ACTA ARITHMETICA
167.1 (2015)

Algebraic S-integers of fixed degree and bounded height

by

Fabrizio Barroero (Pisa)

1. Introduction. In this article we give asymptotic estimates for the cardinality of certain subsets of $\overline{\mathbb{Q}}^n$ of bounded height. By *height* we mean the multiplicative absolute Weil height H on the affine space $\overline{\mathbb{Q}}^n$, whose definition will be recalled in Section 2.

Let k be a number field of degree m over $\mathbb{Q}$ and let n and e be positive integers. We fix an algebraic closure $\overline{k}$ of k and set

$$k(n,e) = \{\boldsymbol{\alpha} \in \overline{k}^n : [k(\boldsymbol{\alpha}) : k] = e\},$$

where $k(\boldsymbol{\alpha})$ is the field obtained by adjoining all the coordinates of $\boldsymbol{\alpha}$ to k. By Northcott's Theorem [12], subsets of $k(n,e)$ of uniformly bounded height are finite. Therefore, for any subset A of $k(n,e)$ and $\mathcal{H} > 0$, we may introduce the following counting function:

$$N(A,\mathcal{H}) = |\{\boldsymbol{\alpha} \in A : H(\boldsymbol{\alpha}) \le \mathcal{H}\}|.$$

Various results about this counting function appear in the literature. One of the earliest is due to Schanuel [13], who gave an asymptotic formula for $N(k(n,1),\mathcal{H})$. Schmidt was the first to consider the case $e > 1$. In [14], he found upper and lower bounds for $N(k(n,e),\mathcal{H})$, while in [15], he gave asymptotics for $N(\mathbb{Q}(n,2),\mathcal{H})$. Shortly afterwards, Gao [8] found the asymptotics for $N(\mathbb{Q}(n,e),\mathcal{H})$, provided $n > e$. Later Masser and Vaaler [11] established an asymptotic estimate for $N(k(1,e),\mathcal{H})$. Finally, Widmer [16] proved an asymptotic formula for $N(k(n,e),\mathcal{H})$, provided $n > 5e/2 + 5 + 2/me$. However, for general n and e even the correct order of magnitude for $N(k(n,e),\mathcal{H})$ remains unknown.

In this article we are interested in counting algebraic S-integers. Let S be a finite set of places of k containing the archimedean ones. As usual, $\mathcal{O}_S$ denotes the ring of S-integers of k. Let $\bar{S}$ be the set of places of $\overline{k}$ that lie above the places in S and let $\mathcal{O}_{\bar{S}}$ be the ring of $\bar{S}$-integers of $\overline{k}$. Alternatively,

2010 *Mathematics Subject Classification*: Primary 11G50, 11R04.
Key words and phrases: heights, algebraic S-integers, counting.

DOI: 10.4064/aa167-1-4

we could think of $\mathcal{O}_{\bar{S}}$ as the ring of those algebraic numbers having minimal polynomial over k that is monic and has coefficients in $\mathcal{O}_S$.

Given n and e positive integers, we set

$$\mathcal{O}_S(n,e) = k(n,e) \cap \mathcal{O}_{\bar{S}}^n = \{\boldsymbol{\alpha} \in \mathcal{O}_{\bar{S}}^n : [k(\boldsymbol{\alpha}) : k] = e\}.$$

Let S_∞ be the set of archimedean places of k. If we choose $S = S_\infty$, then $\mathcal{O}_S = \mathcal{O}_k$ is the ring of algebraic integers of k and we use the notation $\mathcal{O}_k(n,e)$ with the obvious meaning. Besides the trivial cases $\mathcal{O}_{\mathbb{Q}}(n,1) = \mathbb{Z}^n$, the first asymptotic result can probably be found in Lang's book [9]. Lang states, without proof,

$$N(\mathcal{O}_k(1,1), \mathcal{H}) = \gamma_k \mathcal{H}^m (\log \mathcal{H})^q + O(\mathcal{H}^m (\log \mathcal{H})^{q-1}),$$

where $m = [k : \mathbb{Q}]$, q is the rank of the unit group of $\mathcal{O}_k$, and γ_k and the implicit constant in the error term are unspecified positive constants, depending on k. More recently, Widmer [17] established the asymptotic formula

$$N(\mathcal{O}_k(n,e), \mathcal{H}) = \sum_{i=0}^{t} D_i \mathcal{H}^{men} (\log \mathcal{H}^{men})^i + O_{m,e,n}(\mathcal{H}^{men-1} (\log \mathcal{H})^t), \tag{1.1}$$

provided $e = 1$ or $n > e + C_{e,m}$ for some explicit $C_{e,m} \leq 7$. Here $t = e(q+1) - 1$, and the constants $D_i = D_i(k,n,e)$ are explicitly given. Our Theorem 1.1 generalizes Widmer's result in the case $e = 1$ to asymptotics for $N(\mathcal{O}_S(n,1), \mathcal{H})$. However, we do not obtain a multiterm expansion as in (1.1).

