A note on a paper by R. Heath-Brown: "The density of rational points on curves and surfaces"

Niklas Broberg

1 Introduction

Let $\mathbb{P}^n$ denote the n–dimensional projective space over an algebraic number field K. For any quasi-projective variety $V \subset \mathbb{P}^n$ one can define a counting function

$$N(V,B) = \#\{\mathbf{x} \in V(K) \;:\; H(\mathbf{x}) \leq B\},$$

where $H : \mathbb{P}^n(K) \to \mathbb{R}_{>0}$ denotes the multiplicative height relative to K. There are several papers written about the asymptotic behaviour of $N(V,B)$ for various V. One has fairly good knowledge about curves but in higher dimensions the geometry becomes more complicated and so do the arithmetic problems. In [12], Heath-Brown shows, among other things, that

$$N(V',B) = O_{d,\varepsilon}(B^{52/27+\varepsilon})$$

for absolutely irreducible surfaces $V \subset \mathbb{P}^3$ of degree $d \geq 3$, where $V' \subset V$ denotes the complement of the lines on V. The distinguishing feature of this estimate is that it is uniform in the sense that it only depends on the degree of the equation defining V. The basic idea of the proof is to cut V by planes and then estimate the number of rational points on the sections. For that one requires uniform bounds on the number of rational points of bounded height on curves. The aim of this note is to extend the principal result of [12] which is used to obtain estimates for plane curves. In order to state our main result we need some notations and definitions.

We will assume throughout the whole paper that the number field K is fixed with ring of integers R. In particular, any implicitly given constant may depend on K without we saying so explicitly.

Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ be a collection of ideals of R which represent the different ideal classes of K. The set

$$P^n = \bigcup_{i=1}^{h} \{\mathbf{x} \in R^{n+1} \;:\; \langle \mathbf{x} \rangle = \mathfrak{a}_i\}$$

modulo units is then a complete set of representatives of $\mathbb{P}^n(K)$, where $\langle \mathbf{x} \rangle$ denotes the fractional ideal of K generated by the components of $\mathbf{x}$. The non-equivalent multiplicative archimedean valuations $| \ |_1, \ldots, | \ |_s$ on K are supposed to satisfy $\prod_{i=1}^s |x|_i = \aleph\langle x \rangle$ for all $x \in K$, where $\aleph\mathfrak{a}$ denotes the ordinary ideal norm of the fractional ideal $\mathfrak{a}$ of K. Given vectors $\mathbf{r}_0, \ldots, \mathbf{r}_n \in \mathbb{R}^s_{\geq 1}$, we define $P^n(\mathbf{r}_0, \ldots, \mathbf{r}_n)$ to be the set of all $\mathbf{x} \in P^n$ for which $|x_i|_j \leq r_{ij}$ for $0 \leq i \leq n$ and $1 \leq j \leq s$. If $V \subset \mathbb{P}^n$, we write $V(\mathbf{r}_0, \ldots, \mathbf{r}_n)$ for the set of $\mathbf{x} \in P^n(\mathbf{r}_0, \ldots, \mathbf{r}_n)$ which represent points of $V(K)$. The letter $\mathbf{r}$ is reserved to denote elements of $\mathbb{R}^s_{\geq 1}$ and we define the size of $\mathbf{r}$ to be $\|\mathbf{r}\| = \prod_{i=1}^s r_i$. In agreement with this notation we define the size of $\mathbf{x} \in K^{n+1}$ to be the product

$$\|\mathbf{x}\| = \prod_{i=1}^{s} \max_{0 \leq j \leq n} |x_j|_i .$$

The multiplicative height on $\mathbb{P}^n(K)$ relative to K, which was mentioned above, is defined as $H(\mathbf{x}) = \|\mathbf{x}\| / \aleph\langle \mathbf{x} \rangle$.

The non-negative numbers $a_0, \ldots, a_n$ will be defined in the next section. We only mention here that $a_0 + \cdots + a_n = 1$ and that there is one collection of a_i for every graded monomial ordering on $K[x_0, \ldots, x_n]$. The main result of this note is the following.

Theorem 1. *Let $V \subset \mathbb{P}^n$ be an irreducible variety of dimension r and degree d. Suppose that the ideal $I \subset K[\mathbf{x}]$ of V is generated by forms of degrees at most δ, and let $\varepsilon > 0$ be given. Then there exists a form $F \in K[\mathbf{x}] \setminus I$ which vanishes for all $\mathbf{x} \in V(\mathbf{r}_0, \ldots, \mathbf{r}_n)$ and satisfies*

$$\deg F \ll_{n,\delta,\varepsilon} \prod_{i=0}^{n} \|\mathbf{r}_i\|^{a_i \frac{r+1}{d^{1/r}} + \varepsilon} .$$

Moreover, the irreducible factors of F have degrees bounded in terms of n, δ, and ε.

In case V is a hypersurface we recover theorem 14 of Heath-Brown [12] (cf. corollary 2 of the next section). A second consequence is that we may find a form $F \in K[\mathbf{x}] \setminus I$ with

$$\deg F \ll_{n,\delta,\varepsilon} B^{\frac{r+1}{d^{1/r}} + \varepsilon},$$

which vanishes for all points of $V(K)$ of height at most B. We use here that each point of $\mathbb{P}^n(K)$ of height at most B can be represented by an element of $P^n(\mathbf{r}_0, \ldots, \mathbf{r}_n)$ where $r_{ij} = cB^{1/s}$ for some constant c (see e.g. section 13.4 of [20]). We should also mention that δ can be bounded in terms of n

and d in case V is smooth or of dimension 1 (see theorem 3.11 of [2] or [8]). If we use this fact and apply Bezout's theorem

$$\#(X \cap Y) \leq (\deg X)(\deg Y)$$

for any closed sub-varieties X, $Y \subset \mathbb{P}^n$ of finite intersection (see e.g. section 8.4 of [7]), then we get the following corollary of theorem 1.

Corollary 1. *Let $C \subset \mathbb{P}^n$ be an irreducible curve of degree d. Then*

$$N(C, \mathbf{r}_0, \dots, \mathbf{r}_n) \ll_{d,\varepsilon} (\|\mathbf{r}_0\|^{a_0} \cdots \|\mathbf{r}_n\|^{a_n})^{2/d+\varepsilon} \tag{1}$$

for every $\varepsilon > 0$, where $N(C, \mathbf{r}_0, \dots, \mathbf{r}_n)$ counts the number of points of $C(K)$ which have a representative in $C(\mathbf{r}_0, \dots, \mathbf{r}_n)$. In particular,

$$N(C, B) = O_{d,\varepsilon}(B^{2/d+\varepsilon}). \tag{2}$$

In [12], Heath-Brown derives (2) for curves in $\mathbb{P}^3$ from the same result on plane curves by a projection argument. One can prove the estimate for curves in $\mathbb{P}^n$ by similar techniques. What is new about corollary 1 is (1). Some of the results of [12] can be generalised by using this bound. To illustrate, we have included the following theorem which is similar to theorems 10 and 11 of [12] on surfaces in $\mathbb{P}^3$.

Theorem 2. *Let F_1, $F_2 \in \mathbb{Q}[x_0, \dots, x_4]$ be forms of degrees $d_1 \geq 2$ and $d_2 \geq 2$, respectively. Assume that $F_1 = F_2 = 0$ defines a smooth surface $V \subset \mathbb{P}^4$ and let $V' \subset V$ be the complement of the lines on V. Then*

$$N(V', B) \ll_{d_1,d_2,\varepsilon} B^{\frac{5}{4}+\frac{15}{8d_1d_2}+\varepsilon} \tag{3}$$

and

$$N(V', B) \ll_{d_1,d_2,\varepsilon} B^{1+\varepsilon} + B^{\frac{3}{\sqrt{d_1d_2}}+\frac{2}{d_1+d_2-2}+\varepsilon} \tag{4}$$

for every $\varepsilon > 0$.

Estimate (3) is better than (4) only in the cases

$$(d_1, d_2) \in \{(2,2), (2,3), (2,4), (3,3)\},$$

and if $d_1 + d_2 \geq 9$, $(d_1, d_2) \neq (2,7)$, then (4) reads

$$N(V', B) \ll_{d_1,d_2,\varepsilon} B^{1+\varepsilon}.$$

We will also prove the following result.

