Sofos, E. and Wang, Y. (2019) Finite saturation for unirational varieties. International Mathematics Research Notices, 2019(15), pp. 4784-4821.

There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

http://eprints.gla.ac.uk/198846/

Deposited on: 25 October 2019

FINITE SATURATION FOR UNIRATIONAL VARIETIES

EFTHYMIOS SOFOS AND YUCHAO WANG

ABSTRACT. We import ideas from geometry to settle Sarnak's saturation problem for a large class of algebraic varieties.

CONTENTS

1. INTRODUCTION

A topic of central importance in number theory regards prime solutions of Diophantine equations. A principal result in this area is Vinogradov's three primes theorem [36], proved via the Hardy–Littlewood method. This approach has been extended by Hua to representations of integers by powers of primes, see, for example, the work of Kawada and Wooley [21] for further developments and references. A recent prominent work is due to Cook and Magyar [7]. They obtained asymptotic estimates for the number of prime solutions of general systems of Diophantine equations under the assumption that the system has a large number of variables compared to the degrees of the polynomials. This method has also been utilised in the subsequent work of Xiao–Yamagishi [38] and Yamagishi [39].

An approach based on the circle method demands that the number of variables is rather large compared to the degree. Thus when there are fewer variables, investigations have focused on solutions with few prime factors, a prototype result being that of Chen [6] on the binary Goldbach problem, a result using the weighted sieve. One can utilise again the circle method to cover cases where the number of variables is moderately large, see the recent work of Magyar–Titichetrakun [28], Schindler–Sofos [31] and Yamagishi [40]. The natural barrier for cancellation in exponential sums prevents the circle method from working in a small number of variables; for example, in the case of hypersurfaces of degree exceeding 2 it has never been used when the number of variables is less than twice the degree. In this realm one must necessarily combine sieve techniques with analytic methods other than the circle method. There is only a small number of results available in this range of variables. Examples include the work of Marasingha [27] on homogeneous ternary quadratic equations, Wang's work on the Fermat and the Cayley cubic surfaces via universal torsors [37] and the

result of Liu and Sarnak [22] covering non-homogeneous ternary quadratic equations via the use of group actions and the weighted sieve. An important earlier work is due to Nevo and Sarnak [29], which covers *prime* entries of matrices of fixed determinant.

Our aim in the present work is to provide almost prime results for varieties in very few variables and with no underlying group structure. We shall do so by combining sieve tools with geometric arguments. We first introduce the necessary notation. Recall that the function $\Omega : \mathbb{Z} \to \mathbb{N} \cup \infty$ counting the number of prime divisors with multiplicity is defined via

$$\Omega(m) := \sum_p \nu_p(m),$$

where ν_p is the standard p-adic valuation, the sum is over all primes p and $\Omega(m)$ is infinite if and only if $m = 0$. We can extend Ω to a function $\Omega_{\mathbb{P}^n(\mathbb{Q})}$ defined on $\mathbb{P}^n(\mathbb{Q})$ in the obvious way, namely by finding for each $x \in \mathbb{P}^n(\mathbb{Q})$ an element $\mathbf{x} \in \mathbb{Z}^{n+1}_{\mathrm{prim}}$ with $x = [\mathbf{x}]$ and letting

$$\Omega_{\mathbb{P}^n(\mathbb{Q})}(x) := \Omega\left(\prod_{i=0}^n x_i\right).$$

Here $\mathbb{Z}^{n+1}_{\mathrm{prim}}$ stands for integer vectors $\mathbf{x} \in \mathbb{Z}^{n+1}$ with $\gcd(x_0, \ldots, x_n) = 1$; it is easy to see that $\Omega_{\mathbb{P}^n(\mathbb{Q})}$ is well-defined.

Definition 1.1 (Saturation number). Let $X \subset \mathbb{P}^n$ be a variety defined over $\mathbb{Q}$. The saturation number of X, denoted by $r(X)$, is defined as the least $r \in \mathbb{N} \cup \infty$ such that the set of points $x \in X(\mathbb{Q})$ with $\Omega_{\mathbb{P}^n(\mathbb{Q})}(x) \leqslant r$ forms a Zariski dense subset of X.

This definition is essentially due to Bourgain, Gamburd and Sarnak [1]. Varieties X with $X(\mathbb{Q})$ being not Zariski dense will necessarily have $r(X) = \infty$. Let us note that Zariski density is the geometric analog of the existence of infinitely many almost prime elements in a sequence of integers. Indeed, if the Zariski density condition was relaxed to existence of infinitely many points $x \in X(\mathbb{Q})$ with $\Omega_{\mathbb{P}^n(\mathbb{Q})}(x) \leqslant r$ in the definition above then the possible presence of (linear, for example) subspaces defined over $\mathbb{Q}$ and contained in X makes the problem more tractable, see [3]. Recall that a variety X defined over $\mathbb{Q}$ is said to be $\mathbb{Q}$-unirational if there exists a positive integer m and a dominant morphism $\pi : \mathbb{P}^m \dashrightarrow X$ defined over $\mathbb{Q}$.

Theorem 1.2. *Any smooth projective variety defined over $\mathbb{Q}$ has finite saturation if it is $\mathbb{Q}$-unirational.*

We shall prove this by using the dominant map to parametrise points and then apply the weighted sieve to the forms associated to π. Theorem 1.2 covers new cases where the number of variables is small. We illustrate this with a few examples.

Corollary 1.3. *The following varieties have finite saturation:*
  (I) *Del Pezzo surfaces defined over $\mathbb{Q}$, of degree larger than 2 and with at least one $\mathbb{Q}$-point;*
 (II) *Smooth projective cubic hypersurfaces defined over $\mathbb{Q}$, of dimension larger than 1 and with at least one $\mathbb{Q}$-point;*
(III) *Smooth projective hypersurfaces of odd degree $d \geqslant 5$, defined over $\mathbb{Q}$ and of dimension larger than $c = c(d)$;*

(IV) *Smooth projective quadric hypersurfaces defined over $\mathbb{Q}$, of positive dimension and with at least one $\mathbb{Q}$-point.*

The proof of the corollary can be inferred immediately from Theorem 1.2 and the fact that the varieties in the statement are $\mathbb{Q}$-unirational. Indeed, unirationality follows from the work of Manin [25](part (I)), Kollár [20] (part (II)) and Brandes [2, Th.1.3] (part (III)). It is a standard result that all varieties in part (IV) are $\mathbb{Q}$-rational, in particular, they are $\mathbb{Q}$-unirational, thus are covered by Theorem 1.2.

There are additional results on unirationality of hypersurfaces, see, for example, the work of Marchisio [26] and Conte, Marchisio, Murre [8], respectively for quartic and quintic hypersurfaces of small dimension. It is worth mentioning that over algebraically closed fields, unirationality is known to hold for general hypersurfaces of dimension sufficiently large compared to the degree. In the same setting, Harris, Mazur and Pandharipande [18] provided explicit criteria for unirationality of smooth hypersurfaces.

1.1. **Effective saturation.** One would wish to have an explicit bound on the saturation number $r(X)$ in terms of X. In the generality of Theorem 1.2 this bound must necessarily depend on the embedding of X. Indeed, as the example $(m!)^2 x_0 x_1 = x_2^2, (m \in \mathbb{N})$, reveals, the saturation $r(X)$ can be rather large, however, one could still try to bound it in terms of the coefficients. This is achieved in our next result.

Theorem 1.4. *Assume that $X \subset \mathbb{P}^n$ is smooth, defined over $\mathbb{Q}$ and $\mathbb{Q}$-unirational, so that there exists $m \in \mathbb{N}$, forms $f_i \in \mathbb{Z}[x_0, \ldots, x_m]$ and a dominant rational morphism $\pi : \mathbb{P}^m \dashrightarrow X$ given by $\pi = (f_0 : \ldots : f_n)$. Letting $f := \prod_{i=0}^n f_i$, the saturation $r(X)$ is at most*

$$10^5 \deg^7(f) \log(2\|f\|),$$

where $\|f\|$ is the maximum of the absolute values of the coefficients of f.

It is possible that there exists a positive integer greater than 1 that divides $f(\mathbf{x})$ for every $\mathbf{x} \in \mathbb{Z}^{m+1}$. Therefore, if one is allowed to make linear transformations to change the equations defining X, an improved saturation can be obtained, specifically, one depending solely on $\deg(f)$.

1.2. **Improved saturation in the presence of a fibration with a $\mathbb{Q}$-section.** Consider the Fermat cubic surface X, given by $\sum_{i=0}^3 x_i^3 = 0$. It is well-known that it is $\mathbb{Q}$-birational to $\mathbb{P}^2$, thus in particular it is $\mathbb{Q}$-unirational and is therefore covered by Theorem 1.4. One parametrisation was already given by Euler (see [17, §13.7]), however for our needs it will be more convenient to use the one given by Elkies [12]. More specifically, he showed that X is dominated by $\pi : \mathbb{P}^2 \dashrightarrow X$, where π is given by $\pi = (f_0 : \ldots : f_3)$ and

$$f_0 = -(y_1 + y_0)y_2^2 + (y_1^2 + 2y_0^2)y_2 - y_1^3 + y_0 y_1^2 - 2y_0^2 y_1 - y_0^3,$$
$$f_1 = y_2^3 - (y_1 + y_0)y_2^2 + (y_1^2 + 2y_0^2)y_2 + y_0 y_1^2 - 2y_0^2 y_1 + y_0^3,$$
$$f_2 = -y_2^3 + (y_1 + y_0)y_2^2 - (y_1^2 + 2y_0^2)y_2 + 2y_0 y_1^2 - y_0^2 y_1 + 2y_0^3,$$
$$f_3 = (y_1 - 2y_0)y_2^2 + (y_0^2 - y_1^2)y_2 + y_1^3 - y_0 y_1^2 + 2y_0^2 y_1 - 2y_0^3.$$

Thus Theorem 1.4 supplies us with the estimate

$$r(X) \leqslant [10^5 \cdot 12^7 \cdot (\log(2 \cdot 2^4))] = (1.24\ldots) \times 10^{13}.$$

The Elkies parametrisation provides f_i with slightly smaller coefficients compared to the one given by Euler, thus giving a smaller value for $\|f\|$ in Theorem 1.4 and hence a better value for $r(X)$. When a subtler geometric structure is available then one can hope to obtain an improved saturation number. Indeed, we shall see that if a variety can be covered by many lower-dimensional $\mathbb{Q}$-unirational subvarieties then we can parametrise the subvarieties 'uniformly' and apply sieve methods directly to them. Potential examples of such varieties are those that are equipped with a fibration that has a section over the base field. The approach of using sections to reduce the saturation is realised for a class of varieties of dimension 2 in our next result.

Theorem 1.5. *Every smooth cubic surface in $\mathbb{P}^3_{\mathbb{Q}}$ that contains two rational skew lines can be linearly transformed over $\mathbb{Q}$ so that it has saturation at most 32.*

We have allowed for linear transformations in order to eliminate the effect of small prime factors in the saturation. Such surfaces have a conic bundle with a section over $\mathbb{Q}$; indeed, the fibers correspond to the residual conics in the pencil of planes through one of the skew lines and the other skew line ensures that each of these conics has a $\mathbb{Q}$-point, see [13]. It must be pointed out that Theorem 1.5 does not cover the Fermat cubic surface. This surface was proved to have saturation at most 20 in a recent work of Wang [37].

