JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Félicien COMTAT

A uniform estimate for the density of rational points on quadrics

Tome 31, n° 1 (2019), p. 243-253.

<http://jtnb.cedram.org/item?id=JTNB_2019__31_1_243_0>

Journal de Théorie des Nombres
de Bordeaux **31** (2019), 243–253

A uniform estimate for the density of rational points on quadrics

par Félicien COMTAT

Résumé. L'objet de cet article est la densité des points rationnels de hauteur bornée sur une variété définie par une forme quadratique Q à coefficients entiers. Dans le cas de quatre variables, nous donnons une estimation qui ne dépend pas des coefficients de Q. Pour davantage de variables, une estimation similaire reste vérifiée en se restreignant à ne compter que les points qui ne sont contenus dans aucune ligne rationnelle.

Abstract. This paper is concerned with the density of rational points of bounded height lying on a variety defined by an integral quadratic form Q. In the case of four variables, we give an estimate that does not depend on the coefficients of Q. For more variables, a similar estimate still holds with the restriction that we only count points which do not lie on $\mathbb{Q}$-lines.

1. Introduction

Given a non-singular quadratic form $Q \in \mathbb{Z}[x_1, \ldots, x_n]$, we are interested in the asymptotic distribution of rational points lying on the projective hypersurface $\mathscr{V} \subset \mathbb{P}^{n-1}_{\mathbb{Q}}$ defined by $Q = 0$. More precisely, define $N(Q, B)$ to be the number of primitive points $\boldsymbol{x} \in \mathbb{Z}^n$ with $|x_i| \leq B$ for each i and such that $Q(\boldsymbol{x}) = 0$.

In the case $n = 4$, it can be deduced from the work of Heath-Brown [6, Theorems 6,7] that as B tends to infinity

$$N(Q, B) \sim \begin{cases} c_Q B^2 & \text{if } \operatorname{disc}(Q) \text{ is not a square,} \\ c_Q B^2 \log(B) & \text{otherwise,} \end{cases}$$

where $\operatorname{disc}(Q)$ is the discriminant of Q and c_Q is a product of local densities that depends on Q. This result is in accordance with Manin's conjecture. However, in some applications one may be interested in estimates which are uniform with respect to the coefficients of Q. In this spirit, if Q is a

Manuscrit reçu le 2 juillet 2018, révisé le 12 décembre 2018, accepté le 22 décembre 2018.
2010 *Mathematics Subject Classification.* 11D45, 11D09, 11E12.
Mots-clefs. Uniform asymptotic estimates, quadratic forms.
I wish to thank Tim Browning for suggesting me this problem, and Bristol School of Mathematics for welcoming me during my stay.

quadratic form of rank at least 3 in n variables, then for any $\epsilon > 0$ we have [7, Theorem 2]

$$N(Q,B) \ll_\epsilon B^{2+\epsilon},$$

where the implied constant only depends on ϵ. In the case of four variables, we show that this ϵ can be removed, in the following sense.

Theorem 1.1. *Let Q be a non-singular integral quadratic form in four variables. Then*

$$N(Q,B) \ll \begin{cases} B^2 & \text{if } \operatorname{disc}(Q) \text{ is not a square,} \\ B^2\log(B) & \text{otherwise,} \end{cases}$$

the implied constant being absolute.

Theorem 1.1 confirms a conjecture by Browning and Heath-Brown [2, Conjecture 1.2]. In fact, the main result in [2] gives an estimate for $N(Q,B)$ which actually gets sharper than Theorem 1.1 for suitably generic quaternary quadratic forms, namely those for which the discriminant is close to being square-free and of order $\|Q\|^4$, where the height $\|Q\|$ is defined as the maximum of the absolute values of the coefficients.

It is well known that over any field of characteristic different from 2, for any non-singular quadratic form Q in n variables, the maximal dimension of a linear subspaces contained in $\mathscr{V}$ is always less than $\frac{n}{2}-1$. In addition, when n is even and $\mathscr{V} \neq \varnothing$, equality happens if and only if the discriminant is a square. This may be seen by induction by computing the determinant of the matrix of Q in any basis of the form $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_n)$, where $Q(\boldsymbol{x}_1)=0$, $\boldsymbol{x}_2,\dots,\boldsymbol{x}_{n-1}$ lie in the tangent space to $\mathscr{V}$ at $\boldsymbol{x}_1$, and $\boldsymbol{x}_n$ is orthogonal to this tangent space. In particular, in the case $n=4$, one may estimate separately the contribution of points which do not lie on $\mathbb{Q}$-lines contained in $\mathscr{V}$ and the contribution from the $\mathbb{Q}$-lines.