Theorem 3. *Let $V \subset \mathbb{P}^n$ be an absolutely irreducible non-degenerate surface of degree at least 4 which is defined over $\mathbb{Q}$. Let p_V be its Hilbert polynomial. Then*

$$N(V', B) \ll_{p_V,\varepsilon} B^{1+\frac{2(n+1)}{3n}+\varepsilon},$$

for every $\varepsilon > 0$, where $V' \subset V$ is the complement of the lines on V.

2 Graded monomial orderings

In this section we define the numbers a_i which occur in the formulation of theorem 1.

Let $V \subset \mathbb{P}^n$ be an irreducible variety of dimension r and degree d, and assume that its ideal $I \subset K[\mathbf{x}]$ can be generated by forms of degrees at most δ. Let $K[\mathbf{x}]_u$ be the K–vector space consisting of the homogeneous polynomials of total degree u and let $I_u = I \cap K[\mathbf{x}]_u$. The Hilbert function $\phi(u)$ of I is defined to be the dimension of the quotient space $K[\mathbf{x}]_u / I_u$. There is, then, a unique polynomial $p(u) = p_V(u)$ such that $p(u) = \phi(u)$ if u is sufficiently large. This polynomial is called the Hilbert polynomial of V. The dimension r of V is given by the degree of $p(u)$, and the degree of V is defined to be $r!$ times the leading coefficient of $p(u)$. The Hilbert function can be evaluated with the help of some monomial ideals related to I. In order to associate such ideals to I we need some definitions. The approach to Hilbert functions that we use here can be found in [11].

A graded monomial ordering $<$ on $K[\mathbf{x}]$ is a relation on the set of monomials $\mathbf{x}^\alpha = x_0^{\alpha_0} \cdots x_n^{\alpha_n}$ where $\alpha = (\alpha_0, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^{n+1}$, or equivalently, a relation on $\mathbb{Z}_{\geq 0}^{n+1}$ which satisfies:

1. $<$ is a total ordering.
2. $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}_{\geq 0}^{n+1}$.
3. If α, β, $\gamma \in \mathbb{Z}_{\geq 0}^{n+1}$ and $\alpha < \beta$, then $\alpha + \gamma < \beta + \gamma$.
4. If α, $\beta \in \mathbb{Z}_{\geq 0}^{n+1}$ and $\alpha \leq \beta$, then $|\alpha| \leq |\beta|$, where $|\gamma| = \gamma_0 + \cdots + \gamma_n$ denotes the total degree of $\gamma \in \mathbb{Z}_{\geq 0}^{n+1}$.

The standard example is the graded lexicographic ordering: $\mathbf{x}^\alpha < \mathbf{x}^\beta$ if $|\alpha| < |\beta|$ or if $|\alpha| = |\beta|$ and the left-most non-zero entry of $\alpha - \beta$ is negative.

Given a graded monomial ordering, we may consider the leading monomial of a polynomial. More exactly, if

$$f(\mathbf{x}) = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^{n+1}} a_\alpha \mathbf{x}^\alpha,$$

then the leading monomial f^l of f is defined to be $\mathbf{x}^\beta$, where

$$\beta = \max \left\{ \alpha \in \mathbb{Z}_{\geq 0}^{n+1} \ : \ a_\alpha \neq 0 \right\}.$$

The maximum is of course taken with respect to the chosen ordering. We can also consider the monomial ideal I^l which is generated by the leading monomials of the elements of I. One can show that $\phi(u) = \phi_{I^l}(u)$ for all u (see proposition 9 of [11], chapter 9, §3). Hence, if we decompose $K[\mathbf{x}]_u$ as $I_u^l \oplus J_u$, then the K–vector space J_u has a basis of rank $\phi(u)$ consisting of monomials. The sums $\sum_{\mathbf{x}^\alpha \in J_u} \alpha_i$, denoted by $\sigma_i(u)$, therefore satisfy

$$\sigma_0(u) + \cdots + \sigma_n(u) = u\,\phi(u)$$

for all u. The next lemma states that the functions $\sigma_i(u)$ are equal to some polynomials of degrees at most $r+1$ for u sufficiently large. The limits

$$a_i = \lim_{u\to\infty} \frac{\sigma_i(u)}{u\,\phi(u)}$$

therefore exist and can be also defined as the quotients of the leading coefficients of the corresponding polynomials of $\sigma_i(u)$ and $u\,\phi(u)$.

Lemma 1. *There is a positive integer u_0, bounded in terms of n and δ, such that $\phi(u), \sigma_0(u), \ldots, \sigma_n(u)$ are equal to some polynomials for $u \geq u_0$. Furthermore, the coefficients of these polynomials can be bounded in terms of n and δ.*

In [18], there is a proof of the fact that the maximum degree of the polynomials making up a Gröbner base for I can be bounded in terms of n and δ. By definition the leading monomials of the elements of a Gröbner base of I constitute a base for I^l. Suppose that I^l is generated by $\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_m}$ for some $\alpha_i \in \mathbb{Z}_{\geq 0}^{n+1}$. Then the set of exponents of the monomials in I^l is the the union $\bigcup_{i=1}^m [\alpha_i]$, where

$$[\alpha] = \left\{ \alpha + \beta \;:\; \beta \in \mathbb{Z}_{\geq 0}^{n+1} \right\}.$$

The intersection of two such sets is a set of the same type, namely $[\alpha] \cap [\beta] = [\alpha\beta]$, where

$$\alpha\beta = (\max(\alpha_0, \beta_0), \ldots, \max(\alpha_n, \beta_n)).$$

One can check that the number of $\beta \in [\alpha]$ of total degree $u \geq |\alpha|$ is

$$\phi(\alpha, u) = \binom{u + n - |\alpha|}{u - |\alpha|},$$

and that the sum $\sum_{\beta\in[\alpha], |\beta|=u} \beta_i$ is given by

$$\sigma_i(\alpha, u) = \left(\alpha_i + \frac{u - |\alpha|}{n+1} \right) \phi(\alpha, u).$$

In particular this shows that $\phi(\alpha, u)$ and $\sigma_i(\alpha, u)$ are equal to some polynomials for $u \geq |\alpha|$. As $\phi(u) = \phi_{I^l}(u)$ we have

$$\phi(u) = \binom{u+n}{u} - \#\left\{ \beta \in \bigcup_{i=1}^m [\alpha_i] \;:\; |\beta| = u \right\},$$

and by the inclusion-exclusion principle

$$\#\left\{\beta \in \bigcup_{i=1}^{m}[\alpha_i] \;:\; |\beta| = u\right\} = \sum_{j=1}^{m} \sum_{i_1<\cdots<i_j} (-1)^{j+1}\phi(\alpha_{i_1}\cdots\alpha_{i_j}, u).$$

Similarly we have

$$\sigma_i(u) = \frac{u}{n+1}\binom{u+n}{n} - \sum_{j=1}^{m} \sum_{i_1<\cdots<i_j} (-1)^{j+1}\sigma_i(\alpha_{i_1}\cdots\alpha_{i_j}, u).$$

Hence, $\phi(u)$ and $\sigma_i(u)$ are equal to some polynomials for $u \geq |\alpha_1|+\cdots+|\alpha_m|$ whose coefficients can be bounded in terms of $|\alpha_1|, \ldots, |\alpha_m|$.

We end this section by recovering theorem 14 of Heath-Brown [12]. This illustrates the role of monomial orderings. Note also that only the case $K = \mathbb{Q}$ is treated in [12].