In the 'section-approach' one can sometimes replace the sieve tools by results originating in additive combinatorics. This has the advantage of providing an almost best possible saturation number. For example, we shall use work of Green–Tao and Ziegler to show that the smooth cubic surface given by

$$X : \ (x_0 - 6x_1)x_2^2 + 36x_1x_2x_3 + 36(x_0 + 6x_1)x_3^2 = x_0^2x_2 + 216x_1^2x_3 \tag{1.1}$$

has saturation

$$r(X) \leqslant 10,$$

see Remark 4.7. This should be compared with the recent work of Tsang and Zhao [35], a special corollary of which is that for every sufficiently large integer N satisfying certain necessary congruence conditions, the Lagrange equation

$$N = x_0^2 + x_1^2 + x_2^2 + x_3^2$$

has a solution $\mathbf{x} \in \mathbb{N}^4$ with

$$\Omega(x_0x_1x_2x_3) \leqslant 16.$$

1.3. **Improved saturation in the presence of a fibration without a $\mathbb{Q}$-section.** In the setting of Theorem 1.5, the variety is equipped with a conic bundle that has a section over the ground field, i.e. can be covered by curves which *always* have a $\mathbb{Q}$-point. It is therefore desirable to ask whether a geometric approach can still provide a satisfying saturation number in cases where X has a fibration without a section over $\mathbb{Q}$. We answer this affirmatively in our next result.

Theorem 1.6. *The Fermat cubic threefold*

$$\sum_{i=0}^{4} x_i^3 = 0$$

has saturation at most 42.

The method of proof consists of equipping the threefold with a section-less conic bundle fibration over $\mathbb{P}^2$, finding sufficiently many $\mathbb{Q}$-rational fibers, and applying sieve machinery to this thin subset of the fibers. Progress on the arithmetic of cubic hypersurfaces of dimension $3, 4$ and 5 has been sporadic, see [4], [5] and the references therein for progress in higher dimensions. Smooth cubic threefolds over $\mathbb{Q}$ that contain a line defined over $\mathbb{Q}$ have finite saturation by the second part of Corollary 1.3. To obtain a good bound on the saturation one can try to adopt the approach used in the proof of Theorem 1.6 for every threefold in this family, since they are always equipped with a conic bundle over $\mathbb{P}^2_{\mathbb{Q}}$. We hope that the approach in the proof of Theorem 1.6 will assist with future investigations regarding Sarnak's saturation problem for varieties X defined over $\mathbb{Q}$ such that $X(\mathbb{Q})$ is Zariski dense and X is not $\mathbb{Q}$-unirational. For example, Swinnerton-Dyer [34, §5] has given a way to describe curves of genus 0 on the K3 surface

$$x_0^4 + x_1^4 = x_2^4 + x_3^4$$

and one might attempt to adopt his method to produce enough $\mathbb{Q}$-rational curves of genus 0 on quartic surfaces with smaller Picard rank. This would allow to parametrise a large set of these curves and then follow the method in the proof of Theorem 1.6.

Notation. For any functions $f, g : [1, \infty) \to \mathbb{C}$, the equivalent notations $f(x) = O_{\mathscr{S}}(g(x))$, and $f(x) \ll_{\mathscr{S}} g(x)$, will be used to denote the existence of a positive constant λ, which depends at most on the set of parameters $\mathscr{S}$ such that for any $x \geqslant 1$ we have $|f(x)| \leqslant \lambda |g(x)|$. As usual, we denote the Möbius function by $\mu(n)$. We denote the number of prime factors of n without multiplicity by $\nu(n)$. We shall furthermore denote by $\mathrm{Res}(f, g)$ the resultant of two integer binary forms f, g, and by $\mathrm{rad}(n)$ the square-free kernel of n. Finally, the symbol $\|f\|$ is reserved for the maximum absolute value of the coefficients of an integer polynomial f.

2. Sieve preliminaries

Before providing the proofs of our theorems let us record certain auxiliary results. We shall begin by stating a form of the weighted sieve. Suppose that $\mathscr{A}$ is a subset of the integers of cardinality Y and that $\mathscr{P}$ is any set of primes which includes every sufficiently large prime. Our setting includes a non-negative multiplicative arithmetic function ω that is supported on multiples of primes in $\mathscr{P}$. We define for integers d, $\mathscr{A}_d := \{a \in \mathscr{A} : d|a\}$ and we let $\mathscr{R}_d := \#\mathscr{A}_d - \frac{\omega(d)}{d}Y$. The following result appeared in [10, Th.11.1] and in an earlier form in [9, Th. 0 & Th.1].

Theorem 2.1 (Diamond–Halberstam). *Assume that there exist real constants $\kappa > 1$ and $A_1, A_2, A_3, A_4 \geqslant 2$ such that the following conditions are satisfied,*

$$a \in \mathscr{A}, p|a \Rightarrow p \in \mathscr{P},$$

$$0 \leqslant \omega(p) < p \quad \text{for all } p \in \mathscr{P},$$

$$\sum_{\substack{d < Y^\alpha (\log Y)^{-A_3} \\ p \mid d \Rightarrow p \in \mathscr{P}}} \mu^2(d) 4^{\nu(d)} |\mathscr{R}_d| \leqslant A_2 \, Y / (\log Y)^{\kappa+1} \quad \text{for some } 0 < \alpha \leqslant 1,$$

there exists $\mu \in \mathbb{R}$ *such that* $a \in \mathscr{A} \Rightarrow |a| \leqslant Y^{\alpha\mu}$,

$$\prod_{z_1 \leqslant p < z} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \leqslant \left(\frac{\log z}{\log z_1}\right)^\kappa \left(1 + \frac{A_1}{\log z_1}\right) \quad \text{for } 2 \leqslant z_1 < z.$$

Then there exists $\beta_\kappa \geqslant 2$ *such that whenever* $u, v \in \mathbb{R}$ *satisfy* $\alpha^{-1} < u < v, \beta_\kappa < \alpha u$, *and*

$$\sum_{\substack{Y^{1/v} \leqslant p < Y^{1/u} \\ p \in \mathscr{P}}} \#\mathscr{A}_{p^2} \leqslant A_4 \, Y / (\log Y)^{\kappa+1},$$

then for any integer r *with*

$$r > \alpha\mu u - 1 + \frac{\kappa}{f_\kappa(\alpha v)} \int_1^{v/u} F_\kappa(\alpha v - s) \left(1 - \frac{u}{v}s\right) \frac{\mathrm{d}s}{s} \tag{2.6}$$

we have

$$\#\{a \in \mathscr{A} : \Omega(a) \leqslant r\} \gg Y \prod_{p < Y^{1/v}} \left(1 - \frac{\omega(p)}{p}\right).$$

The functions f_κ, F_κ *are defined as the solutions to the delay-differential equations supplied in* [9, Th.0].

Condition (F) is required to ensure that higher prime powers have little effect in the calculations yielding the value of r given in (2.1). This condition is missing from [9, Th. 0 & Th.1] but appears in a slightly more general form in [10, (11.2)] as condition $\mathbf{Q_0}$. It is later stated in the same tract [10, pg. 140] that for the purpose of proving [10, Th.11.1], condition $\mathbf{Q_0}$ is only needed to ensure condition (F) as given in Theorem 2.1.

We shall furthermore use the bound

$$\beta_\kappa \leqslant 3.75\kappa, \tag{2.7}$$

valid for all $\kappa > 1$ and proved in Theorem 17.2 and Proposition 17.3 in [10]. Let us note that, as shown in [10, pg. 146], when $v = \beta_\kappa u$ then the quantity

$$\mu - 1 + (\mu - \kappa)(1 - 1/\beta_\kappa) + (\kappa + 1) \log \beta_\kappa \tag{2.8}$$

is an upper bound for the right side of (2.1) and thus can be used in its place in Theorem 2.1.

While the weighted sieve is useful in situations where $\mathscr{A}$ is composed of values assumed by general integer forms, in the special case that all forms are linear one can do significantly better due to the groundbreaking work of Green, Tao and Ziegler [14, Cor. 1.9], [15] and [16]. We shall later use the following very special case of their work.

Theorem 2.2 (Green, Tao, Ziegler). *Let* $L_1, \ldots, L_5 \in \mathbb{Z}[u, v]$ *be linear forms which are pairwise non-proportional and assume that for each prime p there exists* $(u_0, v_0) \in \mathbb{Z}^2$ *such that p does not divide* $L_i(u_0, v_0)$ *for any* $i = 1, \ldots, 5$. *Let* $\mathscr{R}$ *be a box of* $\mathbb{R}^2$ *containing a point* $(u_0, v_0) \in \mathbb{Z}^2$ *such that* $L_i(u_0, v_0) > 0$ *for* $i = 1, \ldots, 5$. *Then there exist infinitely many pairs* $(u, v) \in \mathscr{R} \cap \mathbb{Z}^2$ *such that* $L_i(u, v)$ *are all prime.*

Lemmas 2.3-2.6 will be used in the proof of Theorem 1.4 to make the dependence of the saturation on the small prime factors completely explicit in terms of the underlying polynomials.

Lemma 2.3. *Assume that $a, b \in \mathbb{R}_{\geqslant 1}$ and that a positive integer m satisfies*

$$m \leqslant ab^{\nu(m)}.$$

Then we have $m \leqslant 16a^2 \exp(b^6)$.

Proof. If $b^{\nu(m)} \leqslant m^{1/2}$ holds, then the assumption of the lemma ensures that $m \leqslant a^2$, which is sufficient for the proof. If $b^{\nu(m)} \leqslant m^{1/2}$ fails, then $\log m \leqslant 2(\log b)\nu(m)$. We are free to assume that $\log \log m > 1$, since otherwise we have $m \leqslant e^e \leqslant 16$ and the lemma holds. Then [30, Eq.(30)] guarantees that $\nu(m) \leqslant 3(\log m)(\log \log m)^{-1}$, hence

$$\log m \leqslant 2(\log b)3(\log m)(\log \log m)^{-1}.$$

Thus we obtain $m \leqslant \exp(b^6)$, which concludes the proof. $\qquad\qquad\square$

For an integer polynomial of degree at least 2 we denote its discriminant by D_f.

Lemma 2.4. *Assume that $f \in \mathbb{Z}[x]$ is a non-constant polynomial with non-zero discriminant and of degree at least 2. Then the set*

$$\{W \in \mathbb{N} : x \in \mathbb{Z} \Rightarrow W \text{ divides } f(x)\}$$

is bounded. Furthermore, every element in this set is at most

$$16D_f \exp(4096(\deg(f))^6). \tag{2.9}$$

Proof. In the case $\deg(f) = 1$ it is easy to see that for every prime p we have

$$\nu_p(W) \leqslant \min\{\nu_p(f(0)), \nu_p(f'(0))\},$$

which is sufficient due to $\|f\| = \max\{|f(0)|, |f'(0)|\}$. Hence we can assume that $\deg(f) \geqslant 2$ for the rest of the proof. First, write $f(x) = c_0 f_0(x)$, where $c_0 \in \mathbb{Z}\backslash\{0\}$ is the greatest common factor of the coefficients of f. Every integer W in the set of the lemma must satisfy

$$x \in \mathbb{Z} \Rightarrow \frac{W}{\gcd(c_0, W)} \mid f_0(x). \tag{2.10}$$

Letting $W_0 := W/\gcd(c_0, W)$ we observe that $D_{f_0} \neq 0$, thus the work of Cameron [33, Eq.(43)] reveals that the number of solutions of

$$f_0(x) \equiv 0 \mod W_0$$

is at most

$$\prod_{p|W_0} \left(2p^{\nu_p(D_{f_0})/2} + \deg(f) - 2\right).$$

By (2.10) the number of solutions is also equal to W_0, therefore we have

$$W_0 \leqslant \prod_{p|W_0} \left(2p^{\nu_p(D_{f_0})/2} + 2\deg(f)\right) \leqslant D_{f_0}^{1/2}(4\deg(f))^{\nu(W_0)}.$$

Combining the last inequality with Lemma 2.3 yields the following bound,

$$W_0 \leqslant 16D_{f_0} \exp(4096(\deg(f))^6).$$

Recall that the discriminant of a polynomial g is an integer form in its coefficients that has degree $2(-1 + \deg(g))$. This shows that, in light of $f = c_0 f_0$, one has

$$D_f = c_0^{2(-1+\deg(f))} D_{f_0},$$

therefore

$$W = \gcd(c_0, W)W_0 \leqslant c_0 W_0 \leqslant 16 c_0^{3-2\deg(f)} D_f \exp(4096(\deg(f))^6).$$

Noting that $\deg(f) \geqslant 2$ guarantees that $c_0^{3-2\deg(f)} \leqslant 1$ concludes the proof of our lemma.   □

We wish to obtain a version of Lemma 2.4 that is valid for polynomials in many variables. To do so we shall assign small integer values to all variables except one and apply Lemma 2.4. We first deduce a weaker, but more useful, version of Lemma 2.4.