Chern and Vaaler [6] proved an asymptotic formula for the number of monic polynomials in $\mathbb{Z}[X]$ of given degree and bounded Mahler measure. Theorem 6 of [6] immediately implies the following estimate:

$$N(\mathcal{O}_{\mathbb{Q}}(1,e), \mathcal{H}) = C_e \mathcal{H}^{e^2} + O_e(\mathcal{H}^{e^2-1})$$

for some explicit constant C_e. This was extended by the author in [1], where an asymptotic estimate is given for $N(\mathcal{O}_k(1,e), \mathcal{H})$. Theorem 1.2 below generalizes this result and gives an asymptotic estimate for $N(\mathcal{O}_S(1,e), \mathcal{H})$ for any finite set of places S containing the archimedean ones.

We write S_{fin} for the set of non-archimedean places of S. Suppose that $S_{\text{fin}} = \{v_1, \dots, v_L\}$ and that v_l corresponds to the prime ideal $\mathfrak{p}_l$ of $\mathcal{O}_k$. We denote by $\mathfrak{N}(\mathfrak{A})$ the norm from k to $\mathbb{Q}$ of the fractional ideal $\mathfrak{A}$ and by $\mathfrak{N}(S)$ the L-tuple $(\mathfrak{N}(\mathfrak{p}_1), \dots, \mathfrak{N}(\mathfrak{p}_L))$. Let r and s be, respectively, the number of real embeddings and pairs of conjugate complex embeddings of k. Moreover, we denote by Δ_k the discriminant of k. Let n be a positive integer. We set

$$B_{k,S}^{(n)} = \frac{n^{r+s-1} 2^{sn} m^{|S|-1}}{(|S|-1)! (\sqrt{|\Delta_k|})^n} \prod_{l=1}^{L} \left(\frac{1}{\log \mathfrak{N}(\mathfrak{p}_l)} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p}_l)^n} \right) \right) \tag{1.2}$$

and

$$C_{\mathbb{R},n} = 2^{n-M}\Big(\prod_{j=1}^{M}\Big(\frac{2j}{2j+1}\Big)^{n-2j}\Big)\frac{n^M}{M!}$$

with $M = \lfloor \frac{n-1}{2} \rfloor$ (as usual, $\lfloor x \rfloor$ is the integer part of $x \in \mathbb{R}$), and

$$C_{\mathbb{C},n} = \pi^n \frac{n^n}{(n!)^2}.$$

In this article, as usual, empty products are understood to be 1.

For non-negative real functions $f(X), g(X), h(X)$ and $X_0 \in \mathbb{R}$, we write $f(X) = g(X) + O(h(X))$ as $X \geq X_0$ tends to infinity if there is C_0 such that $|f(X) - g(X)| \leq C_0 h(X)$ for all $X \geq X_0$.

THEOREM 1.1. *Let n be a positive integer and let k be a number field of degree m over $\mathbb{Q}$. Moreover, let S be a finite set of places of k containing the archimedean ones. Then, as $\mathcal{H} \geq 2$ tends to infinity,*

$$N(\mathcal{O}_S(n,1),\mathcal{H}) = (2^r\pi^s)^n B_{k,S}^{(n)} \mathcal{H}^{mn} (\log \mathcal{H})^{|S|-1} + \begin{cases} O(\mathcal{H}^{mn}(\log \mathcal{H})^{|S|-2}) & \text{if } |S| > 1, \\ O(\mathcal{H}^{mn-1}) & \text{if } |S| = 1. \end{cases}$$

The implicit constant in the error term depends on m, n and $\mathfrak{N}(S)$.

