Lines on Cubic Hypersurfaces Over Finite Fields

Olivier Debarre, Antonio Laface and Xavier Roulleau

Abstract We show that smooth cubic hypersurfaces of dimension n defined over a finite field $\mathbf{F}_q$ contain a line defined over $\mathbf{F}_q$ in each of the following cases:

- $n = 3$ and $q \geq 11$;
- $n = 4$, and $q = 2$ or $q \geq 5$;
- $n \geq 5$.

For a smooth cubic threefold X, the variety of lines contained in X is a smooth projective surface $F(X)$ for which the Tate conjecture holds, and we obtain information about the Picard number of $F(X)$ and the 5-dimensional principally polarized Albanese variety $A(F(X))$.

Keywords Cubic hypersurfaces · Lines in hypersurfaces · Finite fields · Zeta functions · Tate conjecture · Fano varieties

1991 Mathematics Subject Classification 14G15 · 14J70 · 14F20 · 14G10

The second author was partially supported by Proyecto FONDECYT Regular N. 1150732 and Proyecto Anillo ACT 1415 PIA Conicyt.

O. Debarre (✉)
Département Mathématiques et Applications, UMR CNRS 8553, PSL Research University, École Normale Supérieure, 45 rue d'Ulm, 75230 Paris Cedex 05, France
e-mail: olivier.debarre@ens.fr
URL: http://www.math.ens.fr/debarre/

A. Laface
Departamento de Matemática, Universidad de Concepción, Casilla 160-C, Concepción, Chile
e-mail: alaface@udec.cl

X. Roulleau
Laboratoire de Mathématiques et Applications, UMR CNRS 7348, Université de Poitiers, Téléport 2 - BP 30179, 86962 Futuroscope Chasseneuil, France
e-mail: xavier.roulleau@math.univ-poitiers.fr
URL: http://www-math.sp2mi.univ-poitiers.fr/roulleau/

F. Bogomolov et al. (eds.), *Geometry Over Nonclosed Fields*,
Simons Symposia, DOI 10.1007/978-3-319-49763-1_2

1 Introduction

The study of rational points on hypersurfaces in the projective space defined over a finite field has a long history. Moreover, if $X \subset \mathbf{P}^{n+1}$ is a (smooth) cubic hypersurface, the (smooth) variety $F(X)$ parametrizing lines contained in X is an essential tool for the study of the geometry of X. Therefore, it seems natural to investigate $F(X)$ when X is a cubic hypersurface defined over a finite field $\mathbf{F}_q$ and the first question to ask is whether X contains a line defined over $\mathbf{F}_q$.

One easily finds smooth cubic surfaces defined over $\mathbf{F}_q$ containing no $\mathbf{F}_q$-lines, with q arbitrarily large. On the other hand, if $\dim(X) \geq 5$, the variety $F(X)$, when smooth, has ample anticanonical bundle, and it follows from powerful theorems of Esnault and Fakhruddin–Rajan that X always contains an $\mathbf{F}_q$-line (Sect. 6). So the interesting cases are when $\dim(X) = 3$ or 4.

When X is a smooth cubic threefold, $F(X)$ is a smooth surface of general type. Using a recent formula of Galkin–Shinder which relates the number of $\mathbf{F}_q$-points on $F(X)$ with the number of $\mathbf{F}_q$- and $\mathbf{F}_{q^2}$-points on X (Sect. 2.3), we find the zeta function of $F(X)$ (Theorem 4.1). Using the Weil conjectures, we obtain that a smooth X always contains $\mathbf{F}_q$-lines when $q \geq 11$ (Theorem 4.4). $\mathbf{F}_q$-lines using a computer, we produce examples of smooth cubic threefolds containing no lines for $q \in \{2, 3, 4, 5\}$ (Sect. 4.5.4), leaving only the cases where $q \in \{7, 8, 9\}$ open, at least when X is smooth.

Theorem 4.1 can also be used for explicit computations of the zeta function of $F(X)$. For that, one needs to know the number of $\mathbf{F}_{q^r}$-points of X for sufficiently many r. Direct computations are possible for small q or when X has symmetries (see Sect. 4.5.1 for Fermat hypersurfaces, Sect. 4.5.2 for the Klein threefold, and [19] for cyclic cubic threefolds). If X contains an $\mathbf{F}_q$-line, it is in general faster to use the structure of conic bundle on X induced by projection from this line, a method initiated by Bombieri and Swinnerton-Dyer in 1967 (Sect. 4.3). This is illustrated by an example in Sect. 4.5.3, where we compute the zeta function of a cubic X and of its Fano surface $F(X)$ in characteristics up to 31. In all these examples, once one knows the zeta function of $F(X)$, the Tate conjecture (known for Fano surfaces, see Remark 4.2) gives its Picard number. It is also easy to determine whether its 5-dimensional Albanese variety $A(F(X))$ is simple, ordinary, supersingular...

Singular cubics tend to contain more lines (Example 4.17). When X is a cubic threefold with a single node, the geometry of $F(X)$ is closely related to that of a smooth genus-4 curve ([9, 20]; see also [14, Example 5.8]). Using the results of [16] on pointless curves of genus 4, we prove that X always contains $\mathbf{F}_q$-lines when $q \geq 4$ (Corollary 4.8) and produce examples for $q \in \{2, 3\}$ where X contains no $\mathbf{F}_q$-lines (Sect. 4.5.5).

When X is a smooth cubic fourfold, $F(X)$ is a smooth fourfold with trivial canonical class. Using again the Galkin–Shinder formula, we compute the zeta function of $F(X)$ (Theorem 5.1) and deduce from the Weil conjectures that X contains an $\mathbf{F}_q$-line when $q \geq 5$ (Theorem 5.2). Since the cohomology of $\mathscr{O}_{F(X)}$ is very simple (it was determined by Altman and Kleiman; see Proposition 5.3), we apply the Katz trace formula and obtain that X still contains an $\mathbf{F}_q$-line when $q = 2$ (Corollary 5.4). This leaves the cases where $q \in \{3, 4\}$ open, at least when X is smooth. We suspect that any cubic fourfold defined over $\mathbf{F}_q$ should contain an $\mathbf{F}_q$-line.

2 Definitions and Tools

2.1 The Weil and Tate Conjectures

Let $\mathbf{F}_q$ be a finite field with q elements and let ℓ be a prime number prime to q.

Let Y be a projective variety of dimension n defined over $\mathbf{F}_q$. For every integer $r \geq 1$, set

$$N_r(Y) := \mathrm{Card}\big(Y(\mathbf{F}_{q^r})\big)$$

and define the *zeta function*

$$Z(Y,T) := \exp\Big(\sum_{r\geq 1} N_r(Y)\frac{T^r}{r}\Big).$$

Let $\overline{\mathbf{F}_q}$ be an algebraic closure of $\mathbf{F}_q$ and let $\overline{Y}$ be the variety obtained from Y by extension of scalars from $\mathbf{F}_q$ to $\overline{\mathbf{F}_q}$. The Frobenius morphism $F\colon \overline{Y} \to \overline{Y}$ acts on the étale cohomology $H^\bullet(\overline{Y}, \mathbf{Q}_\ell)$ by a $\mathbf{Q}_\ell$-linear map which we denote by F^*. We have Grothendieck's Lefschetz Trace formula ([22, Theorem 13.4, p. 292]): for all integers $r \geq 1$,

$$N_r(Y) = \sum_{0\leq i\leq 2n} (-1)^i \,\mathrm{Tr}\big(F^{*r}, H^i(\overline{Y}, \mathbf{Q}_\ell)\big). \tag{1}$$

If Y is moreover smooth, the Weil conjectures proved by Deligne in [10, Théorème (1.6)] say that for each i, the (monic) characteristic polynomial

$$Q_i(Y,T) := \det\big(T\,\mathrm{Id} - F^*, H^i(\overline{Y}, \mathbf{Q}_\ell)\big)$$

has integral coefficients and is independent of ℓ; in particular, so is its degree $b_i(Y) := h^i(\overline{Y}, \mathbf{Q}_\ell)$, called the *i-th Betti number* of Y. All the conjugates of its complex roots ω_{ij} have modulus $q^{i/2}$. Poincaré duality implies $b_{2n-i}(Y) = b_i(Y)$ and $\omega_{2n-i,j} = q^n/\omega_{ij}$ for all $1 \leq j \leq b_i(Y)$.

We can rewrite the trace formula (1) as

$$N_r(Y) = \sum_{0\leq i\leq 2n} (-1)^i \sum_{j=1}^{b_i(Y)} \omega_{ij}^r \tag{2}$$

or

$$Z(Y,T) = \prod_{0\le i\le 2n} P_i(Y,T)^{(-1)^{i+1}}. \tag{3}$$

Finally, it is customary to introduce the polynomials

$$P_i(Y,T) := \det\big(\mathrm{Id} - TF^*, H^i(\overline{Y}, \mathbf{Q}_\ell)\big) = T^{b_i(Y)} Q_i\Big(Y, \frac{1}{T}\Big) = \prod_{j=1}^{b_i(Y)} (1-\omega_{ij}T). \tag{4}$$

Whenever i is odd, the real roots of $Q_i(Y,T)$ have even multiplicities ([11, Theorem 1.1.(b)]), hence $b_i(Y)$ is even. We can therefore assume $\omega_{i,j+b_i(Y)/2} = \bar{\omega}_{ij}$ for all $1 \le j \le b_i(Y)/2$, or $T^{b_i(Y)} Q_i(Y, q^i/T) = q^{ib_i(Y)/2} Q_i(Y,T)$. If $m := b_1(Y)/2$, we will write

$$Q_1(Y,T) = T^{2m} + a_1T^{2m-1} + \cdots + a_mT^m + qa_mT^{m+1} + \cdots + q^{m-1}a_1T + q^m. \tag{5}$$

The Tate conjecture for divisors on Y states that the $\mathbf{Q}_\ell$-vector space in $H^2\big(\overline{Y}, \mathbf{Q}_\ell(1)\big)$ generated by classes of $\mathbf{F}_q$-divisors is equal to the space of $\mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$-invariants classes and that its dimension is equal to the multiplicity of q as a root of the polynomial $Q_2(Y,T)$ ([29, Conjecture 2, p. 104]).

2.2 The Katz Trace Formula

Let Y be a proper scheme of dimension n over $\mathbf{F}_q$. The endomorphism $f \mapsto f^q$ of $\mathscr{O}_Y$ induces an $\mathbf{F}_q$-linear endomorphism $\mathfrak{F}_q$ of the $\mathbf{F}_q$-vector space $H^\bullet(Y, \mathscr{O}_Y)$ and for all $r \ge 1$, one has ([18], Corollaire 3.2)

$$N_r(Y)\cdot 1_{\mathbf{F}_q} \equiv \sum_{j=0}^{n} (-1)^j \,\mathrm{Tr}\big(\mathfrak{F}_q^r, H^j(Y, \mathscr{O}_Y)\big) \qquad \text{in } \mathbf{F}_q. \tag{6}$$

In particular, the right side, which is a priori in $\mathbf{F}_q$, is actually in the prime subfield of $\mathbf{F}_q$.

2.3 The Galkin–Shinder Formulas

Let $X \subset \mathbf{P}^{n+1}_{\mathbf{F}_q}$ be a reduced cubic hypersurface defined over $\mathbf{F}_q$, with singular set $\mathrm{Sing}(X)$.

We let $F(X) \subset \mathrm{Gr}(1, \mathbf{P}^{n+1}_{\mathbf{F}_q})$ be the scheme of lines contained in X, also defined over $\mathbf{F}_q$. When $n \ge 3$ and $\mathrm{Sing}(X)$ is finite, $F(X)$ is a local complete intersection of dimension $2n-4$, smooth if X is smooth, and geometrically connected ([2, Theorem 1.3 and Corollary 1.12]).

In the Grothendieck ring of varieties over $\mathbf{F}_q$, one has the relation ([14, Theorem 5.1])

$$\mathbb{L}^2[F(X)] = [X^{(2)}] - (1+\mathbb{L}^n)[X] + \mathbb{L}^n[\mathrm{Sing}(X)], \tag{7}$$

where $X^{(2)} := X^2/\mathfrak{S}_2$ is the symmetric square of X and, as usual, $\mathbb{L}$ denotes the class of the affine line. Together with the relation [14, (2.5)], it implies that, for all $r \geq 1$, we have ([14, Corollary 5.2.3)])

$$N_r\big(F(X)\big) = \frac{N_r(X)^2 - 2(1+q^{nr})N_r(X) + N_{2r}(X)}{2q^{2r}} + q^{(n-2)r}N_r\big(\mathrm{Sing}(X)\big). \tag{8}$$

2.4 Abelian Varieties Over Finite Fields

Let A be an abelian variety of dimension n defined over a finite field $\mathbf{F}_q$ of characteristic p and let ℓ be a prime number prime to p. The $\mathbf{Z}_\ell$-module $H^1(\overline{A}, \mathbf{Z}_\ell)$ is free of rank $2n$ and there is an isomorphism

$$\textstyle\bigwedge^\bullet H^1(\overline{A}, \mathbf{Q}_\ell) \xrightarrow{\sim} H^\bullet(\overline{A}, \mathbf{Q}_\ell) \tag{9}$$

of $\mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$-modules.

An elliptic curve E defined over $\overline{\mathbf{F}_q}$ is *supersingular* if its only p-torsion point is 0. All supersingular elliptic curves are isogenous. The abelian variety A is *supersingular* if $A_{\overline{\mathbf{F}_q}}$ is isogenous to E^n, where E is a supersingular elliptic curve (in particular, any two supersingular abelian varieties are isogenous over $\overline{\mathbf{F}_q}$). The following conditions are equivalent ([15, Theorems 110, 111, and 112])

(i) A is supersingular;
(ii) $Q_1(A_{\mathbf{F}_{q^r}}, T) = (T \pm q^{r/2})^{2n}$ for some $r \geq 1$;
(iii) $\mathrm{Card}\big(A(\mathbf{F}_{q^r})\big) = (q^{r/2} \pm 1)^{2n}$ for some $r \geq 1$;
(iv) each complex root of $Q_1(A, T)$ is $\sqrt{q}$ times a root of unity;
(v) in the notation of (5), if $q = p^r$, one has $p^{\lceil rj/2\rceil} \mid a_j$ for all $j \in \{1, \ldots, n\}$.