Lemma 2.5. *Assume that $f \in \mathbb{Z}[x]$ is a non-constant polynomial with non-zero discriminant. Then every element in the set*

$$\{W \in \mathbb{N} : x \in \mathbb{Z} \Rightarrow W \text{ divides } f(x)\}$$

is bounded by

$$\|f\|^{2\deg(f)} \exp(5000 \deg^6(f)).$$

Proof. The case $\deg(f) = 1$ is easy to handle and is thus left to the reader. In all other cases we use the first corollary in page 261 of the work of Mahler [24], which states that

$$|D_f| \leqslant (\deg(f))^{\deg(f)} L^{2\deg(f)-2},$$

where L is the sum of the moduli of the coefficients of f. The inequality

$$L \leqslant (1 + \deg(f))\|f\|$$

is obvious. Using $(k+1)^k \leqslant ek^k$, valid for every $k \in \mathbb{N}$, we see that

$$|D_f| \leqslant (\deg(f))^{3\deg(f)} \|f\|^{2\deg(f)-2}((1 + \deg(f))/e)^{-2}$$

and the bounds (2.9), $((1 + \deg(f))/e)^{-2} \leqslant 2$ show that every element in the set in the statement of our lemma is bounded by

$$32(\deg(f))^{3\deg(f)} \|f\|^{2\deg(f)} \exp(4096(\deg(f))^6).$$

Using the inequality $32d^{3d} \leqslant e^{4d^6}$, valid for all $d \in \mathbb{N}$, concludes our proof.   □

Lemma 2.6. *Let $F \in \mathbb{Z}[x_0, \ldots, x_m]$ be a polynomial of positive degree that does not have repeated polynomial factors. Then every element in the set*

$$\{W \in \mathbb{N} : \mathbf{x} \in \mathbb{Z}^{m+1} \Rightarrow W \text{ divides } F(\mathbf{x})\}$$

is bounded by

$$\|F\|^{2\deg(F)} \exp(6000 \deg^6(F)).$$

Proof. The case $m = 0$ is contained in Lemma 2.5. We can therefore assume that $m \geqslant 1$ for the rest of the proof. We may consider the discriminant of the polynomial in the variable x_0 obtained by fixing every other variable, i.e. we bring into play the integer polynomial

$$H(x_1, \ldots, x_m) := D_{F(x, x_1, \ldots, x_m)}.$$

We note that H is not identically zero, since otherwise there would exist a non-zero integer c and an integer polynomial $h(x_1, \ldots, x_m)$ such that

$$(cx - h(x_1, \ldots, x_m))^2 \text{ divides } F(x, x_1, \ldots, x_m)$$

in the polynomial ring $\mathbb{Q}(x, x_1, \ldots, x_m)$. This would contradict the assumption that F does not have repeated polynomial factors. Now, since $H(x_1, \ldots, x_m)$ is a non-zero polynomial we have the trivial bound

$$\#\{\mathbf{x} \in (\mathbb{N} \cap [1, B])^m : H(\mathbf{x}) = 0\} \leqslant (\deg(H))B^{m-1}, \ (B \in \mathbb{N}),$$

obtained by fixing $m - 1$ of the variables x_i. If every $\mathbf{x} \in (\mathbb{N} \cap [1, B])^m$ is a zero of F then we infer $B \leqslant \deg(H)$, therefore there exists $\mathbf{y} \in \mathbb{N}^m$ with the properties

$$|\mathbf{y}| \leqslant 1 + \deg(H) \text{ and } D_{F(x, y_1, \ldots, y_m)} \neq 0.$$

We fix this choice of $\mathbf{y}$ and define $f(x) = F(x, y_1, \ldots, y_m)$. We have $\deg(f) \leqslant \deg(F)$ and

$$\|f\| \leqslant \|F\|(1 + \deg(H))^{\deg(F)}.$$

Recalling that the discriminant of a polynomial of degree d is a polynomial in the coefficients that has degree $2(d-1)$ we see that $\deg(H) \leqslant 2(\deg(F)-1)$, hence $\|f\| \leqslant \|F\|(2 \deg(F))^{\deg(F)}$. As a final step, we apply Lemma 2.5 to f, thus getting that every integer W in our lemma must be at most

$$\|f\|^{2\deg(f)} \exp(5000 \deg^6(f)) \leqslant \|F\|^{2\deg(F)}(2 \deg(F))^{2\deg^2(F)} \exp(5000 \deg^6(F)).$$

The inequality $(2d)^{2d^2} \leqslant \exp(1000d^6)$, valid for all $d \in \mathbb{N}$, concludes the proof. $\qquad\square$

Finally, we shall need certain results on the number of zeros of affine varieties over finite rings.

Lemma 2.7. *Let $F \in \mathbb{Z}[x_0, \ldots, x_m]$ be a primitive polynomial. Then for all primes p we have*

$$\#\{\mathbf{x} \in (\mathbb{Z}/p\mathbb{Z})^{m+1} : F(\mathbf{x}) \equiv 0 \mod p\} \leqslant (\deg(F))p^m.$$

Proof. A hypersurface $F = 0$ can have at most $\deg(F)$ irreducible components, thus one might try to use the Lang–Weil estimate [23]. However, their upper bound is of the form $\deg(F)p^m + O_F(p^{m-1/2})$, and for the purpose of proving Theorem 1.4 we need explicit constants. We begin the proof by remarking that since the polynomial F is primitive, it contains a term of the form $c \prod_{i=0}^m x_i^{d_i}$, where $c \in \mathbb{Z}$ is coprime with p and the $d_i \in \mathbb{Z}_{\geqslant 0}$ are such that $\sum d_i = \sum \deg(F_i)$ (here c and d_i depend on p). We infer that there exists i such that $d_i > 0$, therefore we may view F as a polynomial in the variable x_i by fixing every other variable. The fact that c is coprime to p ensures that this polynomial is not identically zero in $\mathbb{F}_p$, thus fixing any of the variables $x_j, j \neq i$, we obtain a non-zero element in $\mathbb{F}_p(x_i)$ that must therefore have at most $\deg(F)$ roots. $\qquad\square$

Lemma 2.8. *Let $F \in \mathbb{Z}[x_0, \ldots, x_m]$ be a polynomial of positive degree that does not have repeated polynomial factors. Then for all primes p we have*

$$\#\{\mathbf{x} \in (\mathbb{Z}/p^2\mathbb{Z})^{m+1} : F(\mathbf{x}) \equiv 0 \mod p^2\} \ll_F p^{2m}.$$

Proof. We begin by estimating the number of zeros of F in $(\mathbb{Z}/p^2\mathbb{Z})^{m+1}$ that are lifted from smooth zeros of F in $\mathbb{F}_p$, we call this cardinality X_p. By Hensel's lemma, smooth zeros of F in $\mathbb{F}_p$ can lift to at most $\ll_F p^m$ zeros in $(\mathbb{Z}/p\mathbb{Z})^{m+1}$. Thus, in light of Lemma 2.7 we obtain $X_p \ll \#\{\mathbf{x} \in \mathbb{F}_p^{m+1} : F = 0\}p^m \ll_F p^{2m}$. Next, we estimate the number of zeros of F in $(\mathbb{Z}/p^2\mathbb{Z})^{m+1}$ that reduce to singular zeros of F in $\mathbb{F}_p$, we call this cardinality Y_p. Note that such zeros can certainly exist (e.g. when $F = F_1 F_2$ then every non-zero $\mathbb{F}_p$-point in $F_1 = F_2 = 0$ is singular) and these can lift in any number of ways to $\mathbb{Z}/p^2\mathbb{Z}$; the trivial bound for such lifts is $\leqslant p^{m+1}$. The number of singular zeros is however rather small: the

variety Z given by $F = \nabla F = 0$ and defined over $\mathbb{F}_p$ is a subvariety of $\mathbb{A}^{m+1}(\mathbb{F}_p)$ that has codimension at least 2 for all sufficiently large primes p. This is because F is separable over $\mathbb{Q}$, therefore it reduces to a separable polynomial in $\mathbb{F}_p$ for all sufficiently large primes p. Now by the Lang–Weil estimate [23] we see that $Z(\mathbb{F}_p)$ has at most $\ll_F p^{m-1}$ points, therefore $Y_p \ll_F p^{m-1} \#\{\text{lifts}\} \leqslant p^{2m}$. We obtain that the number of zeros of F in $(\mathbb{Z}/p^2\mathbb{Z})^{m+1}$ is $X_p + Y_p \ll_F p^{2m}$, thus concluding our proof. $\qquad\square$

3. The proof of Theorems 1.2 and 1.4

We commence by recording a result regarding almost prime values of completely general forms. The result is a straightforward application of the weighted sieve.

Theorem 3.1. *Let $f \in \mathbb{Z}[x_0, \dots, x_m]$ be any form of positive degree. Then there exists $r \in \mathbb{N}$ such that for any non-empty box $\mathscr{R}^{(0)} \subset \mathbb{R}^{m+1}$ we have*

$$\#\left\{ \mathbf{x} \in \mathbb{Z}^{m+1} \cap \mathscr{R}^{(0)}B, \Omega(|f(\mathbf{x})|) \leqslant r \right\} \gg_{f,r,\mathscr{R}^{(0)}} B^{m+1}(\log B)^{-\deg(f)},$$

for all sufficiently large B. Furthermore, one can take r as the integer part of

$$6 \deg^2(f)(\log 2\|f\|) + 10^4 \deg^7(f)$$

Although we make no claim as to the given value of r being best possible, the example $f(x_0, \dots, x_m) = 2^n(x_0 \dots x_m)^m$ illustrates that r must depend on $\|f\|$ and $\deg(f)$, unless the lower bound $B^{m+1+o(1)}$ is replaced by $B^{m+o(1)}$. This is because

$$\Omega(2^n(x_0 \dots x_m)^m) \geqslant n + m(m+1) \geqslant \frac{\log\|f\|}{\log 2} + (\deg f)^2$$

holds for all integer vectors $|\mathbf{x}| \leqslant B$, except those at a set of size $O(B^m)$. For the application towards Theorem 1.2 it is important to stress that we need a lower bound of the form $B^{m+1+o(1)}$ in Theorem 3.1, otherwise Zariski density might not be obtained.

Theorem 3.1 is proved immediately after the proof of the next proposition.