Let $F \in R[\mathbf{x}]$ be an irreducible form of degree d. Suppose that $\mathbf{x}^\alpha$ is a monomial which occurs in F with non-zero coefficient and is maximal among all such monomials with respect to some graded monomial ordering on $K[\mathbf{x}]$. The corresponding monomial ideal I^l is then generated by $\mathbf{x}^\alpha$ and the formulas above give

$$\begin{aligned} \phi(u) &= \frac{|\alpha|}{(n-1)!}\, u^{n-1} + O(u^{n-2}), \\ \sigma_i(u) &= \frac{|\alpha| - \alpha_i}{n!}\, u^n + O(u^{n-1}), \\ a_i &= \frac{|\alpha| - \alpha_i}{n\;|\alpha|} = \frac{d-\alpha_i}{n\,d}. \end{aligned}$$

If we use the notation from [12] and define

$$\begin{aligned} V &= \|\mathbf{r}_0\| \cdots \|\mathbf{r}_n\|, \\ T &= \|\mathbf{r}_0\|^{\alpha_0} \cdots \|\mathbf{r}_n\|^{\alpha_n}, \end{aligned}$$

then we have the following corollary of theorem 1.

Corollary 2. *Let $\varepsilon > 0$, $\mathbf{r}_0, \ldots, \mathbf{r}_n \in \mathbb{R}^s_{\geq 1}$, and an irreducible form $F \in K[\mathbf{x}]$ of degree d be given. Then there exists an integer D depending only on n, d, and ε, and an integer k satisfying*

$$k \ll_{n,d,\varepsilon} (V^d/T)^{d^{-n/(n-1)}} V^\varepsilon$$

with the following properties. For each $j \leq k$, there is a form $F_j \in K[\mathbf{x}]$, having degree at most D, such that

1. *$F(\mathbf{x}) \nmid F_j(\mathbf{x})$ for $1 \le j \le k$,*

2. *For each $\mathbf{x} \in P^n(\mathbf{r}_0, \dots, \mathbf{r}_n)$, with $F(\mathbf{x}) = 0$, there is an integer $j \le k$ such that $F_j(\mathbf{x}) = 0$.*

In [12], the number T is defined a bit differently as

$$T = \max_{a_\alpha \neq 0} \left(\|\mathbf{r}_0\|^{\alpha_0} \cdots \|\mathbf{r}_n\|^{\alpha_n} \right), \tag{5}$$

where $F(\mathbf{x}) = \sum_\alpha a_\alpha \mathbf{x}^\alpha$. It is however always possible to find a graded monomial ordering such that our T is given by (5). To see this, choose algebraically independent $q_0, \dots, q_n \in \mathbb{R}_{\ge 1}$, and define a graded monomial ordering by letting $\mathbf{x}^\alpha < \mathbf{x}^\beta$ if $|\alpha| < |\beta|$ or if $|\alpha| = |\beta|$ and $\mathbf{q}^\alpha < \mathbf{q}^\beta$. Provided that $|\|\mathbf{r}_i\| - q_i|$ are sufficiently small for all $i = 0, 1, \dots, n$, one has

$$\|\mathbf{r}_0\|^{\alpha_0} \cdots \|\mathbf{r}_n\|^{\alpha_n} < \|\mathbf{r}_0\|^{\beta_0} \cdots \|\mathbf{r}_n\|^{\beta_n} \quad \text{if and only if} \quad \mathbf{q}^\alpha < \mathbf{q}^\beta,$$

for all α and β such that $a_\alpha a_\beta \neq 0$.

3 Proof of the main result

In this section we prove theorem 1. The overall structure of the proof is similar to Heath-Brown's proof of theorem 14 in [12].

Suppose that $V \subset \mathbb{P}^n$ is an irreducible variety whose ideal I is generated by some forms $F_1, \dots, F_t \in R[\mathbf{x}]$. We shall use the same notation as in the previous section. Thus, δ stands for the maximal degree among the forms $F_1, \dots, F_t$ and r and d are the dimension and degree of V, respectively. We first explain what we mean by a point of $\mathbb{P}^n(K)$ or $V(K)$ modulo a power of a prime ideal $\mathfrak{p}$ of R. As the local ring $R_\mathfrak{p}$ is a unique factorisation domain, we can represent a point of $\mathbb{P}^n(K)$ by a primitive vector of $R_\mathfrak{p}^{n+1}$. The reduction modulo $\mathfrak{p}^m$ of any such representative gives a point of $\mathbb{P}^n(R/\mathfrak{p}^m)$ and it is obvious that this map from $\mathbb{P}^n(K)$ to $\mathbb{P}^n(R/\mathfrak{p}^m)$ is well-defined. Likewise, when we consider rational points of V modulo $\mathfrak{p}^m$, we mean the image of the points in $V(R/\mathfrak{p}^m)$, where this last set is the set of solutions $\mathbf{x} \in \mathbb{P}^n(R/\mathfrak{p}^m)$ of

$$F_1(\mathbf{x}) = \cdots = F_t(\mathbf{x}) = 0.$$

Recall that a point $\mathbf{x} \in V(K)$ is said to be smooth if the Jacobian matrix

$$J(F_1, \dots, F_t) = \begin{pmatrix} \frac{\partial F_1}{\partial x_0} & \cdots & \frac{\partial F_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial F_t}{\partial x_0} & \cdots & \frac{\partial F_t}{\partial x_n} \end{pmatrix}$$

evaluated at $\mathbf{x}$ has rank $n-r$. The singular locus of V is a proper subset so we can assume that the sub-determinant

$$D(\mathbf{x}) = \begin{vmatrix} \frac{\partial F_1}{\partial x_1}(\mathbf{x}) & \cdots & \frac{\partial F_1}{\partial x_{n-r}}(\mathbf{x}) \\ \vdots & & \vdots \\ \frac{\partial F_{n-r}}{\partial x_1}(\mathbf{x}) & \cdots & \frac{\partial F_{n-r}}{\partial x_{n-r}}(\mathbf{x}) \end{vmatrix}$$

of $J(F_1, \ldots, F_t)$ does not belong to I. It is thus sufficient for the proof to find a form $F \in K[\mathbf{x}] \setminus I$ which vanishes for points of

$$S(\mathbf{r}_0, \ldots, \mathbf{r}_n) = \{\mathbf{x} \in V(\mathbf{r}_0, \ldots, \mathbf{r}_n) \ : \ D(\mathbf{x}) \neq 0\}.$$

Following [12], we let

$$S_{\mathfrak{p}}(\mathbf{r}_0, \ldots, \mathbf{r}_n) = \left\{\mathbf{x} \in V(\mathbf{r}_0, \ldots, \mathbf{r}_n) \ : \ D(\mathbf{x}) \in R_{\mathfrak{p}}^*\right\},$$

for each prime ideal $\mathfrak{p}$. Here $R_{\mathfrak{p}}^*$ denotes the group of units of $R_{\mathfrak{p}}$.

Lemma 2. *Suppose that $P \gg \log \|D(\mathbf{x})\|$ for all $\mathbf{x} \in S(\mathbf{r}_0, \ldots, \mathbf{r}_n)$, and let k be the smallest integer such that $k > \log \|D(\mathbf{x})\| / \log P$. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ such that $P \leq \aleph\mathfrak{p}_i \ll P$ and*

$$S(\mathbf{r}_0, \ldots, \mathbf{r}_n) = \bigcup_{i=1}^{k} S_{\mathfrak{p}_i}(\mathbf{r}_0, \ldots, \mathbf{r}_n).$$

To see this, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the different prime ideals of smallest possible norm greater than P. If $D(\mathbf{x}) \in \mathfrak{p}_i$ for all $i = 1, 2, \ldots, k$, then

$$\|D(\mathbf{x})\| \geq (\aleph\mathfrak{p}_1) \cdots (\aleph\mathfrak{p}_k) \geq P^k,$$

which is contradictory provided that $D(\mathbf{x}) \neq 0$. One can check that $\aleph\mathfrak{p}_i \ll P$ by using bounds of Tchebycheff-type for the number of prime ideals of bounded norm.

The principal ingredient of the proof of theorem 1 is the following lemma which we prove at the end of this section.

Lemma 3. *For any $\varepsilon > 0$, there exists a constant c, which depends on n, δ, and ε, with the following property. If $\mathfrak{p}$ is a prime ideal of R such that*

$$\aleph\mathfrak{p} \geq c \prod_{i=0}^{n} \|\mathbf{r}_i\|^{a_i \frac{r+1}{r d^{1/r}} + \varepsilon} \tag{6}$$

and $\mathbf{x}_1 \in S_{\mathfrak{p}}(\mathbf{r}_0, \ldots, \mathbf{r}_n)$, then there exists a form $F \in R[\mathbf{x}] \setminus I$ such that $F(\mathbf{x}) = 0$ for every $\mathbf{x} \in V(\mathbf{r}_0, \ldots, \mathbf{r}_n)$ which represents the same point as $\mathbf{x}_1$ modulo $\mathfrak{p}$. Moreover, the degree of F can be bounded in terms of n, δ, and ε.