If condition (ii) is satisfied, one has $Q_2(A_{\mathbf{F}_{q^r}}, T) = (T - q^r)^{n(2n-1)}$ and the Tate conjecture, which holds for divisors on abelian varieties, implies that the Picard number of $A_{\mathbf{F}_{q^r}}$, hence also the geometric Picard number of A, is $n(2n-1)$, the maximal possible value. Conversely, when $n > 1$, if $A_{\mathbf{F}_{q^r}}$ has maximal Picard number for some r, the abelian variety A is supersingular.

The abelian variety A is *ordinary* if it contains p^n (the maximal possible number) p-torsion $\overline{\mathbf{F}_q}$-points. This is equivalent to the coefficient a_n of T^n in $Q_1(A, T)$ being prime to p; if this is the case, A is simple (over $\mathbf{F}_q$) if and only if the polynomial $Q_1(A, T)$ is irreducible (see [17, Sect. 2]).

3 Cubic Surfaces

There exist smooth cubic surfaces defined over $\mathbf{F}_q$ containing no $\mathbf{F}_q$-lines, with q arbitrarily large. This is the case for example for the diagonal cubics defined by

$$x_1^3 + x_2^3 + x_3^3 + ax_4^3 = 0,$$

where $a \in \mathbf{F}_q$ is not a cube. If $q \equiv 1 \pmod 3$, there is such an a, since there are elements of order 3 in $\mathbf{F}_q^\times$, hence the morphism $\mathbf{F}_q^\times \to \mathbf{F}_q^\times$, $x \mapsto x^3$ is not injective, hence not surjective.

4 Cubic Threefolds

4.1 The Zeta Function of the Surface of Lines

Let $X \subset \mathbf{P}^4_{\mathbf{F}_q}$ be a *smooth* cubic hypersurface defined over $\mathbf{F}_q$. Its Betti numbers are 1, 0, 1, 10, 1, 0, 1, and the eigenvalues of the Frobenius morphism acting on the 10-dimensional vector space $H^3(\overline{X}, \mathbf{Q}_\ell)$ are all divisible by q as algebraic integers ([18, Remark 5.1]). We can therefore write (1) as

$$N_r(X) = 1 + q^r + q^{2r} + q^{3r} - q^r \sum_{j=1}^{10} \omega_j^r,$$

where, by the Weil conjectures proved by Deligne (Sect. 2.1), the complex algebraic integers ω_j (and all their conjugates) have modulus $\sqrt{q}$. The trace formula (3) reads

$$Z(X, T) = \frac{P_3(X, T)}{(1-T)(1-qT)(1-q^2T)(1-q^3T)},$$

where $P_3(X, T) = \prod_{j=1}^{10}(1 - q\omega_j T)$. If we set

$$M_r(X) := \frac{1}{q^r}\big(N_r(X) - (1 + q^r + q^{2r} + q^{3r})\big) = -\sum_{j=1}^{10} \omega_j^r, \tag{10}$$

we obtain

$$P_3(X,T) = \exp\Big(\sum_{r\ge 1} M_r(X)\frac{(qT)^r}{r}\Big). \tag{11}$$

We will show in Sect. 4.3 that the numbers $M_r(X)$ have geometric significance.

Theorem 4.1 *Let $X \subset \mathbf{P}^4_{\mathbf{F}_q}$ be a* smooth *cubic hypersurface defined over $\mathbf{F}_q$ and let $F(X)$ be the smooth surface of lines contained in X. With the notation (4), we have*

$$P_1(F(X),T) = P_3(X,T/q) =: \prod_{1\le j\le 10}(1-\omega_j T),$$

$$P_2(F(X),T) = \prod_{1\le j<k\le 10}(1-\omega_j\omega_k T),$$

$$P_3(F(X),T) = P_3(X,T) = \prod_{1\le j\le 10}(1-q\omega_j T),$$

where the complex numbers $\omega_1,\dots,\omega_{10}$ have modulus $\sqrt{q}$. In particular,

$$Z(F(X),T) = \frac{\prod_{1\le j\le 10}(1-\omega_j T)\prod_{1\le j\le 10}(1-q\omega_j T)}{(1-T)(1-q^2T)\prod_{1\le j<k\le 10}(1-\omega_j\omega_k T)}. \tag{12}$$

Proof There are several ways to prove this statement. The first is to prove that there are isomorphisms

$$H^3(\overline{X},\mathbf{Q}_\ell) \xrightarrow{\sim} H^1\big(\overline{F(X)},\mathbf{Q}_\ell(-1)\big) \quad \text{and} \quad \bigwedge^2 H^1(\overline{F(X)},\mathbf{Q}_\ell) \xrightarrow{\sim} H^2(\overline{F(X)},\mathbf{Q}_\ell)$$

of $\mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$-modules. The first isomorphism holds with $\mathbf{Z}_\ell$-coefficients: if we introduce the incidence variety $I = \{(L,x) \in F(X)\times X \mid x \in L\}$ with its projections $\mathrm{pr}_1\colon I \to F(X)$ and $\mathrm{pr}_2\colon I \to X$, it is given by $\mathrm{pr}_{1*}\mathrm{pr}_2^*$ ([8, p. 256]). The second isomorphism follows, by standard arguments using smooth and proper base change, from the analogous statement in singular cohomology, over $\mathbf{C}$, which is proven in [25, Proposition 4].

These isomorphisms (and Poincaré duality) then imply the formulas for the polynomials $P_i(F(X),T)$ given in the theorem.

Alternatively, simply substituting in the definition of $Z(F(X),T)$ the values for $N_r(F(X))$ given by the Galkin–Shinder formula (8) directly gives (12), from which one deduces the formulas for the polynomials $P_i(F(X),T)$. □

Remark 4.2 (The Tate conjecture for $F(X)$) The Tate conjecture for the surface $F(X)$ (see Sect. 2.1) was proved in [25] over any field $\mathbf{k}$ of finite type over the prime field, *of characteristic other than* 2. This last restriction can in fact be lifted as follows: the proof in [25] rests on the following two facts

(a) $F(X)$ maps to its (5-dimensional) Albanese variety $A(F(X))$ onto a surface with class a multiple of θ^3, where θ is a principal polarization on $A(F(X))$;

(b) $b_2(A(F(X))) = b_2(F(X))$.

Item (a) is proved (in characteristic $\neq 2$) via the theory of Prym varieties ([4, Proposition 7]). For item (b), we have $\dim(A(F(X))) = h^1(F(X), \mathscr{O}_{F(X)}) = 5$ ([2, Proposition (1.15)]), hence $b_2(A(F(X))) = \binom{2\dim(A(X))}{2} = 45$, whereas $b_2(F(X)) = \deg\big(P_2(F(X),T)\big) = 45$ by Theorem 4.1.

To extend (a) to all characteristics, we consider X as the reduction modulo the maximal ideal $\mathfrak{m}$ of a smooth cubic $\mathscr{X}$ defined over a valuation ring of characteristic zero. There is a "difference morphism" $\delta_{F(X)}\colon F(X)\times F(X)\to A(F(X))$, defined over $\mathbf{k}$, which is the reduction modulo $\mathfrak{m}$ of the analogous morphism $\delta_{F(\mathscr{X})}\colon F(\mathscr{X})\times F(\mathscr{X})\to A\big(F(\mathscr{X})\big)$. By [4, Proposition 5], the image of $\delta_{F(\mathscr{X})}$ is a divisor which defines a principal polarization ϑ on $A\big(F(\mathscr{X})\big)$, hence the image of $\delta_{F(X)}$ is also a principal polarization on $A(F(X))$, defined over $\mathbf{k}$.

Since the validity of the Tate conjecture is not affected by passing to a finite extension of $\mathbf{k}$, we may assume that $F(X)$ has a $\mathbf{k}$-point, which we lift to $F(\mathscr{X})$. We can then define Albanese morphisms, and $a_{F(X)}\colon F(X)\to A(F(\mathscr{X}))$ is the reduction modulo $\mathfrak{m}$ of $a_{F(\mathscr{X})}\colon F(\mathscr{X})\to A(F(\mathscr{X}))$. The image of $a_{\mathscr{X}}$ has class $\vartheta^3/3!$ ([4, Proposition 7]), hence the image of $a_{F(X)}$ also has class $(\vartheta|_{A(X)})^3/3!$ (this class is not divisible in $H^6(A(X),\mathbf{Z}_\ell)$, hence $a_{F(X)}$ is generically injective). This proves (a), hence the Tate conjecture for $F(X)$, in all characteristics.

Going back to the case where $\mathbf{k}$ is finite, Theorem 4.1 implies the equality $Q_2(F(X),T) = Q_2(A(F(X)),T)$. Since the Tate conjecture holds for divisors on abelian varieties, this proves that $F(X)$ and $A(F(X))$ have the same Picard numbers, whose maximal possible value is 45.

Corollary 4.3 *Let $2m_\pm$ be the multiplicity of the root $\pm\sqrt{q}$ of $Q_1(F(X),T)$ and let $m_1,\dots,m_c$ be the multiplicities of the pairs of non-real conjugate roots of $Q_1(F(X),T)$, so that $m_+ + m_- + \sum_{i=1}^{c} m_i = 5$. The Picard number of $F(X)$ is then*

$$\rho(F(X)) = m_+(2m_+ - 1) + m_-(2m_- - 1) + \sum_{i=1}^{c} m_i^2.$$

We have $\rho(F(X)) \geq 5$, with equality if and only if $Q_1(F(X),T)$ has no multiple roots.

If q is not a square, the possible Picard numbers are all odd numbers between 5 and 13, 17, and 25.

If q is a square, the possible Picard numbers are all odd numbers between 5 and 21, 25, 29, and 45. We have $\rho(F(X)) = 45$ if and only if $Q_1(F(X),T) = (T\pm\sqrt{q})^{10}$.

Proof The Tate conjecture holds for divisors on $F(X)$ (Remark 4.2). As explained at the end of Sect. 2.1, it says that the rank of the Picard group is the multiplicity of q as a root of $Q_2(F(X),T)$. The remaining statements then follow from Theorem 4.1 by inspection of all possible cases for the values of $m_+, m_-, m_1, \dots, m_c$. □

4.2 Existence of Lines on Smooth Cubic Threefolds Over Large Finite Fields

We can now bound the number of $\mathbf{F}_q$-lines on a smooth cubic threefold defined over $\mathbf{F}_q$.

Theorem 4.4 *Let X be a smooth cubic threefold defined over $\mathbf{F}_q$ and let $N_1(F(X))$ be the number of $\mathbf{F}_q$-lines contained in X. We have*

$$N_1(F(X)) \geq \begin{cases} 1+45q+q^2-10(q+1)\sqrt{q} & \text{if } q \geq 64; \\ 1+13q+q^2-6(q+1)\sqrt{q} & \text{if } 16 \leq q \leq 61; \\ 1-3q+q^2-2(q+1)\sqrt{q} & \text{if } q \leq 13. \end{cases}$$

In particular, X contains at least 10 $\mathbf{F}_q$-lines if $q \geq 11$.

Moreover, for all q,

$$N_1(F(X)) \leq 1+45q+q^2+10(q+1)\sqrt{q}.$$

Proof As we saw in Sect. 2.1, we can write the roots of $Q_1(F(X),T)$ as $\omega_1,\dots,\omega_5$, $\overline{\omega}_1,\dots,\overline{\omega}_5$. The $r_j := \omega_j+\overline{\omega}_j$ are then real numbers in $[-2\sqrt{q}, 2\sqrt{q}]$ and, by (2) and Theorem 4.1, we have

$$\begin{aligned} N_1\bigl(F(X)\bigr) &= 1-\sum_{1\leq j\leq 5} r_j + 5q + \sum_{1\leq j<k\leq 5} (\omega_j\omega_k+\overline{\omega}_j\omega_k+\omega_j\overline{\omega}_k+\overline{\omega}_j\overline{\omega}_k) - \sum_{1\leq j\leq 5} qr_j + q^2 \\ &= 1+5q+q^2-(q+1)\sum_{1\leq j\leq 5} r_j + \sum_{1\leq j<k\leq 5} r_j r_k \\ &=: F_q(r_1,\dots,r_5). \end{aligned}$$

Since the real function $F_q\colon [-2\sqrt{q}, 2\sqrt{q}]^5 \to \mathbf{R}$ is *linear in each variable,* its extrema are reached on the boundary of its domain, i.e., at one of the points $2\sqrt{q}\,(\pm 1,\dots,\pm 1)$. At such a point $\mathbf{r}_l$ (with l positive coordinates), we have

$$F_q(\mathbf{r}_l) = 1+5q+q^2-2(2l-5)(q+1)\sqrt{q}+\frac{1}{2}\bigl(4q(2l-5)^2-20q\bigr).$$

The minimum is obviously reached for $l \in \{3,4,5\}$, the maximum for $l=0$, and the rest is easy. □

4.3 Computing Techniques: The Bombieri–Swinnerton-Dyer Method

By Theorem 4.1, the zeta function of the surface $F(X)$ of lines contained in a smooth cubic threefold $X \subset \mathbf{P}^4_{\mathbf{F}_q}$ defined over $\mathbf{F}_q$ is completely determined by the roots

$q\omega_1, \dots, q\omega_{10}$ of the degree-10 characteristic polynomial of the Frobenius morphism acting on $H^3(\overline{X}, \mathbf{Q}_\ell)$. If one knows the numbers of points of X over sufficiently many finite extensions of $\mathbf{F}_q$, these roots can be computed from the relations

$$\exp\Big(\sum_{r\geq 1} M_r(X)\frac{T^r}{r}\Big) = P_3(X, T/q) = P_1(F(X), T) = \prod_{1\leq j\leq 10}(1-\omega_j T),$$

where $M_r(X) = \frac{1}{q^r}\big(N_r(X) - (1 + q^r + q^{2r} + q^{3r})\big)$ was defined in (10).

The reciprocity relation (5) implies that the polynomial $P_1(F(X), T)$ is determined by the coefficients of $1, T, \dots, T^5$, hence by the numbers $N_1(X), \dots, N_5(X)$. The direct computation of these numbers is possible (with a computer) when q is small (see Sect. 4.5 for examples), but the amount of calculations quickly becomes very large.