To this end, it is also useful to have precise estimates for the distribution of rational points in arbitrary boxes instead of hypercubes only. Namely, for $B_1,\dots,B_n \geq 1$, let $N(Q,\boldsymbol{B})$ be the number of primitive points on the hypersurface $\mathscr{V}$ with $|x_i| \leq B_i$ for each i, and let $N_1(Q,\boldsymbol{B})$ be the number of points $\boldsymbol{x}$ counted by $N(Q,\boldsymbol{B})$ with the additional condition that $\boldsymbol{x}$ does not lie on a $\mathbb{Q}$-line included in $\mathscr{V}$. Work of Browning and Heath-Brown [1] gives precise estimates for these counting functions in the more general case of any irreducible homogeneous polynomial defined over $\mathbb{Z}$. By revisiting their argument we shall prove the following result.

Theorem 1.2. *Let $n \geq 3$, $B_1,\dots,B_n \geq 1$ and define $V = \prod_{i=1}^n B_i$. Let $Q \in \mathbb{Z}[x_1,\dots,x_n]$ be any quadratic form. Then $N_1(Q,\boldsymbol{B}) \ll_n V^{\frac{n-2}{n}}$, where the implied constant depends only on n.*

Theorem 1.2 is a refinement of [1, Theorem 2] in the particular case of quadratic forms, as we get rid of all the logarithmic factors. Combined with an estimation of the contribution from the lines separately, it will prove a vital tool in the proof of Theorem 1.1.

2. Preliminaries

In order to estimate the counting functions we are interested in, we shall need to deal with various maximal rank sublattices of $\mathbb{Z}^n$. We therefore introduce for any such lattice Λ, and $B_1, \dots, B_n \geq 1$

$$P(Q, \boldsymbol{B}, \Lambda) = \Big\{ [\boldsymbol{x}] : \boldsymbol{x} \in \Lambda, Q(\boldsymbol{x}) = 0, \max_i |x_i| \leq B_i \Big\},$$

where $[\boldsymbol{x}]$ is the image in $\mathbb{P}^{n-1}(\mathbb{Q})$ of $\boldsymbol{x}$. We also define

$$S(Q, \boldsymbol{B}, \Lambda) = \Big\{ \boldsymbol{x} \in \Lambda : c_\Lambda(\boldsymbol{x}) = 1, Q(\boldsymbol{x}) = 0, \max_i |x_i| \leq B_i \Big\},$$

where $c_\Lambda(\boldsymbol{x})$ denotes the gcd of the coefficients of $\boldsymbol{x}$ in some basis of Λ (and is independent of the choice of the basis), and

$$Z(Q, \boldsymbol{B}, \Lambda) = \Big\{ \boldsymbol{x} \in \Lambda : Q(\boldsymbol{x}) = 0, \gcd(x_1, \dots, x_n) = 1, \max_i |x_i| \leq B_i \Big\}.$$

There is an obvious 2-to-1 correspondence between the sets $S(Q, \boldsymbol{B}, \Lambda)$ and $P(Q, \boldsymbol{B}, \Lambda)$, and when $\Lambda = \mathbb{Z}^n$ we have $Z(Q, \boldsymbol{B}, \Lambda) = S(Q, \boldsymbol{B}, \Lambda)$. However in general there is only an inclusion of $Z(Q, \boldsymbol{B}, \Lambda)$ into $S(Q, \boldsymbol{B}, \Lambda)$. When $B_1 = \cdots = B_n = B$, we shall denote these sets by $P(Q, B, \Lambda)$, $S(Q, B, \Lambda)$ and $Z(Q, B, \Lambda)$, respectively.

We begin with a reminder of some useful facts about lattices, all of which can be found in Chapters 1 and 8 of [3]. Given any lattice $\Lambda \subset \mathbb{Z}^n$ of dimension r, its *determinant* is the r-dimensional volume of any fundamental parallelepiped of Λ. If M is the $n \times r$ matrix whose columns are the vectors of any basis of Λ, then we have

$$(\det \Lambda)^2 = \det(M^T M).$$

It follows that if $\Lambda_1 \subset \Lambda_2$ have the same dimension then $\det \Lambda_2 \mid \det \Lambda_1$.

