \hookleftarrow \bar{L} \hookrightarrow \bar{K}$.

Next we have a commutative square

$$\begin{array}{ccc} \mathrm{CH}^i(X_{\bar K}) & \xrightarrow{\mathrm{cl}} & H^{2i}_{\text{ét}}(X_{\bar K}, \mathbb{Z}_\ell(i)) \\ \downarrow \sigma & & \downarrow \cong \\ \mathrm{CH}^i(X_{\bar k}) & \xrightarrow{\mathrm{cl}} & H^{2i}_{\text{ét}}(X_{\bar k}, \mathbb{Z}_\ell(i)), \end{array}$$

where the left-hand vertical map is the specialization map for Chow groups; see Fulton [11, Example 20.3.5] for the commutativity of the square. Thus the rank of the image of the top horizontal map is less than or equal to that of the bottom one.

Finally we consider the cycle class map after tensoring with $\mathbb{Q}_\ell$

$$\mathrm{CH}^i(X_{\bar k}) \otimes \mathbb{Q}_\ell \xrightarrow{\mathrm{cl}} H^{2i}(X_{\bar k}, \mathbb{Q}_\ell(i))$$

and recall that cycles on $X_{\bar k}$ are defined over some finite extension of k, hence are fixed by some power of Frobenius, hence their classes in cohomology are eigenvectors with eigenvalues a root of unity as in the proof of [22, Cor. 6.3]. □

In our application, we will take $R = \mathbb{Z}_{(2)}$, so $L = \mathbb{Q}$, $q = p = 2$, and $K = \mathbb{Q}_2$.

Now specialize to the case where X is a cubic fourfold. The Hodge conjecture holds for cubic fourfolds [26, 18, 25], so to show that $H^{2,2}_{\mathrm{prim}}(X, \mathbb{Z}) = 0$ it is enough to show that no eigenvalue of Φ^* acting on

$$V := H^4_{\text{ét},\mathrm{prim}}(X_{\bar k}, \mathbb{Q}_\ell(2)) \cong \mathbb{Q}_\ell^{22}$$

is a root of unity, or equivalently that the characteristic polynomial

$$\chi(t) := \det(t \cdot \mathrm{Id}_V - \Phi^*|_V)$$

has no cyclotomic factor. For this it is enough to show that χ is irreducible over $\mathbb{Q}$ and that not all its coefficients are integers.

The cohomology of X is

$$H^i_{\text{ét}}(X_{\bar k}, \mathbb{Q}_l(i)) = \begin{cases} \mathbb{Q}_l & i = 0, \\ \mathbb{Q}_l \cdot h & i = 2 \\ \mathbb{Q}_l \cdot h^2 \oplus V & i = 4 \\ \mathbb{Q}_l \cdot h^3 & i = 6 \\ \mathbb{Q}_l \cdot h^4 & i = 8 \\ 0 & \text{otherwise,} \end{cases}$$

where h is the hyperplane class, so by the Lefschetz trace formula we have

$$\#X(\mathbb{F}_{q^m}) = 1 + q^m + q^{2m}\Big(1 + \mathrm{tr}(\Phi^{*m}|_V)\Big) + q^{3m} + q^{4m}. \qquad (2)$$

The method of passing from traces of powers of $\Phi^*|_V$ to the characteristic polynomial using Newton's identities is discussed in [23, §3], [9, §3], or [16,

§6.1]. Thanks to the functional equation $\chi(t) = \pm t^{22}\chi(t^{-1})$ it is usually enough to count up to $m = 11$.

3. The algorithm using conic bundles

How then can we compute the point counts (2) for an explicit cubic with $q = 2$ and $m = 1, 2, \ldots, 11$? As we said in the introduction, it is not feasible to iterate over $\mathbb{P}^5(\mathbb{F}_{2^m})$, evaluating our cubic polynomial at every point: in Magma this would take many years, and in a program written optimized specially for the purpose it would take months, or at best weeks. Instead we project from a line to obtain a conic fibration.