We also need the following standard fact.

Lemma 4. *There are $O_{n,r,t,\delta}(\aleph\mathfrak{p}^r)$ points of $V(R/\mathfrak{p})$ for which $J(F_1,\dots,F_t)$ has rank $n-r$.*

To prove this, we use Bezout's theorem,

$$\sum_{i=1}^{k} \deg V_i \le \prod_{i=1}^{t} \deg F_i \le \delta^t,$$

where V_i are the irreducible components of V (see e.g. example 8.4.6 of [7]). Hence, $k \le \delta^t$ and $\deg V_i \le \delta^t$. We are only interested in points of $V(R/\mathfrak{p})$ for which $J(F_1,\dots,F_t)$ has rank $n-r$, and such points can only belong to components V_i of dimension at most r. Lemma 4 now follows from the fact that

$$\#W(R/\mathfrak{p}) \ll_{n,\dim W,\deg W} \aleph\mathfrak{p}^{\dim W}$$

for any irreducible variety $W \subset \mathbb{P}^n_{R/\mathfrak{p}}$ (see [17]).

Theorem 1 follows when we combine these lemmas. Let P be the right-hand side of (6) times the factor

$$\max_{\mathbf{x}\in S(\mathbf{r}_0,\dots,\mathbf{r}_n)} \log\|D(\mathbf{x})\|.$$

Multiply together all the forms given by lemma 3 as $\mathbf{x}_1$ runs over the elements of $S_{\mathfrak{p}_i}(\mathbf{r}_0,\dots,\mathbf{r}_n)$ modulo $\mathfrak{p}_i$ as $\mathfrak{p}_i$ runs over the primes given by lemma 2. Let F be the resulting form. Then $F \notin I$, $F(\mathbf{x}) = 0$ for all $\mathbf{x} \in S(\mathbf{r}_0,\dots,\mathbf{r}_n)$, and

$$\deg F \ll_{n,t,\delta,\varepsilon} \left(\prod_{i=0}^{n} \|\mathbf{r}_i\|^{a_i \frac{r+1}{d^{1/r}}+\varepsilon}\right)\left(\max_{\mathbf{x}\in S(\mathbf{r}_0,\dots,\mathbf{r}_n)} \log\|D(\mathbf{x})\|\right)^{r+1}.$$

That is, theorem 1 is proved if we can get rid of the dependence of the choice of generators of I. The following lemma is an adjustment of theorem 4 of [12].

Lemma 5. *Either there exists a form $F \in K[\mathbf{x}]\setminus I$ of degree at most δ such that $F(\mathbf{x}) = 0$ for all $\mathbf{x} \in V(\mathbf{r}_0,\dots,\mathbf{r}_n)$, or I can be generated by $O_{n,\delta}(1)$ forms $F_1,\dots,F_t \in R[\mathbf{x}]$ of degrees at most δ such that*

$$\prod_{i=1}^{t} \|F_i\| \ll_{n,\delta} (\|\mathbf{r}_0\|\cdots\|\mathbf{r}_n\|)^{\delta^2\binom{n+\delta}{\delta}}.$$

To prove this, let $\mathbf{x}_1, \dots, \mathbf{x}_N$ be the elements of $V(\mathbf{r}_0, \dots, \mathbf{r}_n)$, and let $\mathbf{x}^{\alpha_{k1}}, \dots, \mathbf{x}^{\alpha_{ke_k}}$ be an enumeration of the monomials of degree k in $n+1$ variables. If we identify the vector space $K[\mathbf{x}]_k$ with K^{e_k} using the basis $\mathbf{x}^{\alpha_{k1}}, \dots, \mathbf{x}^{\alpha_{ke_k}}$, then, obviously, the subspace $I_k \subset K[\mathbf{x}]_k$ is contained in the kernel of the matrix

$$A_k = \begin{pmatrix} \mathbf{x}_1^{\alpha_{k1}} & \cdots & \mathbf{x}_1^{\alpha_{ke_k}} \\ \vdots & & \vdots \\ \mathbf{x}_N^{\alpha_{k1}} & \cdots & \mathbf{x}_N^{\alpha_{ke_k}} \end{pmatrix}.$$

There are two cases to consider. If $I_k \subsetneqq \ker A_k$ for some $1 \le k \le \delta$, then there exists a form $F \in K[\mathbf{x}]_k \setminus I_k$ which vanishes for all $\mathbf{x}_i$. The alternative case, $I_k = \ker A_k$ for all $k = 1, 2, \dots, \delta$, requires some more work. First we form a new matrix A_k' out of rows of A_k so that A_k' has $m_k = \operatorname{rank} A_k$ rows. We then define $\mathbf{a}_k$ to be a vector consisting of all the $m_k \times m_k$–minors of A_k'. It will have $\binom{e_k}{m_k}$ components, each belonging to R. Let l_k denote the dimension of $\ker A_k'$. Theorem 9 of [3] states that we can find a basis $\mathbf{y}_{k1}, \dots, \mathbf{y}_{kl_k} \in R^{e_k}$ of $\ker A_k'$ which satisfies

$$\prod_{i=1}^{l_k} H(\mathbf{y}_{ki}) \le c^{l_k} H(A_k'),$$

for some constant c which only depends on K, and where

$$H(A_k') = \frac{1}{\aleph\langle \mathbf{a}_k \rangle} \left[\prod_{|\,|_i \text{ real}} \left(\sum_j |a_{kj}|_i^2 \right)^{1/2} \right] \left[\prod_{|\,|_i \text{ complex}} \left(\sum_j |a_{kj}|_i \right) \right].$$

It is straightforward to check that

$$H(A_k') \ll_{n,k} (\|\mathbf{r}_0\| \cdots \|\mathbf{r}_n\|)^{km_k}.$$

The basis $\mathbf{y}_{k1}, \dots, \mathbf{y}_{kl_k}$ of $\ker A_k' = I_k$ corresponds to some forms of degree k. Consequently, we have a basis $G_{k1}, \dots, G_{kl_k}$ of I_k which satisfies

$$\prod_{i=1}^{l_k} \|G_{ki}\| \ll_{n,k} (\|\mathbf{r}_0\| \cdots \|\mathbf{r}_n\|)^{km_k}.$$

But $I_1, \dots, I_\delta$ generate I. Thus we have a set $G_{11}, \dots, G_{\delta l_\delta}$ of generators of I which satisfies

$$\prod \|G_{ij}\| \ll_{n,\delta} (\|\mathbf{r}_0\| \cdots \|\mathbf{r}_n\|)^{\delta^2 \binom{n+\delta}{\delta}}.$$

This completes the proof of lemma 5.