Let $\boldsymbol{m}_1$ be any shortest non-zero vector in Λ with respect to the Euclidean length, and for $i < r$, define $\boldsymbol{m}_{i+1}$ as any shortest vector in Λ not contained in the span of $\boldsymbol{m}_1, \dots, \boldsymbol{m}_i$. We obtain a so-called *minimal basis* $\boldsymbol{m}_1, \dots, \boldsymbol{m}_r$ of Λ, and the corresponding $s_i = \|\boldsymbol{m}_i\|$ are the *successive minima* of Λ. Then we have

$$\prod_{i=1}^r s_i \ll \det \Lambda \leq \prod_{i=1}^r s_i. \tag{2.1}$$

In addition, we have the following useful lemma (see [4, Lemma 5]).

Lemma 2.1. *Let $\Lambda \subset \mathbb{Z}^n$ be a lattice of dimension r, with successive minima $s_1 \leq \cdots \leq s_r$ and let $\boldsymbol{m}_1, \ldots, \boldsymbol{m}_r$ be a minimal basis of Λ. Then there is a constant $c_{r,n}$ depending only on r and n such that for any*

$$\boldsymbol{x} = \sum_{i=1}^{r} \lambda_i \boldsymbol{m}_i \in \Lambda,$$

we have $|\lambda_i| \leq c_{r,n} \frac{\|\boldsymbol{x}\|}{s_i}$ for all $i \leq r$.

The next result shows that we can restrict attention to quadratic forms Q of height bounded in terms of B.

Lemma 2.2. *Let $Q \in \mathbb{Z}[x_1, \ldots, x_n]$ be a quadratic form and denote by $\|Q\|$ the maximum of the absolute values of the coefficients of Q. Then for any $B_1 \leq \cdots \leq B_n$ there exists a quadratic form $G \in \mathbb{Z}[x_1, \ldots, x_n]$ with $\|G\| \ll_n B_n^{n(n+1)-2}$ (the implied constant only depends on n) such that $P(Q, \boldsymbol{B}, \mathbb{Z}^n) \subset P(G, \boldsymbol{B}, \mathbb{Z}^n)$.*

A more general result holding for any homogeneous polynomial defined over $\mathbb{Z}$ is established in the proof of Theorem 4 in [7], but we give a proof for completeness.

Proof. Choose a set of representatives $\{\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(N)}\}$ of $P(Q, \boldsymbol{B}, \mathbb{Z}^n)$ such that each $\boldsymbol{x}^{(i)}$ is contained in the box $\boldsymbol{B}$. Let C be the $N \times \frac{n(n+1)}{2}$ matrix whose i-th row consists of all the possible monomials of degree 2 in the coordinates of $\boldsymbol{x}^{(i)}$, arranged in the same order. Let $\boldsymbol{y}$ be the vector whose coordinates are the coefficients of Q ordered accordingly to the monomials in the rows of C. By construction, $C\boldsymbol{y} = 0$. It follows that C has rank at most $\frac{n(n+1)}{2} - 1$. Therefore, one can construct an integral nonzero vector in the kernel of C using subdeterminants of size at most $\frac{n(n+1)}{2} - 1$. Since all the entries of C are less than B_n^2 in absolute value, this vector has norm $\ll B_n^{n(n+1)-2}$, and we can take for G the corresponding quadratic form. $\square$

3. Proof of Theorem 1.2

We proceed by induction on n. The base case $n = 3$ is Theorem 6 of [1]. Note that if Q is singular, then the claim of Theorem 1.2 is automatically verified because either $\mathscr{V}(\mathbb{Q})$ contains a single projective point or all points lie on a line. Indeed, we can find a nonzero vector $\boldsymbol{x}$ in the kernel of Q. For any $\boldsymbol{y} \in \mathscr{V}(\mathbb{Q})$, one has $Q(\boldsymbol{y} + \lambda\boldsymbol{x}) = 0$ for all $\lambda \in \mathbb{Q}$. Thus if $\boldsymbol{y}$ is not proportional to $\boldsymbol{x}$, this gives a whole projective line passing through $\boldsymbol{y}$. On the other hand, if $\boldsymbol{y}$ is proportional to $\boldsymbol{x}$, then under the assumption that $\mathscr{V}(\mathbb{Q})$ contains more than one projective point, one may find another $\boldsymbol{z} \in \mathscr{V}(\mathbb{Q})$ not proportional to $\boldsymbol{y}$, and $Q(\boldsymbol{y} + \lambda\boldsymbol{z}) = 0$ for all $\lambda \in \mathbb{Q}$.