We will explain a method for computing directly the numbers $M_1(X), \dots, M_5(X)$. It was first introduced in [5] and uses a classical geometric construction which expresses the blow up of X along a line as a conic bundle. It is valid only in characteristics $\neq 2$ and requires X to contain an $\mathbf{F}_q$-line L.

Let $\widetilde{X} \to X$ be the blow up of L. Projecting from L induces a morphism $\pi_L : \widetilde{X} \to \mathbf{P}^2_{\mathbf{F}_q}$ which is a conic bundle and we denote by $\Gamma_L \subset \mathbf{P}^2_{\mathbf{F}_q}$ its discriminant curve, defined over $\mathbf{F}_q$. *Assume from now on that q is odd;* the curve Γ_L is then a nodal plane quintic curve and the associated double cover $\rho\colon \widetilde{\Gamma}_L \to \Gamma_L$ is admissible in the sense of [3, Définition 0.3.1] (the curve $\widetilde{\Gamma}_L$ is nodal and the fixed points of the involution associated with ρ are exactly the nodes of $\widetilde{\Gamma}_L$; [5, Lemma 2]).[1]

One can then define the Prym variety associated with ρ and it is isomorphic to the Albanese variety of the surface $F(X)$ ([24, Theorem 7] when Γ_L is smooth). The following is [5, Formula (18)].

Proposition 4.5 *Let $X \subset \mathbf{P}^4_{\mathbf{F}_q}$ be a smooth cubic threefold defined over $\mathbf{F}_q$, with q odd, and assume that X contains an $\mathbf{F}_q$-line L. With the notation (10), we have, for all $r \geq 1$,*

$$M_r(X) = N_r(\widetilde{\Gamma}_L) - N_r(\Gamma_L).$$

Proof We will go quickly through the proof of [5] because it is the basis of our algorithm. A point $x \in \mathbf{P}^2(\mathbf{F}_q)$ corresponds to an $\mathbf{F}_q$-plane $P_x \supset L$ and the fiber $\pi_L^{-1}(x)$ is isomorphic to the conic C_x such that $X \cap P_x = L + C_x$. We have four cases:

(i) either C_x is geometrically irreducible, i.e., $x \notin \Gamma_L(\mathbf{F}_q)$, in which case $\pi_L^{-1}(x)(\mathbf{F}_q)$ consists of $q+1$ points;
(ii) or C_x is the union of two different $\mathbf{F}_q$-lines, i.e., x is smooth on Γ_L and the 2 points of $\rho^{-1}(x)$ are in $\widetilde{\Gamma}_L(\mathbf{F}_q)$, in which case $\pi_L^{-1}(x)(\mathbf{F}_q)$ consists of $2q+1$ points;

[1]In characteristic 2, the curves Γ_L and $\widetilde{\Gamma}_L$ might not be nodal (see Lemma 4.13).

(iii) or C_x is the union of two different conjugate $\mathbf{F}_{q^2}$-lines, i.e., x is smooth on Γ_L and the 2 points of $\rho^{-1}(x)$ are *not* in $\widetilde{\Gamma}_L(\mathbf{F}_q)$, in which case $\pi_L^{-1}(x)(\mathbf{F}_q)$ consists of 1 point;

(iv) or C_x is twice an $\mathbf{F}_q$-line, i.e., x is singular on Γ_L, in which case $\pi_L^{-1}(x)(\mathbf{F}_q)$ consists of $q+1$ points.

The total number of points of $\widetilde{\Gamma}_L(\mathbf{F}_q)$ lying on a degenerate conic C_x is therefore $qN_1(\widetilde{\Gamma}_L) + N_1(\Gamma_L)$ and we obtain

$$N_1(\widetilde{X}) = (q+1)\big(N_1(\mathbf{P}^2_{\mathbf{F}_q}) - N_1(\Gamma_L)\big) + qN_1(\widetilde{\Gamma}_L) + N_1(\Gamma_L).$$

Finally, since each point on $L \subset X$ is replaced by a $\mathbf{P}^1_{\mathbf{F}_q}$ on $\widetilde{X}$, we have

$$N_1(\widetilde{X}) = N_1(X) - (q+1) + (q+1)^2,$$

thus $N_1(X) = q^3 + q^2 + q + 1 + q\big(N_1(\widetilde{\Gamma}_L) - N_1(\Gamma_L)\big)$. Since the same conclusion holds upon replacing q with q^r, this proves the proposition. □

Let $x \in \Gamma_L(\mathbf{F}_q)$. In order to compute the numbers $N_1(\Gamma_L) - N_1(\widetilde{\Gamma}_L)$, we need to understand when the points of $\rho^{-1}(x)$ are defined over $\mathbf{F}_q$.

We follow [5, p. 6]. Take homogenous $\mathbf{F}_q$-coordinates $x_1, \dots, x_5$ on $\mathbf{P}^4$ so that L is given by the equations $x_1 = x_2 = x_3 = 0$. The equation of the cubic X can then be written as

$$f + 2q_1x_4 + 2q_2x_5 + \ell_1x_4^2 + 2\ell_2x_4x_5 + \ell_3x_5^2 = 0,$$

where f is a cubic form, q_1, q_2 are quadratic forms, and ℓ_1, ℓ_2, ℓ_3 are linear forms in the variables x_1, x_2, x_3. We choose the plane $\mathbf{P}^2_{\mathbf{F}_q} \subset \mathbf{P}^4_{\mathbf{F}_q}$ defined by $x_4 = x_5 = 0$. If $x = (x_1, x_2, x_3, 0, 0) \in \mathbf{P}^2_{\mathbf{F}_q}$, the conic C_x considered above is defined by the equation

$$fy_1^2 + 2q_1y_1y_2 + 2q_2y_1y_3 + \ell_1y_2^2 + 2\ell_2y_2y_3 + \ell_3y_3^2 = 0$$

and the quintic $\Gamma_L \subset \mathbf{P}^2_{\mathbf{F}_q}$ is defined by the equation $\det(M_L) = 0$, where

$$M_L := \begin{pmatrix} f & q_1 & q_2 \\ q_1 & \ell_1 & \ell_2 \\ q_2 & \ell_2 & \ell_3 \end{pmatrix}. \tag{13}$$

For each $i \in \{1, 2, 3\}$, let $\delta_i \in H^0\big(\Gamma_L, \mathscr{O}(a_i)\big)$, where $a_i = 2, 4$, or 4, be the determinant of the submatrix of M_L obtained by deleting its ith row and ith column. The $-\delta_i$ are transition functions of an invertible sheaf $\mathscr{L}$ on Γ_L such that $\mathscr{L}^{\otimes 2} = \omega_{\Gamma_L}$ (a theta characteristic). It defines the double cover $\rho\colon \widetilde{\Gamma}_L \to \Gamma_L$.

A point $x \in \mathbf{P}^2_{\mathbf{F}_q}$ is singular on Γ_L if and only if $\delta_1(x) = \delta_2(x) = \delta_3(x) = 0$. These points do not contribute to M_r since the only point of $\rho^{-1}(x)$ is defined over the field of definition of x. This is the reason why we may assume that x is smooth in the next proposition.

Proposition 4.6 *Let x be a smooth $\mathbf{F}_q$-point of Γ_L. The curve $\widetilde{\Gamma}_L$ has two $\mathbf{F}_q$-points over $x \in \Gamma_L(\mathbf{F}_q)$ if and only if either $-\delta_1(x) \in (\mathbf{F}_q^\times)^2$, or $\delta_1(x) = 0$ and either $-\delta_2(x)$ or $-\delta_3(x)$ is in $(\mathbf{F}_q^\times)^2$.*

Proof With the notation above, the line $L = V(y_1) \subset \mathbf{P}^2_{\mathbf{F}_q}$ meets the conic $C_x \subset \mathbf{P}^2_{\mathbf{F}_q}$ at the points $(0, y_2, y_3)$ such that

$$\ell_1 y_2^2 + 2\ell_2 y_2 y_3 + \ell_3 y_3^2 = 0.$$

Therefore, if $-\delta_1(x) = \ell_2^2(x) - \ell_1(x)\ell_3(x)$ is non-zero, the curve $\widetilde{\Gamma}_L$ has two rational points over $x \in \Gamma_L(\mathbf{F}_q)$ if and only if $-\delta_1(x) \in (\mathbf{F}_q^\times)^2$.

When $\delta_1(x) = 0$, we have $C_x = L_1 + L_2$, where L_1 and L_2 are lines meeting in an $\mathbf{F}_q$-point z of L which we assume to be $(0, 0, 1)$. This means that there is no y_3 term in the equation of C_x, hence $\ell_2(x) = \ell_3(x) = q_2(x) = 0$. The conic C_x is defined by the equation

$$\ell_1(x)y_2^2 + 2q_1(x)y_1y_2 + f(x)y_1^2 = 0$$

and the two lines L_1 and L_2 are defined over $\mathbf{F}_q$ if and only if $-\delta_3(x) = q_1^2(x) - \ell_1(x)f(x) \in (\mathbf{F}_q^\times)^2$ (since $\delta_1(x) = \delta_2(x) = 0$, this is necessarily non-zero because x is smooth on Γ_L).

For the general case: if $y_3(z) \neq 0$, we make a linear change of coordinates $y_1 = y_1'$, $y_2 = y_2' + ty_3'$, $y_3 = y_3'$ in order to obtain $y_2'(z) = 0$, and we check that $-\delta_3(x)$ is unchanged; if $z = (0, 1, 0)$, we obtain as above $\delta_1(x) = \delta_3(x) = 0$ and L_1 and L_2 are defined over $\mathbf{F}_q$ if and only if $-\delta_2(x) \in (\mathbf{F}_q^\times)^2$. This proves the proposition. □

We can now describe our algorithm for the computation of the numbers $M_r(X) = N_r(\widetilde{\Gamma}_L) - N_r(\Gamma_L)$.

The input data is a cubic threefold X over $\mathbf{F}_q$ containing an $\mathbf{F}_q$-line L. We choose coordinates as above and construct the matrix M_L of (13) whose determinant is the equation of the quintic $\Gamma_L \subset \mathbf{P}^2_{\mathbf{F}_q}$. We compute M_r with the following simple algorithm.

Input: (X, L, r)
Output: M_r
Compute the matrix M_L, the three minors $\delta_1, \delta_2, \delta_3$ and the curve Γ_L;
$M_r := 0$;
while $p \in \{p \,:\, p \in \Gamma_L(\mathbf{F}_{q^r}) \mid \Gamma_L$ *is smooth at* $p\}$ **do**
    if $-\delta_1(p) \in (\mathbf{F}_{q^r}^\times)^2$ *or* $(\delta_1(p) = 0$ *and* $(-\delta_2(p) \in (\mathbf{F}_{q^r}^\times)^2$ *or* $-\delta_3(p) \in (\mathbf{F}_{q^r}^\times)^2))$ **then**
        $M_r := M_r + 1$;
    else
        $M_r := M_r - 1$;
    end
end
return M_r;

Algorithm 1: Computing M_r

4.4 Lines on Mildly Singular Cubic Threefolds

We describe a method based on results of Clemens–Griffiths and Kouvidakis–van der Geer which reduces the computation of the number of $\mathbf{F}_q$-lines on a cubic threefold with a single singular point, of type A_1 or A_2,[2] to the computation of the number of points on a smooth curve of genus 4. One consequence is that there is always an $\mathbf{F}_q$-line when $q > 3$.

Let C be a smooth non-hyperelliptic curve of genus 4 defined over a perfect field $\mathbf{F}$. We denote by g^1_3 and $h^1_3 = K_C - g^1_3$ the (possibly equal) degree-3 pencils on C. The canonical curve $\phi_{K_C}(C) \subset \mathbf{P}^3_{\mathbf{F}}$ is contained in a unique geometrically integral quadric surface Q whose rulings cut out the degree-3 pencils on C; more precisely,

- either $Q \simeq \mathbf{P}^1_{\mathbf{F}} \times \mathbf{P}^1_{\mathbf{F}}$ and the two rulings of Q cut out distinct degree-3 pencils g^1_3 and $h^1_3 = K_C - g^1_3$ on C which are defined over $\mathbf{F}$;
- or Q is smooth but its two rulings are defined over a quadratic extension of $\mathbf{F}$ and are exchanged by the Galois action, and so are g^1_3 and h^1_3;
- or Q is singular and its ruling cuts out a degree-3 pencil g^1_3 on C which is defined over $\mathbf{F}$ and satisfies $K_C = 2g^1_3$.

Let $\rho\colon \mathbf{P}^3_{\mathbf{F}} \dashrightarrow \mathbf{P}^4_{\mathbf{F}}$ be the rational map defined by the linear system of cubics containing $\phi_{K_C}(C)$. The image of ρ is a cubic threefold X defined over $\mathbf{F}$; it has a single singular point, $\rho(Q)$, which is of type A_1 if Q is smooth, and of type A_2 otherwise. Conversely, every cubic threefold $X \subset \mathbf{P}^4_{\mathbf{F}}$ defined over $\mathbf{F}$ with a single singular point x, of type A_1 or A_2, is obtained in this fashion: the curve C is $\mathbf{T}_{X,x} \cap X$ and parametrizes the lines in X through x ([7, Corollary 3.3]).

The surface $F(X)$ is isomorphic to the non-normal surface obtained by gluing the images C_g and C_h of the morphisms $C \to C^{(2)}$ defined by $p \mapsto g^1_3 - p$ and $p \mapsto h^1_3 - p$ (when Q is singular, $F(X)$ has a cusp singularity along the curve $C_g = C_h$). This was proved in [9, Theorem 7.8] over $\mathbf{C}$ and in [20, Proposition 2.1] in general.

Proposition 4.7 *Let $X \subset \mathbf{P}^4_{\mathbf{F}_q}$ be a cubic threefold defined over $\mathbf{F}_q$ with a single singular point, of type A_1 or A_2. Let C be the associated curve of genus 4, with degree-3 pencils g^1_3 and h^1_3. For any $r \geq 1$, set $n_r := \mathrm{Card}(C(\mathbf{F}_{q^r}))$. We have*

$$\mathrm{Card}\big(F(X)(\mathbf{F}_q)\big) = \begin{cases} \frac12(n_1^2 - 2n_1 + n_2) & \text{if } g^1_3 \text{ and } h^1_3 \text{ are distinct and defined over } \mathbf{F}_q;\\ \frac12(n_1^2 + 2n_1 + n_2) & \text{if } g^1_3 \text{ and } h^1_3 \text{ are not defined over } \mathbf{F}_q;\\ \frac12(n_1^2 + n_2) & \text{if } g^1_3 = h^1_3. \end{cases}$$

[2] A hypersurface singularity is of type A_j if it is, locally analytically, given by an equation $x_1^{j+1} + x_2^2 + \cdots + x_{n+1}^2 = 0$. Type A_1 is also called a node.