Proposition 3.2. *Let $F_1, \dots, F_g \in \mathbb{Z}[x_0, \dots, x_m]$ be non-zero, primitive, irreducible forms of positive degree such that $F(\mathbf{x}) := \prod_{i=1}^{g} F_i(\mathbf{x})$ does not have repeated polynomial factors. Then there exists $r_0 \in \mathbb{N}$, such that for any non-empty box $\mathscr{R}^{(0)} \subset \mathbb{R}^{m+1}$ we have*

$$\#\left\{ \mathbf{x} \in \mathbb{Z}^{m+1} \cap \mathscr{R}^{(0)}B, \Omega(|F(\mathbf{x})|) \leqslant r_0 \right\} \gg_{F_i,r_0,\mathscr{R}^{(0)}} \frac{B^{m+1}}{(\log B)^{\deg(F)}},$$

as $B \to +\infty$. Furthermore, one can take r_0 as the integer part of

$$4 \deg(F)(\log 2\|F\|) + 10^4 \deg^6(F).$$

Proof. The main tool used in the proof is Theorem 2.1. Before using it we need to study the following function, defined for $d \in \mathbb{N}$,

$$\omega_0(d) := \frac{1}{d^m} \#\left\{ \mathbf{x} \in (\mathbb{Z}/d\mathbb{Z})^{m+1} : \prod_{i=1}^{g} F_i(\mathbf{x}) \equiv 0 \mod d \right\}.$$

Note that ω_0 is multiplicative, therefore Lemma 2.7 shows that for every $d \in \mathbb{N}$ we have

$$\mu(d)^2 \omega_0(d) \leqslant \left(\sum_{i=1}^{g} \deg(F_i) \right)^{\nu(d)}, \tag{3.1}$$

while Lemma 2.8 ensures that for every prime p we have

$$\omega_0(p^2) \ll_{F_i} 1. \tag{3.2}$$

We now continue with the application of the weighted sieve by introducing the related set-up. Let D be the maximum positive integer dividing $F(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}^{m+1}$. By Lemma 2.6 we obtain

$$D \leqslant \|F\|^{2\deg(F)} \exp(6000 \deg^6(F)). \tag{3.3}$$

Define $G(\mathbf{x}) := F(\mathbf{x})/D$ and observe that $G(\mathbf{x})$ attains integer values for all $\mathbf{x} \in \mathbb{Z}^{m+1}$. The definition of D shows that for every prime p the integer $p^{1+\nu_p(D)}$ cannot divide $F(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}^{m+1}$. Hence for each $p|D$ there exists $\mathbf{z}_p \in \mathbb{Z}^{m+1}$ with $p^{1+\nu_p(D)} \nmid F(\mathbf{z}_p)$ and letting

$$W := \prod_{p|D} p^{1+\nu_p(D)},$$

we get the existence of some $\mathbf{z} \in \mathbb{Z}^{m+1}$ such that

$$\mathbf{x} \equiv \mathbf{z} \mod W \Rightarrow \gcd(G(\mathbf{x}), W) = 1. \tag{3.4}$$

We denote the set of prime divisors of D by $\mathscr{P}$ and we define the multiplicative function ω via $\omega(p) := \mathbf{1}_{\mathscr{P}}(p)\omega_0(p)$. Note that by (3.1) we have the following for all $d \in \mathbb{N}$,

$$\mu(d)^2 \omega(d) \leqslant (\deg F)^{\nu(d)}. \tag{3.5}$$

Next, we define

$$\Psi := \{\mathbf{x} \in \mathbb{Z}^{m+1} : \mathbf{x} \equiv \mathbf{z} \mod W\}.$$

We shall use Theorem 2.1 to sieve the multiset of integers given by

$$\mathscr{A} := \{G(\mathbf{x}) : \mathbf{x} \in \mathbb{Z}^{m+1} \cap B\mathscr{R}^{(0)} \cap \Psi\}.$$

For all integers d coprime to W define $\mathscr{A}_d := \{a \in \mathscr{A} : d|a\}$. For $d \in \mathbb{N}$ we have

$$\#\mathscr{A}_d = \sum_{\substack{\mathbf{u} \mod d \\ G(\mathbf{u}) \equiv 0 \mod d}} \#\{\mathbf{x} \in \mathbb{Z}^{m+1} \cap B\mathscr{R}^{(0)}, \mathbf{x} \equiv \mathbf{z} \mod W, \mathbf{x} \equiv \mathbf{u} \mod d\},$$

thus a simple counting argument involving integer points in boxes gives

$$\#\mathscr{A}_d = \frac{\omega(d)}{d} \frac{B^{m+1}\mathrm{vol}(\mathscr{R}^{(0)})}{W^{m+1}} + O_{F_i, W, \mathscr{R}^{(0)}} \left(\omega(d)d^m + \omega(d)B^m \right). \tag{3.6}$$

Invoking (3.5) and writing

$$Y := \frac{B^{m+1}\mathrm{vol}(\mathscr{R}^{(0)})}{W^{m+1}},$$

allows us to infer that for square-free d that are coprime to D one has

$$\mathscr{R}_d := \left| \#\mathscr{A}_d - \frac{\omega(d)}{d} Y \right| \ll (\deg F)^{\nu(d)} \left(d^m + Y^{1-\frac{1}{m+1}} \right), \tag{3.7}$$

where the implied constant depends at most on $F_i, \mathscr{R}^{(0)}$ and W.

Next, we fix any values $\alpha \in (0, 1/(m+1))$, $\kappa \geqslant \deg(F)$, $\mu > \frac{\kappa}{\alpha(m+1)}$, and verify the conditions of Theorem 2.1. Condition (A) holds owing to the observation that if $p \mid G(\mathbf{x})$ for some $\mathbf{x} \in \mathscr{A}$ then $p \nmid D$ due to (3.4). Condition (B) follows from the fact that the definition of D implies that if $p \nmid D$ then there exists $\mathbf{x} \in \mathbb{Z}^{m+1}$ such that $p \nmid F(\mathbf{x})$. Condition (C)

is satisfied as a consequence of (3.7) while condition (D) is validated with any choice of $\mu > \frac{\kappa}{\alpha(m+1)}$. Condition (E) holds due to (3.5) and the estimate

$$\prod_{z_1 \leqslant p < z} \left(1 - \frac{\kappa}{p}\right)^{-1} = \left(\frac{\log z}{\log z_1}\right)^{\kappa} \left(1 + O\left(\frac{1}{\log z_1}\right)\right).$$

Combining (3.2) with (3.6), one sees that

$$\sum_{\substack{Y^{1/v} \leqslant p < Y^{1/u} \\ p \in \mathscr{P}}} \#\mathscr{A}_{p^2} \ll Y\Big(\sum_{Y^{1/v} < p} p^{-2}\Big) + Y^{1 - \frac{1}{m+1} + \frac{1}{u}} + Y^{\frac{2m+1}{u}}.$$

The sum over p is $\ll Y^{-1/v}$, hence condition (F) is satisfied since $2 \leqslant \beta_\kappa < \alpha u$ combined with $\alpha < 1/(m+1)$ imply that $u > 2m+1$. Therefore Theorem 2.1 yields a finite value r such that

$$\#\{\mathbf{x} \in \mathbb{Z}^{m+1} \cap \mathscr{R}^{(0)}B : \Omega(G(\mathbf{x})) \leqslant r\} \gg_F B^{m+1}(\log B)^{-\kappa},$$

as $B \to \infty$. We can provide an explicit value for r, namely r can be be the least integer which is greater than $10^3 \deg^6(F)$ because it can be shown that c_0 is small enough so that

$$10^3 \deg^6(F) \geqslant 2\deg(F) + (1 + \deg(F))\log(3.75\deg(F))$$

and, furthermore, we can choose $\kappa = \deg(F)$, α sufficiently close to $1/(m+1)$ and μ sufficiently close to $\kappa/(\alpha(m+1))$, observe that

$$\mu - 1 + (\mu - \kappa)(1 - 1/\beta_\kappa) + (\kappa + 1)\log\beta_\kappa \leqslant 2\deg(F) + (1 + \deg(F))\log(3.75\deg(F))$$

and allude to (2.7) and (2.8). Note that (3.3) reveals that

$$\Omega(D) \leqslant \frac{\log D}{\log 2} \leqslant 4\deg(F)(\log\|F\|) + 9000\deg^6(F),$$

which, when coupled with the equality $\Omega(|F(\mathbf{x})|) = \Omega(D) + \Omega(|G(\mathbf{x})|)$, proves our lemma. $\square$

To prove Theorem 3.1 we factorise f as

$$f(\mathbf{x}) = c\prod_{i=1}^{g} F_i(\mathbf{x})^{\nu_i} \ (\nu_i \in \mathbb{N}, c \in \mathbb{Z} - \{0\}),$$

where each F_i is a primitive irreducible integer form of positive degree, and then apply Proposition 3.2 to $F := \prod_{i=1}^{g} F_i$. Utilising the inequalities

$$\Omega\left(|f(\mathbf{x})|\right) \leqslant \Omega\left(|c|\right) + (\deg f)\Omega\left(|F(\mathbf{x})|\right)$$

and $\Omega(|c|) \leqslant (\log|c|)/(\log 2) \leqslant (\log\|f\|)/(\log 2) \leqslant 2\log\|f\|$ yields the desired value of r.

We are now ready to prove Theorems 1.2 and 1.4.

It is sufficient to show that with the value of r given in Theorem 1.4 the set of rational points $x \in X(\mathbb{Q})$ satisfying $\Omega_{\mathbb{P}^n(\mathbb{Q})}(x) \leqslant r$, is dense in the image of the $\mathbb{Q}$-points of $\mathbb{P}^m$ under the map π and with respect to the real analytic topology. Let us therefore fix any $\varepsilon > 0$ and a rational point $\pi(y)$, where $y = [\mathbf{y}] \in \mathbb{P}^m_{\mathbb{Q}}$ for some integer vector $\mathbf{y} = (y_i)_{i=0}^{m}$. By continuity of the forms f_j there exists $\delta > 0$, which depends on ε, f_i and $\mathbf{y}$, such that for any $\mathbf{X} \in \mathbb{R}^{m+1}$ specified by $|\mathbf{X} - \mathbf{y}| \leqslant \delta$, one has $|f_j(X_i) - f_j(y_i)| < \varepsilon$ for all i and j. Applying Theorem 3.1

to the form $f := \prod_{i=0}^{n} f_i$ and the box $\mathscr{R}^{(0)} = \prod_{i=0}^{m}[y_i - \delta, y_i + \delta]$, we are presented with a value of r in the range

$$r \leqslant 6 \deg^2(f)(\log 2\|f\|) + 10^4 \deg^7(f),$$

a rational point $x = [\mathbf{x}]$ satisfying $\Omega_{\mathbb{P}^n(\mathbb{Q})}(x) \leqslant r$ and whose image is ε-close to $\pi(y)$ due to

$$\left| \frac{f_j(x_i)}{B^{\deg f_j}} - f_j(y_i) \right| < \varepsilon.$$

This concludes the proof of Theorems 1.2 and 1.4 owing to

$$6 \deg^2(f)(\log 2\|f\|) + 10^4 \deg^7(f) \leqslant 10^5 \deg^7(f) \log(2\|f\|).$$

4. The proof of Theorem 1.5

Throughout this section X will be a smooth cubic surface with two rational skew lines. We begin by picking an appropriate model for X.