It remains to prove lemma 3. Suppose that $\mathbf{x}_1, \dots, \mathbf{x}_N$ are all the points of $S_{\mathfrak{p}}(\mathbf{r}_0, \dots, \mathbf{r}_n)$ which represent the same point as $\mathbf{x}_1$ modulo the prime ideal

$\mathfrak{p}$. To find a form F which does not belong to the ideal I we shall consider elements of J_u. Remember that we had $K[\mathbf{x}]_u = I_u^l \oplus J_u$, where I^l was the ideal generated by the leading monomials of I. Now, it is a linear problem to show that there exists a form $F \in J_u$ with the required properties. That is, there exists such an F exactly when the matrix

$$M = \begin{pmatrix} \mathbf{x}_1^{\alpha_1} & \cdots & \mathbf{x}_1^{\alpha_{\phi(u)}} \\ \vdots & & \vdots \\ \mathbf{x}_N^{\alpha_1} & \cdots & \mathbf{x}_N^{\alpha_{\phi(u)}} \end{pmatrix}$$

has rank at most $\phi(u) - 1$. To simplify the notation we have chosen an enumeration $\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_{\phi(u)}}$ of the monomials of J_u. If $N < \phi(u) - 1$ then obviously the rank of M is at most $\phi(u) - 1$. We can thus assume that $N \geq \phi(u) - 1$. In that case M has rank at most $\phi(u) - 1$ only if all the $\phi(u) \times \phi(u)$–sub-determinants of M vanish. Without loss of generality we may consider the sub-determinant

$$\Delta = \begin{vmatrix} \mathbf{x}_1^{\alpha_1} & \cdots & \mathbf{x}_1^{\alpha_{\phi(u)}} \\ \vdots & & \vdots \\ \mathbf{x}_{\phi(u)}^{\alpha_1} & \cdots & \mathbf{x}_{\phi(u)}^{\alpha_{\phi(u)}} \end{vmatrix}.$$

By expanding Δ and remembering the definitions of the functions $\sigma_i(u)$ from the previous section, we see that

$$\|\Delta\| \leq (\phi(u)!)^{[K:\mathbb{Q}]}(\|\mathbf{r}_0\|^{\sigma_0(u)} \cdots \|\mathbf{r}_n\|^{\sigma_n(u)}). \tag{7}$$

The rest of the proof will be concerned with the order of Δ at $\mathfrak{p}$. If $\Delta \in \mathfrak{p}^m$ for some positive integer m and $(\aleph\mathfrak{p})^m$ exceeds the right-hand side of (7), then Δ must vanish. It is this comparison that will eventually give us condition (6).

Before we continue we make a remark. It may seem strange to assume that $N \geq \phi(u) - 1$ without knowing what u is. But u is supposed to be a fixed constant which is bounded in terms of n, δ, and ε. At this point we do not know how to choose it. This will become apparent later.

Now, since we are only interested in the order of Δ at $\mathfrak{p}$, we may change to affine coordinates. We may also assume that $\mathbf{x}_1$ does not belong to the hyperplane $x_0 = 0$ modulo $\mathfrak{p}$. Then

$$\mathbf{y}_i = x_{i0}^{-1}(x_{i1}, \ldots, x_{in})$$

are elements of $R_{\mathfrak{p}}^n$ for $i = 1, 2, \ldots, N$. We introduce affine equations for $V \setminus \{x_0 = 0\}$ by putting

$$f_i(\mathbf{y}) = F_i(1, y_1, \ldots, y_n)$$

for $i = 1, 2, \ldots, t$. We know that the matrix

$$\begin{pmatrix} \frac{\partial f_1}{\partial y_1} & \cdots & \frac{\partial f_1}{\partial y_{n-r}} \\ \vdots & & \vdots \\ \frac{\partial f_{n-r}}{\partial y_1} & \cdots & \frac{\partial f_{n-r}}{\partial y_{n-r}} \end{pmatrix} \tag{8}$$

is invertible over $R_\mathfrak{p}$ when evaluated at $\mathbf{y}_1$ by the assumption that $\mathbf{x}_1 \in S_\mathfrak{p}(\mathbf{r}_0, \ldots, \mathbf{r}_n)$. The following version of the implicit function theorem is well-known (see e.g. corollary 3 of [4], chapter III, §4.5).

Lemma 6. *Suppose that $\mathbf{y}_1 \in R_\mathfrak{p}^n$ is a common zero of $f_1, \ldots, f_{n-r}$, and that the matrix (8) is invertible over $R_\mathfrak{p}$ at $\mathbf{y}_1$. Then, for each $m \geq 1$, there exists $n-r$ polynomials $g_{mi}(\mathbf{y}) \in R_\mathfrak{p}[\mathbf{y}]$ in r variables, such that*

$$y_i \equiv g_{mi}(y_{n-r+1}, \ldots, y_n) \pmod{\mathfrak{p}^m}$$

for $i = 1, 2, \ldots, n-r$, whenever $f_1(\mathbf{y}) = \cdots = f_{n-r}(\mathbf{y}) = 0$ and $\mathbf{y} \equiv \mathbf{y}_1$ $\pmod{\mathfrak{p}}$.

We can use this lemma to eliminate some variables from our determinant Δ. First we note that the order of Δ at $\mathfrak{p}$ is the same as the order of

$$\Delta' = \begin{vmatrix} \mathbf{y}_1^{\beta_1} & \cdots & \mathbf{y}_1^{\beta_{\phi(u)}} \\ \vdots & & \vdots \\ \mathbf{y}_{\phi(u)}^{\beta_1} & \cdots & \mathbf{y}_{\phi(u)}^{\beta_{\phi(u)}} \end{vmatrix},$$

where $\beta_i \in \mathbb{Z}_{\geq 0}^n$ is the projection of $\alpha_i \in \mathbb{Z}_{\geq 0}^{n+1}$ onto the last n coordinates. This follows from the assumption that x_{i0} are units of $R_\mathfrak{p}$. By the lemma above, we can replace $\mathbf{y}_i$ by

$$\big(g_{m1}(y_{n-r+1}, \ldots, y_n), \ldots, g_{m(n-r)}(y_{n-r+1}, \ldots, y_n), y_{n-r+1}, \ldots, y_n\big)$$

modulo $\mathfrak{p}^m$. If we let $\mathbf{z}_i$ be the last r coordinates of $\mathbf{y}_1 - \mathbf{y}_i \in \mathfrak{p}^{(n+1)}$, we see that

$$\Delta' \equiv \begin{vmatrix} h_1(\mathbf{z}_1) & \cdots & h_{\phi(u)}(\mathbf{z}_1) \\ \vdots & & \vdots \\ h_1(\mathbf{z}_{\phi(u)}) & \cdots & h_{\phi(u)}(\mathbf{z}_{\phi(u)}) \end{vmatrix} \pmod{\mathfrak{p}^m},$$

for some polynomials h_i with coefficients in $R_\mathfrak{p}$. Note that the polynomials depend on $\mathbf{x}_1$ and the integer m which will be specified below. If we denote the smallest monomial of g by g^s, with respect to some graded monomial ordering on $k[\mathbf{z}]$, then it is not hard to see that we can find a new base

$p_1, \ldots, p_{\phi(u)}$, with the property $p_1^s < \cdots < p_{\phi(u)}^s$, for the $R_\mathfrak{p}$–submodule of $R_\mathfrak{p}[\mathbf{z}]$ generated by $h_1, \ldots, h_{\phi(u)}$. Consequently,

$$\begin{vmatrix} p_1(\mathbf{z}_1) & \cdots & p_{\phi(u)}(\mathbf{z}_1) \\ \vdots & & \vdots \\ p_1(\mathbf{z}_{\phi(u)}) & \cdots & p_{\phi(u)}(\mathbf{z}_{\phi(u)}) \end{vmatrix} \equiv 0 \pmod{\mathfrak{p}^{\sigma(u)}},$$

where $\sigma(u) = \sum |\alpha_i|$ for the smallest elements $\alpha_1, \ldots, \alpha_{\phi(u)}$ of $\mathbb{Z}_{\geq 0}^r$ with respect to the graded monomial ordering. Hence, if we choose $m = \sigma(u)$, we find that the order of Δ at $\mathfrak{p}$ is at least $\sigma(u)$. This observation together with (7), implies that Δ has to vanish as soon as

$$(\aleph\mathfrak{p})^{\sigma(u)} > (\phi(u)!)^{[K:\mathbb{Q}]} \left(\|\mathbf{r}_0\|^{\sigma_0(u)} \cdots \|\mathbf{r}_n\|^{\sigma_n(u)} \right). \tag{9}$$

To get the condition (6) from this inequality we make some remarks.