THEOREM 1.2. *Let e be a positive integer and let k be a number field of degree m over $\mathbb{Q}$. Moreover, let S be a finite set of places of k containing the archimedean ones. Then, as $\mathcal{H} \geq 2$ tends to infinity,*

$$N(\mathcal{O}_S(1,e),\mathcal{H}) = e^{|S|} C_{\mathbb{R},e}^r C_{\mathbb{C},e}^s B_{k,S}^{(e)} \mathcal{H}^{me^2} (\log \mathcal{H})^{|S|-1} + \begin{cases} O(\mathcal{H}^{me^2}(\log \mathcal{H})^{|S|-2}) & \text{if } |S| > 1, \\ O(\mathcal{H}^{e(me-1)}\mathcal{L}) & \text{if } |S| = 1, \end{cases}$$

where $\mathcal{L} = \log \mathcal{H}$ if $(m,e) = (1,2)$ and $\mathcal{L} = 1$ otherwise. The implicit constant in the error term depends on m, e and $\mathfrak{N}(S)$.

As mentioned before, if $S = S_\infty$, then Theorem 1.1 reduces to (1.1), although with a larger error term, and Theorem 1.2 to the result in [1]. However, for the case $S_\infty \neq S$ our results appear to be new.

As in [1], our proof relies on work of the author and Widmer [2] about counting lattice points in definable sets in o-minimal structures. Our approach is similar to the one in [1], but in the case $S = S_\infty$ the result is more straightforward, because the embedding of $\mathcal{O}_k$ in $\mathbb{R}^m$ is a lattice. On the other hand, if $S \supsetneq S_\infty$, the embedding of $\mathcal{O}_S$ is dense in $\mathbb{R}^m$, and a more elaborate proof is needed.

Let us apply our theorems to a few simple examples. Fix a prime number p. One can see, as an easy exercise and as a special case of both theorems,

that the number of elements of $\mathbb{Z}[1/p]$ of height at most $\mathcal{H}$ is

$$\frac{2}{\log p}\left(1-\frac{1}{p}\right)\mathcal{H}\log\mathcal{H}+O_p(\mathcal{H}).$$

Now, let d be a square-free positive integer with $d \equiv 3 \bmod 4$. Consider $k=\mathbb{Q}(\sqrt{d})$ and set S to consist of the place corresponding to the prime ideal $(2, 1+\sqrt{d})$, in addition to the two archimedean places. Then

$$N(\mathcal{O}_S(n,1),\mathcal{H})=\frac{2n(2^n-1)}{d^{n/2}\log 2}\mathcal{H}^{2n}(\log\mathcal{H})^2+O_n(\mathcal{H}^{2n}\log\mathcal{H}).$$

Let again $k=\mathbb{Q}$ and suppose the non-archimedean places in S are associated to the primes 2 and 3. Then

$$N(\mathcal{O}_S(1,2),\mathcal{H})=\frac{32}{3\log 2\log 3}\mathcal{H}^4(\log\mathcal{H})^2+O(\mathcal{H}^4\log\mathcal{H}).$$

In [11], Masser and Vaaler observed that the limit as $\mathcal{H}\to\infty$ of

$$\frac{N(k(1,e),\mathcal{H}^{1/e})}{N(k(e,1),\mathcal{H})}$$

is a rational number. Moreover, they asked if this can be extended to some sort of reciprocity law, i.e., whether

$$\lim_{\mathcal{H}\to\infty}\frac{N(k(n,e),\mathcal{H}^{1/e})}{N(k(e,n),\mathcal{H}^{1/n})}\in\mathbb{Q}.$$

Analogously we notice that

$$\lim_{\mathcal{H}\to\infty}\frac{N(\mathcal{O}_S(1,e),\mathcal{H}^{1/e})}{N(\mathcal{O}_S(e,1),\mathcal{H})}=e\left(\frac{C_{\mathbb{R},e}}{2^e}\right)^r\left(\frac{C_{\mathbb{C},e}}{\pi^e}\right)^s$$

is a rational number depending only on e, r and s, as already pointed out in [1] for the case $S=S_\infty$. As Masser and Vaaler did, one can ask again whether

$$\lim_{\mathcal{H}\to\infty}\frac{N(\mathcal{O}_S(n,e),\mathcal{H}^{1/e})}{N(\mathcal{O}_S(e,n),\mathcal{H}^{1/n})}\in\mathbb{Q}.$$

2. Preliminaries. Let k be a number field of degree m over $\mathbb{Q}$ and let M_k be the set of places of k. For $v\in M_k$, we indicate by k_v the completion of k with respect to v. We write $\mathbb{Q}_v$ for the completion of $\mathbb{Q}$ with respect to the unique place of $\mathbb{Q}$ that lies below v. Moreover, we set $d_v=[k_v:\mathbb{Q}_v]$ to be the local degree of k at v.