Continue to work with a smooth cubic X defined over an arbitrary $\mathbb{F}_q$. Choose a line $l \subset X$ defined over $\mathbb{F}_q$; by [7] such a line always exists for $q = 2$ or $q \geq 5$, and probably for $q = 3$ or 4 as well. Change variables so that l is given by $y_0 = y_1 = y_2 = y_3 = 0$. Then we can write the equation of X as

$$Ay_4^2 + By_4y_5 + Cy_5^2 + Dy_4 + Ey_5 + F,$$

where A, B, and C are linear in $y_0, \ldots, y_3$, C and D are quadratic, and F is cubic. If $A, \ldots, F$ vanish simultaneously at some point of $\mathbb{P}^3$ then X contains a plane, contributing an unwanted Frobenius eigenvalue, so we stop. Otherwise we obtain a flat conic bundle

$$\mathrm{Bl}_l(X) \longrightarrow \mathbb{P}^3_{(y_0:\ldots:y_3)},$$

with fibers given by the homogenization of the quadratic form above. Now we use the following:

Proposition 3.1. *Let $\pi\colon Y \to Z$ be a conic bundle defined over $\mathbb{F}_q$, let $\Delta \subset Z$ be the locus parametrizing degenerate conics, and let $\tilde{\Delta}$ be the (possibly branched) double cover of Δ parametrizing lines in the fibers of π. Then*

$$\#Y(\mathbb{F}_q) = (q+1)\cdot \#Z \; + \; q\cdot(\#\tilde{\Delta} - \#\Delta). \tag{3}$$

Proof. A smooth conic over $\mathbb{F}_q$ is isomorphic to $\mathbb{P}^1$, hence has $q+1$ points. For a singular conic, there are three possibilities:

- a pair of lines defined over $\mathbb{F}_q$, contributing $2q+1$ points;
- a pair of conjugate lines defined over $\mathbb{F}_{q^2}$, contributing only one $\mathbb{F}_q$-point;
- a double line, contributing $q+1$ points.

The fiber of $\tilde{\Delta}$ over the relevant point of Δ consists of 2, 0, or 1 points respectively. Thus we have

$$\#Y(\mathbb{F}_q) = \underbrace{(q+1)\cdot(\#Z - \#\Delta)}_{\text{from smooth conics}} + \underbrace{(q\cdot\#\tilde{\Delta} + \#\Delta)}_{\text{from singular conics}},$$

which simplifies to give (3). □

In our case, with $Y = \mathrm{Bl}_l(X)$ and $Z = \mathbb{P}^3$, this yields

$$\#X(\mathbb{F}_q) = q^4 + q^3 + q(\#\tilde{\Delta} - \#\Delta) + q + 1.$$

The discriminant locus $\Delta \subset \mathbb{P}^3$ is cut out by the quintic polynomial

$$AE^2 + B^2F + CD^2 - BDE - 4ACF. \tag{4}$$

This formula remains valid in characteristic 2, although of course the last term vanishes. The double cover $\tilde{\Delta}$ can also be described as the variety of lines on X that meet l.[2]

So we iterate over $\mathbb{P}^3$ and count points on Δ and $\tilde{\Delta}$. To count points on $\tilde{\Delta}$ in characteristic 2, we note that if $B = D = E = 0$ then the conic is a double line; otherwise we compute an Arf invariant: if $B \neq 0$ (resp. $D \neq 0$ or $E \neq 0$), then the conic has $2q + 1$ points if AC/B^2 (resp. AF/D^2 or CF/E^2) is of the form $a^2 + a$ for some $a \in \mathbb{F}_q$, and 1 point if it is not.

This algorithm runs up to $q = 2^{11}$ in about half a minute on the first author's laptop. But to find the explicit cubics below we had to search through dozens of candidates, so it was worthwhile to make a further optimization, iterating only over Δ rather than all of $\mathbb{P}^3$, as follows.

The quintic Δ is not smooth; in characteristic 2, it is singular at least along the locus where

$$B = D = E = 0,$$

which has expected dimension 0 and degree 4. Suppose this locus contains an $\mathbb{F}_2$-point y.[3] Projecting from y, the quintic Δ becomes a 3-to-1 cover of $\mathbb{P}^2$, so we can iterate over $\mathbb{P}^2$ and find the three (or fewer) sheets of the cover at each point with a suitable version of Cardano's formula [8, Exercise 14.7.15].