Proof Points of $C^{(2)}(\mathbf{F}_q)$ correspond to

- the $\frac{1}{2}(n_1^2 - n_1)$ pairs of distinct points of $C(\mathbf{F}_q)$,
- the n_1 $\mathbf{F}_q$-points on the diagonal,
- the $\frac{1}{2}(n_2 - n_1)$ pairs of distinct conjugate points of $C(\mathbf{F}_{q^2})$,

for a total of $\frac{1}{2}(n_1^2 + n_2)$ points (compare with [14, (2.5)]). When g_3^1 and h_3^1 are distinct and defined over $\mathbf{F}_q$, the gluing process eliminates n_1 $\mathbf{F}_q$-points. When g_3^1 and h_3^1 are not defined over $\mathbf{F}_q$, the curves C_g and C_h contain no pairs of conjugate points, and the gluing process creates n_1 new $\mathbf{F}_q$-points. Finally, when $g_3^1 = h_3^1$, the map $C^{(2)}(\mathbf{F}_q) \to F(X)(\mathbf{F}_q)$ is a bijection. □

Corollary 4.8 *When $q \geq 4$, any cubic threefold $X \subset \mathbf{P}^4_{\mathbf{F}_q}$ defined over $\mathbf{F}_q$ with a single singular point, of type A_1 or A_2, contains an $\mathbf{F}_q$-line.*

For $q \in \{2, 3\}$, we produce in Sect. 4.5.5 explicit examples of cubic threefolds with a single singular point, of type A_1, but containing no $\mathbf{F}_q$-lines: the bound in the corollary is the best possible.

Proof Assume that X contains no $\mathbf{F}_q$-lines. Proposition 4.7 then implies that either $n_1 = n_2 = 0$, or $n_1 = n_2 = 1$ and g_3^1 and h_3^1 are distinct and defined over $\mathbf{F}_q$. The latter case cannot in fact occur: if $C(\mathbf{F}_q) = \{x\}$, we write $g_3^1 \equiv x + x' + x''$. Since g_3^1 is defined over $\mathbf{F}_q$, so is $x' + x''$, hence x' and x'' are both defined over $\mathbf{F}_{q^2}$. But $C(\mathbf{F}_{q^2}) = \{x\}$, hence $x' = x'' = x$ and $g_3^1 \equiv 3x$. We can do the same reasoning with h_3^1 to obtain $h_3^1 \equiv 3x \equiv g_3^1$, a contradiction.

Therefore, we have $n_1 = n_2 = 0$. According to [16, Theorem 1.2], every genus-4 curve over $\mathbf{F}_q$ with $q > 49$ has an $\mathbf{F}_q$-point so we obtain $q \leq 7$.

Because of the reciprocity relation (5), there is a monic degree-4 polynomial H with integral coefficients that satisfies $Q_1(C, T) = T^4 H(T + q/T)$. If $\omega_1, \ldots, \omega_4, \bar{\omega}_1, \ldots, \bar{\omega}_4$ are the roots of $Q_1(C, T)$ (see Sect. 2.4), with $|\omega_j| = \sqrt{q}$, the roots of H are the $r_j := \omega_j + \bar{\omega}_j$, and

$$q + 1 - n_1 = \sum_{1 \leq j \leq 4} r_j \quad , \quad q^2 + 1 - n_2 = \sum_{1 \leq j \leq 4} (\omega_j^2 + \bar{\omega}_j^2) = \sum_{1 \leq j \leq 4} (r_j^2 - 2q).$$

Since $n_1 = n_2 = 0$, we obtain $\sum_{1 \leq j \leq 4} r_j = q + 1$ and $\sum_{1 \leq j \leq 4} r_j^2 = q^2 + 8q + 1$, so that $\sum_{1 \leq i < j \leq 4} r_i r_j = -3q$; we can therefore write

$$H(T) = T^4 - (q+1)T^3 - 3qT^2 + aT + b. \tag{14}$$

Finally, since $|r_j| \leq 2\sqrt{q}$ for each j, we also have $|b| = |r_1 r_2 r_3 r_4| \leq 16q^2$ and $|a| = |\sum_{j=1}^4 b/r_j| \leq 32q^{3/2}$. A computer search done with these bounds shows that polynomials of the form (14) with four real roots and $q \in \{2, 3, 4, 5, 7\}$ only exist for $q \leq 3$, which proves the corollary. □

Remark 4.9 For $q \in \{2, 3\}$, the computer gives a list of all possible polynomials

$$(q=2)\quad H(T) = \begin{cases} T^4-3T^3-6T^2+24T-16 \\ T^4-3T^3-6T^2+24T-15\ (\star) \\ T^4-3T^3-6T^2+23T-13 \\ T^4-3T^3-6T^2+22T-10\ (\star) \\ T^4-3T^3-6T^2+21T-7 \\ T^4-3T^3-6T^2+18T+1\ \ (\star) \end{cases}, \quad (q=3)\quad H(T) = \begin{cases} T^4-4T^3-9T^2+48T-36\ (?) \\ T^4-4T^3-9T^2+47T-32\ (\star) \\ T^4-4T^3-9T^2+46T-29\ (\star) \\ T^4-4T^3-9T^2+44T-22\ (?) \end{cases}.$$

The nodal cubics of Sect. 4.5.5, defined over $\mathbf{F}_2$ and $\mathbf{F}_3$, correspond to the polynomials $T^4 - 3T^3 - 6T^2 + 24T - 15$ and $T^4 - 4T^3 - 9T^2 + 47T - 32$, respectively. Over $\mathbf{F}_2$, it is possible to list all genus-4 canonical curves and one obtains that only the polynomials marked with $(\star)$ actually occur (all three are irreducible).

Over $\mathbf{F}_3$, our computer searches show that the two polynomials marked with $(\star)$ actually occur (both are irreducible). We do not know whether the other two, $T^4 - 4T^3 - 9T^2 + 48T - 36 = (T-1)(T-3)(T^2-12)$ and $T^4 - 4T^3 - 9T^2 + 44T - 22 = (T^2 - 4T + 2)(T^2 - 11)$ (marked with (?)), actually occur.

4.5 Examples of Cubic Threefolds

In this section, we present some of our calculations and illustrate our techniques for some cubic threefolds. We begin with Fermat cubics (Sect. 4.5.1), which have good reduction in all characteristics but 3. The case of general Fermat hypersurfaces was worked out by Weil in [30] (and was an inspiration for his famous conjectures discussed in Sect. 2.1). We explain how Weil's calculations apply to the zeta function of Fermat cubics (Theorem 4.11) and we compute, in dimension 3, the zeta function of their surface of lines (Corollary 4.12).

The Fermat cubic threefold contains the line $L := \langle(1, -1, 0, 0, 0), (0, 0, 1, -1, 0)\rangle$ and we compute the discriminant quintic $\Gamma_L \subset \mathbf{P}^2$ defined in Sect. 4.3, exhibiting strange behavior in characteristic 2.

In Sect. 4.5.2, we turn our attention to the Klein cubic, which has good reduction in all characteristics but 11. It also contains an "obvious" line L' and we compute the discriminant quintic $\Gamma_{L'} \subset \mathbf{P}^2$, again exhibiting strange behavior in characteristic 2. Using the Bombieri–Swinnerton-Dyer method, we determine the zeta function of $F(X)$ over $\mathbf{F}_p$, for $p \le 13$. We also compute the geometric Picard numbers of the reduction of $F(X)$ modulo any prime, using the existence of an isogeny between $A(F(X))$ and the self-product of an elliptic curve.

In Sect. 4.5.3, we compute, using the same method, the zeta function of $F(X)$ of a "random" cubic threefold X containing a line, over the fields $\mathbf{F}_5$, $\mathbf{F}_7$, $\mathbf{F}_{23}$, $\mathbf{F}_{29}$, and $\mathbf{F}_{31}$. Note that existing programs are usually unable to perform calculations in such high characteristics.

In Sect. 4.5.4, we present examples, found by computer searches, of smooth cubic threefolds defined over $\mathbf{F}_2$, $\mathbf{F}_3$, $\mathbf{F}_4$, or $\mathbf{F}_5$ with no lines. We were unable to find examples over $\mathbf{F}_q$ for the remaining values $q \in \{7, 8, 9\}$ (by Theorem 4.4, there are always $\mathbf{F}_q$-lines for $q \geq 11$). For the example over $\mathbf{F}_2$, we compute directly the number of points over small extensions and deduce the polynomial P_1 for the Fano surface $F(X)$. For the example over $\mathbf{F}_3$, we obtain again the polynomial P_1 for the Fano surface $F(X)$ by applying the Bombieri–Swinnerton-Dyer method over $\mathbf{F}_9$.

Finally, in Sect. 4.5.5, we exhibit cubic threefolds with one node but no lines, defined over $\mathbf{F}_2$ or $\mathbf{F}_3$, thereby proving that the bound in Corollary 4.8 is optimal.

4.5.1 Fermat Cubics

The n-dimensional Fermat cubic $X^n \subset \mathbf{P}^{n+1}_{\mathbf{Z}}$ is defined by the equation

$$x_1^3 + \cdots + x_{n+2}^3 = 0. \tag{15}$$

It has good reduction at every prime $p \neq 3$.

Remark 4.10 In general, if $q \equiv 2 \pmod 3$ and $X \subset \mathbf{P}^{n+1}_{\mathbf{F}_q}$ is a cyclic cubic hypersurface defined by the equation $f(x_1, \ldots, x_{n+1}) + x_{n+2}^3 = 0$, the projection $\pi\colon X \to \mathbf{P}^n_{\mathbf{F}_q}$ defined by $(x_1, \ldots, x_{n+2}) \mapsto (x_1, \ldots, x_{n+1})$ induces a bijection $X(\mathbf{F}_q) \to \mathbf{P}^n(\mathbf{F}_q)$, because the map $x \mapsto x^3$ is a bijection of $\mathbf{F}_q$ ([19, Observation 1.7.2]).

The remark gives in particular $\mathrm{Card}\big(X^n(\mathbf{F}_2)\big) = \mathrm{Card}\big(\mathbf{P}^n(\mathbf{F}_2)\big) = 2^{n+1} - 1$. For the number of points of $X^n(\mathbf{F}_4)$, observe that the cyclic cover π is 3-to-1 outside its branch divisor $V(f)$. Let $(x_1, \ldots, x_{n+1}) \in \mathbf{P}^n(\mathbf{F}_4)$. Since $x^3 \in \{0, 1\}$ for any $x \in \mathbf{F}_4$, either $x_1^3 + \cdots + x_{n+1}^3 = 0$ and the inverse image by π has one $\mathbf{F}_4$-point, or $x_1^3 + \cdots + x_{n+1}^3 = 1$ and the inverse image by π has three $\mathbf{F}_4$-points. One obtains the inductive formula

$$\mathrm{Card}\big(X^n(\mathbf{F}_4)\big) = \mathrm{Card}\big(X^{n-1}(\mathbf{F}_4)\big) + 3\big(\mathrm{Card}\big(\mathbf{P}^n(\mathbf{F}_4)\big) - \mathrm{Card}\big(X^{n-1}(\mathbf{F}_4)\big)\big).$$

Since $\mathrm{Card}\big(X^0(\mathbf{F}_4)\big) = 3$, we get

$$\mathrm{Card}\big(X^n(\mathbf{F}_4)\big) = \frac{1}{3}\left(2^{2n+3} - (-2)^{n+1} - 1\right).$$

Using (8), we see that the number of $\mathbf{F}_2$-lines on $X^n_{\mathbf{F}_2}$ is

$$\frac{(2^{n+1}-1)^2 - 2(1+2^n)(2^{n+1}-1) + \frac{1}{3}(2^{2n+3} - (-2)^{n+1} - 1)}{8} = \frac{2^{2n} + 1 + ((-1)^n - 9)2^{n-2}}{3}.$$

For example, the 15 $\mathbf{F}_2$-lines contained in $X^3_{\mathbf{F}_2}$ are the line $L_{\mathbf{F}_2}$ and its images by permutations of the coordinates.

In fact, general results are available in the literature on the zeta function of Fermat hypersurfaces over finite fields (starting with [30]; see also [26, Sect. 3]), although they do not seem to have been spelled out for cubics. Let us first define

$$P_n^0(X^n_{\mathbf{F}_p}, T) = \begin{cases} P_n(X^n_{\mathbf{F}_p}, T) & \text{if } n \text{ is odd,} \\ \frac{P_n(X^n_{\mathbf{F}_p}, T)}{1-p^{n/2}T} & \text{if } n \text{ is even} \end{cases}$$

(this is the reciprocal characteristic polynomial of the Frobenius morphism acting on the *primitive* cohomology of $X^n_{\mathbf{F}_p}$) and set $b_n^0(X^n) := \deg(P_n^0)$; this is $b_n(X^n)$ if n is odd, and $b_n(X^n) - 1$ if n is even.

Theorem 4.11 (Weil) *Let $X^n \subset \mathbf{P}^{n+1}_{\mathbf{Z}}$ be the Fermat cubic hypersurface. Let p be a prime number other than* 3.

- *If $p \equiv 2 \pmod 3$, we have*

$$P_n^0(X^n_{\mathbf{F}_p}, T) = (1 - (-p)^n T^2)^{b_n^0(X^n)/2}.$$

- *If $p \equiv 1 \pmod 3$, one can write uniquely $4p = a^2 + 27b^2$ with $a \equiv 1 \pmod 3$ and $b > 0$, and*

$$P_n^0(X^n_{\mathbf{F}_p}, T) = \begin{cases} 1 + aT + pT^2 & \textit{when } n = 1, \\ (1 - pT)^6 & \textit{when } n = 2, \\ (1 + apT + p^3T^2)^5 & \textit{when } n = 3, \\ (1 + (2p - a^2)T + p^2T^2)(1 - p^2T)^{20} & \textit{when } n = 4, \\ (1 + ap^2T + p^5T^2)^{21} & \textit{when } n = 5. \end{cases}$$

As will become clear from the proof, it would be possible to write down (complicated) formulas for all n in the case $p \equiv 1 \pmod 3$. We leave that exercise to the interested reader and restrict ourselves to the lower-dimensional cases.