Any $v\in M_k$ corresponds either to a non-zero prime ideal $\mathfrak{p}_v$ of $\mathcal{O}_k$ or to an embedding of k into $\mathbb{C}$. In the first case v is called a *finite* or *non-archimedean place* and we write $v\nmid\infty$. In the second case v is called an *infinite* or *archimedean place* and we write $v\mid\infty$. We set, for $v\nmid\infty$,

$$|\alpha|_v=\mathfrak{N}(\mathfrak{p}_v)^{-\mathrm{ord}_{\mathfrak{p}_v}(\alpha)/d_v}$$

for every $\alpha \in k \setminus \{0\}$, where $\mathrm{ord}_{\mathfrak{p}_v}(\alpha)$ is the power of $\mathfrak{p}_v$ in the factorization of the principal fractional ideal $\alpha\mathcal{O}_k$. Furthermore, $|0|_v = 0$. If $v \mid \infty$ corresponds to $\sigma_v : k \hookrightarrow \mathbb{C}$, we set

$$|\alpha|_v = |\sigma_v(\alpha)|$$

for every $\alpha \in k$, where $|\cdot|$ is the usual absolute value on $\mathbb{C}$. The *absolute multiplicative Weil height* $H : k^n \to [1, \infty)$ is defined by

$$H(\alpha_1, \dots, \alpha_n) = \prod_{v \in M_k} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{d_v/m}. \tag{2.1}$$

Note that for $\alpha \in k \setminus \{0\}$, $|\alpha|_v \neq 1$ for finitely many v. Therefore, the above product contains only finitely many terms different from 1. Moreover, this definition is independent of the field containing the coordinates, and therefore the height is defined on $\overline{\mathbb{Q}}^n$. For properties of the Weil height we refer to the first chapter of [4].

We conclude this section by introducing semialgebraic sets and stating the Tarski–Seidenberg principle.

Definition 2.1. Let N and M_i, for $i = 1, \dots, N$, be positive integers. A *semialgebraic subset* of $\mathbb{R}^n$ is a set of the form

$$\bigcup_{i=1}^{N} \bigcap_{j=1}^{M_i} \{\boldsymbol{x} \in \mathbb{R}^n : f_{i,j}(\boldsymbol{x}) *_{i,j} 0\},$$

where $f_{i,j} \in \mathbb{R}[X_1, \dots, X_n]$ and the $*_{i,j}$ are either $<$ or $=$.

Let $A \subseteq \mathbb{R}^n$ be a semialgebraic set. A function $f : A \to \mathbb{R}^{n'}$ is called *semialgebraic* if its graph $\Gamma(f)$ is a semialgebraic set of $\mathbb{R}^{n+n'}$.

If we identify $\mathbb{C}$ with $\mathbb{R}^2$, then the definitions of semialgebraic set and function are extended to subsets of $\mathbb{C}^n$ and to functions of complex variables in a natural way. We will need the following theorem, which is usually known as the Tarski–Seidenberg principle.

Theorem 2.2 ([3, Theorem 1.5]). *Let $A \in \mathbb{R}^{n+1}$ be a semialgebraic set. Then $\pi(A) \in \mathbb{R}^n$ is semialgebraic, where $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$ is the projection map on the first n coordinates.*

3. A generalization. In this section we formulate a theorem which will be used later to derive Theorems 1.1 and 1.2.

In the following definition we consider functions whose domain is $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$. We use the notation $\boldsymbol{z}$ to indicate a vector with entries in a generic field, while $\boldsymbol{x}$ will be a vector with real coordinates. We are often going to identify a function $f : \mathbb{C}^n \to \mathbb{R}$ with $f : \mathbb{R}^{2n} \to \mathbb{R}$ where if $\boldsymbol{x} = (x_1, \dots, x_{2n}) \in \mathbb{R}^{2n}$, $f(\boldsymbol{x}) = f(x_1 + ix_2, \dots, x_{2n-1} + ix_{2n})$.

Definition 3.1. Let n be a positive integer. A *semialgebraic distance function* (of dimension n) is a continuous function N from $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$ to the interval $[0,\infty)$ satisfying the following conditions:

(i) $N(\boldsymbol{z}) = 0$ if and only if $\boldsymbol{z}$ is the zero vector;
(ii) $N(w\boldsymbol{z}) = |w|N(\boldsymbol{z})$ for any scalar w in $\mathbb{R}$ or in $\mathbb{C}$;
(iii) N is a semialgebraic function.