Consider now $n \geq 4$ and assume Q is a fixed non singular integral quadratic form in n variables. Let $B_1 \leq B_2 \leq \cdots \leq B_n$ (this condition is not restrictive since we can permute variables) and $V = \prod_{i=1}^n B_i$. We may assume without loss of generality that the B_i are powers of two. By Lemma 2.2 we may furthermore assume without loss of generality that Q is primitive and $\|Q\| \ll B_n^{n(n+1)-2}$.

For any prime p we introduce

$$S(Q, \boldsymbol{B}, \Lambda, p) = \{\boldsymbol{x} \in S(Q, \boldsymbol{B}, \Lambda) : p \nmid \nabla Q(\boldsymbol{x})\}$$

and

$$Z(Q, \boldsymbol{B}, \Lambda, p) = \{\boldsymbol{x} \in Z(Q, \boldsymbol{B}, \Lambda) : p \nmid \nabla Q(\boldsymbol{x})\}.$$

We will strongly rely on the following result from [1, Lemma 8].

Lemma 3.1. *Let $\mathcal{B} \geq 1$ and $\Lambda \subset \mathbb{Z}^n$ be a lattice of dimension $r \geq 2$, with largest successive minimum $\ll \mathcal{B}$. Let p be a prime not dividing* $\det \Lambda$. *Then there is an integer $I \ll p^{r(r-2)}(\frac{\mathcal{B}^r}{\det \Lambda})^{\frac{r-2}{r}}$ and lattices $\Lambda_1, \ldots, \Lambda_I \subset \Lambda$ of dimension $r-1$ such that*

$$S(Q, \mathcal{B}, \Lambda, p) \subset \bigcup_{i=1}^{I} \Lambda_i.$$

(where in the left hand side we mean that we consider the box of side length $\mathcal{B}$). For any i, the successive minima of Λ_i are all $O(p^r\mathcal{B})$. Moreover for any $\alpha > 0$ we have

$$\#\{i : \det \Lambda_i \leq \alpha \det \Lambda\} \ll p^{r-2}(\alpha\mathcal{B})^{\frac{r-2}{r}}. \tag{3.1}$$

Remark 3.1. What is denoted by $S(Q, \mathcal{B}, \Lambda)$ in [1] is what we denote here by $Z(Q, \mathcal{B}, \Lambda)$. Thus it might seem that we should have replaced $S(Q, \mathcal{B}, \Lambda, p)$ with $Z(Q, \mathcal{B}, \Lambda, p)$ in the above statement. However, going through the proof, one can ensure this is what is proven in [1]. Indeed, the authors proceed by sending the lattice Λ to $\mathbb{Z}^n$, then by embedding the primitive points on the accordingly transformed quadric into a collection of sublattices, and eventually by taking back the image of these sublattices in Λ. The point is that not only vectors from $Z(Q, \mathcal{B}, \Lambda)$, but actually from $S(Q, \mathcal{B}, \Lambda)$ (with our notation), have an image in $\mathbb{Z}^n$ that is primitive. Another slight difference is that in the original formulation of [1], it is assumed that $\alpha \geq 1$. However, here again this condition can be relaxed. The construction is such that to each lattice Λ_i is assigned a "depth" k. Moreover, there are at most $p^{k(r-2)}$ lattices of depth k, and Λ_i has determinant at least $p^{(k-1)r}\mathcal{B}^{-1} \det \Lambda$. Thus, for any $\alpha > 0$, $\det \Lambda_i \leq \alpha \det \Lambda$ implies $p^k \ll p(\alpha\mathcal{B})^{1/r}$. Therefore there are at most $p^{r-2}(\alpha\mathcal{B})^{\frac{r-2}{r}}$ such lattices Λ_i.

Remark 3.2. Before going back to the proof of Theorem 1.2, we give an overview of the proof of Lemma 3.1, as it is the core of the inductive argument. The general idea is to consider the reduction of $Q=0$ modulo p^k for some appropriate exponents k, and to perform a Taylor expansion of order 2 in order to embed the lifts in Λ of every projective point $[\boldsymbol{x}]$ modulo p^k in a corresponding lattice $M_{[\boldsymbol{x}]}\subset\Lambda$ of dimension r. Moreover, for k big enough these lattices $M_{[\boldsymbol{x}]}$ have largest successive minimum $\gg\mathcal{B}$. Hence, by Lemma 2.1, under the assumption that $|\boldsymbol{x}|\leq\mathcal{B}$, one can restrict to the sublattice of $M_{[\boldsymbol{x}]}$ generated by the first $r-1$ vectors of a minimal basis. On the other hand, the larger k is, the more points modulo p^k have to be considered. Thus one has to choose k carefully.