With this improvement the algorithm runs up to $q = 2^{11}$ in less than a second, and up to $q = 2^{14}$ in a little more than a minute. In §5 we make some practical comments about our implementation of the algorithm, and sanity checks on the output.

4. The explicit cubics

4.1. **Proof of Theorem 1.**

Let us begin by discussing the map $m^\vee$ from the introduction in very concrete terms, embracing the monomial basis for the polynomial ring rather than working invariantly, and staying in characteristic 0 as long as possible to avoid discussing divided powers.

[2] The topology of $\tilde{\Delta}$ over $\mathbb{C}$ has been studied in [24, §3, Lemmas 1–3]. For a generic $l \subset X$, it is a smooth surface with Hodge diamond

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 6 & & 50 & & 6 \\ & 0 & & 0 & \\ & & 1 & & \end{array}.$$

[3] In practice this usually happens, although not always. That is, there exist smooth cubics X and $\mathbb{F}_2$-lines $l \subset X$ such that Δ_{sing} has no $\mathbb{F}_2$-point, but they are relatively rare. We have not encountered a cubic X such that for *every* $\mathbb{F}_2$-line $l \subset X$, Δ_{sing} has no $\mathbb{F}_2$-point. We wonder whether any such cubic exists.

Let $R = \mathbb{C}[x_0, \dots, x_n]$, and let $R_d \subset R$ be the subspace of homogeneous polynomials of degree d. We identify R_1 with its dual via the pairing

$$\langle x_i, x_j \rangle = \frac{\partial}{\partial x_i} x_j = \delta_{ij},$$

and extend this to a pairing

$$R_k \otimes R_d \to R_{d-k}$$

for positive integers $k \leq d$, again by differentiation. If $k = d$ this is a perfect, symmetric pairing. We have, for example,

$$\langle x_0 x_1,\, x_0 x_1 \rangle = \tfrac{\partial}{\partial x_0} \tfrac{\partial}{\partial x_1} x_0 x_1 = 1,$$

but

$$\langle x_0^2,\, x_0^2 \rangle = \tfrac{\partial}{\partial x_0} \tfrac{\partial}{\partial x_0} x_0^2 = 2,$$

so the monomials form an orthogonal basis for R_d but not an orthonormal basis. For $k > d$ we set $\langle R_k, R_d \rangle = 0$.

Now with a view toward Theorem 1, let $R = \mathbb{C}[x_0, x_1, x_2]$ and $S = \mathbb{C}[y_0, \dots, y_5]$. The isomorphism

$$m\colon S_1 \to R_2$$

given by

$$\begin{array}{lll} y_0 \mapsto x_0^2 & y_1 \mapsto x_0 x_1 & y_2 \mapsto x_0 x_2 \\ y_3 \mapsto x_1^2 & y_4 \mapsto x_1 x_2 & y_5 \mapsto x_2^2. \end{array}$$

induces a map

$$m\colon S_d \to R_{2d}$$

for all d.

Let $g \in R_6$ be given by

$$\begin{aligned} g = {} & \frac{1}{30} x_0^5 x_1 + \frac{1}{6} x_0^4 x_1^2 + \frac{1}{6} x_0^2 x_1^4 + \frac{1}{30} x_0 x_1^5 + \frac{1}{120} x_1^6 \\ & + \frac{4}{3} x_0^3 x_1^2 x_2 + \frac{2}{3} x_0^2 x_1^3 x_2 + \frac{1}{6} x_0^4 x_2^2 + 2 x_0^2 x_1^2 x_2^2 + \frac{1}{3} x_0 x_1^3 x_2^2 \\ & + \frac{1}{12} x_1^4 x_2^2 + \frac{2}{3} x_0^2 x_1 x_2^3 + \frac{1}{6} x_1^3 x_2^3 + \frac{1}{3} x_0^2 x_2^4 + \frac{1}{15} x_1 x_2^5, \end{aligned}$$