Let r and s be non-negative integers, not both zero. A system $\mathcal{N}$ of r real and s complex semialgebraic distance functions (of dimension n) is called an (r,s)-*system* (of dimension n).

Let us fix a number field k with $[k:\mathbb{Q}] = m$. Let r and s be, respectively, the number of real and pairs of conjugate complex embeddings of k. These induce $r+s$ archimedean places of k, with respective completions $\mathbb{R}$ or $\mathbb{C}$. Given an (r,s)-system $\mathcal{N}$ of dimension n, we can associate to every archimedean place v a semialgebraic distance function N_v on k_v^{n+1}. We will mostly use the alternative notation $N_1,\dots,N_r$ for the r real distance functions and $N_{r+1},\dots,N_{r+s}$ for the s complex ones, and we set $d_i = 1$ for $i = 1,\dots,r$, and $d_i = 2$ for $i = r+1,\dots,r+s$. For the non-archimedean places we set

$$N_v(\boldsymbol{z}) = \max\{|z_0|_v,\dots,|z_n|_v\}$$

for $\boldsymbol{z} = (z_0,\dots,z_n) \in k_v^{n+1}$. Now we can define, for $\boldsymbol{\alpha} \in k^{n+1}$, a height function associated to $\mathcal{N}$,

$$H_{\mathcal{N}}(\boldsymbol{\alpha})^m = \prod_{v\in M_k} N_v(\sigma_v(\boldsymbol{\alpha}))^{d_v},$$

where σ_v is the embedding of k into k_v corresponding to v, extended componentwise to k^{n+1}.

Now, let $\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})$ be the set of $\boldsymbol{a} \in \mathcal{O}_S^n$ with $H_{\mathcal{N}}(1,\boldsymbol{a}) \le \mathcal{H}$. We are interested in obtaining an estimate for $|\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})|$ as $\mathcal{H}\to\infty$.

Let us introduce some notation and impose some conditions on the functions N_i in view of the application of this estimate. For $i = 1,\dots,r+s$, we set $\widetilde{N}_i(\boldsymbol{z}) = N_i(1,\boldsymbol{z})$ and suppose that

$$\widetilde{N}_i(\boldsymbol{z}) \ge 1 \tag{3.1}$$

for every $\boldsymbol{z} \in \mathbb{R}^n$ or $\mathbb{C}^n$. We define the sets

$$Z_i(T) = \{\boldsymbol{z} : \widetilde{N}_i(\boldsymbol{z}) \le T\}, \tag{3.2}$$

and suppose that

$$\text{the } Z_i(T) \text{ have volume } p_i(T) \text{ for every } T \ge 1, \tag{3.3}$$

where $p_i(X) \in \mathbb{R}[X]$ is a polynomial of degree $d_i n$ and leading coefficient C_i.

Moreover, let

$$C_{\mathcal{N},k,S} = \frac{n^{r+s-1}2^{sn}m^{|S|-1}}{(|S|-1)!(\sqrt{|\Delta_k|})^n}\Big(\prod_{i=1}^{r+s} C_i\Big)\prod_{l=1}^{L}\Big(\frac{1}{\log \mathfrak{N}(\mathfrak{p}_l)}\Big(1-\frac{1}{\mathfrak{N}(\mathfrak{p}_l)^n}\Big)\Big). \tag{3.4}$$

THEOREM 3.2. *Let $\mathcal{N}$ be an (r,s)-system of dimension n, satisfying the above hypotheses* (3.1) *and* (3.3). *Moreover, suppose S is a finite set of places of k containing the archimedean ones. Then, for every $\mathcal{H}_0 > 1$, there exists a positive $C_0 = C_0(\mathcal{N}, \mathfrak{N}(S), \mathcal{H}_0)$ such that for every $\mathcal{H} \geq \mathcal{H}_0$,*

$$\big||\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})| - C_{\mathcal{N},k,S}\mathcal{H}^{mn}(\log \mathcal{H})^{|S|-1}\big| \leq \begin{cases} C_0\mathcal{H}^{mn}(\log \mathcal{H})^{|S|-2} & \text{if } |S| > 1, \\ C_0\mathcal{H}^{mn-1} & \text{if } |S| = 1. \end{cases}$$