Lemma 4.1 (Minimal model). *There exist integers a_i, d_i, f_i $(i = 0, 1)$ and b_j, e_j $(j = 0, 1, 2)$ such that X is given by $F = 0$, where*

$$F = a(x_0, x_1)x_2^2 + d(x_0, x_1)x_2x_3 + f(x_0, x_1)x_3^2 + b(x_0, x_1)x_2 + e(x_0, x_1)x_3, \quad (4.1)$$

$$\begin{pmatrix} a(x_0, x_1) \\ d(x_0, x_1) \\ f(x_0, x_1) \end{pmatrix} := \begin{pmatrix} a_0 & a_1 \\ d_0 & d_1 \\ f_0 & f_1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

and

$$\begin{pmatrix} b(x_0, x_1) \\ e(x_0, x_1) \end{pmatrix} := \begin{pmatrix} b_0 & b_1 & b_2 \\ e_0 & e_1 & e_2 \end{pmatrix} \begin{pmatrix} x_0^2 \\ x_0x_1 \\ x_1^2 \end{pmatrix}.$$

Furthermore these integers satisfy the following two properties.

(1) *The greatest common factor of the six integers a_i, d_i, f_i $(i = 0, 1)$ is 1 and this also holds for the six integers b_j, e_j $(j = 0, 1, 2)$.*

(2) *The integers a_0b_0 and 6 are coprime and each other of the aforementioned twelve integers is divisible by 6.*

Proof. A linear change of variables over $\mathbb{Q}$ allows us to assume that the pair of skew lines is given by $x_0 = x_1 = 0$ and $x_2 = x_3 = 0$. Therefore X is given by $C_1 + C_2 = 0$, where C_1 is linear in x_0, x_1 and quadratic in x_2, x_3 and the opposite is true for C_2, a statement which immediately shows (4.1). It follows from the non-singularity of the surface that the polynomials a and b are not identically zero. Then under a suitable linear change of variables, if necessary, we may have $a_0b_0 \neq 0$.

Let k_1 and k_2 be the greatest common divisor of the the six integers b_j, e_j $(j = 0, 1, 2)$ and a_i, d_i, f_i $(i = 0, 1)$ respectively. Then the linear change of variables

$$(x_0, x_1, x_2, x_3) \mapsto (k_2x_0, k_2x_1, k_1x_2, k_1x_3)$$

shows that we can assume that $k_1 = k_2 = 1$, which proves (1). In order to prove claim (2), let us define the integers

$$\alpha = 1 + \max\{\nu_2(a_0) + \nu_2(b_0), 2\nu_2(b_0)\} \text{ and } \beta = 1 + \max\{\nu_2(a_0) + \nu_2(b_0), 2\nu_2(a_0)\}.$$

Then the transformation

$$(x_0, x_1, x_2, x_3) \mapsto \left(2^{\nu_2(a_0)}x_0, 2^\beta x_1, 2^{\nu_2(b_0)}x_2, 2^\alpha x_3\right)$$

reveals that property (2) holds for the prime 2. An identical argument for the prime 3 concludes the proof of the lemma. □

We turn our attention to the conic bundle structure present in X. Writing $F = x_0 Q_0 - x_1 Q_1$, where Q_i are integral quaternary quadratic forms, we see that X is equipped with a dominant morphism $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ such that

$$\pi(x) = \begin{cases} [x_0 : x_1] & \text{if } (x_0, x_1) \neq 0, \\ [Q_1(x) : Q_0(x)] & \text{if } (Q_1(x), Q_0(x)) \neq 0. \end{cases}$$

Lemma 4.1 reveals that the fibres $\pi^{-1}(s : t)$ are the conics $Q_{s,t} = 0$ given by

$$Q_{s,t}(x, y, z) := a(s,t)x^2 + d(s,t)xz + f(s,t)z^2 + b(s,t)xy + e(s,t)zy.$$

Their discriminant

$$\Delta(s, t) = \left(ae^2 + fb^2 - bde \right)(s, t)$$

is a quintic binary form and is separable owing to the non-singularity of X (see [32, 80, II.6.4, Proposition 1]).

Lemma 4.2. *The following polynomials are not identically zero,*

$$a, b, e, f, d^2 - 4af.$$

Furthermore the forms a, d, f do not share a common polynomial divisor and the same holds for b and e.

Proof. If the forms a, d, f had a common divisor in $\mathbb{Q}[s, t]$ then the polynomials

$$p_1(x, y) = a_0 x^2 + d_0 xy + f_0 y^2 \text{ and } p_2(x, y) = a_1 x^2 + d_1 xy + f_1 y^2,$$

would share a common zero $[\alpha : \beta] \in \mathbb{P}^1(\overline{\mathbb{Q}})$. We would then obtain a singularity on the cubic surface, since $\nabla F(0, 0, x, y) = (p_1(x, y), p_2(x, y), 0, 0)$. If $a = 0$ or $f = 0$ then the partial derivatives of F vanish at the points $(0, 0, 1, 0)$ and $(0, 0, 1, 0)$ respectively. These observations prove that $d^2 \neq 4af$ since $\mathbb{Q}[s, t]$ is a unique factorisation ring. The fact that the discriminant $\Delta(s, t)$ is separable implies that b and e are coprime forms. In particular they can neither be identically zero, which finishes our proof. □

We deduce that the resultant $W_0 := \text{Res}(b, e)$ is a non-zero integer. We furthermore get that at least one pair of the linear forms a, d, f has a non-zero resultant, say W_1.

Define for $(s, t) \in \mathbb{Z}^2_{\text{prim}}$ the forms

$$G_{s,t}(u, v) := b(s,t) u + e(s,t) v \text{ and } H_{s,t}(u, v) := a(s,t) u^2 + d(s,t) uv + f(s,t) v^2,$$

where the polynomials $a, \ldots, f$ were defined in Lemma 4.1.

Each conic $Q_{s,t} = 0$ contains the obvious point $(0, 1, 0)$, a fact which can be used to provide the following parametrisation of $Q_{s,t}(x, y, z) = 0$,

$$(x, y, z) = (uG_{s,t}(u, v), -H_{s,t}(u, v), vG_{s,t}(u, v)).$$

The weighted sieve will allow us to to show that for appropriate values of s, t both forms $G_{s,t}(u, v)$ and $H_{s,t}(u, v)$ attain almost prime values. We begin by establishing certain facts required for the sieving process.

Lemma 4.3. *For each prime p there exists $s_0, t_0 \in (\mathbb{Z}/p\mathbb{Z})^*$ such that both integers*

$$\gcd(b(s_0, t_0), e(s_0, t_0)) \quad and \quad \gcd(a(s_0, t_0), d(s_0, t_0), f(s_0, t_0))$$

are coprime to p.

Proof. The second part of Lemma 4.1 implies that one can take $s_0 \equiv t_0 \equiv 1 \mod p$ when $p = 2$ or 3. Let p be any prime larger than 3. The first part of Lemma 4.1 states that p cannot divide all six integers b_j, e_j $(j = 0, 1, 2)$ so we may assume by symmetry that $p \nmid \gcd(b_0, b_1, b_2)$. We may similarly assume that $p \nmid \gcd(a_0, a_1)$. We proceed to show the validity of the bounds

$$\sharp\{s, t \in (\mathbb{Z}/p\mathbb{Z})^*, \ p|b(s, t)\} \leqslant 2(p-1) \quad and \quad \sharp\{s, t \in (\mathbb{Z}/p\mathbb{Z})^*, \ p|a(s, t)\} \leqslant p - 1.$$

The first bound is obvious in the case $p|(b_0, b_2)$. In the opposite case we may assume that $p \nmid b_0$ so the number of solutions of $b(s, t) \equiv 0 \mod p$ is the same as the number of solutions of $(2b_0 s + b_1 t)^2 \equiv (b_1^2 - 4b_0 b_2) t^2 \mod p$, which is at most $2(p-1)$. The second bound follows by the fact that $p \nmid (a_0, a_1)$. Combining the two bounds implies that

$$\sharp\{s, t \in (\mathbb{Z}/p\mathbb{Z})^*, \ p|a(s, t) b(s, t)\} \leqslant 3(p-1),$$

which is strictly smaller than $(p-1)^2$ for $p > 3$ and that concludes the proof of the lemma. $\square$

Lemma 4.4. *There exists a square-free W and integers s_0, t_0 with $(s_0 t_0, W) = 1$ such that whenever the coprime integers s and t satisfy $(s, t) \equiv (s_0, t_0) \mod W$, then both integer forms $G_{s,t}, H_{s,t}$ are primitive.*

Proof. We define W as the product of the primes appearing in W_0 and W_1. Combining the Chinese remainder theorem and Lemma 4.3 for the primes dividing W provides congruence classes $\mod W$, say s_0 and t_0. Assume that the coprime integers s and t satisfy

$$(s, t) \equiv (s_0, t_0) \mod W$$

and suppose for a contradiction that $G_{s,t}$ is not primitive so that there exists a prime p that divides both $b(s, t)$ and $e(s, t)$. Elimination theory applied to $b(x, 1), e(x, 1)$ and $b(1, x), e(1, x)$ shows that there are integer binary forms $g_i(s, t)$ $(i = 1, \ldots, 4)$ and non-negative integers μ_j $(j = 1, 2)$ such that

$$b(s, t)g_1(s, t) + e(s, t)g_2(s, t) = W_0 t^{\mu_1} \quad and \quad b(s, t)g_3(s, t) + e(s, t)g_4(s, t) = W_0 s^{\mu_2}.$$

The coprimality of s and t implies that p divides W_0 and this contradicts the choice of s_0, t_0 by Lemma 4.3. A similar argument works proves that $H_{s,t}$ is also primitive and thus the proof is complete. $\square$

Define the following binary integer forms,

$$\Phi_1(u, v) := u,$$
$$\Phi_2(u, v) := v,$$
$$\Phi_3(u, v) := bu + ev,$$
$$\Phi_4(u, v) := au^2 + duv + fv^2$$

and let

$$\Phi := \Phi_1 \Phi_2 \Phi_3^2 \Phi_4^2.$$

Our aim henceforth is to show that the form $\Phi(u, v)$ attains almost prime values infinitely often. To this aim it is natural to assume the following local conditions,

$$6 \mid (e, d, f), \qquad\qquad \gcd(6, ab) = 1, \qquad\qquad (4.2)$$
$$\gcd(b, e) = 1, \qquad\qquad \gcd(a, d, f) = 1, \qquad\qquad (4.3)$$
$$D \text{ is a non-zero integer}, \qquad\qquad (4.4)$$

where

$$D := \operatorname{rad}\Big(2 \cdot 3 \cdot 5 \cdot abef \left(d^2 - 4af\right)\left(ae^2 + fb^2 - bde\right)\Big).$$

There are two cases to consider according to the splitting behavior of the quadratic form Φ_4 over the rationals. Although both cases can be treated via the weighted sieve we shall use Theorem 2.2 for the former case. The reason is that this approach provides special examples of smooth cubic surfaces (see (1.1)) for which the saturation number is particularly small. As an application we deduce the following lemma.

Lemma 4.5. *Assume that the integers* a, b, d, e, f *satisfy conditions* (4.2)-(4.4) *and that* $d^2 - 4af$ *is a non-zero integer square. Let* $\mathscr{R}$ *be any non-empty box in* $\mathbb{R}^2$. *Then*

$$\lim_{B \to +\infty} \sharp\{(u, v) \in \mathbb{Z}^2 \cap \mathscr{R}B, \ \Omega(\Phi(u, v)) \leqslant 8\} = +\infty.$$

Proof. Assume that $d^2 - 4af = \delta^2$ for some natural δ. This implies that there are integers a_1, a_2 with $a = a_1 a_2$ that divide the integers $(d - \delta)/2, (d + \delta)/2$ respectively. The identity

$$\Phi_4(u, v) = \left(a_2 u + \frac{(d - \delta)}{2a_1} v\right)\left(a_1 u + \frac{(d + \delta)}{2a_2} v\right)$$

shows that Φ_4 splits into two integer linear binary forms, say L_4, L_5. Note that Φ_4 has no fixed prime divisor owing to (4.2) and (4.3) and thus this property also holds for both linear forms.