and let $f \in S_3$ be given by

$$\begin{aligned} f = {} & 2y_0^2 y_1 + 4y_0 y_1^2 + 8y_1^2 y_2 + 4y_0 y_2^2 + 4y_0^2 y_3 + 4y_1^2 y_3 \\ & + 16 y_0 y_2 y_3 + 8 y_1 y_2 y_3 + 8 y_2^2 y_3 + 4 y_0 y_3^2 + 2 y_1 y_3^2 + y_3^3 \\ & + 16 y_0 y_1 y_4 + 4 y_1^2 y_4 + 16 y_1 y_2 y_4 + 4 y_2^2 y_4 + 8 y_0 y_3 y_4 \\ & + 4 y_2 y_3 y_4 + 8 y_0 y_4^2 + 2 y_1 y_4^2 + 2 y_3 y_4^2 + y_4^3 + 4 y_0^2 y_5 \\ & + 8 y_1^2 y_5 + 8 y_1 y_2 y_5 + 8 y_2^2 y_5 + 16 y_0 y_3 y_5 + 4 y_1 y_3 y_5 \\ & + 2 y_3^2 y_5 + 8 y_0 y_4 y_5 + 6 y_3 y_4 y_5 + 8 y_0 y_5^2 + 4 y_4 y_5^2. \end{aligned}$$

We claim that $f = m^\vee(g)$, i.e. that

$$\langle h, f\rangle = \langle m(h), g\rangle$$

for all $h \in S_3$. This can be checked tediously by hand, or with the Macaulay2 code given in the ancillary file `thm1.m2`.

Let $X \subset \mathbb{P}^5$ be the hypersurface cut out by f. After substituting

$$y_1 \mapsto \tfrac{1}{2} y_1, \qquad y_2 \mapsto \tfrac{1}{2} y_2, \qquad y_5 \mapsto \tfrac{1}{2} y_5,$$

we obtain a model of X with good reduction modulo 2. Its reduction contains the line

$$y_0 + y_3 = y_1 = y_2 + y_3 = y_4 = 0.$$

The point counts of X over $\mathbb{F}_{2^m}$ are given in Table 1. Thus the characteristic polynomial of Φ^* acting on $H^4_{\text{ét,prim}}(X_{\bar{k}}, \mathbb{Q}_\ell(2))$ is

$$\begin{aligned}\chi(t) = t^{22} - \frac{3}{2}t^{20} + \frac{3}{2}t^{18} - t^{16} + \frac{1}{2}t^{15} + \frac{1}{2}t^{14} - t^{13} + \frac{3}{2}t^{11} \\ - t^9 + \frac{1}{2}t^8 + \frac{1}{2}t^7 - t^6 + \frac{3}{2}t^4 - \frac{3}{2}t^2 + 1,\end{aligned}$$

which is irreducible over $\mathbb{Q}$. By our discussion in §2, this proves Theorem 1.

4.2. **Proof of Theorem 2.**

Continue to let $S = \mathbb{C}[y_0, \dots, y_5]$. A homogeneous polynomial $f \in S$ is said to be *apolar* to a homogeneous ideal $I \subset S$ if

$$\langle i, f\rangle = 0 \qquad \text{for all } i \in I.$$

It is enough to check this on a set of generators for I.

Ranestad and Voisin observe [20, Lem. 1.7] that a cubic is in the image of $m^\vee \colon R_6 \to S_3$ if and only if it is apolar to ideal generated by the 2×2 minors of

$$\begin{pmatrix} y_0 & y_1 & y_2 \\ y_1 & y_3 & y_4 \\ y_2 & y_4 & y_5 \end{pmatrix},$$

which cuts out a Veronese surface. This is checked for the previous section's cubic in `thm1.m2`.

For Theorem 2, we take

$$\begin{aligned} f = y_0^3 + 2y_1y_2^2 + y_2^3 + y_0^2y_3 + 2y_0y_1y_3 + 8y_1y_2y_3 + y_0^2y_4 + 4y_1^2y_4 \\ + 8y_0y_2y_4 + y_2^2y_4 + 4y_2y_3y_4 + y_3^2y_4 + 2y_1y_4^2 + y_2y_4^2 + y_4^3 \\ + 8y_0y_1y_5 + 2y_1y_2y_5 + 4y_1y_3y_5 + 2y_2y_3y_5 + 4y_0y_4y_5 + 2y_1y_4y_5 \\ + 6y_3y_4y_5 + y_4^2y_5 + y_0y_5^2 + y_2y_5^2 + y_3y_5^2 + y_4y_5^2. \end{aligned}$$