Proof Assume first $p \equiv 2 \pmod 3$. It follows from Remark 4.10 that the polynomial $P_n^0(X^n_{\mathbf{F}_p}, T)$ is even (this is explained by (19) and (20) when $n = 4$). It is therefore equivalent to prove $P_n^0(X^n_{\mathbf{F}_{p^2}}, T) = (1 - (-p)^n T)^{b_n^0(X^n)}$. We follow the geometric argument of [26].

It is well known that $P_1(X^1_{\mathbf{F}_p}, T) = 1 + pT^2$, hence $P_1(X^1_{\mathbf{F}_{p^2}}, T) = (1 + pT)^2$. In other words, the Frobenius morphism of $\mathbf{F}_{p^2}$ acts on the middle cohomology of $X^1_{\mathbf{F}_{p^2}}$ by multiplication by $-p$. By the Künneth formula, it acts by multiplication by $(-p)^2$ on the middle cohomology of $X^1_{\mathbf{F}_{p^2}} \times X^1_{\mathbf{F}_{p^2}}$. The proof by induction on n of [26, Theorem 2.10] then applies and gives that the Frobenius morphism acts by multiplication by $(-p)^n$ on the middle cohomology of $X^n_{\mathbf{F}_{p^2}}$.

Assume now $p \equiv 1 \pmod 3$. The number of points of $X^1(\mathbf{F}_p)$ was computed by Gauss ([28, Theorem 4.2]): writing $4p = a^2 + 27b^2$ as in the theorem, one has $\mathrm{Card}(X^1(\mathbf{F}_p)) = p + 1 + a$, i.e., $P_1(X^1_{\mathbf{F}_p}, T) = 1 + aT + pT^2 =: (1 - \omega T)(1 - \bar{\omega}T)$. In other words, the eigenvalues of the Frobenius morphism of $\mathbf{F}_p$ acting on the first cohomology group are ω and $\bar{\omega}$. They are therefore the Jacobi sums denoted by

$j(1,2)$ and $j(2,1)$ in [26, (3.1)], and also the generators of the prime ideals $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ in $\mathbf{Z}[\zeta]$ ($\zeta = \exp(2i\pi/3)$) such that $(p) = \mathfrak{p}\bar{\mathfrak{p}}$.

The eigenvalues of the Frobenius morphism acting on the primitive middle cohomology of $X^n_{\mathbf{F}_p}$ are denoted $j(\alpha)$ by Weil, where α runs over the set

$$\mathfrak{U}_n = \{(\alpha_0, \dots, \alpha_{n+1}) \in \{1,2\}^{n+2} \mid \alpha_0 + \cdots + \alpha_{n+1} \equiv 0 \pmod 3\}.$$

The ideal $(j(\alpha))$ in $\mathbf{Z}[\zeta]$ is invariant under permutations of the α_i and its decomposition is computed by Stickelberger (see [26, (3.10)]):

$$(j(\alpha)) = \mathfrak{p}^{A(\alpha)}\bar{\mathfrak{p}}^{A(\bar\alpha)},$$

with $A(\alpha) = \left\lfloor \sum_{j=1}^{n+1} \frac{\alpha_j}{3} \right\rfloor$ and $\bar\alpha_j = 3 - \alpha_j$.

The elements of $\mathfrak{U}_1$ are $(1,1,1)$ and $(2,2,2)$, and the corresponding values of A are 0 and 1. The eigenvalues are therefore (up to multiplication by a unit of $\mathbf{Z}[\zeta]$), ω and $\bar\omega$. By Gauss' theorem, we know they are exactly ω and $\bar\omega$. By induction on n, it then follows from the embeddings [26, (2.17)] that

$$j(\alpha) = \omega^{A(\alpha)}\bar\omega^{A(\bar\alpha)}.$$

The elements of $\mathfrak{U}_2$ are (up to permutations) $(1,1,2,2)$ and the corresponding value of A is 1. The only eigenvalue is therefore $\omega\bar\omega = p$, with multiplicity $\binom{4}{2}$.

The elements of $\mathfrak{U}_3$ are (up to permutations) $(1,1,1,1,2)$ and $(1,2,2,2,2)$, and the corresponding values of A are 1 and 2. The eigenvalues are therefore $\omega^2\bar\omega = p\omega$ and $p\bar\omega$, with multiplicity 5.

The elements of $\mathfrak{U}_4$ are (up to permutations) $(1,1,1,1,1,1)$, $(1,1,1,2,2,2)$, and $(2,2,2,2,2,2)$, and the corresponding values of A are 1, 2, and 3. The eigenvalues are therefore $p\omega^2$ and $p\bar\omega^2$, with multiplicity 1, and p^2, with multiplicity $\binom{6}{3}$.

The elements of $\mathfrak{U}_5$ are (up to permutations) $(1,1,1,1,1,2,2)$ and $(1,1,2,2,2,2,2)$, and the corresponding values of A are 2 and 3. The eigenvalues are therefore $p^2\omega$ and $p^2\bar\omega$, with multiplicity $\binom{7}{2}$. This finishes the proof of the theorem. □

Corollary 4.12 *Let $X \subset \mathbf{P}^4_{\mathbf{Z}}$ be the Fermat cubic threefold defined by the equation $x_1^3 + \cdots + x_5^3 = 0$ and let $F(X)$ be its surface of lines. Let p be a prime number other than* 3.

The Albanese variety $A(F(X))_{\mathbf{F}_p}$ is isogenous to $E^5_{\mathbf{F}_p}$, where E is the Fermat plane cubic curve. Moreover,

- *if $p \equiv 2 \pmod 3$, we have*

$$Z(F(X)_{\mathbf{F}_p}, T) = \frac{(1+pT^2)^5(1+p^3T^2)^5}{(1-T)(1-p^2T)(1+pT)^{20}(1-pT)^{25}},$$

the Picard number of $F(X)_{\mathbf{F}_p}$ is 25 and that of $F(X)_{\mathbf{F}_{p^2}}$ is 45, and the abelian variety $A(F(X))_{\mathbf{F}_p}$ is supersingular;

- *if* $p \equiv 1 \pmod 3$, *we have (with the notation of Theorem 4.11)*

$$Z(F(X)_{\mathbf{F}_p}, T) = \frac{(1 + aT + pT^2)^5 (1 + apT + p^3T^2)^5}{(1 - T)(1 - p^2T)(1 + (2p - a^2)T + p^2T^2)^{10}(1 - pT)^{25}},$$

the Picard and absolute Picard numbers of $F(X)_{\mathbf{F}_p}$ *are 25, and the abelian variety* $A(F(X))_{\mathbf{F}_p}$ *is ordinary.*

Proof Theorems 4.1 and 4.11 imply that the characteristic polynomials of the Frobenius morphisms acting on H^1 are the same for the abelian varieties $A(F(X))_{\mathbf{F}_p}$ and $E^5_{\mathbf{F}_p}$; they are therefore isogenous ([23, Appendix I, Theorem 2]). The statements about $A(F(X))_{\mathbf{F}_p}$ being supersingular or ordinary follow from the analogous statements about $E_{\mathbf{F}_p}$.

The values of the zeta functions also follow from Theorems 4.1 and 4.11, and the statements about the Picard numbers from Corollary 4.3. □

We now restrict ourselves to the Fermat cubic threefold $X \subset \mathbf{P}^4_{\mathbf{Z}}$ $(n = 3)$. We parametrize planes containing the line $L := \langle (1, -1, 0, 0, 0), (0, 0, 1, -1, 0) \rangle \subset X$ by the $\mathbf{P}^2$ defined by the equations $x_1 = x_3 = 0$ and determine the discriminant quintic $\Gamma_L \subset \mathbf{P}^2$ (see Sect. 4.3).

Lemma 4.13 *In the coordinates* x_2, x_4, x_5, *an equation of the discriminant quintic* $\Gamma_L \subset \mathbf{P}^2$ *is* $x_2x_4(x_2^3 + x_4^3 + 4x_5^3) = 0$. *Therefore,*

- *in characteristics other than 2 and 3, it is a nodal quintic which is the union of two lines and an elliptic curve, all defined over the prime field;*
- *in characteristic 2, it is the union of 5 lines meeting at the point* $(0, 0, 1)$*; 3 of them are defined over* $\mathbf{F}_2$*, the other 2 over* $\mathbf{F}_4$.

Proof We use the notation of the proof of Proposition 4.5 (although the choice of coordinates is different). If $x = (0, x_2, 0, x_4, x_5) \in \mathbf{P}^2$, the residual conic C_x is defined by the equation

$$\frac{1}{y_1}(y_2^3 + (x_2y_1 - y_2)^3 + y_3^3 + (x_4y_1 - y_3)^3 + y_1^3x_5^3) = y_1^2(x_2^2 + x_4^2 + x_5^2) - 3x_2^2y_1y_2 - 3x_4^2y_1y_3 + 3x_2y_2^2 + 3x_4y_3^2$$

in the coordinates (y_1, y_2, y_3). In characteristics other than 2 and 3, an equation of Γ_L is therefore given by

$$\begin{vmatrix} x_2^3+x_4^3+x_5^3 & -\frac{3}{2}x_2^2 & -\frac{3}{2}x_4^2 \\ -\frac{3}{2}x_2^2 & 3x_2 & 0 \\ -\frac{3}{2}x_4^2 & 0 & 3x_4 \end{vmatrix} = \frac{9}{4}x_2x_4 \begin{vmatrix} 4(x_2^3+x_4^3+x_5^3) & 3x_2 & 3x_4 \\ x_2^2 & 1 & 0 \\ x_4^2 & 0 & 1 \end{vmatrix} = \frac{9}{4}x_2x_4(x_2^3 + x_4^3 + 4x_5^3) = 0.$$

In characteristic 2, the Jacobian criterion says that the singular points of C_x must satisfy $y_1 = 0$ and $x_2y_2^2 + x_4y_3^2 = x_2^2y_2 + x_4^2y_3 = 0$. The curve Γ_L is therefore defined by $\begin{vmatrix} x_2^{1/2} & x_4^{1/2} \\ x_2^2 & x_4^2 \end{vmatrix} = 0$, or $x_2x_4(x_2^3 + x_4^3) = 0$. It is therefore the "same" equation reduced modulo 2. □

4.5.2 The Klein Threefold

This is the cubic threefold $X \subset \mathbf{P}^4_{\mathbf{Z}}$ defined by the equation

$$x_1^2x_2 + x_2^2x_3 + x_3^2x_4 + x_4^2x_5 + x_5^2x_1 = 0. \tag{16}$$

It has good reduction at every prime $p \neq 11$.

It contains the line $L' = \langle(1,0,0,0,0),(0,0,1,0,0)\rangle$ and we parametrize planes containing L' by the $\mathbf{P}^2$ defined by $x_1 = x_3 = 0$.

Lemma 4.14 *In the coordinates x_2, x_4, x_5, an equation of the discriminant quintic $\Gamma_{L'} \subset \mathbf{P}^2$ is $x_2^5 + x_4x_5^4 - 4x_2x_4^3x_5 = 0$. Therefore,*

- *in characteristics other than 2 and 11, it is a geometrically irreducible quintic with a single singular point,* $(0,1,0)$*, which is a node;*
- *in characteristic 2, it is a geometrically irreducible rational quintic with a single singular point of multiplicity 4,* $(0,1,0)$.

Proof We proceed as in the proof of Lemma 4.13. If $x = (0, x_2, 0, x_4, x_5) \in \mathbf{P}^2$, an equation of the residual conic C_x is

$$\frac{1}{y_1}\left(y_2^2x_2y_1 + x_2^2y_1^2y_3 + y_3^2x_4y_1 + x_4^2y_1^2x_5y_1 + x_5^2y_1^2y_2\right) = y_2^2x_2 + x_2^2y_1y_3 + y_3^2x_4 + x_4^2y_1^2x_5 + x_5^2y_1y_2$$

in the coordinates (y_1, y_2, y_3). In characteristic other than 2, an equation of $\Gamma_{L'}$ is therefore

$$\begin{vmatrix} x_4^2x_5 & \frac{1}{2}x_5^2 & \frac{1}{2}x_2^2 \\ \frac{1}{2}x_5^2 & x_2 & 0 \\ \frac{1}{2}x_2^2 & 0 & x_4 \end{vmatrix} = \frac{1}{4}(x_2^5 + x_4x_5^4 - 4x_2x_4^3x_5) = 0.$$

In characteristic 2, one checks that $\Gamma_{L'}$ is defined by the equation $x_2^5 + x_4x_5^4 = 0$. In both cases, the singularities are easily determined. □

In characteristic 11, $X_{\mathbf{F}_{11}}$ has a unique singular point, $(1, 3, 3^2, 3^3, 3^4)$, which has type A_2. The quintic $\Gamma_{L'} \subset \mathbf{P}^2$ is still geometrically irreducible, with a node at $(0, 1, 0)$ and an ordinary cusp (type A_2) at $(5, 1, 3)$.

In characteristic 2, the isomorphism $(x_1, \ldots, x_5) \mapsto (x_1 + x_5, x_2 + x_5, x_3 + x_5, x_4 + x_5, x_1 + x_2 + x_3 + x_4 + x_5)$ maps $X_{\mathbf{F}_2}$ to the cyclic cubic defined by $x_5^3 + (x_1 + x_2 + x_3 + x_4)^3 + x_1^2x_2 + x_2^2x_3 + x_3^2x_4 = 0$. Thus $M_{2m+1}(X_{\mathbf{F}_2}) = 0$ for any $m \geq 0$ (reasoning as in Sect. 4.5.1). The computer gives $M_2(X_{\mathbf{F}_2}) = M_4(X_{\mathbf{F}_2}) = 0$. Using (8), we find that $X_{\mathbf{F}_2}$ contains 5 $\mathbf{F}_2$-lines; they are the line L' and its images by the cyclic permutations of the coordinates.