Let v be the integer defined by

$$\binom{r+v}{v} \leq \phi(u) < \binom{r+v+1}{v+1}.$$

Then $r!\phi(u) \sim du^r \sim v^r$, where $f(u) \sim g(u)$ means that the quotient $f(u)/g(u)$ tends to 1 as $u \to \infty$. One can check that

$$\sigma(u) = \frac{r}{r+1} v\phi(u) + O_r(v^r).$$

Hence,

$$\frac{\sigma_i(u)}{\sigma(u)} \sim \frac{\sigma_i(u)}{\frac{r}{r+1}\, v\, \phi(u)} \sim \left(\frac{r+1}{r}\right) \frac{u}{v} \frac{\sigma_i(u)}{u\, \phi(u)} \sim \left(\frac{r+1}{r}\right) \frac{a_i}{d^{1/r}}.$$

By lemma 1 we know that $\sigma_0, \ldots, \sigma_n$ are equal to some polynomials for u sufficiently large in terms of n and δ. Moreover, the coefficients of these polynomials are bounded in terms of n and δ. Hence, we can find u, bounded in terms of n, δ, and ε, such that

$$\frac{\sigma_i(u)}{\sigma(u)} \leq \left(\frac{r+1}{r}\right) \frac{a_i}{d^{1/r}} + \varepsilon.$$

The remaining factor $(\phi(u)!)^{[K:\mathbb{Q}]/\sigma(u)}$ of (9) can bounded in terms of r, that is, in terms of n. This completes the proof of lemma 3.

4 Rational points on surfaces in $\mathbb{P}^n$

The aim of this section is to prove theorem 3. For simplicity, we will assume that $K = \mathbb{Q}$. But we expect that it is possible to prove the result over any algebraic number field by similar arguments. We will also write $P^n(B)$ instead of $P^n(B_0, \dots, B_n)$ whenever $B = B_0 = \cdots = B_n$.

Let $V \subset \mathbb{P}^n$ be an absolutely irreducible non-degenerate surface of degree d. Given $\mathbf{y} \in P^n$ we define $H_{\mathbf{y}} \subset \mathbb{P}^n$ to be the hyperplane

$$\mathbf{x} \cdot \mathbf{y} = x_0 y_0 + \cdots + x_n y_n = 0.$$

According to a lemma of Siegel (see e.g. lemma 1 of [12]), there is a constant c_1, which depends only on n, such that the points of $\mathbb{P}^n(\mathbb{Q})$ of height at most B are contained in

$$\bigcup_{\mathbf{y} \in P^n(c_1 B^{1/n})} H_{\mathbf{y}}(\mathbb{Q}).$$

Hence, if we let $V_k(T)$ be the union of all irreducible components of

$$\bigcup_{\mathbf{y} \in P^n(T)} (V \cap H_{\mathbf{y}})$$

of degree k, we have

$$N(V', B) \leq \sum_{k=2}^{\deg V} N(V_k(c_1 B^{1/4}), B). \tag{10}$$

We shall estimate the different terms on the right-hand side of (10).

The following estimate will be used in the proof of theorem 2. We do not really need the full strength of the result for theorem 3.

Lemma 7. *If $T \leq B$, then*

$$N(V_k(T), B) \ll_{n,d,\varepsilon} B^{2/k+\varepsilon} T^{n+1-2/kn+\varepsilon},$$

for every $\varepsilon > 0$.

To prove this, we define $C_{\mathbf{y},k}$ to be the union of the irreducible components of $V \cap H_{\mathbf{y}}$ of degree k. We then have

$$N(V_k(T), B) \leq \sum_{\mathbf{y} \in P^n(T)} N(C_{\mathbf{y},k}, B).$$

For each $\mathbf{y} \in P^n(T)$ we can find a basis $\mathbf{x}_1, \dots, \mathbf{x}_n$ of the lattice $\mathbf{x} \cdot \mathbf{y} = 0$ such that

$$\|\mathbf{y}\| \ll_n \|\mathbf{x}_1\| \cdots \|\mathbf{x}_n\| \ll_n \|\mathbf{y}\|.$$

It will have the property that if

$$z_1\mathbf{x}_1 + \cdots + z_n\mathbf{x}_n \in P^n(B)$$

then $|z_i| \le c_2 B/\|\mathbf{x}_i\|$, for some constant c_2 which only depends on n (see e.g. lemma 1 of [12]). Without loss of generality, we may assume that

$$\|\mathbf{x}_1\| \le \cdots \le \|\mathbf{x}_n\|.$$

Let $D_{\mathbf{y},k} \subset \mathbb{P}^{n-1}$ be the image of $C_{\mathbf{y},k}$, under the map

$$H_{\mathbf{y}} \to \mathbb{P}^{n-1}, \quad z_1\mathbf{x}_1 + \cdots + z_n\mathbf{x}_n \mapsto (z_1, \ldots, z_n).$$

We then have that

$$N(C_{\mathbf{y},k}, B) \le N\left(D_{\mathbf{y},k}, \frac{c_2 B}{\|\mathbf{x}_1\|}, \ldots, \frac{c_2 B}{\|\mathbf{x}_n\|}\right) \ll_{n,d,\varepsilon} \left(\frac{B}{\|\mathbf{x}_1\|}\right)^{2/k+\varepsilon},$$

by corollary 1. Note that we may assume that $c_2 B/\|\mathbf{x}_i\| \ge 1$ by choosing c_2 properly. Suppose that $C_i < \|\mathbf{x}_i\| \le 2C_i$ for some constants $C_i \le T$. The vector $\mathbf{y}$ belongs to the n–dimensional lattice defined by $\mathbf{x}_1$, and provided that $R \gg \|\mathbf{x}_1\|$, there are $O_n(R^n/\|\mathbf{x}_1\|)$ elements of the lattice of height at most R (see e.g. lemma 1 of [12]). Hence, there are $O_n(C_1^{n-1}C_2^n \cdots C_n^n)$ vectors $\mathbf{y}$ for a fixed $\mathbf{x}_1$. The number of $\mathbf{x}_1$ for which $C_1 < \|\mathbf{x}_1\| \le 2C_1$ is $O(C_1^{n+1})$ so there are $O_n(C_1^{2n}C_2^n \cdots C_n^n)$ vectors $\mathbf{y}$ such that $C_i < \|\mathbf{x}_i\| \le 2C_i$. Consequently, the total contribution to our sum from these $\mathbf{y}$ is

$$\begin{aligned}
&\ll_{n,d,\varepsilon} B^{2/k+\varepsilon} C_1^{2n-2/k} C_2^n \cdots C_n^n \\
&\ll B^{2/k+\varepsilon} (C_1 \cdots C_n)^{n+1-2/kn} \\
&\ll_n B^{2/k+\varepsilon} T^{n+1-2/kn}.
\end{aligned}$$

By letting C_i run over powers of 2 and sum the resulting bounds we obtain the promised result.

Lemma 7 is valid for all k but it is not very useful for small k. We shall study the cases $k = 2$ and $k = 3$ more carefully. The following fact was explained to us by P. Salberger.

Lemma 8. *Let $V \subset \mathbb{P}^n$ be an absolutely irreducible non-degenerate variety with Hilbert polynomial p_V. Let p be a polynomial of degree* $\dim V - 1$ *such that its leading coefficient is smaller than* $\dim V$ *times the leading coefficient of p_V. Then there exists a non-trivial form E in $n+1$ variables of degree bounded in terms of n, p_V, and p, such that $E(\mathbf{y}) = 0$ whenever $V \cap H_{\mathbf{y}}$ has a sub-variety with Hilbert polynomial p.*

We only sketch the proof here. Let $\mathcal{H}_1 \subset \mathbb{P}^m$ and $\mathcal{H}_2$ be the Hilbert schemes which parametrise sub-schemes of $\mathbb{P}^n$ with Hilbert polynomials p_V and p, respectively. Let $\mathcal{Y} \subset \mathcal{H}_1 \times \mathcal{H}_2 \times \mathbb{P}^{n*}$ be the closed sub-scheme consisting of the triples (H_1, H_2, H_3) such that $H_2 \subset H_1$ and $H_2 \subset H_3$. The projection

$$\mathcal{H}_1 \times \mathcal{H}_2 \times \mathbb{P}^{n*} \to \mathcal{H}_1 \times \mathbb{P}^{n*} \subset \mathbb{P}^m \times \mathbb{P}^{n*}$$

is proper so the image of $\mathcal{Y}$ in $\mathbb{P}^m \times \mathbb{P}^{n*}$ is closed, defined by finitely many bihomogeneous polynomials $E_i(\mathbf{x}, \mathbf{y})$. Let $\mathbf{x} \in \mathcal{H}_1(K) \subset \mathbb{P}^m(K)$ be the rational point representing $V \subset \mathbb{P}^n$ and put $E_{i,V}(\mathbf{y}) = E_i(\mathbf{x}, \mathbf{y})$. Then all $E_{i,V}$ cannot vanish identically since $V \cap H$ is irreducible for some H by Bertini's theorem. We can take E to be any of these forms.