This is apolar to the ideal generated by the 2×2 minors of the matrix

$$\begin{pmatrix} y_0 & y_1 & y_3 & y_4 \\ y_1 & y_2 & y_4 & y_5 \end{pmatrix},$$

which cuts out a quartic scroll. Apolarity can be checked by hand or with `thm2.m2`.[4]

Let $X \subset \mathbb{P}^5$ be the hypersurface cut out by f. After substituting $y_1 \mapsto \frac{1}{2}y_1$ we obtain a model of X with good reduction modulo 2. It contains the line

$$y_0 = y_2 = y_3 = y_4 = 0.$$

The point counts of X over $\mathbb{F}_{2^m}$ are given in Table 1. Thus the characteristic polynomial of Φ^* acting on $H^4_{\text{ét,prim}}(X_{\bar{k}}, \mathbb{Q}_\ell(2))$ is

$$\chi(t) = t^{22} + t^{20} + \frac{1}{2}t^{19} + \frac{1}{2}t^{18} + \frac{1}{2}t^{17} - \frac{1}{2}t^{14} - \frac{1}{2}t^{13} - \frac{3}{2}t^{12} - \frac{1}{2}t^{11} - \frac{3}{2}t^{10} - \frac{1}{2}t^{9} - \frac{1}{2}t^{8} + \frac{1}{2}t^{5} + \frac{1}{2}t^{4} + \frac{1}{2}t^{3} + t^2 + 1,$$

which is irreducible over $\mathbb{Q}$. By our discussion in §2, this proves Theorem 2.

4.3. **Proof of Theorem 3.**

The cubic fourfold X cut out by

$$\begin{aligned} f = {} & y_0^2y_1 + y_0^2y_2 + y_0y_1y_2 + y_1y_2^2 + y_2^3 + y_1^2y_3 + y_0y_2y_3 + y_0y_3^2 \\ & + y_1y_3^2 + y_0y_1y_4 + y_0y_2y_4 + y_1y_2y_4 + y_2^2y_4 + y_0y_3y_4 + y_1y_3y_4 \\ & + y_2y_3y_4 + y_0y_4^2 + y_1y_4^2 + y_4^3 + y_3^2y_5 + y_3y_4y_5 + y_4^2y_5 + y_4y_5^2 + y_5^3 \end{aligned}$$

has good reduction modulo 2. The polynomial f is apolar to the ideal

$$\langle y_0y_5,\ y_1y_5,\ y_2y_5\rangle,$$

as can be checked by hand or with `thm3.m2`. We do not review the definition of D_{rk3}, but only refer to the proof of [20, Lem. 2.1] for the fact that this implies $X \in D_{rk3}$.

The reduction of X contains the line

$$y_0 = y_1 + y_3 = y_2 = y_4 + y_5 = 0.$$

The point counts of X over $\mathbb{F}_{2^m}$ are given in Table 1. Thus the characteristic polynomial of Φ^* acting on $H^4_{\text{ét,prim}}(X_{\bar{k}}, \mathbb{Q}_\ell(2))$ is

$$\chi(t) = t^{22} - \frac{1}{2}t^{21} + \frac{3}{2}t^{20} - \frac{1}{2}t^{19} - \frac{3}{2}t^{16} + \frac{1}{2}t^{15} - t^{14} + \frac{1}{2}t^{13} + \frac{1}{2}t^{12} + \frac{1}{2}t^{11} + \frac{1}{2}t^{10} + \frac{1}{2}t^{9} - t^{8} + \frac{1}{2}t^{7} - \frac{3}{2}t^{6} - \frac{1}{2}t^{3} + \frac{3}{2}t^{2} - \frac{1}{2}t + 1.$$

which is irreducible over $\mathbb{Q}$. By our discussion in §2, this proves Theorem 3.