By the reciprocity property (5), we obtain

$$P_1(F(X)_{\mathbf{F}_2}, T) = P_3(X_{\mathbf{F}_2}, T/2) = 1 + 2^5T^{10}.$$

Since this polynomial has simple roots, the Picard number of $F(X)_{\mathbf{F}_2}$ is 5 (Corollary 4.3). The eigenvalues of the Frobenius morphism F are $\omega \exp(2ik\pi/10)$, for $k \in \{0, \dots, 9\}$, where $\omega^{10} = -2^5$; hence F^{10} acts by multiplication by -2^5. This implies $P_1(F(X)_{\mathbf{F}_{2^{10}}}, T) = (1 + 2^5 T)^{10}$. It follows that $F(X)_{\mathbf{F}_{2^{10}}}$ has maximal Picard number 45 (Corollary 4.3) and that $A(F(X))$ is isogenous to E^5 over $\mathbf{F}_{2^{10}}$, where E is the Fermat plane cubic defined in Sect. 4.5.1.

We also get $P_2(F(X)_{\mathbf{F}_2}, T) = (1 - 2^5 T^5)(1 - 2^{10} T^{10})^4 = (1 - 2^5 T^5)^5 (1 + 2^5 T^5)^4$ and

$$Z(F(X)_{\mathbf{F}_2}, T) = \frac{(1 + 2^5 T^{10})(1 + 2^{15} T^{10})}{(1 - T)(1 - 4T)(1 - 2^5 T^5)^5 (1 + 2^5 T^5)^4}.$$

Over other small fields, we find, using the Bombieri–Swinnerton-Dyer method (Proposition 4.5) and a computer,

$$\begin{aligned} P_1(F(X)_{\mathbf{F}_3}, T) &= 1 + 31T^5 + 3^5 T^{10} \\ P_1(F(X)_{\mathbf{F}_5}, T) &= 1 - 57T^5 + 5^5 T^{10} \\ P_1(F(X)_{\mathbf{F}_7}, T) &= 1 + 7^5 T^{10} \\ P_1(F(X)_{\mathbf{F}_{13}}, T) &= 1 + 13^5 T^{10}. \end{aligned}$$

Note that $A(F(X))$ is ordinary in the first two cases and supersingular with maximal Picard number in the other two cases. One can easily compute the Picard numbers and write down the corresponding zeta functions if desired. We compute the geometric Picard numbers by a different method. Note that -11 is a square modulo 3 or 5, but not modulo 7 or 13.

Proposition 4.15 *Let $X \subset \mathbf{P}^4_{\mathbf{Z}}$ be the Klein cubic threefold with Eq.* (16) *and let $F(X)$ be its surface of lines. Suppose $p \neq 2$. If -11 is a square modulo p, the reduction modulo p of $F(X)$ has geometric Picard number* 25*, otherwise it has geometric Picard number* 45.

Proof Set $\nu := \frac{-1+\sqrt{-11}}{2}$ and $E'_{\mathbf{C}} := \mathbf{C}/\mathbf{Z}[\nu]$. By [1, Corollary 4, p. 138], $A(F(X))_{\mathbf{C}}$ is isomorphic to $(E'_{\mathbf{C}})^5$. By [27, Appendix A3], the elliptic curve $E'_{\mathbf{C}}$ has a model defined by the equations

$$y^2 + y = x^3 - x^2 - 7x + 10 = 0$$

over $\mathbf{Q}$, which we denote by E'. Since $A(F(X))_{\mathbf{C}}$ and $E'^5_{\mathbf{C}}$ are isomorphic, $A(F(X))$ and E'^5 are isomorphic over some number field ([23, Appendix I, p. 240]).

We use Deuring's criterion [21, Chapter 13, Theorem 12)]: for odd $p \neq 11$, the reduction of E' modulo p is supersingular if and only if p is inert or ramified in $\mathbf{Z}[\nu]$. By classical results in number theory, an odd prime $p \neq 11$ is inert or ramified in $\mathbf{Z}[\nu]$ if and only if -11 is not a square modulo p. The geometric Picard number of the reduction modulo p of $A(F(X))$ is therefore 45 if -11 is not a square modulo p, and 25 otherwise. □

4.5.3 An Implementation of Our Algorithm

We use the notation of Sect. 4.3. Let $X \subset \mathbf{P}^4_{\mathbf{Z}}$ be the cubic threefold defined by the equation

$$f + 2q_1x_4 + 2q_2x_5 + x_1x_4^2 + 2x_2x_4x_5 + x_3x_5^2 = 0,$$

where

$$\begin{aligned} f &= x_2^2x_3 - (x_1^3 + 4x_1x_3^2 + 2x_3^3),\\ q_1 &= x_1^2 + 2x_2^2 + x_2x_3 + x_3^2,\\ q_2 &= x_1x_2 + 4x_2x_3 + x_3^2. \end{aligned}$$

It contains the line L defined by the equations $x_1 = x_2 = x_3 = 0$.

In characteristics ≤ 31, the cubic X is smooth except in characteristics 2 or 3 and the plane quintic curve Γ_L is smooth except in characteristics 2 or 5.

We implemented in `Sage` the algorithm described in Algorithm 1 (see [31]). Over $\mathbf{F}_5$, we get

$$P_1(F(X)_{\mathbf{F}_5}, T) = (1 + 5T^2)(1 + 2T^2 + 8T^3 - 6T^4 + 40T^5 + 50T^6 + 625T^8).$$

It follows that $A(F(X)_{\mathbf{F}_5})$ is not ordinary and not simple (it contains an elliptic curve).

Over the field $\mathbf{F}_7$, we compute that $P_1(F(X)_{\mathbf{F}_7}, T)$ is equal to

$$1 + 4T + 15\,T^2 + 46\,T^3 + 159\,T^4 + 460\,T^5 + 1\,113\,T^6 + 2\,254\,T^7 + 5\,145\,T^8 + 9\,604\,T^9 + 16\,807\,T^{10}.$$

This polynomial is irreducible over $\mathbf{Q}$; it follows that $A(F(X)_{\mathbf{F}_7})$ is ordinary and simple (Sect. 2.4). We can even get more by using a nice criterion from [17].

Proposition 4.16 *The abelian variety $A(F(X)_{\mathbf{F}_7})$ is absolutely simple, i.e., it remains simple over any field extension.*

Proof We want to apply the criterion [17, Proposition 3 (1)] to the abelian variety $A := A(F(X)_{\mathbf{F}_7})$. Let $d > 1$. Since the characteristic polynomial $Q_1(A, T)$ (which is also the minimal polynomial) of the Frobenius morphism F is not in $\mathbf{Z}[T^d]$, it is enough to check that, for any $d > 1$, there are no dth roots of unity ζ such that $\mathbf{Q}(F^d) \subsetneq \mathbf{Q}(F)$ and $\mathbf{Q}(F^d, \zeta) = \mathbf{Q}(F)$. If this is the case, $\mathbf{Q}(\zeta)$ is contained in $\mathbf{Q}(F)$, hence $\phi(d)$ (where ϕ is the Euler totient function) divides $\deg\big(Q_1(A, T)\big) = 10$. This implies $d \in \{2, 3, 4, 6, 11, 22\}$. But for these values of d, one computes that the characteristic polynomial $Q_1(A_{\mathbf{F}_{7^d}}, T)$ of F^d is irreducible (of degree 10), and this contradicts $\mathbf{Q}(F^d) \subsetneq \mathbf{Q}(F)$. Thus A is absolutely simple. □

Here are some more computations in "high" characteristics:

$$P_1(F(X)_{\mathbf{F}_{23}},T) = 1+21T^2-35T^3+759T^4-890T^5+17\,457T^6-18\,515T^7+255\,507T^8+6\,436\,343T^{10},$$
$$P_1(F(X)_{\mathbf{F}_{29}},T) = 1+3T+5T^2+15T^3+352T^4+2\,828T^5+10\,208T^6+12\,615T^7+121\,945T^8+2\,121\,843T^9+20\,511\,149T^{10},$$
$$P_1(F(X)_{\mathbf{F}_{31}},T) = 1+2T+2T^2+72T^3+117T^4-812T^5+3\,627T^6+69\,192T^7+59\,582T^8+1\,847\,042T^9+28\,629\,151T^{10}.$$

4.5.4 Smooth Cubic Threefolds over $\mathbf{F}_2$, $\mathbf{F}_3$, $\mathbf{F}_4$, or $\mathbf{F}_5$ with No Lines

Using a computer, it is easy to find many smooth cubic threefolds defined over $\mathbf{F}_2$ with no $\mathbf{F}_2$-lines (see Example 4.17). For example, the cubic threefold $X \subset \mathbf{P}^4_{\mathbf{F}_2}$ defined by the equation

$$x_1^3 + x_2^3 + x_3^3 + x_1^2x_2 + x_2^2x_3 + x_3^2x_1 + x_1x_2x_3 + x_1x_4^2 + x_1^2x_4 + x_2x_5^2 + x_2^2x_5 + x_4^2x_5 = 0$$

contains no $\mathbf{F}_2$-lines. We also have[3]

$$N_1(X) = 9, N_2(X) = 81, N_3(X) = 657, N_4(X) = 4\,225, N_5(X) = 34\,049,$$

hence (see (10) for the definition of $M_r(X)$)

$$M_1(X) = -3, M_2(X) = -1, M_3(X) = 9, M_4(X) = -9, M_5(X) = 7.$$

The polynomial $P_1(F(X),T) = P_3(X,T/2) = \prod_{j=1}^{10}(1-\omega_jT)$ is then given by

$$\exp\Big(\sum_{r=1}^{5} M_r(X)\frac{T^r}{r}\Big) + O(T^6) = 1 - 3T + 4T^2 - 10T^4 + 20T^5 + O(T^6).$$

Using the reciprocity property (5), we obtain

$$P_1(F(X),T) = 1 - 3T + 4T^2 - 10T^4 + 20T^5 - 10\cdot 2T^6 + 4\cdot 2^3T^8 - 3\cdot 2^4T^9 + 2^5T^{10}.$$

Since this polynomial has no multiple roots, the Picard number of $F(X)$ is 5 (Corollary 4.3).

We found by random computer search the smooth cubic threefold $X' \subset \mathbf{P}^4_{\mathbf{F}_3}$ defined by the equation

$$2x_1^3 + 2x_2^3 + x_1x_3^2 + x_2^2x_4 + 2x_3^2x_4 + x_1^2x_5 + x_2x_3x_5 + 2x_1x_4x_5 + 2x_2x_4x_5 + 2x_4^2x_5 + 2x_4x_5^2 + x_5^3 = 0.$$

[3] Among smooth cubics in $\mathbf{P}^4_{\mathbf{F}_2}$ with no $\mathbf{F}_2$-lines, the computer found examples whose number of $\mathbf{F}_2$-points is any odd number between 3 and 13.

It contains no $\mathbf{F}_3$-lines and 25 $\mathbf{F}_3$-points. Computing directly the number of points on extensions of $\mathbf{F}_3$, as we did above for $\mathbf{F}_2$, takes too much time, and it is quicker to use the Bombieri–Swinnerton-Dyer method (Proposition 4.5) on $X'_{\mathbf{F}_9}$, which contains an $\mathbf{F}_9$-line. The result is that $P_1(F(X')_{\mathbf{F}_9}, T)$ is equal to

$$1 - 5T + 8T^2 + 10T^3 - 124T^4 + 515T^5 - 1\,116T^6 + 810T^7 + 5\,832T^8 - 32\,805T^9 + 59\,049T^{10}.$$

Using the fact that X' has 25 $\mathbf{F}_3$-points and that the roots of $P_1(F(X')_{\mathbf{F}_3}, T)$ are square roots of the roots of $P_1(F(X')_{\mathbf{F}_9}, T)$, one finds

$$P_1(F(X')_{\mathbf{F}_3}, T) = 1 - 5T + 10T^2 - 2T^3 - 36T^4 + 95T^5 - 108T^6 - 18T^7 + 270T^8 - 405T^9 + 243T^{10},$$

and the numbers of $\mathbf{F}_{3^r}$-lines in $X'_{\mathbf{F}_{3^r}}$, for $r \in \{1, \dots, 5\}$, are 0, 40, 1 455, 5 740, 72 800, respectively.

Similarly, the smooth cubic threefold in $\mathbf{P}^4_{\mathbf{F}_4}$ defined by the equation

$$x_1^3 + x_1^2x_2 + x_2^3 + x_1^2x_3 + ux_1x_3^2 + ux_2x_3^2 + u^2x_1x_2x_4 + x_2^2x_4 + ux_4^3 + x_2^2x_5 + ux_2x_3x_5 + x_3^2x_5 + x_3x_5^2 + x_5^3 = 0,$$

where $u^2 + u + 1 = 0$, contains no $\mathbf{F}_4$-lines and 61 $\mathbf{F}_4$-points.

Finally, the smooth cubic threefold in $\mathbf{P}^4_{\mathbf{F}_5}$ defined by the equation

$$\begin{aligned} x_1^3 + 2x_2^3 + x_2^2x_3 + 3x_1x_3^2 + x_1^2x_4 + x_1x_2x_4 + x_1x_3x_4 + 3x_2x_3x_4 + 4x_3^2x_4 + x_2x_4^2 \\ + 4x_3x_4^2 + 3x_2^2x_5 + x_1x_3x_5 + 3x_2x_3x_5 + 3x_1x_4x_5 + 3x_4^2x_5 + x_2x_5^2 + 3x_5^3 = 0 \end{aligned}$$

contains no $\mathbf{F}_5$-lines and 126 $\mathbf{F}_5$-points.

We were unable to find smooth cubic threefolds defined over $\mathbf{F}_q$ with no $\mathbf{F}_q$-lines for the remaining values $q \in \{7, 8, 9\}$ (by Theorem 4.4, there are always $\mathbf{F}_q$-lines for $q \geq 11$).

4.5.5 Nodal Cubic Threefolds over $\mathbf{F}_2$ or $\mathbf{F}_3$ with No Lines

Regarding cubic threefolds with one node and no lines, we found the following examples.