We apply Theorem 2.2 with $L_i = \Phi_i$ for $i = 1, 2, 3$. The condition (4.4) guarantees that the linear forms are pairwise non-proportional. Let us verify the remaining condition of Theorem 2.2 by contradiction. Assume that for every prime p and all integers u, v there exists an index $1 \leqslant i \leqslant 5$ such that $p \mid L_i(u, v)$. We may show that we only need to restrict attention to the primes $p = 2, 3$ since if $p \geqslant 5$ then

$$\sharp\{u, v \in (\mathbb{Z}/p\mathbb{Z})^*, p \nmid (L_3 L_4 L_5)(u, v)\} \leqslant 3(p - 1),$$

which is strictly smaller than $(p - 1)^2$. Regarding the primes $p = 2, 3$ we note that conditions (4.2) and (4.3) ensure that we get a contradiction.

Theorem 2.2 provides a choice of signs $s_i \in \{1, -1\}, i = 1, \ldots, 5$, such that the 5 linear form $s_i L_i$ attain prime values infinitely often. Recalling the extended definition of Ω given in the introduction proves the statement of our lemma. $\qquad\square$

We next apply a level of distribution result [27, Th.3] to prove the corresponding result in the remaining case.

Lemma 4.6. *Assume that the integers* a, b, d, e, f *satisfy conditions* (4.2)-(4.4)*, that* $d^2 - 4af$ *is not an integer square and let* $\mathscr{R}$ *be a box of* $\mathbb{R}^2$*. Then*

$$\sharp\{(u, v) \in \mathbb{Z}^2 \cap \mathscr{R}B, \ \Omega(\Phi(u, v)) \leqslant 30\} \gg \frac{B^2}{(\log B)^4},$$

for $B \geqslant 2$. The implied constant in the lower bound depends at most on the coefficients of Φ and $\mathscr{R}$.

Proof. Arguing as in Lemma 4.3 for every prime $p|D$ and using the Chinese remainder theorem, we get that there are integers $u_0, v_0 \mod D$ such that

$$\gcd(\Phi(u_0, v_0), D) = 1. \tag{4.5}$$

Define the integer binary form $\Phi' := \Phi_1 \Phi_2 \Phi_3 \Phi_4$ and the subset of $\mathbb{Z}^2$,

$$\Psi := \{(u, v) \in \mathbb{Z}^2 : (u, v) \equiv (u_0, v_0) \mod D\}.$$

We write $\mathscr{A}' := \{\Phi'(u, v) : (u, v) \in \mathscr{R}B \cap \Psi\}$ and we let for every non-zero integer d,

$$\mathscr{A}'_d := \{a' \in \mathscr{A}' : d|a'\}.$$

Let for any $\mathbf{c} = (c_1, \dots, c_4) \in \mathbb{N}^4$, $\rho(\mathbf{c})$ be the the multiplicative function given by

$$\rho(\mathbf{c}) := \sharp\{(u, v) \mod c_1 \dots c_4 : c_i | \Phi_i(u, v), i = 1, \dots, 4\}.$$

Define the following sets of primes,

$$\mathfrak{P} := \{p \text{ prime} : p \nmid D\} \text{ and } \overline{\mathfrak{P}} := \{p \text{ prime} : p|D\}$$

and define the multiplicative function $\varpi(n)$ to be supported on square-free integers and

$$\varpi(p) := \mathbb{1}_{\mathfrak{P}}(p) \, p \sum_{\substack{c_i | p \\ i = 1, \dots, 4 \\ p | c_1 \dots c_4}} \mu(p) \mu(c_1) \dots \mu(c_4) \frac{\rho(c_1, \dots, c_4)}{(c_1 \dots c_4)^2},$$

where $\mathbb{1}_{\mathfrak{P}}$ is the characteristic function of the primes in $\mathfrak{P}$. Let

$$Y := B^2 \frac{\operatorname{vol}(\mathscr{R})}{D^2}$$

and define for $d \in \mathbb{N}$ the quantity

$$R_d := \sharp \mathscr{A}'_d - \frac{\varpi(d)}{d} Y.$$

We need to verify the conditions (A)-(E) appearing in [27, Th.3] as well as condition Q_0 appearing in [10, Eq.(11.2)], which does not seem to appear in [27].

Condition (Q_0): Here we have to verify that the estimate

$$\sum_{z < p \leqslant y} \sharp \mathscr{A}'_{p^2} \ll \frac{Y \log Y}{z} + y$$

holds for all $2 \leqslant z < y$ with an implied constant that is independent of z, y and Y. The equality

$$\mathscr{A}'_{p^2} = \left\{(u, v) \in \mathscr{R}B : (u, v) \equiv (u_0, v_0) \mod D, p^2 | \Phi_1(u, v) \dots \Phi_4(u, v)\right\}$$

shows by (4.5) that $\mathscr{A}'_{p^2}$ is empty if $p|D$. Note that since $\gcd(D, \Phi(u_0, v_0)) = 1$ and $(u, v) \equiv (u_0, v_0) \mod D$ we get that $\gcd(D, \Phi'(u, v)) = 1$ and hence no pair of integers (u, v) with

$\Phi'(u, v) = 0$ is counted by $\mathscr{A}'_{p^2}$. We therefore obtain that $\sum_{z<p\leqslant y} \sharp\mathscr{A}'_{p^2}$ is

$$\ll \sum_{i=1}^{4} \sum_{\substack{z<p\leqslant y \\ p\nmid D}} \sharp\Big\{(u, v) \in \mathscr{R}B, \Phi'(u, v) \neq 0, \gcd(D, \Phi_i(u, v)) = 1, p^2|\Phi_i(u, v)\Big\}$$

$$+ \sum_{\substack{1\leqslant i,j\leqslant 4 \\ i\neq j}} \sum_{\substack{z<p\leqslant y \\ p\nmid D}} \sharp\Big\{(u, v) \in \mathscr{R}B, \Phi'(u, v) \neq 0, p|(\Phi_i(u, v), \Phi_j(u, v))\Big\}.$$

Recall the definition of D given immediately after (4.4) and note that the primes dividing the resultants of each pair of forms Φ_i, Φ_j divides D. Hence, since $p \nmid D$ in the previous sums, we see that

$$\sharp\Big\{(u, v) \in \mathscr{R}B, p|(\Phi_i(u, v), \Phi_j(u, v))\Big\} \ll \sharp\Big\{(u, v) \in \mathscr{R}B, p|(u, v)\Big\} \ll \frac{B^2}{p^2} + 1.$$

For $i = 1$ we have $\sharp\{(u, v) \in \mathscr{R}B, \Phi'(u, v) \neq 0, p^2|\Phi_i(u, v)\} \ll \sharp\{(u, v) \in \mathscr{R}B, uv \neq 0, p^2|u\}$, which is at most $\ll B^2p^{-2}$ and one obtains the same upper bound in the case $i = 2$. For $i = 3$ we have the bound $\ll \sharp\{(u, v) \in \mathscr{R}B, (bu + ev)v \neq 0, p^2|bu + ev\}$ and the change of variables $x_1 := bu + ev, x_2 := v$ reveals that the quantity is bounded by $\ll \sharp\{|x_1|, |x_2| \ll B, x_1x_2 \neq 0, p^2|x_1\}$, which is easily seen to be at most $\ll B^2p^{-2}$. For $i = 4$ we have

$$\sharp\Big\{(u, v) \in \mathscr{R}B, uv\Phi_4(u, v) \neq 0, \gcd(D, \Phi_i(u, v)) = 1, p^2|\Phi_i(u, v)\Big\} \ll \sum_{\substack{1\leqslant p^2n\ll B^2 \\ \gcd(pn,D)=1}} r_{D_0}(p^2n),$$

where the function $r_{D_0}(n)$ denotes the number of representations of an integer n by all binary quadratic forms forming a set of representatives of discriminant equal to

$$D_0 := \operatorname{disc}(\Phi_4) = d^2 - 4af.$$

Note that D_0 is a non-zero integer which is not a square since Φ_4 is irreducible and that $\gcd(n, D_0) = 1$ holds in the previous summation since all primes dividing D_0 also divide D by its definition. Using the fact that r_{D_0} can be written as a Dirichlet convolution of 1 and a quadratic character we obtain the trivial bound $r_{D_0}(n) \ll \tau(n)$, where τ denotes the classical divisor function. Writing $n = p^\nu n_0$ with $p \nmid n_0$ we obtain

$$\sum_{\substack{1\leqslant p^2n\ll B^2 \\ \gcd(pn,D)=1}} r_{D_0}(p^2n) \ll \sum_{\nu=0}^{\infty} \tau(p^{2+\nu}) \sum_{\substack{n_0\ll B^2/p^{2+\nu} \\ p\nmid n_0}} \tau(n_0) \ll \frac{B^2 \log B}{p^2} \sum_{\nu=0}^{\infty} \frac{\tau(p^{2+\nu})}{p^\nu}.$$

The function $\sum_{\nu>0}(3+\nu)p^{-\nu} = (3-2/p)(1-1/p)^{-2}$ has modulus at most 8 for $p \geqslant 2$. Hence, we get that $\#\mathscr{A}'_{p^2} \ll 1 + \frac{B^2 \log B}{p^2}$, which along with the estimate $\sum_{p>z} p^{-2} \ll z^{-1}$ shows that

$$\sum_{z<p\leqslant y} \#\mathscr{A}'_{p^2} \ll \frac{B^2 \log B}{z} + y.$$

This is the required estimate since Y is of order B^2.

Condition (A): It is shown in [27, §3.1,pg. 310] that $\varpi(p) < p$ for all $p > 5$ and since $\{2, 3, 5\} \subseteq \overline{\mathfrak{P}}$ we get that $\varpi(p) = 0$ for $p = 2, 3$ and 5.

Condition (B): Everything goes through as in [27, §3.2,pg.311] where the dimension of the sieve is $\kappa = 4$.

Condition (C): It appears that the argument justifying the analogous result in [27, pg.314] is not sufficiently detailed. More specifically, for values of k that are small in comparison to Y the term $\frac{Y^{1/2}2^Q}{k}$ in line 17 has order of magnitude which is larger than the claimed bound for $E(k)$ in line 21. Correcting this inaccuracy we get

$$E(k) \ll Q^\nu \Big(2^Q + \frac{\big(2^Q Y\big)^{1/2}}{k} + \frac{Y^{1/2}2^Q}{k} \Big),$$

for some absolute constant ν. Therefore condition (C) is satisfied with $\alpha = 1/2 - \eta$, for any arbitrarily small and positive value of η.

Condition (D): Follows directly from (4.5).

Condition (E): Every element $a' \in \mathscr{A}'$ satisfies $a' \ll B^5$, where the implied constant depends on F and $\mathscr{R}$. Therefore there exists $\mu > \frac{5}{\alpha}$, which depends on $F, \mathscr{R}$ and η, such that

$$|a'| \leqslant Y^{\alpha\mu}.$$

Hence the conditions of theorem [27, Th.3] are fulfilled.