4. Proofs of Theorems 1.1 and 1.2. In this section we apply Theorem 3.2 to prove Theorems 1.1 and 1.2. Let us start with the first one. We choose our system $\mathcal{N}$ to consist of the max norm

$$N_v(\boldsymbol{z}) = |\boldsymbol{z}|_\infty = \max\{|z_0|, \dots, |z_n|\},$$

for every archimedean place v of k. These N_v clearly satisfy the definition of semialgebraic distance function. The sets $Z_i(T)$ defined in (3.2) have volume $(2T)^n$ for $i = 1, \dots, r$ and $\pi^n T^{2n}$ for $i = r+1, \dots, r+s$, for every $T \geq 1$. Therefore, the hypotheses of Theorem 3.2 are satisfied.

Note that, for every $\boldsymbol{a} \in k^n$,

$$H_{\mathcal{N}}(1, \boldsymbol{a}) = \prod_v N_v(1, \sigma_v(\boldsymbol{a}))^{d_v/m} = \prod_v \max\{1, |a_1|_v, \dots, |a_n|_v\}^{d_v/m} = H(\boldsymbol{a}).$$

Therefore $H_{\mathcal{N}}$ is the usual absolute Weil height defined in (2.1). The claim of Theorem 1.1 follows by applying Theorem 3.2 with $\mathcal{H}_0 = 2$.

Now let us prove Theorem 1.2. We choose $\mathcal{N}$ to consist of the Mahler measure function

$$N_i(z_0, \dots, z_n) = M(z_0X^n + z_1X^{n-1} + \cdots + z_n) =: M(z_0, \dots, z_n)$$

for every $i = 1, \dots, r+s$. Let us recall its definition. If $f = z_0X^d + z_1X^{d-1} + \cdots + z_d$ is a non-zero polynomial of degree d with complex coefficients and roots $\alpha_1, \dots, \alpha_d$, the *Mahler measure* of f is defined to be

$$M(f) = |z_0| \prod_{h=1}^{d} \max\{1, |\alpha_h|\}. \tag{4.1}$$

Moreover, we set $M(0) = 0$.

In what follows we are going to consider the Mahler measure as a function of the coefficients of a polynomial:

$$M : \mathbb{R}^{d+1} \text{ or } \mathbb{C}^{d+1} \to [0, \infty), \quad (z_0, \dots, z_d) \mapsto M(z_0X^d + z_1X^{d-1} + \cdots + z_d).$$

Mahler [10, Lemma 1] proved that such an M is continuous and it is easy to see that it satisfies conditions (i) and (ii) of Definition 3.1. We now prove that it is a semialgebraic function.

LEMMA 4.1. *The Mahler measure M, as a function of the coefficients of a polynomial, is a semialgebraic function.*

Proof. We start by proving the claim for the complex Mahler measure. We need to show that, for every positive integer n, the function

$$\begin{aligned} M_n : \mathbb{R}^{2(n+1)} &\to [0,\infty), \\ (x_0,\dots,x_{2n+1}) &\mapsto M((x_0+ix_1)X^n+\cdots+(x_{2n}+ix_{2n+1})), \end{aligned}$$

is semialgebraic, i.e., its graph

$$\Gamma(M_n)=\{(x_0,\dots,x_{2n+1},t)\in\mathbb{R}^{2(n+1)+1} : M(x_0,\dots,x_{2n+1})=t\}$$

is a semialgebraic set.

We prove this by induction on n. For $n=1$,

$$\Gamma(M_1)=\left\{(x_0,x_1,x_2,x_3,t)\in\mathbb{R}^5 : \max\{x_0^2+x_1^2,x_2^2+x_3^2\}=t^2,\ t\geq 0\right\}$$

is clearly semialgebraic. Now suppose $n>1$. Let $\Gamma(M_n)=A\cup B$, where

$$\begin{aligned} A&=\{(x_0,\dots,x_{2n+1},t)\in\Gamma(M_n) : x_0^2+x_1^2\neq 0\}, \\ B&=\{(x_0,\dots,x_{2n+1},t)\in\Gamma(M_n) : x_0=x_1=0\}. \end{aligned}$$