The next step to prove Theorem 1.2 is to come down from $S(Q,\mathcal{B},\Lambda)$ to $S(Q,\mathcal{B},\Lambda,p)$. To this end, one has to find a set of primes p in a way that ensures that for each $\boldsymbol{x}\in S(Q,\mathcal{B},\Lambda)$, at least one of these p does not divide $\nabla Q(\boldsymbol{x})$. To this end, p has to range in some interval depending on $\|Q\|\mathcal{B}$, and that is where the logarithmic factors enter into the picture in [1]. In our work, the main idea is to exploit the situation $p\mid\nabla Q(\boldsymbol{x})$ as an additional constraint on $\boldsymbol{x}$.

For any positive integer m, let p_m denote the m-th prime number. For simplicity, in the sequel we shall use the notation $q_m=p_2\dots p_{m-1}$ for the product of the first $m-2$ odd primes. For any lattice $\Lambda\subset\mathbb{Z}^n$, denote by

$$\Lambda(m)=\{\boldsymbol{x}\in\Lambda : q_m\mid\nabla Q(\boldsymbol{x})\}.$$

Since Q is quadratic, ∇Q is linear and $\Lambda(m)$ is a lattice. Let M be the half-integer symmetric matrix corresponding to Q, so that $Q(\boldsymbol{x})={}^T\boldsymbol{x}M\boldsymbol{x}$. Write $2M$ under Smith normal form: $2M=SDT$ with S and T unimodular, and $D=\operatorname{diag}(d_i)$,with $d_i\mid d_{i+1}$ for $1\leq i\leq n$. Hence $d_1\in\{1,2\}$ since Q is primitive.

Lemma 3.2. *Let $b_1,\dots,b_n$ be powers of two, $\Lambda_{\boldsymbol{b}}=\prod_{i=1}^n(b_i\mathbb{Z})$, and $v=\prod_{i=1}^n b_i$. Then*

$$\det\Lambda_{\boldsymbol{b}}(m)=v\prod_{i=1}^n a_i$$

with $a_i=\frac{q_m}{\gcd(q_m,d_i)}$. In particular, it is divisible by q_m since $a_1=q_m$.

Proof. Write $\Lambda_{\boldsymbol{b}}(m)=\mathbb{Z}^n(m)\cap\Lambda_{\boldsymbol{b}}$. Obviously, $\Lambda_{\boldsymbol{b}}$ has determinant v. It follows that $\operatorname{lcm}(\det\mathbb{Z}^n(m),v)\mid\det\Lambda_{\boldsymbol{b}}(m)$. We have

$$\begin{aligned}\mathbb{Z}^n(m)&=\{\boldsymbol{x}\in\mathbb{Z}^n : q_m\mid\nabla Q(\boldsymbol{x})\}\\&=\{\boldsymbol{x}\in\mathbb{Z}^n : q_m\mid SDT\boldsymbol{x}\}\\&=\{T^{-1}\boldsymbol{y} : \boldsymbol{y}\in T\mathbb{Z}^n : q_m\mid SD\boldsymbol{y}\}\\&=\{T^{-1}\boldsymbol{y} : \boldsymbol{y}\in\mathbb{Z}^n : q_m\mid D\boldsymbol{y}\}\end{aligned}$$

since S,T are unimodular. Therefore a basis for $\mathbb{Z}^n(m)$ is given by

$$T^{-1}\left(a_1\boldsymbol{e}_1,\dots,a_n\boldsymbol{e}_n\right),$$

where $(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)$ is the canonical basis of $\mathbb{Z}^n$. In particular

$$\det \mathbb{Z}^n(m) = \prod_{i=1}^{n} a_i$$

and the above least common multiple is the product of both arguments since v is a power of two and $\det \mathbb{Z}^n(m)$ is odd. On the other hand, $v \prod_{i=1}^{n} a_i \mathbb{Z}^n \subset \Lambda_b(m)$ so $\det \Lambda_b(m) \mid v \prod_{i=1}^{n} a_i$ and we are done. □