Furthermore, arguing similarly as in [22, §6], we obtain that one may take any value of r larger than $m(\lambda) := 4\log\beta_4 + (5 - \frac{1}{\beta_4} + \log\beta_4)\lambda - 4\log\lambda - \lambda\log\lambda$. Note that by [11, App.III] we have $\beta_4 = 9.0722\dots$. We thus deduce that

$$\min_{0 < \lambda < \beta_4} m(\lambda) = m(0.606519\dots) = 15.4274522\dots$$

and therefore with the value $r = 16$ one has

$$\#\Big\{ (u,v) \in \mathbb{Z}^2 \cap \mathscr{R}B, \Omega(\Phi'(u,v)) \leqslant r \Big\} \gg \frac{B^2}{(\log B)^4},$$

as $B \to \infty$. The pairs of integers $(u,v) \in \mathscr{R}B$ with $\Omega(uv) \leqslant 1$ are such that $|uv|$ is $0, 1$ or a prime, thereby showing that there are at most $\ll B$ such pairs. We conclude that

$$\#\Big\{ (u,v) \in \mathbb{Z}^2 \cap \mathscr{R}B, \Omega(\Phi'(u,v)) \leqslant 16 \text{ and } \Omega(uv) \geqslant 2 \Big\} \gg \frac{B^2}{(\log B)^4},$$

as $B \to \infty$. This observation coupled with the equality $\Omega(\Phi(u,v)) = 2\,\Omega(\Phi'(u,v)) - \Omega(uv)$ completes the proof of Theorem 4.6. □

We continue by using Lemmas 4.5 and 4.6 to ensure that the $\mathbb{Q}$-rational fibre $\pi^{-1}([s:t])$ is birationally equivalent to $\mathbb{P}^1_{\mathbb{Q}}$ through almost prime values.

The case corresponding to $n = 2$ of [20, Th.1.1] implies that $\overline{X}(\mathbb{R}) = X$. For any point $\boldsymbol{\xi} = (\xi_0, \dots, \xi_3) \in X(\mathbb{R})$ let us define

$$M_{\boldsymbol{\xi}} := b(\xi_0, \xi_1)\xi_2 + e(\xi_0, \xi_1)\xi_3$$
$$= -a(\xi_0, \xi_1)\xi_2^2 - d(\xi_0, \xi_1)\xi_2\xi_3 - f(\xi_0, \xi_1)\xi_3^2$$

and note that the points satisfying $\xi_0\xi_1 M_{\boldsymbol{\xi}} \neq 0$ are also Zariski dense. Hence in order to prove Zariski density of almost prime points it suffices to prove that given any such $\boldsymbol{\xi}$ and any $\varepsilon > 0$ there exists $B \in \mathbb{Q}^*$ and $\mathbf{x} \in \mathbb{Z}^4$ with $\Omega(|x_0 \dots x_3|) \leqslant 34$ such that $[\mathbf{x}] \in X$ and

$$\max_{0 \leqslant i \leqslant 3} \left| \frac{x_i}{B} - \xi_i \right| < \varepsilon. \tag{4.6}$$

Let $\delta \in (0,1)$ be a constant to be specified in due course and consider the following box of $\mathbb{R}^2$,

$$\mathscr{B} := [\xi_0 - \delta, \xi_0 + \delta] \times [\xi_1 - \delta, \xi_1 + \delta].$$

The prime number theorem for arithmetic progressions [19, §5.6] supplies a large positive number P such that the box $P\mathscr{B}$ contains a pair of, not necessarily positive, primes (s, t) lying in the progressions mod W specified by Lemma 4.4. A standard application of the mean value theorem yields

$$\left| b\left(\frac{s}{P}, \frac{t}{P}\right)\xi_2 + e\left(\frac{s}{P}, \frac{t}{P}\right)\xi_3 - M_{\boldsymbol{\xi}} \right| \ll_{X,\boldsymbol{\xi}} \delta \tag{4.7}$$

and

$$\left| a\left(\frac{s}{P}, \frac{t}{P}\right)\xi_2^2 + d\left(\frac{s}{P}, \frac{t}{P}\right)\xi_2\xi_3 + f\left(\frac{s}{P}, \frac{t}{P}\right)\xi_3^2 + M_{\boldsymbol{\xi}} \right| \ll_{X,\boldsymbol{\xi}} \delta, \tag{4.8}$$

where the implied constant in both bounds is independent of P and δ. Let

$$\mathscr{R} := \left[\frac{\xi_2 - \delta}{P\sqrt{M_{\boldsymbol{\xi}}}}, \frac{\xi_2 + \delta}{P\sqrt{M_{\boldsymbol{\xi}}}}\right] \times \left[\frac{\xi_3 - \delta}{P\sqrt{M_{\boldsymbol{\xi}}}}, \frac{\xi_3 + \delta}{P\sqrt{M_{\boldsymbol{\xi}}}}\right].$$

Applying Lemma 4.5 or Lemma 4.6 respectively according to as if $(d^2 - 4af)(s, t)$ is an integer square or not, provides integers $(u, v) \in B^{\frac{1}{2}}\mathscr{R}$ such that $uvH_{s,t}^2(u, v) G_{s,t}^2(u, v)$ has respectively at most 8 or 30 prime factors counted with multiplicity. Define $\mathbf{x} \in \mathbb{Z}^4$ by

$$x_0 = -sH_{s,t}(u, v),$$
$$x_1 = -tH_{s,t}(u, v),$$
$$x_2 = u\, G_{s,t}(u, v),$$
$$x_3 = v\, G_{s,t}(u, v).$$

A further application of the mean value theorem and a use of (4.7)- (4.8) shows that

$$\max_{0 \leqslant i \leqslant 3} \left| \frac{x_i}{B} - \xi_i \right| \ll_{X,\boldsymbol{\xi}} \delta,$$

thereby proving (4.6) for an appropriate $\delta := \delta\left(\varepsilon, X, \boldsymbol{\xi}\right)$.

Remark 4.7. It is worth pointing out that a special corollary of the work in this section is that whenever $a_i, e_i, f_i, (i = 0, 1)$ $b_j, d_j (j = 0, 1, 2)$ are 12 integers with

$$\gcd_{i=0,1}(a_i, d_i, f_i) = \gcd_{j=0,1,2}(b_j, e_j) = 1, \gcd(6, a_0 b_0) = 1, 6 \mid \gcd(a_1, b_1, b_2), 6 \mid \gcd_{i=0,1}(d_i, e_i, f_i)$$

and the binary integer quadratic form

$$(d_0 s + d_1 t)^2 - 4(a_0 s + a_1 t)(f_0 s + f_1 t)$$

is the square of a polynomial in $\mathbb{Q}[s, t]$, then the cubic surface X given by the vanishing of

$$(a_0 x_0 + a_1 x_1)x_2^2 + (d_0 x_0 + d_1 x_1)x_2 x_3 + (f_0 x_0 + f_1 x_1)x_3^2$$
$$+ (b_0 x_0^2 + b_1 x_0 x_1 + b_2 x_0^2)x_2 + (e_0 x_0^2 + e_1 x_0 x_1 + e_2 x_0^2)x_3$$

is smooth and has saturation number

$$r(X) \leqslant 10.$$

It is easily seen that (1.1) constitutes a special case of the surfaces alluded to in the present remark. This proves the claim regarding the saturation of the surface in (1.1) that was made in the introduction.

5. The proof of Theorem 1.6

The Fermat cubic threefold is equipped with a conic bundle over $\mathbb{P}^2_{\mathbb{Q}}$ and we begin by describing its structure. The change of variables

$$y_0 = x_0, y_1 = \frac{x_1 + x_3}{2}, y_2 = \frac{x_2 + x_4}{2}, y_3 = \frac{x_1 - x_3}{2}, y_4 = \frac{x_2 - x_4}{2},$$

transforms the hypersurface

$$X : x_0^3 + x_1^3 + x_2^3 + x_3^3 + x_4^3 = 0$$

into

$$Y : y_0^3 + 2y_1 \left(y_1^2 + 3y_3^2\right) + 2y_2 \left(y_2^2 + 3y_4^2\right) = 0.$$

Let us record here that any $y \in Y(\mathbb{R})$ has y_0, y_1, y_2 not of the same sign. Projecting away from the line $y_0 = y_1 = y_2 = 0$ contained in Y provides a conic bundle morphism $\pi : Y \to \mathbb{P}^2_{\mathbb{Q}}$. The transformation $\mathbf{y} = (rx, sx, tx, y, z)$ shows that the fibres $Q_{r,s,t} = 0$ are given by

$$x^2 \left(r^3 + 2s^3 + 2t^3\right) + y^2 \left(6s\right) + z^2 \left(6t\right) = 0.$$

We wish to construct an infinite family of conic fibres each member of which is $\mathbb{Q}$-rational and with a parametrisation for their rational points which is easy to describe. We focus on the conics given by $Q_{p_1, -p_2^2, p_3^2} = 0$, where p_i are primes. Note that they contain the obvious point $(0, p_3, p_2)$, thus providing the parametrisation

$$x = 12 p_2 p_3^2 uv,$$
$$y = 6 p_3^3 u^2 + p_3 \left(p_1^3 - 2p_2^6 + 2p_3^6\right) v^2,$$
$$z = -6 p_2 p_3^2 u^2 + p_2 \left(p_1^3 - 2p_2^6 + 2p_3^6\right) v^2.$$

Tracing the substitutions backwards allows us to conclude that the points $(x_0, \dots x_4)$ given by

$$\left(12 p_1 p_2 p_3^2 f_0(u, v), p_3 f_1(u, v), p_3 f_2(u, v), p_2 f_3(u, v), p_2 f_4(u, v)\right)$$

lie in the threefold X, where the binary integer forms $f_j \in \mathbb{Z}[u, v]$ are defined through

$$f_0 := uv,$$
$$f_1 := 6p_3^2 u^2 - 12 p_2^3 p_3 uv + \left(p_1^3 - 2p_2^6 + 2p_3^6\right) v^2,$$
$$f_2 := -6p_3^2 u^2 - 12 p_2^3 p_3 uv - \left(p_1^3 - 2p_2^6 + 2p_3^6\right) v^2,$$
$$f_3 := -6p_3^2 u^2 + 12 p_3^4 uv + \left(p_1^3 - 2p_2^6 + 2p_3^6\right) v^2,$$
$$f_4 := 6p_3^2 u^2 + 12 p_3^4 uv - \left(p_1^3 - 2p_2^6 + 2p_3^6\right) v^2.$$

Observe that all $\mathbf{x} \in \mathbb{Z}^5$ on X satisfy $7 | \prod_{i=0}^4 x_i$. We have

$$\prod_{i=0}^4 x_i = 84 p_1 p_2^3 p_3^4 \left(\frac{1}{7} \prod_{i=0}^4 f_i(u, v)\right).$$

Now suppose that we are given a point $(\xi_0, \dots, \xi_4) \in X(\mathbb{R})$ which we shall approximate. The linear change of variables

$$\zeta_0 = \xi_0, \zeta_1 = \frac{\xi_1 + \xi_3}{2}, \zeta_2 = \frac{\xi_2 + \xi_4}{2}, \zeta_3 = \frac{\xi_1 - \xi_3}{2}, \zeta_4 = \frac{\xi_2 - \xi_4}{2}$$

shows that $\boldsymbol{\zeta} \in Y(\mathbb{R})$ thus allowing us to assume without loss of generality that

$$\zeta_0 > 0, \zeta_1 < 0, \zeta_2 > 0.$$

owing to an earlier observation.