Lemma 9. *If* $\deg V > 2$ *and* $T \leq B^{3/(n-2)}$, *then*

$$N(V_2(T), B) \ll_{n, p_V, \varepsilon} B^{1+\varepsilon} T^{\frac{2}{3}(n+1)+\varepsilon},$$

for every $\varepsilon > 0$.

Obviously we may redefine $V_2(T)$ by removing those components which do not contain any rational points. Let $C \subset V_2(T)$ be an irreducible component of this new $V_2(T)$. Since every curve of degree 2 which contains a rational point is plane, we can find $\mathbf{y}_1, \ldots, \mathbf{y}_{n-2} \in P^n$ such that

$$C = H_{\mathbf{y}_1} \cap \cdots \cap H_{\mathbf{y}_{n-2}} \cap Q,$$

for some quadratic hypersurface $Q \subset \mathbb{P}^n$. As in the proof of lemma 7 we can find a basis $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \in P^n$ of the lattice

$$\mathbf{x} \cdot \mathbf{y}_1 = \cdots = \mathbf{x} \cdot \mathbf{y}_{n-2} = 0,$$

such that $|z_i| \leq c_3 B / \|\mathbf{x}_i\|$ for some constant c_3, whenever

$$z_1 \mathbf{x}_1 + z_2 \mathbf{x}_2 + z_3 \mathbf{x}_3 \in P^n(B).$$

By the definition of $V_2(T)$ we can assume that $\mathbf{y}_1 \in P^n(T)$. We may also assume that

$$\|\mathbf{y}_1\|^{n-2} \ll_n \|\mathbf{x}_1\| \, \|\mathbf{x}_2\| \, \|\mathbf{x}_3\|$$

(see e.g. chapter I of [21]). Let $D \subset \mathbb{P}^2$ be the irreducible quadratic curve which is the image of C under the map

$$H_{\mathbf{y}_1} \cap \cdots \cap H_{\mathbf{y}_{n-2}} \to \mathbb{P}^2, \quad z_1 \mathbf{x}_1 + z_2 \mathbf{x}_2 + z_3 \mathbf{x}_3 \mapsto (z_1, z_2, z_3).$$

According to theorem 3 of [12], we have

$$\begin{aligned} N(C,B) &\le N\left(D, \frac{c_3 B}{\|\mathbf{x}_1\|}, \frac{c_3 B}{\|\mathbf{x}_2\|}, \frac{c_3 B}{\|\mathbf{x}_3\|}\right) \\ &\ll_{n,\varepsilon} \frac{B^{1+\varepsilon}}{(\|\mathbf{x}_1\|\,\|\mathbf{x}_2\|\,\|\mathbf{x}_3\|)^{1/3}} \\ &\ll_n \frac{B^{1+\varepsilon}}{\|\mathbf{y}_1\|^{(n-2)/3}}, \end{aligned}$$

provided that $c_3 B/\|\mathbf{x}_i\| \ge 1$ for $i = 1,2,3$. On the other hand, we have $N(C,B) \le 2$ otherwise, so the estimate is still valid by the assumption $T \le B^{3/(n-2)}$. Theorem 1 of [12] states that $N(X,R) = O_{n,d}(R^n)$ for any hypersurface $X \subset \mathbb{P}^n$ of degree d. Hence, if we combine this result with lemma 8, we see that the number of $C \subset V_2(T)$ for which $R \le \|\mathbf{y}_1\| < 2R$ for some $R \le T$ is $O_{n,p_V}(R^n)$. Note that there can only be $O_d(1)$ curves C with the same $\mathbf{y}_1$. Consequently, the components of $V_2(T)$ with $R < \|\mathbf{y}_1\| \le 2R$ contribute with

$$\ll_{n,p_V,\varepsilon} B^{1+\varepsilon} R^{n-(n-2)/3} \le B^{1+\varepsilon} T^{\frac{2}{3}(n+1)}$$

to $N(V_2(T),B)$. By summing over dyadic intervals once again we get the desired estimate.

Lemma 10. *If* $\deg V > 3$, *then*

$$N(V_3(T),B) \ll_{p_V,\varepsilon} B^{2/3+\varepsilon} T^n$$

for every $\varepsilon > 0$.

To see this, let $C \subset V$ be any absolutely irreducible curve of degree 3. It is well-known that C is either a plane curve or a twisted cubic curve in $\mathbb{P}^3$ (see e.g. exercise 3.4(d), page 315 in [9]). The arithmetic genus of C is thus either 0 or 1 so there are only two possible Hilbert polynomials of C. If C is not absolutely irreducible then C consists of three conjugated lines, or a line and a conic. There are only a finite number of possible Hilbert polynomials for such configurations. Hence, lemma 8 states that there exists a non-trivial form E such that $E(\mathbf{y}) = 0$ when $V \cap H_{\mathbf{y}}$ contains a curve of degree 3. There are $O_{n,p_V}(T^n)$ elements $\mathbf{y} \in P^n(T)$ which satisfies $E(\mathbf{y}) = 0$. According to corollary 1, $N(C,B) = O_\varepsilon(B^{2/3+\varepsilon})$. Hence,

$$N(V_3(T),B) \ll_{p_V,\varepsilon} B^{2/3+\varepsilon} T^n,$$

which was to be proved.

If we study the different estimates given by these lemmas we see that the estimate given by lemma 9 will dominate the sum in (10) provided that $\deg V \ge 4$. Hence,

$$N(V',B) \ll_{p_V,\varepsilon} B^{1+\frac{2(n+1)}{3n}+\varepsilon},$$

which completes the proof of theorem 3.

5 Rational points on smooth surfaces in $\mathbb{P}^4$

In this section we shall prove theorem 2. One advantage of restricting to smooth surfaces is that one has more information about the curves on such surfaces. The following result was proved by Colliot-Thélène [5] in the case $d_1 = 1$.

Lemma 11. *For every triple (d_1, d_2, k) of positive integers such that $d_1 + d_2 \geq 4$ and $k < d_1 + d_2 - 2$ there is an integer $N(d_1, d_2, k)$ such that for any smooth surface $V \subset \mathbb{P}^4$ defined by $F_1 = F_2 = 0$ where $\deg F_i = d_i$, there are at most $N(d_1, d_2, k)$ irreducible curves of degree k lying on V.*

We will not prove this in detail. The crucial observation in [5] is that the Castelnuovo's bound for the arithmetic genus $p_a(C) = \dim H^1(C, \mathcal{O}_C)$ (cf. [1], p. 116) is not only valid for smooth curves but also for other classes of curves like curves lying on smooth surfaces. We thus have the following.

Lemma 12. *Let $V \subset \mathbb{P}^4$ be a smooth surface. If $C \subset V$ is an absolutely irreducible curve of degree k, then*

$$p_a(C) \leq \begin{cases} \frac{k^2}{2} - \frac{3k}{2} + 1, & \text{if } C \text{ is plane,} \\ \frac{k^2}{4} - k + 1, & \text{if } C \text{ is degenerate but not plane,} \\ \frac{k^2}{6} - \frac{5k}{6} + 1, & \text{if } C \text{ is non-degenerate.} \end{cases}$$

Exercise 1.3 on page 366 and 8.4(c) on page 188 of [9] gives

$$2p_a(C) - 2 = C.(C + K_V) = C.C + k(d_1 + d_2 - 5)$$

for any absolutely irreducible curve of degree k on a smooth surface V as in lemma 11. If we use lemma 12 we see that $C.C < 0$ whenever $d_1 + d_2 \geq 4$ and $k < d_1 + d_2 - 2$. By lemma 12 we also see that there are only a finite number of possible Hilbert polynomials for a given irreducible curve of degree k which lies on $V \subset \mathbb{P}^4$. Consequently, these curves are parametrised by an open subset of a Hilbert scheme of finite type. Colliot-Thélène uses this fact to show that there can only be a finite number of irreducible curves of degree k on V if $C.C < 0$ for every such curve. To find the uniform bound $N(d_1, d_2, k)$ of the number of curves one uses parameter spaces. See [5] for further details.