Since any point $\boldsymbol{x}$ on $\mathscr{V}$ is non-singular, we have $\nabla Q(\boldsymbol{x}) \neq 0$. Hence there exists $m \geq 2$ such that p_m is the smallest odd prime not dividing $\nabla Q(\boldsymbol{x})$. Then $\boldsymbol{x} \in \mathbb{Z}^n(m)$ and we can write

$$Z(Q, \boldsymbol{B}, \mathbb{Z}^n) = \bigcup_m Z(Q, \boldsymbol{B}, \mathbb{Z}^n(m), p_m).$$

Note that if $Z(Q, \boldsymbol{B}, \mathbb{Z}^n(m), p_m)$ is non empty then there exists a primitive vector $\boldsymbol{x}$ with $|\boldsymbol{x}| \leq B_n$ and $q_m \leq |\nabla Q(\boldsymbol{x})| \ll \|Q\| |\boldsymbol{x}| \ll B_n^{n(n+1)-1}$ by assumption. Hence we must have $m \ll \log(B_n)$.

Next consider

$$\begin{aligned} \phi : \mathbb{Z}^n &\to \mathbb{Z}^n \\ \boldsymbol{x} &\mapsto \left(\frac{V}{B_1} x_1, \dots, \frac{V}{B_n} x_n \right), \end{aligned}$$

which sends the box $\boldsymbol{B}$ to the hypercube of side length V centered at the origin. Then for any $\boldsymbol{x} \in \mathbb{Z}^n$ we have $Q(\boldsymbol{x}) = 0$ if and only if $Q(\phi^{-1}(\boldsymbol{y})) = 0$, where $\boldsymbol{y} = \phi(\boldsymbol{x})$. Therefore, the zeros of Q correspond under this linear transformation to those of the form $Q_\phi = V^2 Q \circ \phi^{-1}$, where the scaling factor V^2 is only there to ensure that the coefficients are integers. Of course, the image by ϕ of a primitive point needs not be primitive any more. However if $\boldsymbol{x}$ and $\boldsymbol{x}'$ are two distinct primitive points in the box $\boldsymbol{B}$ then $\phi(\boldsymbol{x})$ and $\phi(\boldsymbol{x}')$ define two distinct projective points of height at most V. Clearly, $\nabla Q_\phi(\boldsymbol{y}) = V^2 \phi^{-1}(\nabla Q(\boldsymbol{x}))$. Thus for any lattice Λ and any odd prime p, we have

$$\#S(Q, \boldsymbol{B}, \Lambda, p) \leq \#S(Q_\phi, V, \phi(\Lambda), p).$$

In view of what precedes, we have the following inequalities

$$\#Z(Q, \boldsymbol{B}, \mathbb{Z}^n) \leq \sum_m \#S(Q, \boldsymbol{B}, \mathbb{Z}^n(m), p_m)$$

and, in the notation of Lemma 3.2,

$$\#S(Q, \boldsymbol{B}, \mathbb{Z}^n(m), p_m) \leq \#S(Q_\phi, V, \Lambda_{\boldsymbol{b}}(m), p_m),$$

with $b_i = \frac{V}{B_i}$. For future use we note that for this choice of $\boldsymbol{b}$, Lemma 3.2 implies

$$\det \Lambda_{\boldsymbol{b}}(m) \geq V^{n-1} q_m. \tag{3.2}$$

For each m, two cases can occur. First, $\Lambda_{\boldsymbol{b}}(m)$ may have largest successive minimum strictly larger $c_{n,n}V$, where $c_{n,n}$ is the constant given by Lemma 2.1, which then implies that any point of height at most V contained in $\Lambda_{\boldsymbol{b}}(m)$ is actually contained in the $(n-1)$-dimensional sublattice of $\Lambda_{\boldsymbol{b}}(m)$ generated by the $n-1$ first vectors of a minimal basis. Otherwise Lemma 3.1 applies with $\Lambda = \Lambda_{\boldsymbol{b}}(m)$ and $\mathcal{B} = V$.