The unique singular point of the cubic in $\mathbf{P}^4_{\mathbf{F}_2}$ defined by the equation

$$x_2^3 + x_2^2x_3 + x_3^3 + x_1x_2x_4 + x_3^2x_4 + x_4^3 + x_1^2x_5 + x_1x_3x_5 + x_2x_4x_5 = 0$$

is an ordinary double point at $x := (0, 1, 0, 0, 1)$ and this cubic contains no $\mathbf{F}_2$-lines. As we saw during the proof of Corollary 4.8, the base of the cone $\mathbf{T}_{X,x} \cap X$ is a smooth genus-4 curve defined over $\mathbf{F}_2$ with no $\mathbf{F}_4$-points. The pencils g^1_3 and h^1_3 are defined over $\mathbf{F}_2$.

The unique singular point of the cubic in $\mathbf{P}^4_{\mathbf{F}_3}$ defined by the equation

$$2x_1^3 + 2x_1^2x_2 + x_1x_2^2 + 2x_2x_3^2 + 2x_1x_2x_4 + x_2x_3x_4 \\ + x_1x_4^2 + 2x_4^3 + x_2x_3x_5 + 2x_3^2x_5 + x_2x_5^2 + x_5^3 = 0$$

is an ordinary double point at $x := (1, 0, 0, 0, 1)$ and this cubic contains no $\mathbf{F}_3$-lines. Again, the base of the cone $\mathbf{T}_{X,x} \cap X$ is a smooth genus-4 curve defined over $\mathbf{F}_3$ with no $\mathbf{F}_9$-points, and the pencils g_3^1 and h_3^1 are defined over $\mathbf{F}_3$.

4.6 Average Number of Lines

Consider the Grassmannian $G := \mathrm{Gr}(1, \mathbf{P}^{n+1}_{\mathbf{F}_q})$, the parameter space $\mathbf{P} = \mathbf{P}\big(H^0\big(\mathbf{P}^{n+1}_{\mathbf{F}_q}, \mathscr{O}_{\mathbf{P}^{n+1}_{\mathbf{F}_q}}(d)\big)\big)$ for all degree-d hypersurfaces in $\mathbf{P}^{n+1}_{\mathbf{F}_q}$, and the incidence variety $I = \{(L, X) \in G \times \mathbf{P} \mid L \subset X\}$. The first projection $I \to G$ is a projective bundle, hence it is easy to compute the number of $\mathbf{F}_q$-points of I. The fibers of the second projection $I \to \mathbf{P}$ are the varieties of lines. The average number of lines (on *all* degree-d n-folds) is therefore

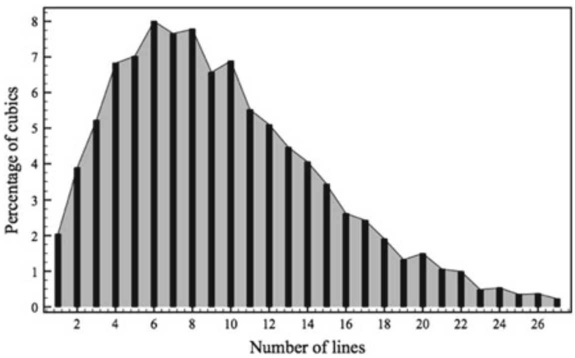
$$\frac{\mathrm{Card}\big(G(\mathbf{F}_q)\big)(q^{\dim(\mathbf{P})-d} - 1)}{q^{\dim(\mathbf{P})+1} - 1} \sim \mathrm{Card}\big(G(\mathbf{F}_q)\big)q^{\dim(\mathbf{P})-d-1}. \tag{17}$$

Recall that $\mathrm{Card}\big(G(\mathbf{F}_q)\big) = \sum_{0\le i<j\le n+1} q^{i+j-1}$. For cubic 3-folds, the right side of (17) is

$$q^2 + q + 2 + 2q^{-1} + 2q^{-2} + q^{-3} + q^{-4}.$$

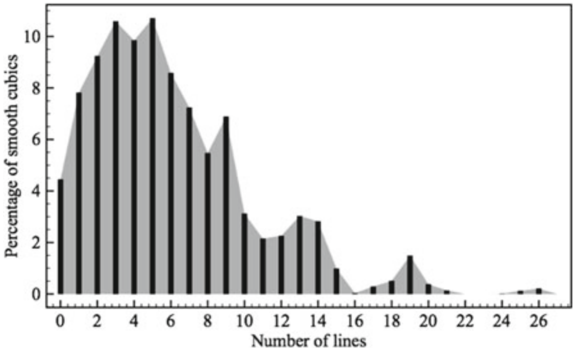
For $q = 2$, the average number of lines on a cubic threefold is therefore $\sim$9.688 (compare with Example 4.17 below).

Example 4.17 (Computer experiments) For a random sample of $5 \cdot 10^4$ cubic threefolds defined over $\mathbf{F}_2$, we computed for each the number of $\mathbf{F}_2$-lines.



The average number of lines in this sample is $\sim$9.651.

Smooth cubic threefolds contain less lines: here is the distribution of the numbers of $\mathbf{F}_2$-lines for a random sample of $5 \cdot 10^4$ *smooth* cubic threefolds defined over $\mathbf{F}_2$.



The average number of lines in this sample is $\sim$6.963.

5 Cubic Fourfolds

We now examine cubic fourfolds over $\mathbf{F}_q$. We expect them to contain "more" lines than cubic threefolds (indeed, all the examples we computed do contain $\mathbf{F}_q$-lines). Unfortunately, we cannot just take $\mathbf{F}_q$-hyperplane sections and apply our results from Sect. 4, because these results only concern mildly singular cubic threefolds, and there is no *a priori* reason why there would exist a hyperplane section defined over $\mathbf{F}_q$ with these suitable singularities.

We follow the same path as in Sect. 4. Recall that for any field $\mathbf{k}$, the scheme $F(X)$ of lines contained in a cubic fourfold $X \subset \mathbf{P}^5_{\mathbf{k}}$ with finite singular set is a geometrically connected local complete intersection fourfold (Sect. 2.3) with trivial canonical sheaf ([2, Proposition (1.8)]).

5.1 The Zeta Function of the Fourfold of Lines

Let $X \subset \mathbf{P}^5_{\mathbf{F}_q}$ be a *smooth* cubic hypersurface defined over $\mathbf{F}_q$. Its Betti numbers are 1, 0, 1, 0, 23, 0, 1, 0, 1, and the eigenvalues of the Frobenius morphism acting on $H^4(\overline{X}, \mathbf{Q}_\ell)$ are all divisible by q as algebraic integers ([18, Remark 5.1]). We write

$$N_r(X) = 1 + q^r + q^{3r} + q^{4r} + q^r \sum_{j=1}^{23} \omega_j^r,$$

where the complex algebraic integers ω_j (and all their conjugates) have modulus q, with $\omega_{23} = q$ (it corresponds to the part of the cohomology that comes from $H^4(\mathbf{P}^5_{\overline{\mathbf{F}}_q}, \mathbf{Q}_\ell)$). The trace formula (3) reads

$$Z(X,T) = \frac{1}{(1-T)(1-qT)(1-q^2T)(1-q^3T)(1-q^4T)P_4^0(X,T)},$$

where

$$P_4^0(X,T) := \frac{P_4(X,T)}{1-q^2T} = \prod_{j=1}^{22}(1-q\omega_j T). \tag{18}$$

If we set

$$M_r(X) := \frac{1}{q^r}\big(N_r(X) - (1+q^r+q^{2r}+q^{3r}+q^{4r})\big) = \sum_{j=1}^{22}\omega_j^r, \tag{19}$$

we obtain

$$P_4^0(X,T) = \exp\Big(\sum_{r\geq 1} M_r(X)\frac{(qT)^r}{r}\Big). \tag{20}$$

Theorem 5.1 *Let $X \subset \mathbf{P}^5_{\mathbf{F}_q}$ be a* smooth *cubic hypersurface defined over $\mathbf{F}_q$ and let $F(X)$ be the smooth fourfold of lines contained in X. With the notation above, we have $P_i(F(X),T) = 0$ for i odd and*

$$P_2(F(X),T) = P_6(F(X),T/q^2) = P_4(X,T/q) = \prod_{1\leq j\leq 23}(1-\omega_j T)$$
$$P_4(F(X),T) = \prod_{1\leq j\leq k\leq 23}(1-\omega_j\omega_k T),$$

where the complex numbers $\omega_1,\ldots,\omega_{22}$ have modulus q and $\omega_{23} = q$, and

$$Z(F(X),T) = \frac{1}{(1-T)(1-q^4T)\prod_{1\leq j\leq 23}\big((1-\omega_jT)(1-q^2\omega_jT)\big)\prod_{1\leq j\leq k\leq 23}(1-\omega_j\omega_kT)}. \tag{21}$$

Proof The various methods of proof described in the proof of Theorem 4.1 are still valid here. For example, one may deduce the theorem from the isomorphisms

$$H^4(\overline{X},\mathbf{Q}_\ell) \xrightarrow{\sim} H^2\big(\overline{F(X)},\mathbf{Q}_\ell(1)\big) \quad \text{and} \quad \mathrm{Sym}^2 H^2(\overline{F(X)},\mathbf{Q}_\ell) \xrightarrow{\sim} H^4(\overline{F(X)},\mathbf{Q}_\ell)$$

obtained from the Galkin–Shinder relation (7) ([14, Example 6.4]) or the analogous (known) statements in characteristic 0. We leave the details to the reader. □

5.2 *Existence of Lines over Large Finite Fields*

As we did for cubic threefolds, we use the Deligne–Weil estimates to find a lower bound for the number of $\mathbf{F}_q$-lines on a smooth cubic fourfold defined over $\mathbf{F}_q$.

Theorem 5.2 *Let X be a smooth cubic fourfold defined over $\mathbf{F}_q$ and let $N_1(F(X))$ be the number of $\mathbf{F}_q$-lines contained in X. For $q \geq 23$, we have*

$$N_1(F(X)) \geq q^4 - 21q^3 + 210q^2 - 21q + 1$$

and, for smaller values of q,

q	5	7	8	9	11	13	16	17	19
$N_1(F(X)) \geq$	26	638	1 337	2 350	5 930	12 338	29 937	38 438	61 010

In particular, X always contains an $\mathbf{F}_q$-line when $q \geq 5$.

When $q = 2$, we will see in Corollary 5.4 that X always contains an $\mathbf{F}_2$-line. These leaves only the cases $q = 3$ or 4 open (see Sect. 5.4.3).

Proof Write the roots of $Q_2(F(X), T)$ as q (with multiplicity a), $-q$ (with multiplicity b), $\omega_1, \dots, \omega_c, \overline{\omega}_1, \dots, \overline{\omega}_c$, with $a + b + 2c = 23$. The $r_j := \omega_j + \overline{\omega}_j$ are then real numbers in $[-2q, 2q]$ and, by (2) and Theorem 5.1, we have

$$\begin{aligned}
N_1\big(F(X)\big) &= 1 + q^4 + \sum_{1\leq j\leq k\leq 23} \omega_j\omega_k + (1+q^2)\sum_{1\leq j\leq 23}\omega_j \\
&= 1 + q^4 + \Big(\frac{1}{2}\big(a(a+1) + b(b+1)\big) - ab\Big)q^2 + (a-b)q\sum_{1\leq j\leq c} r_j \\
&\qquad + cq^2 + \sum_{1\leq j<k\leq c} r_j r_k + (1+q^2)\Big((a-b)q + \sum_{1\leq j\leq c} r_j\Big) \\
&= 1 + q^4 + \frac{1}{2}\big((a-b)^2 + 23\big)q^2 + (1+q^2)(a-b)q \\
&\qquad + \sum_{1\leq j<k\leq c} r_j r_k + \big(1 + q^2 + (a-b)q\big)\sum_{1\leq j\leq c} r_j.
\end{aligned}$$

Since $a + b = 23 - 2c$ is odd, it is enough to study the cases $a = 1$ and $b = 0$, or $a = 0$ and $b = 1$, since we can always consider pairs q, q, or $-q, -q$, as $\omega, \overline{\omega}$. We then have $c = 22$ and we set $\varepsilon := a - b \in \{-1, 1\}$.

As in the proof of Theorem 4.4, we note that this last expression $G_q^{\varepsilon}(\mathbf{r})$ is linear in each variable, hence its minimum is reached at a point on the boundary, when the r_j are all equal to $\pm 2q$. At such a point $\mathbf{r}_l$ (with l positive coordinates), we compute

$$G_q^{\varepsilon}(\mathbf{r}_l) = 1 + q^4 + 12q^2 + \varepsilon q(1+q^2) + 2q^2((2l-11)^2 - 11) + 2(2l-11)q(1+q^2+\varepsilon q).$$

Since q is always an eigenvalue, we must have $\varepsilon = 1$ when $l = 0$. As a function of l, the minimum is reached for $2l - 11 = -\frac{1+q^2+\varepsilon q}{2q}$. For $q \geq 23$, the allowable values for which $G_q^\varepsilon(\mathbf{r}_l)$ is smallest are $l = 0$ and $\varepsilon = 1$, and the minimum is $q^4 - 21q^3 + 210q^2 - 21q + 1 > 0$.

For $q \leq 19$, the numbers in the table follow from a longish comparison of the various functions G_q^ε. □

5.3 *Existence of Lines over Some Finite Fields*

The cohomology of the structure sheaf of the fourfold $F(X)$ is particularly simple and this can be used to prove congruences for its number of $\mathbf{F}_q$-points by using the Katz formula (6).