[4] Ranestad and Voisin gave a different definition of D_{IR} and proved that a cubic of Waring rank 10 (the maximum possible) is in D_{IR} if and only if it is apolar to a quartic scroll [20, Lem. 2.4] . Our cubic does have rank 10, as can be checked using [20, Lem. 3.18]. But in fact the rank condition can be ignored: the cubic forms that are apolar to a given quartic scroll form a linear space, in which the general one has rank 10, so D_{IR} consists of all cubics apolar to a quartic scroll, with no restriction on rank. We thank K. Ranestad for explaining this to us.

m	$\#X(\mathbb{F}_{2^m})$		
	Theorem 1	Theorem 2	Theorem 3
1	31	31	33
2	389	309	297
3	4 681	4 585	4 641
4	69 521	69 905	70 945
5	1 082 401	1 082 401	1 084 033
6	17 040 449	17 050 689	17 057 409
7	270 491 777	270 577 793	270 525 953
8	4 311 818 497	4 312 006 913	4 311 720 449
9	68 854 546 945	68 854 448 641	68 853 843 969
10	1 100 584 649 729	1 100 596 118 529	1 100 585 936 897
11	17 600 762 873 857	17 600 774 408 193	17 600 759 586 817

Table 1. Point counts.

5. Verification and implementation

Our implementation of the algorithm described in §3 is included as an ancillary file `count.cpp`. We double-checked its output very thoroughly:

- For small m, we checked the counts over $\mathbb{F}_{2^m}$ using the naive algorithm discussed at the beginning of §3.
- We checked the counts up to about $m = 9$ with a "semi-sophisticated" algorithm that projects from a point rather than a line.
- We projected from several different lines and got the same counts.
- After finding the characteristic polynomial one can predict the counts for all m. We checked these up to $m = 14$, and even $m = 15$ on a computer with much more memory than the first author's laptop.
- The characteristic polynomial of Φ^* acting on
$$H^4_{\text{ét,prim}}(X_{\bar{\mathbb{F}}_2}, \mathbb{Q}_l),$$
with no Tate twist, is $4^{22}\chi(t/4)$, and this must have integer coefficients. But even stronger, we have
$$H^4_{\text{ét,prim}}(X_{\bar{\mathbb{F}}_2}, \mathbb{Q}_l(1)) \cong H^2_{\text{ét,prim}}(F_{\bar{\mathbb{F}}_2}, \mathbb{Q}_l),$$
where F is the Fano variety of lines on X, so $2^{22}\chi(t/2)$ must have integer coefficients. We verified this.
- We used our program to count points on Elsenhans and Jahnel's cubic [10, Example 3.15], and our numbers agreed with theirs.

We conclude with a few practical comments about our implementation:

- We represented elements of $\mathbb{F}_{2^m}$ as unsigned integers, interpreting the bits as coefficients of a polynomial in $\mathbb{F}_2[x]$ modulo a fixed irreducible polynomial of degree m. Thus addition is given by "xor" and multiplication by a well-known algorithm.

- We stored multiplication in a lookup table, which sped up the program by an order of magnitude.
- We also stored division in a lookup table, as well as roots of quadratic and depressed cubic polynomials, which saved us the trouble of writing those algorithms. This did not start to use an unreasonable amount of memory until $m = 14$.
- Following [9, Alg. 15] and [16, §8], we pre-computed a list of Galois orbit representatives (and orbit sizes) in $\mathbb{F}_{2^m}$, and then touched each Galois orbit of $\mathbb{P}^2$ only once, which sped up the program by a factor of m.
- We did not bother with parallelization, although this problem is ideally suited to it.

References

[1] T. Abbott, K. Kedlaya, and D. Roe. Bounding Picard numbers of surfaces using p-adic cohomology. In *Arithmetics, geometry, and coding theory (AGCT 2005)*, volume 21 of *Sémin. Congr.*, pages 125–159. Soc. Math. France, Paris, 2010. Also math/0601508.

[2] A. Auel, M. Bernardara, M. Bolognesi, and A. Várilly-Alvarado. Cubic fourfolds containing a plane and a quintic del Pezzo surface. *Algebr. Geom.*, 1(2):181–193, 2014. Also arXiv:1205.0237.

[3] E. Bombieri and H. P. F. Swinnerton-Dyer. On the local zeta function of a cubic threefold. *Ann. Scuola Norm. Sup. Pisa (3)*, 21:1–29, 1967.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[5] F. Charles and C. Schnell. Notes on absolute Hodge classes. In *Hodge theory*, volume 49 of *Math. Notes*, pages 469–530. Princeton Univ. Press, Princeton, NJ, 2014. Also 1101.3647.