Lemma 13. *Let $V \subset \mathbb{P}^4$ be a smooth surface which is defined by $F_1 = F_2 = 0$ where $\deg F_i = d_i \geq 2$. Then, for every $\varepsilon > 0$, there are $O_{d_1,d_2,\varepsilon}(T^{7/2+\varepsilon})$ points $\mathbf{y} \in P^4(T)$ for which $V \cap H_{\mathbf{y}}$ is reducible.*

If $V \cap H_{\mathbf{y}}$ is reducible, then $\mathbf{y}$ belongs to the dual $V^* \subset \mathbb{P}^4$ which is an irreducible hypersurface of degree bounded in terms of d_1 and d_2 (see e.g. proposition 5.7.2 of [13]). First we show that V^* cannot be linear. Assume on the contrary that it is given by an equation $\mathbf{z} \cdot \mathbf{y} = 0$ for some $\mathbf{z}$. Then $\mathbf{z} \cdot \nabla F_1(\mathbf{x}) = \mathbf{z} \cdot \nabla F_2(\mathbf{x}) = 0$ for all $\mathbf{x} \in V$. Thus the forms $\mathbf{z} \cdot \nabla F_1$ and $\mathbf{z} \cdot \nabla F_2$ belong to the ideal generated by F_1 and F_2. We have assumed that $d_i \geq 2$, so the only possibility is that $\mathbf{z} \cdot \nabla F_1$ and $\mathbf{z} \cdot \nabla F_2$ vanish identically. But then

$$d_j F_j(\mathbf{z}) = \mathbf{z} \cdot \nabla F_j(\mathbf{z}) = 0,$$
$$d_j \frac{\partial F_j}{\partial x_i}(\mathbf{z}) = \left(\frac{\partial}{\partial x_i}(\mathbf{z} \cdot \nabla F_j) \right)(\mathbf{z}) = 0,$$

for $j = 1, 2$ and $0 \leq i \leq 4$ so $\mathbf{z}$ is a singular point of V. The conclusion is that $\deg V^* \geq 2$. Theorem B in [19] gives

$$N(V^*, T) \ll_{d_1, d_2, \varepsilon} T^{7/2+\varepsilon},$$

which is the statement of lemma 13.

We are now in position to prove theorem 2. Assume that $V \subset \mathbb{P}^4$ is a smooth surface defined by $F_1 = F_2 = 0$ for some forms F_1 and F_2 with $d_i = \deg F_i \geq 2$. As in the previous section we define $V_k(T)$ to be the union of the irreducible curves of degree k which are contained in $\bigcup_{\mathbf{y} \in P^4(T)} (V \cap H_{\mathbf{y}})$. Corollary 1 and lemma 11 give

$$N(V_k(B^{1/4}), B) \ll_{d_1, d_2, \varepsilon} B^{2/k+\varepsilon}$$

for $k < d_1 + d_2 - 2$, corollary 1 and lemma 13 give

$$N(V_k(B^{1/4}), B) \ll_{d_1, d_2, \varepsilon} B^{7/8+2/k+\varepsilon}$$

for $d_1 + d_2 - 2 \leq k < d_1 d_2$, and by lemma 7,

$$N(V_{d_1 d_2}(B^{1/4}), B) \ll_{d_1, d_2, \varepsilon} B^{\frac{5}{4} + \frac{15}{8 d_1 d_2} + \varepsilon}.$$

Taken together,

$$\begin{aligned} N(V', B) &\ll \sum_{k=2}^{d_1 d_2} N(V_k(B^{1/4}), B) \\ &\ll_{d_1, d_2, \varepsilon} B^{1+\varepsilon} + B^{\frac{7}{8} + \frac{2}{d_1 + d_2 - 2} + \varepsilon} + B^{\frac{5}{4} + \frac{15}{8 d_1 d_2} + \varepsilon}. \end{aligned}$$

It is easy to see that the last term dominates when $d_1 + d_2 \geq 8$, so it is straightforward to check that it dominates for all $d_1 \geq 2$, $d_2 \geq 3$. The estimate is valid for $d_1 = d_2 = 2$, but then the term in the middle dominates. However, if we reprove lemma 9 using the bound $O_\varepsilon(T^{7/2+\varepsilon})$ for the number of $\mathbf{y} \in P^4(T)$ for which $V \cap H_{\mathbf{y}}$ contains a curve of degree 2, we see that theorem 2 holds for $d_1 = d_2 = 2$ as well.

To prove the second estimate of theorem 2, we shall apply theorem 1 in the case $n = 4$. Let $H \subset \mathbb{P}^4$ be a hypersurface such that V is not contained in H but such that the rational points of height at most B on V are contained in $V \cap H$. We define V_k to be the union of the irreducible components of $V \cap H$ of degree k. Theorem 1 says that we may choose H such that V_k consists of $O_{d_1,d_2,\varepsilon}(B^{3/\sqrt{d_1 d_2}+\varepsilon})$ irreducible curves and that $V_k = \emptyset$ for $k \gg_{d_1,d_2,\varepsilon} 1$. According to corollary 1,

$$N(V_k, B) \ll_{d_1,d_2,\varepsilon} B^{3/\sqrt{d_1 d_2}+2/k+\varepsilon},$$

and if we use lemma 11 we have

$$N(V_k, B) \ll_{d_1,d_2,\varepsilon} B^{2/k+\varepsilon}$$

for $k < d_1 + d_2 - 2$. Hence,

$$N(V', B) \leq \sum_{k \geq 2} N(C_k, B) \ll_{d_1,d_2,\varepsilon} B^{1+\varepsilon} + B^{\frac{3}{\sqrt{d_1 d_2}} + \frac{2}{d_1+d_2-2} + \varepsilon},$$

and this completes the proof of theorem 2.

References

[1] E. Arbarello, M. Cornalba, P.A. Griffiths, and J. Harris, *Geometry of Algebraic Curves, Volume 1*, Springer-Verlag, 1985.

[2] D. Bayer and D. Mumford, What can be computed in algebraic geometry?, *Computational algebraic geometry and commutative algebra (Cortina, 1991)*, Cambridge Univ. Press, 1993.

[3] E. Bombieri and J. Vaaler, On Siegel's lemma, *Invent. Math.*, 73 (1983), 11–32.

[4] N. Bourbaki, *Elements of mathematics. Commutative algebra.*, Hermann, 1972.

[5] J.-L. Colliot-Thélène, *Appendix of [12]*, Preprint.

[6] D. Eisenbud and J. Harris, *The geometry of schemes*, Springer-Verlag, 2000.

[7] W. Fulton, *Intersection theory*, Springer-Verlag, 1984.

[8] L. Gruson, R. Lazarsfeld, and C. Peskine, On a theorem of Castelnuovo, and the equations defining space curves, *Invent. Math.*, 72 (1983), 491–506.

[9] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, 1977.

[10] J. Harris, *Algebraic Geometry*, Springer-Verlag, 1995.

[11] D. Cox, J. Little, and D. O'shea, *Ideals, varieties, and algorithms*, Springer-Verlag, second edition, 1997.

[12] R. Heath-Brown, The density of rational points on curves and surfaces, Preprint.

[13] N. Katz, Expose XVII, *SGA 7 II*, Springer-Verlag, 1973.

[14] J. Kollár, *Rational curves on algebraic varieties*, Springer-Verlag, 1996.

[15] S. Lang, *Number Theory III*, Springer-Verlag, 1991.

[16] S. Lang, *Algebraic number theory*, Springer-Verlag, second edition, 1994.

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

[18] M. Möller and F. Mora, Upper and lower bounds for the degree of Groebner bases, *EUROSAM 84 (Cambridge 84)*, Springer, 1984, 172–183.

[19] J. Pila, Density of Integral and Rational Points on Varieties, *Astérisque No. 228*, 1995, 183–187.

[20] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Friedr. Vieweg & Sohn, 1989.

[21] W. M. Schmidt, *Diophantine approximations and Diophantine equations*, Springer-Verlag, 1991.