In the first case, taking the preimage by ϕ, each point in the box $\boldsymbol{B}$ contained in $\mathbb{Z}^n(m)$ is actually contained in some $(n-1)$-dimensional sublattice Λ of $\mathbb{Z}^n(m)$. It means that one of the coordinates can be expressed as a linear function of the other ones, say $x_1 = \ell(x_2, \dots, x_n)$. Furthermore, ℓ is defined over $\mathbb{Q}$. Therefore for some integer d, the form $Q_\ell = dQ(\ell(x_2, \dots, x_n), x_2, \dots, x_n)$ has integral coefficients. Then we have

$$\begin{aligned}\#S(Q, \boldsymbol{B}, \Lambda, p_m) &\leq \#S(Q, \boldsymbol{B}, \mathbb{Z}^n)\\ &\leq \#S(Q_\ell, \boldsymbol{B}', \mathbb{Z}^{n-1}).\end{aligned}$$

By the induction hypothesis, the number of points not contained in a line coming from $\mathbb{Z}^n(m)$ is in this case $\ll (B_2 \cdots B_n)^{\frac{n-3}{n-1}}$. Since $m \ll \log(B_n)$, the total contribution of this case is

$$\ll (B_2 \cdots B_n)^{\frac{n-3}{n-1}} \log(B_n) \ll (B_1 \cdots B_n)^{\frac{n-2}{n}}$$

since $B_1 \gg 1$ and $\log(B_n) \ll B_n^{\frac{2}{n(n-1)}}$.

Consider now the second case. Let $\Lambda_i \subset \Lambda_{\boldsymbol{b}}(m) \subset \mathbb{Z}^n(m)$ be any sublattice of dimension $n-1$ arising from Lemma 3.1 applied to Q_ϕ, with minimal basis $(\boldsymbol{t}_1, \dots, \boldsymbol{t}_{n-1})$ and successive minima $s_1, \dots, s_{n-1}$ say. Set

$$\begin{aligned}\psi : \mathbb{Z}^{n-1} &\to \Lambda_i\\ \boldsymbol{x} &\mapsto \sum_{j=1}^{n-1} x_j \boldsymbol{t}_j.\end{aligned}$$

By Lemma 2.1, we are left with counting primitive points $\boldsymbol{x}$ of $\mathbb{Z}^{n-1}$ with $|x_j| \leq \frac{V}{s_j}$, such that $Q_\phi(\psi(\boldsymbol{x})) = 0$, and not lying on any line. However, to apply the induction hypothesis, we must ensure that the sides of the box we consider are larger than 1. We know that the successive minima of Λ_i are all $\leq c p_m^n V$ for some constant c depending only on n. We shall rather count those points $\boldsymbol{x}$ in the larger box $|x_j| \leq \frac{V_0}{s_j}$, where $V_0 = c p_m^n V$. By the induction hypothesis, we find

$$\begin{aligned}&\ll \left(\frac{V_0}{s_1} \cdots \frac{V_0}{s_{n-1}}\right)^{(n-3)/(n-1)}\\ &\ll \left(\frac{V_0^{n-1}}{\det \Lambda_i}\right)^{(n-3)/(n-1)}\end{aligned}$$

such points for each sublattice Λ_i. By (3.1), for any $\alpha > 0$, the lattices Λ_i such that

$$\frac{\alpha}{2}\det\Lambda_{\boldsymbol{b}}(m) < \det\Lambda_i \le \alpha\det\Lambda_{\boldsymbol{b}}(m) \tag{3.3}$$

yield a total contribution of at most

$$p_m^{n-2}(\alpha V)^{\frac{n-2}{n}}\left(\frac{V_0^{n-1}}{\alpha\det\Lambda_{\boldsymbol{b}}(m)}\right)^{(n-3)/(n-1)}.$$

Since the successive minima of Λ_i are all $\le V_0$, we have

$$\det\Lambda_i \ll V_0^{n-1}.$$

Hence for each possible i, $\det\Lambda_i$ has to lay in one of the dyadic intervals (3.3) for some α in the range

$$\alpha \ll \frac{V_0^{n-1}}{\det\Lambda_{\boldsymbol{b}}(m)} \doteq X,$$

say. Summing for each m in the second case the contributions of these dyadic intervals, we get at most

$$p_m^{n-2}V^{\frac{n-2}{n}}X^{\frac{n-3}{n-1}}\sum_{\substack{2^k\ll X\\ k\in\mathbb{Z}}}2^{k\left(\frac{n-2}{n}-\frac{n-3}{n-1}\right)} \ll p_m^{n-2}V^{\frac{n-2}{n}}X^{\frac{n-2}{n}}.$$

By (3.2), we have

$$X \ll \frac{p_m^{n(n-1)}}{q_m},$$

thus the total contribution from each m in the second case is

$$\ll p_m^{n(n-2)}\left(\frac{V}{q_m}\right)^{\frac{n-2}{n}}.$$

But $p_m^a q_m^{-b} \ll (m\log m)^a 2^{-bm}$ for any $a, b > 0$ by the prime number theorem. Hence the series

$$\sum_m p_m^{n(n-2)}q_m^{-\frac{n-2}{n}} \tag{3.4}$$

converges. Adding up all these contributions, we therefore get $\ll V^{\frac{n-2}{n}}$ points, which finally establishes Theorem 1.2.