By the inductive hypothesis, B is a semialgebraic set since $B=\{(0,0)\}\times\Gamma(M_{n-1})$. Now let A' be the set of points

$$(x_0,\dots,x_{2n+1},t,\alpha_1,\beta_1,\dots,\alpha_n,\beta_n)\in\mathbb{R}^{2(n+1)+1+2n}$$

such that $x_0^2+x_1^2\neq 0$, $\alpha_h+i\beta_h$ for $h=1,\dots,n$ are the roots of $(x_0+ix_1)X^n+\cdots+(x_{2n}+ix_{2n+1})$, and

$$|x_0+ix_1|\prod_{h=1}^{n}\max\{1,|\alpha_h+i\beta_h|\}=t. \tag{4.2}$$

This set A' is defined by the symmetric functions that link the coefficients of a polynomial with its roots and by (4.2). It is therefore semialgebraic. Since A is the projection of A' on the first $2(n+1)+1$ coordinates, it is also semialgebraic by the Tarski–Seidenberg principle (Theorem 2.2). We have the claim for the complex Mahler measure.

For the real one it is sufficient to note that its graph is nothing but the projection that forgets the coordinates $x_1,x_3,\dots,x_{2n-1},x_{2n+1}$ of

$$\Gamma(M_n)\cap\{(x_0,\dots,x_{2n+1},t) : x_{2j+1}=0 \text{ for } j=0,\dots,n\}. \ \blacksquare$$

Since M satisfies the three conditions of Definition 3.1, it is a semialgebraic distance function. Moreover, in [6], Chern and Vaaler calculated the volume of the sets of the form (3.2) for the real and the complex monic

Mahler measure. By (1.16) and (1.17) of [6], for every $T \geq 1$ the volumes of the sets

$$\{(z_1, \dots, z_n) \in \mathbb{R}^n : M(1, z_1, \dots, z_n) \leq T\},$$
$$\{(z_1, \dots, z_n) \in \mathbb{C}^n : M(1, z_1, \dots, z_n) \leq T\}$$

are, respectively, polynomials $p_{\mathbb{R}}(T)$ and $p_{\mathbb{C}}(T)$ of degree n and $2n$ and leading coefficients

$$C_{\mathbb{R},n} = 2^{n-M} \Bigg(\prod_{j=1}^{M} \Big(\frac{2j}{2j+1} \Big)^{n-2j} \Bigg) \frac{n^M}{M!} \ ([1]),$$

with $M = \lfloor \frac{n-1}{2} \rfloor$, and

$$C_{\mathbb{C},n} = \pi^n \frac{n^n}{(n!)^2}.$$

We have just shown that $\mathcal{N}$ satisfies the hypothesis of Theorem 3.2, therefore for every $\mathcal{H}_0 > 1$ there exists a positive $C_0 = C_0(m, n, \mathfrak{N}(S), \mathcal{H}_0)$, such that for every $\mathcal{H} \geq \mathcal{H}_0$,

$$\big| |\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})| - C_{\mathbb{R},n}^r C_{\mathbb{C},n}^s B_{k,S}^{(n)} \mathcal{H}^{mn} (\log \mathcal{H})^{|S|-1} \big| \leq \begin{cases} C_0 \mathcal{H}^{mn} (\log \mathcal{H})^{|S|-2} & \text{if } |S| > 1, \\ C_0 \mathcal{H}^{mn-1} & \text{if } |S| = 1, \end{cases} \tag{4.3}$$

where $B_{k,S}^{(n)}$ is the constant defined in (1.2).

Let us reformulate these considerations in terms of polynomials. We proceed in a similar way to [1, Section 2]. For any positive integer n we fix the system $\mathcal{N}_n$ of dimension n to consist of Mahler measure distance functions and we define

$$M^k : k[X] \to [0, \infty), \qquad a_0 X^n + a_1 X^{n-1} + \cdots + a_n \mapsto H_{\mathcal{N}_n}(a_0, a_1, \dots, a_n).$$

Therefore we can write

$$M^k(a_0, \dots, a_n) = \Big(\prod_{i=1}^{r+s} M\big(\sigma_i(a_0) X^n + \cdots + \sigma_i(a_n)\big)^{d_i/m} \Big) \prod_{v \nmid \infty} \max\{|a_0|_v, \dots, |a_n|_v\}^{d_v/m}.$$