Proposition 5.3 (Altman–Kleiman) *Let $X \subset \mathbf{P}^5_{\mathbf{k}}$ be a cubic hypersurface defined over a field* $\mathbf{k}$*, with finite singular set. We have*

$$h^0(F(X), \mathscr{O}_{F(X)}) = h^2(F(X), \mathscr{O}_{F(X)}) = h^4(F(X), \mathscr{O}_{F(X)}) = 1$$
$$h^1(F(X), \mathscr{O}_{F(X)}) = h^3(F(X), \mathscr{O}_{F(X)}) = 0.$$

Proof The scheme $F(X)$ is the zero scheme of a section of the rank-4 vector bundle $\mathscr{E}^\vee := \mathrm{Sym}^3 \mathscr{S}^\vee$ on $G := \mathrm{Gr}(1, \mathbf{P}^5_{\mathbf{k}})$ and the Koszul complex

$$0 \to \bigwedge^4 \mathscr{E} \to \bigwedge^3 \mathscr{E} \to \bigwedge^2 \mathscr{E} \to \mathscr{E} \to \mathscr{O}_G \to \mathscr{O}_{F(X)} \to 0 \tag{22}$$

is exact. By [2, Theorem (5.1)], the only non-zero cohomology groups of $\bigwedge^r \mathscr{E}$ are

$$H^8(G, \bigwedge^4 \mathscr{E}) \simeq H^4(G, \bigwedge^2 \mathscr{E}) \simeq \mathbf{k}.$$

Chasing through the cohomology sequences associated with (22), we obtain $H^1(F(X), \mathscr{O}_{F(X)}) = H^3(F(X), \mathscr{O}_{F(X)}) = 0$ and

$$H^0(F(X), \mathscr{O}_{F(X)}) \simeq H^0(G, \mathscr{O}_G),$$
$$H^2(F(X), \mathscr{O}_{F(X)}) \simeq H^4(G, \bigwedge^2 \mathscr{E}),$$
$$H^4(F(X), \mathscr{O}_{F(X)}) \simeq H^8(G, \bigwedge^4 \mathscr{E}).$$

This proves the proposition. □

Since $\omega_{F(X)}$ is trivial, the multiplication product

$$H^2(F(X), \mathscr{O}_{F(X)}) \otimes H^2(F(X), \mathscr{O}_{F(X)}) \to H^4(F(X), \mathscr{O}_{F(X)}) \tag{23}$$

is the Serre duality pairing. It is therefore an isomorphism.

Corollary 5.4 *Let $X \subset \mathbf{P}^5_{\mathbf{F}_q}$ be a cubic hypersurface with finite singular set, defined over $\mathbf{F}_q$. If $q \equiv 2 \pmod 3$, the hypersurface X contains an $\mathbf{F}_q$-line.*

Proof The $\mathbf{F}_q$-linear map $\mathfrak{F}_q$ defined in Sect. 2.2 acts on the one-dimensional $\mathbf{F}_q$-vector space $H^2(F(X), \mathscr{O}_{F(X)})$ (Proposition 5.3) by multiplication by some $\lambda \in \mathbf{F}_q$; since (23) is an isomorphism, $\mathfrak{F}_q$ acts on $H^4(F(X), \mathscr{O}_{F(X)})$ by multiplication by λ^2. It then follows from the Katz formula (6) that we have

$$N_1(F(X)) \cdot 1_{\mathbf{F}_q} = 1 + \lambda + \lambda^2 \qquad \text{in } \mathbf{F}_q.$$

If $1 + \lambda + \lambda^2 = 0_{\mathbf{F}_q}$, we have $\lambda^3 = 1_{\mathbf{F}_q}$. Since $3 \nmid q - 1$, there are no elements of order 3 in $\mathbf{F}_q^\times$, hence the morphism $\mathbf{F}_q^\times \to \mathbf{F}_q^\times$, $x \mapsto x^3$ is injective. Therefore, $\lambda = 1_{\mathbf{F}_q}$, hence $3 \cdot 1_{\mathbf{F}_q} = 1_{\mathbf{F}_q}$, but this contradicts our hypothesis.

We thus have $1 + \lambda + \lambda^2 \neq 0_{\mathbf{F}_q}$, hence $N_1(F(X))$ is not divisible by the characteristic of $\mathbf{F}_q$ and the corollary is proved. □

5.4 *Examples of Cubic Fourfolds*

5.4.1 Fermat Cubics

If $X \subset \mathbf{P}^5_{\mathbf{F}_p}$ is the Fermat fourfold, it is a simple exercise to write down the zeta function of $F(X)$ using Theorems 4.11 and 5.1, as we did in dimension 3 in Corollary 4.12.

5.4.2 Cubic Fourfolds over $\mathbf{F}_2$ with only One Line

Smooth cubic fourfolds defined over $\mathbf{F}_2$ always contain an $\mathbf{F}_2$-line by Corollary 5.4. Random computer searches produce examples with exactly one $\mathbf{F}_2$-line: for example, the only $\mathbf{F}_2$-line contained in the smooth cubic fourfold defined by the equation

$$\begin{aligned} x_1^3 + x_2^3 + x_3^3 + x_1^2x_2 + x_2^2x_1 + x_3^2x_1 + x_1x_2x_3 + x_1x_4^2 + x_1^2x_4 + x_2x_5^2 + x_2^2x_5 \\ + x_4^2x_5 + x_4x_5^2 + x_3x_6^2 + x_3^2x_6 + x_4^2x_6 + x_4x_6^2 + x_5^2x_6 + x_5x_6^2 + x_4x_5x_6 = 0 \end{aligned}$$

is the line $\langle (0, 0, 0, 0, 1, 1), (0, 0, 0, 1, 0, 1) \rangle$; the fourfold contains 13 $\mathbf{F}_2$-points.

5.4.3 Cubic Fourfolds over $\mathbf{F}_3$ or $\mathbf{F}_4$

Our results say nothing about the existence of lines in smooth cubic fourfolds defined over $\mathbf{F}_3$ or $\mathbf{F}_4$. Our computer searches only produced fourfolds containing lines (and over $\mathbf{F}_3$, both cases $N_1(F(X)) \equiv 0$ or $1 \pmod 3$ do occur), leading us to suspect that all (smooth) cubic fourfolds defined over $\mathbf{F}_3$ or $\mathbf{F}_4$ should contain lines.

6 Cubics of Dimensions 5 or More

In higher dimensions, the existence of lines is easy to settle.

Theorem 6.1 *Any cubic hypersurface $X \subset \mathbf{P}^{n+1}_{\mathbf{F}_q}$ of dimension $n \geq 6$ defined over $\mathbf{F}_q$ contains $\mathbf{F}_q$-points and through any such point, there is an $\mathbf{F}_q$-line contained in X.*

Proof This is an immediate consequence of the Chevalley–Warning theorem: $X(\mathbf{F}_q)$ is non-empty because $n + 2 > 3$ and given $x \in X(\mathbf{F}_q)$, lines through x and contained in X are parametrized by a subscheme of $\mathbf{P}^n_{\mathbf{F}_q}$ defined by equations of degrees 1, 2, and 3 and coefficients in $\mathbf{F}_q$. Since $n + 1 > 1 + 2 + 3$, this subscheme contains an $\mathbf{F}_q$-point. □

The Chevalley–Warning theorem implies $N_1(X) \geq \frac{q^{n-1}-1}{q-1}$. When $n \geq 6$, we obtain from the theorem $N_1(F(X)) \geq \frac{q^{n-1}-1}{q^2-1}$; when X (hence also $F(X)$) is smooth, the Deligne–Weil estimates for $F(X)$ provide better bounds.

When $n \geq 5$, we may also use the fact that the scheme of lines contained in a smooth cubic hypersurface is a Fano variety (its anticanonical bundle $\mathscr{O}(4 - n)$ is ample).

Theorem 6.2 *Assume $n \geq 5$ and let $X \subset \mathbf{P}^{n+1}_{\mathbf{F}_q}$ be any cubic hypersurface defined over $\mathbf{F}_q$. The number of $\mathbf{F}_q$-lines contained in X is $\equiv 1 \pmod{q}$.*

Proof When X is smooth, the variety $F(X)$ is also smooth, connected, and a Fano variety. The result then follows from [12, Corollary 1.3].

To prove the result in general, we consider as in Sect. 4.6 the parameter space $\mathbf{P}$ for all cubic hypersurfaces in $\mathbf{P}^{n+1}_{\mathbf{F}_q}$ and the incidence variety $I = \{(L, X) \in G \times \mathbf{P} \mid L \subset X\}$. The latter is smooth and geometrically irreducible; the projection $\mathrm{pr}\colon I \to \mathbf{P}$ is dominant and its geometric generic fiber is a (smooth connected) Fano variety ([2, Theorem (3.3)(ii), Proposition (1.8), Corollary (1.12), Theorem (1.16)(i)]). It follows from [13, Corollary 1.2] that for any $x \in \mathbf{P}(\mathbf{F}_q)$ (corresponding to a cubic hypersurface $X \subset \mathbf{P}^{n+1}_{\mathbf{F}_q}$ defined over $\mathbf{F}_q$), one has $\mathrm{Card}\big(\mathrm{pr}^{-1}(x)\big) \equiv 1 \pmod{q}$. Since $\mathrm{pr}^{-1}(x) = F(X)$, this proves the theorem. □

Acknowledgements This collaboration started after a mini-course given by the first author for the CIMPA School "II Latin American School of Algebraic Geometry and Applications" given in Cabo Frio, Brazil. We thank CIMPA for financial support and the organizers C. Araujo and S. Druel for making this event successful. Many thanks also to F. Charles, S. Elsenhans, B. van Geemen, F. Han, E. Howe, T. Katsura, Ch. Liedtke, and O. Wittenberg for useful correspondences and conversations. The computations made for this paper were done with the computer algebra programs `Magma` [6] and `Sage`.

References

1. A. Adler, Some integral representations of $PSL_2(\mathbf{F}_p)$ and their applications. J. Algebra **72**, 115–145 (1981)
2. A. Altman, S. Kleiman, Foundations of the theory of Fano schemes. Compos. Math. **34**, 3–47 (1977)
3. A. Beauville, Variétés de Prym et jacobiennes intermédiaires. Ann. Sci. Éc. Norm. Sup. **10**, 309–391 (1977)
4. A. Beauville, Les singularités du diviseur Theta de la jacobienne intermédiaire de l'hypersurface cubique dans $\mathbf{P}^4$, in *Algebraic Threefolds, Varenna 1981*, Lecture Notes in Mathematics, vol. 947 (Springer, Heidelberg, 1982), pp. 190–208
5. E. Bombieri, H.P.F. Swinnerton-Dyer, On the local zeta function of a cubic threefold. Ann. Scuola Norm. Sup. Pisa **21**, 1–29 (1967)
6. W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput. **24**, 235–265 (1997)
7. S. Casalaina-Martin, R. Laza, The moduli space of cubic threefolds via degenerations of the intermediate Jacobian. J. reine angew. Math. **663**, 29–65 (2009)
8. F. Charles, A. Pirutka, La conjecture de Tate entière pour les cubiques de dimension quatre. Compos. Math. **151**, 253–264 (2015)
9. C.H. Clemens, P.A. Griffiths, The intermediate Jacobian of the cubic threefold. Ann. Math. **95**, 281–356 (1972)
10. P. Deligne, La conjecture de Weil I. Publ. Math. Inst. Hautes Études Sci. **43**, 273–308 (1974)
11. A.-S. Elsenhans, J. Jahnel, On the characteristic polynomial of the Frobenius on étale cohomology. Duke Math. J. **164**, 2161–2184 (2015)
12. H. Esnault, Varieties over a finite field with trivial Chow group of 0-cycles have a rational point. Invent. Math. **151**, 187–191 (2003)
13. N. Fakhruddin, C.S. Rajan, Congruences for rational points on varieties over finite fields. Math. Ann. **333**, 797–809 (2005)
14. S. Galkin, E. Shinder, The Fano variety of lines and rationality problem for a cubic hypersurface. eprint arXiv:1405.5154v2
15. N.E. Hurt, in *Many Rational Points: Coding Theory and Algebraic Geometry*, Mathematics and its Applications, vol. 564 (Kluwer, Dordrecht, 2003)
16. E.W. Howe, K.E. Lauter, J. Top, Pointless curves of genus three and four, in *Arithmetic, Geometry and Coding Theory (AGCT 2003)*, Séminaries & Congres, vol. 11 (société mathématique de France, Paris, 2005), pp. 125–141
17. E.W. Howe, H.J. Zhu, On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. J. Number Theory **92**, 139–163 (2002)
18. N. Katz, Une formule de congruence pour la fonction ζ, Exposé XXII, in *Groupes de Monodromie en Géométrie Algébrique (SGA 7 II)*, Lecture Notes in Mathematics, vol. 340 (Springer, Heidelberg, 1973), pp. 401–438
19. K. Kedlaya, Effective p-adic cohomology for cyclic cubic threefolds, in *Computational Algebraic and Analytic Geometry*, Contemporary Mathematics, vol. 572 (American Mathematical Society, Providence, 2012), pp. 127–171
20. A. Kouvidakis, G. van der Geer, A note on Fano surfaces of nodal cubic threefolds, in *Algebraic and Arithmetic Structures of Moduli Spaces, Sapporo 2007*, Advanced Studies in Pure Mathematics, vol. 58 (Mathematical Society of Japan, Tokyo, 2010), pp. 27–45
21. S. Lang, *Elliptic Functions* (Addison-Wesley Publishing Co., Inc., Reading, 1973)
22. J.S. Milne, in *Étale Cohomology*, Princeton Mathematical Series, vol. 33 (Princeton University Press, Princeton, 1980)
23. D. Mumford, in *Abelian Varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5 (Oxford University Press, Oxford, 1970)
24. J.P. Murre, Some results on cubic threefolds, in *Classification of Algebraic Varieties and Compact Complex Manifolds*, Lecture Notes in Mathematics, vol. 412 (Springer, Berlin, 1974), pp. 140–160

25. X. Roulleau, On the Tate conjecture for the Fano surfaces of cubic threefolds. J. Number Theory **133**, 2320–2323 (2013)
26. T. Shioda, T. Katsura, On Fermat varieties. Tôhoku Math. J. **31**, 97–115 (1979)
27. J.H. Silverman, in *Advanced Topics in The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 151 (Springer, New York, 1994)
28. J.H. Silverman, J. Tate, in *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics (Springer, New York, 1992)
29. J. Tate, Algebraic cycles and poles of zeta functions, in *Arithmetical Algebraic Geometry, Purdue University 1963*, ed. by O. Schilling (Harper and Row, New York, 1965), pp. 93–110
30. A. Weil, Numbers of solutions of equations in finite fields. Bull. Amer. Math. Soc. **55**, 497–508 (1949)
31. Computer computations, https://github.com/alaface/CubLin

Springer

http://www.springer.com/978-3-319-49762-4

Geometry Over Nonclosed Fields
Bogomolov, F.; Hassett, B.; Tschinkel, Y. (Eds.)
2017, IX, 261 p. 3 illus., 1 illus. in color., Hardcover
ISBN: 978-3-319-49762-4