Now let δ be a small positive constant satisfying $0 < \delta < 1$. For a large constant $C > 0$, the Siegel–Walfisz theorem allows us to pick primes p_1, p_2, p_3 satisfying

$$p_i \equiv 1 \mod q \text{ for all } i = 1, 2, 3 \text{ for all } q = 2, 3, 5, 49, \tag{5.1}$$

$$(p_1, -p_2^2, p_3^2) \in C((\zeta_0 - \delta, \zeta_0 + \delta) \times (\zeta_1 - \delta, \zeta_1 + \delta) \times (\zeta_2 - \delta, \zeta_2 + \delta)),$$

$$p_3 \nmid p_1^3 - 2p_2^6,$$

$$p_1^3 - 8p_2^6 + 2p_3^6 \neq 0,$$

$$p_3 \left(p_1^3 - 2p_2^6 + 2p_3^6 \right) \neq 0, \tag{5.2}$$

With this choice of p_i we shall apply the weighted sieve, as in the proof of Lemma 4.6, in order to deduce that the form

$$F(u, v) := \frac{1}{7} \prod_{i=0}^{4} f_i (u, v)$$

attains almost prime values infinitely often. Firstly, for $i = 1, \ldots, 4$, each f_i is irreducible,

$$\operatorname{disc}(f_1) = \operatorname{disc}(f_2) = 24 p_3^2 \left(-p_1^3 + 8p_2^6 - 2p_3^6 \right).$$

The condition (5.1) yields $-p_1^3 + 8p_2^6 - 2p_3^6 \equiv 2 \mod 3$ and hence $\operatorname{disc}(f_1) \neq 0$. Furthermore the same condition gives $3 \| \operatorname{disc}(f_1)$, i.e. f_1 and f_2 are irreducible over $\mathbb{Q}$. A similar argument shows that the same holds true for both f_3 and f_4. We next deduce that for $i = 1, \ldots, 4$ since the assumptions $p_i \equiv 1 \mod 6, i = 1, 2, 3$ yield that

$$\gcd \left(6, p_1^3 - 2p_2^6 + 2p_3^6 \right) = 1$$

and it suffices to note that $p_3 \nmid (p_1^3 - 2p_2^6)$. Condition (C) is then proved as follows. Let us define

$$D := \operatorname{rad}\left(\left(\prod_{p<10} p \right) \left(\prod_{i=1}^{4} a_i c_i \operatorname{disc}(f_i) \right) \left(\prod_{1 \leqslant i, j \leqslant 4} \operatorname{Res}(f_i, f_j) \right) \right),$$

where a_i and c_i are the coefficient of u^2 and v^2 in f_i respectively. Note that (5.2) guarantees that u or v are coprime forms to each $f_i, \forall i \neq 0$. We need to find some $\mathbf{z}$ such that

$$(u, v) \equiv \mathbf{z} \mod D$$

in order to have

$$\gcd \left(\frac{1}{7} \prod_{i=0}^{4} f_i(u, v), D \right) = 1. \tag{5.3}$$

For the primes $p = 2, 3, 5, 7$ we make the choices for $(u, v) \mod p$ given by

$$(1, 1), (1, 1), (1, 2), (1, 1)$$

respectively. For the primes $p \geqslant 11$ we have the estimate

$$\sharp\{u, v \in (\mathbb{Z}/p\mathbb{Z})^*, p| \prod_{i=0}^{4} f_i(u, v)\} \leqslant 8(p - 1),$$

which implies that we can pick an admissible vector $(u, v) \mod p$. Alluding to the Chinese remainder theorem we deduce that there exists $\mathbf{z}$ satisfying (5.3) thus allowing any value r satisfying

$$r > (3 + 6 \log \beta_6) + (10 - \frac{4}{\beta_6} + \log \beta_6)\lambda - 6 \log \lambda - \lambda \log \lambda := m(\lambda)$$

to work. Note that condition Q_0 is verified as previously, the key element of this verification being that each $f_i, i \neq 0$ is irreducible, and that f_i, f_j are coprime for $i \neq j$. Indeed since f_i, f_j are coprime as polynomials, there are non-zero integers $R_{i,j}$ such that if $p|f_i(u, v)$ and $p|f_j(u, v)$ then $p|R_{i,j}u$ and $p|R_{i,j}v$. Hence

$$\#\{u, v \sim B : p|(f_i(u, v), f_j(u, v))\} \ll \#\{u, v \sim B : p|(u, v)\} \ll \frac{B^2}{p^2} + 1.$$

Using [11, App.III] we deduce that

$$\min_{0 < \lambda < \beta_6} m(\lambda) = m(0.4978357377\ldots) = 29.1527037101\ldots,$$

so we can choose $r = 30$.

In order to finalise the Zariski density argument we need to prove that $|x_i/B - \xi_i| < \varepsilon$, for which it suffices to establish that $|y_i/B - \zeta_i| < \varepsilon/2$. To this end suppose that (α, β) is the solution to the system

$$\alpha\beta = \frac{1}{12\sqrt{-\zeta_1}\zeta_3} \quad \text{and} \quad 6\zeta_3\alpha^2 + \left(\zeta_0^3 + 2\zeta_1^3 + 2\zeta_3^3\right)\beta^2 = \frac{\zeta_2}{\sqrt{\zeta_3}}.$$

Then the choices

$$u \in \left((\alpha - \delta)\, C^{-\frac{3}{4}} B^{\frac{1}{2}}, (\alpha + \delta)\, C^{-\frac{3}{4}} B^{\frac{1}{2}}\right) \quad \text{and} \quad v \in \left((\beta - \delta)\, C^{-\frac{7}{4}} B^{\frac{1}{2}}, (\beta + \delta)\, C^{-\frac{7}{4}} B^{\frac{1}{2}}\right)$$

make the inequality $|y_i(u, v)/B - \zeta_i| < \delta\, M_i(\boldsymbol{\xi})$ available. We deduce that the saturation number satisfies

$$r(F) \leqslant 42.$$

The final stage of the proof of Theorem 1.6 is similar to that of Theorem 1.5 and is therefore omitted.

References

[1] J. Bourgain, A. Gamburd and P. Sarnak, Affine linear sieve, expanders, and sum-product. *Invent. Math.* **179** (2010), 559–644.

[2] J. Brandes, Linear spaces on hypersurfaces over number fields. `arXiv:1610.08863`, (2016).

[3] J. Brüdern, R. Dietmann, J. Y. Liu, T. D. Wooley, A Birch-Goldbach theorem. *Arch. Math. (Basel)* **94** (2010), 53–58.

[4] T. D. Browning and P. Vishe, Cubic hypersurfaces and a version of the circle method for number fields. *Duke Math. J.* **163** (2014), 1825–1883.

[5] ——, Rational points on cubic hypersurfaces over $\mathbb{F}_q(t)$. *Geom. Funct. Anal.* **25** (2015), 671–732.

[6] J. R. Chen, On the representation of a larger even integer as the sum of a prime and the product of at most two primes. *Sci. Sinica* **16** (1973), 157–176.

[7] B. Cook and Á. Magyar, Diophantine equations in the primes. *Invent. Math.* **198** (2014), 701–737.

[8] A. Conte, M. R. Marchisio and J. P. Murre, On the unirationality of the quintic hypersurface containing a 3-dimensional linear space. *Atti Accad. Sci. Torino Cl. Sci. Fis. Mat. Natur.* **142** (2008), 89–96.

[9] H. Diamond and H. Halberstam, Some applications of sieves of dimension exceeding 1, *Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995)*. Cambridge Univ. Press, Cambridge (1997).

[10] _____ *A higher-dimensional sieve method.* Cambridge University Press, Cambridge, (2008).

[11] H. Diamond, H. Halberstam and H.-E. Richert, Combinatorial sieves of dimension exceeding one. *J. Number Theory* **28** (1988), 306–346.

[12] N. Elkies, Complete cubic parametrization of the Fermat cubic surface. `http://www.math.harvard.edu/ elkies/4cubes.html`.

[13] C. Frei and E. Sofos, Counting rational points on smooth cubic surfaces. *Math. Res. Lett.* **23** (2016), 127–143.

[14] B. Green and T. Tao, Linear equations in primes. *Ann. of Math. (2)* **171** (2010), 1753–1850.

[15] _____, The Möbius function is strongly orthogonal to nilsequences. *Ann. of Math. (2)* **175** (2012), 541–566.

[16] B. Green, T. Tao and T. Ziegler, An inverse theorem for the Gowers $U^{s+1}[N]$-norm. *Ann. of Math. (2)* **176** (2012), 1231–1372.

[17] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers.* Oxford University Press, Oxford, Sixth edition, (2008).

[18] J. Harris, B. Mazur and R. Pandharipande, Hypersurfaces of low degree. *Duke Math. J.* **95** (1998), 125–160.

[19] H. Iwaniec and E. Kowalski, *Analytic number theory.* American Math. Soc. Providence, RI, (2004).

[20] J. Kollár, Unirationality of cubic hypersurfaces. *J. Inst. Math. Jussieu* **1** (2002), 467–476.

[21] K. Kawada and T. D. Wooley, On the Waring-Goldbach problem for fourth and fifth powers. *Proc. London Math. Soc.* **83** (2001), 1–50.

[22] J. Liu and P. Sarnak, Integral points on quadrics in three variables whose coordinates have few prime factors. *Israel J. Math.* **178** (2010), 393–426.

[23] S. Lang and A. Weil, Number of points of varieties in finite fields. *Amer. J. Math.* **76** (1954), 819–827.

[24] K. Mahler, An inequality for the discriminant of a polynomial. *Michigan Math. J.* **11** (1964), 257–262.

[25] Y. I. Manin, *Cubic forms.* North-Holland Publishing Co., Amsterdam, (1986).

[26] M. R. Marchisio, Unirational quartic hypersurfaces. *Boll. Unione Mat. Ital. Sez. B Artic. Ric. Mat. (8)* **3** (2000), 301–314.

[27] G. Marasingha, Almost primes represented by binary forms. *J. Lond. Math. Soc. (2)* **82** (2010), 295–316.

[28] Á. Magyar and T. Titichetrakun, Almost prime solutions to diophantine systems of high rank. *Int. J. Number Theory* **13** (2017), 1491–1514.

[29] A. Nevo and P. Sarnak, Prime and almost prime integral points on principal homogeneous spaces. *Acta Math.* **205** (2010), 361–402.

[30] G. Robin, Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. *Acta Arith.* **42** (1983), 367–389.

[31] D. Schindler and E. Sofos, Sarnak's saturation problem for complete intersections. `arXiv:1705.09133`, (2017).

[32] I. R. Shafarevich, *Basic algebraic geometry. 1.* Springer-Verlag, Berlin, (1994).

[33] C. L. Stewart, On the number of solutions of polynomial congruences and Thue equations. *J. Amer. Math. Soc.* **4** (1991), 793–835.

[34] H. P. F. Swinnerton-Dyer, Applications of algebraic geometry to number theory. *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969).* Amer. Math. Soc., Providence, R.I., (1971), 1–52.

[35] K.-M. Tsang and L. Zhao, On Lagrange's four squares theorem with almost prime variables. *J. reine angew. Math.* **726** (2017), 129–171.

[36] I. M. Vinogradov, Representation of an odd number as a sum of three primes. *C. R. Acad. Sci. URSS* **15** (1937), 169–172.

[37] Y. Wang, On the saturation number for cubic surfaces. *J. Number Theory* **156** (2015), 52–74.

[38] S. Y. Xiao and S. Yamagishi, Zeroes of polynomials in many variables with prime inputs. `arXiv:1512.01258`, (2015).

[39] S. Yamagishi, Prime solutions to polynomial equations in many variables and differing degrees. `arXiv:1703.03332`, (2017).

[40] _____, Diophantine equations in semiprimes. `arXiv:1709.03605`, (2017).

Max Planck Institute for Mathematics, Vivatsgasse 7, Bonn, 53111, Germany
E-mail address: sofos@mpim-bonn.mpg.de

Department of Mathematics, Shanghai University, Shanghai, 200444, China
E-mail address: yuchaowang@shu.edu.cn