4. Proof of Theorem 1.1

We have to add to the estimate given by Theorem 1.2 the contribution of points lying on the various lines included in the surface $Q = 0$.

The argument involved for the case of four variables is quite similar to the last section of [2], with a slight modification due to the fact that we do not consider the same collection of hyperplanes, so we do not get the same number of lines. Consider the hyperplanes $\Lambda_i \otimes_{\mathbb{Z}} \mathbb{R}$ generated by the various sublattices Λ_i of dimension 3 that we used above. Recalling that we applied Lemma 3.1 for each m in the second case with $\mathcal{B} = V$ and $\Lambda = \Lambda_{\boldsymbol{b}}(m)$, we have at most

$$I \ll p_m^8 \left(\frac{V^4}{\det \Lambda_{\boldsymbol{b}(m)}} \right)^{\frac{1}{2}} \ll p_m^8 \left(\frac{V}{q_m} \right)^{\frac{1}{2}}$$

such hyperplanes. Hence using again the fact that the series (3.4) converges, the total number of hyperplanes is $O(V^{\frac{1}{2}}) = O(B^2)$. To this collection we further add the $O(\log(B))$ hyperplanes of the form $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ with Λ a sublattice of dimension 3 arising from those m in the first case. But the intersection of each plane with the surface $\mathscr{V}$ is either a conic or at most two lines. Further, since we proceed by summing up the contributions from all the above mentioned lattices, we do not need to consider every $\mathbb{Q}$-line included in $\mathscr{V}$, but only those arising as intersection with one of these lattices. Hence we have the contribution of at most $N \ll B^2$ lines to take into account. The integral points on each line L form a certain sublattice Λ_L of dimension 2. By Lemma 2.1, this lattice contributes $O(1 + \frac{B^2}{\det \Lambda_L})$. But L also corresponds to a point in the variety $F_1(Q) \subset \mathbb{G}(1,3)$ of lines included in $Q = 0$. This point has a height $H(L)$ given by the Euclidean norm of the corresponding point via the Plücker embedding, and in fact $H(L) = \det \Lambda_L$, which follows from the Cauchy–Binet formula. Order the lines $L_1, \dots, L_N$ by non-decreasing height. By [5, Exercise 6.7], $F_1(Q)$ is a smooth conic in $\mathbb{P}^5_{\mathbb{Q}}$. Hence by the work of Walsh [8], it has $O(H)$ points of height at most H with an absolute implied constant. Thus we get for all $n \le N$ that

$$n \le \#\{L_i : H(L_i) \le H(L_n)\} \ll H(L_n).$$

Therefore the total contribution from the $\mathbb{Q}$-lines is

$$\ll \sum_{n \le N} 1 + \frac{B^2}{H(L_n)} \ll N + B^2 \log(N) \ll B^2 \log(B),$$

which establishes Theorem 1.1.

References

[1] T. D. BROWNING & D. R. HEATH-BROWN, “Counting rational points on hypersurfaces”, *J. Reine Angew. Math.* **584** (2005), p. 83-115.

[2] ———, “Counting rational points on quadric surfaces”, *Discrete Anal.* **2018** (2018), article ID 15 (29 pages).

[3] J. W. S. CASSELS, *An introduction to the geometry of numbers*, Grundlehren der Mathematischen Wissenschaften, vol. 99, Springer, 1959.

[4] H. DAVENPORT, “Cubic forms in sixteen variables”, *Proc. R. Soc. Lond., Ser. A* **272** (1963), p. 285-303.

[5] J. HARRIS, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 133, Springer, 1992.

[6] D. R. HEATH-BROWN, “A new form of the circle method, and its application to quadratic forms”, *J. Reine Angew. Math.* **481** (1996), p. 149-206.

[7] ———, "The density of rational points on curves and surfaces", *Ann. Math.* **155** (2002), no. 2, p. 553-595.

[8] M. N. Walsh, "Bounded rational points on curves", *Int. Math. Res. Not.* **2015** (2015), no. 14, p. 5644-5658.

Félicien Comtat
France House
Queen Mary University of London
E14QA London, United Kingdom
E-mail: felicien.comtat@ens-cachan.fr
URL: https://www.qmul.ac.uk/maths/profiles/comtatf.html