[6] E. Costa, D. Harvey, and K. Kedlaya. Zeta functions of nondegenerate toric hypersurfaces via controlled reduction in p-adic cohomology. In preparation.

[7] O. Debarre, A. Laface, and X. Roulleau. Lines on cubic hypersurfaces over finite fields. *Simons Publication Series*, to appear. Also arXiv:1510.05803.

[8] D. Dummit and R. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[9] A.-S. Elsenhans and J. Jahnel. K3 surfaces of Picard rank one and degree two. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 212–225. Springer, Berlin, 2008.

[10] A.-S. Elsenhans and J. Jahnel. On the characteristic polynomial of the Frobenius on étale cohomology. *Duke Math. J.*, 164(11):2161–2184, 2015. Also arXiv:1106.3953.

[11] W. Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge.* Springer-Verlag, Berlin, second edition, 1998.

[12] D. Grayson and M. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at `www.math.uiuc.edu/Macaulay2/`.

[13] D. Harvey. Computing zeta functions of arithmetic schemes. *Proc. Lond. Math. Soc. (3)*, 111(6):1379–1401, 2015. Also arXiv:1402.3439.

[14] B. Hassett. Cubic fourfolds, K3 surfaces, and rationality questions. Preprint, arXiv:1601.05501.

[15] B. Hassett. Special cubic fourfolds. *Compositio Math.*, 120(1):1–23, 2000. Also `math.brown.edu/~bhassett/papers/cubics/cubic.pdf`.

[16] B. Hassett, A. Várilly-Alvarado, and P. Varilly. Transcendental obstructions to weak approximation on general K3 surfaces. *Adv. Math.*, 228(3):1377–1404, 2011. Also arXiv:1005.1879.

[17] S. Mukai. Fano 3-folds. In *Complex projective geometry (Trieste, 1989/Bergen, 1989)*, volume 179 of *London Math. Soc. Lecture Note Ser.*, pages 255–263. Cambridge Univ. Press, Cambridge, 1992. Also `www.kurims.kyoto-u.ac.jp/~mukai/paper/Trieste.pdf`.

[18] J. P. Murre. On the Hodge conjecture for unirational fourfolds. *Indagationes Math. (Proc.)*, 80(3):230–232, 1977.

[19] K. Ranestad and F.-O. Schreyer. Varieties of sums of powers. *J. Reine Angew. Math.*, 525:147–181, 2000. Also math/9801110.

[20] K. Ranestad and C. Voisin. Variety of power sums and divisors in the moduli space of cubic fourfolds. *Documenta Math.*, to appear. Also arXiv:1309.1899.

[21] T. Terasoma. Complete intersections with middle Picard number 1 defined over $\mathbf{Q}$. *Math. Z.*, 189(2):289–296, 1985.

[22] R. van Luijk. An elliptic K3 surface associated to Heron triangles. *J. Number Theory*, 123(1):92–119, 2007. Also math/0411606.

[23] R. van Luijk. K3 surfaces with Picard number one and infinitely many rational points. *Algebra Number Theory*, 1(1):1–15, 2007. Also math/0506416.

[24] C. Voisin. Théorème de Torelli pour les cubiques de $\mathbb{P}^5$. *Invent. Math.*, 86(3):577–601, 1986. Also `webusers.imj-prg.fr/~claire.voisin/Articlesweb/torelli.pdf`.

[25] C. Voisin. Some aspects of the Hodge conjecture. *Jpn. J. Math.*, 2(2):261–296, 2007. Also `webusers.imj-prg.fr/~claire.voisin/Articlesweb/takagifinal.pdf`.

[26] S. Zucker. The Hodge conjecture for cubic fourfolds. *Compositio Math.*, 34(2):199–209, 1977.

Nicolas Addington, Department of Mathematics, University of Oregon, Eugene, OR 97403-1222, United States

E-mail address: `adding@uoregon.edu`

Asher Auel, Department of Mathematics, Yale University, 10 Hillhouse Avenue, New Haven, CT 06511, USA

E-mail address: `asher.auel@yale.edu`