Let $\mathcal{M}_{k,S}(n, \mathcal{H})$ be the set of monic polynomials $f \in \mathcal{O}_S[X]$ of degree n with $M^k(f) \leq \mathcal{H}$. Clearly $|\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})| = |\mathcal{M}_{k,S}(n, \mathcal{H})|$ and (4.3) is an estimate for such cardinality. Fixing m, n, $|S|$ and an $|S|$-tuple of prime powers, and letting k vary among all number fields of degree m and S among the sets of places of the chosen number field with the prescribed set of norms of the non-archimedean places, the constants $C_{\mathbb{R},n}^r$, $C_{\mathbb{C},n}^s$ and $B_{k,S}^{(n)}$ are bounded and therefore there exists a constant $G_{m,\mathfrak{N}(S)}^{(n)}$, depending on n, m and $\mathfrak{N}(S)$, such

([1]) There is a misprint in (1.16) of [6]: 2^{-N} should read 2^{-M}.

that

$$|\mathcal{M}_{k,S}(n,\mathcal{H})| \le G^{(n)}_{m,\mathfrak{N}(S)}\mathcal{H}^{mn}(\log\mathcal{H}+1)^{|S|-1} \tag{4.4}$$

for every $\mathcal{H} \ge 1$.

Note that, for every $\alpha \in k$,

$$M^k(X-\alpha) = \prod_{v\in M_k} \max\{1,|\alpha|_v\}^{d_v/m} = H(\alpha). \tag{4.5}$$

It is clear from the definition of Mahler measure (4.1) that

$$M(fg) = M(f)M(g),$$

and therefore, by [4, Lemma 1.6.3], one can see that

$$M^k(fg) = M^k(f)M^k(g)$$

for every $f, g \in k[X]$.

Now we want to restrict to monic f irreducible over k. Let $\widetilde{\mathcal{M}}_{k,S}(n,\mathcal{H})$ be the set of monic irreducible polynomials $f \in \mathcal{O}_S[X]$ of degree n with $M^k(f) \le \mathcal{H}$, i.e., the polynomials in $\mathcal{M}_{k,S}(n,\mathcal{H})$ that are irreducible over k.

COROLLARY 4.2. *For every $\mathcal{H}_0 > 1$ there exists a positive D_0, depending on n, m, $\mathfrak{N}(S)$ and $\mathcal{H}_0$, such that for every $\mathcal{H} \ge \mathcal{H}_0$ we have*

$$\big||\widetilde{\mathcal{M}}_{k,S}(n,\mathcal{H})| - C^r_{\mathbb{R},n}C^s_{\mathbb{C},n}B^{(n)}_{k,S}\mathcal{H}^{mn}(\log\mathcal{H})^{|S|-1}\big| \le \begin{cases} D_0\mathcal{H}^{mn}(\log\mathcal{H})^{|S|-2} & \text{if } |S|>1,\\ D_0\mathcal{H}^{mn-1}\mathcal{L} & \text{if } |S|=1,\end{cases}$$

where $\mathcal{L} = \log\mathcal{H}$ if $(m,n) = (1,2)$ and $\mathcal{L} = 1$ otherwise.

Proof. For $n = 1$, there is nothing to prove. Suppose $n > 1$. We show that, up to a constant, the number of all monic reducible $f \in \mathcal{O}_S[X]$ of degree n with $M^k(f) \le \mathcal{H}$ is not larger than the right hand side of (4.3), except for the case $|S| = 1$ and $(m,n) = (1,2)$.

Consider all $f = gh \in \mathcal{M}_{k,S}(n,\mathcal{H})$ with $g, h \in \mathcal{O}_S[X]$ monic of degree a and b respectively, with $0 < a \le b < n$ and $a + b = n$. We have $1 \le M^k(g), M^k(h) \le \mathcal{H}$ because g and h are monic. Thus, there exists a positive integer d such that $2^{d-1} \le M^k(g) < 2^d$. Note that d must satisfy

$$1 \le d \le \frac{\log\mathcal{H}}{\log 2} + 1 \le 2\log\mathcal{H} + 1. \tag{4.6}$$

Since M^k is multiplicative,

$$M^k(h) = \frac{M^k(f)}{M^k(g)} \le 2^{1-d}\mathcal{H}.$$

Using (4.4) and noting that $2^d \le 2\mathcal{H}$, we can see that there are at most

$$G^{(a)}_{m,\mathfrak{N}(S)}(2^d)^{ma}(\log 2^d+1)^{|S|-1} \le G^{(a)}_{m,\mathfrak{N}(S)}(2^d)^{ma}(\log\mathcal{H}+2)^{|S|-1}$$

possibilities for g and

$$G^{(b)}_{m,\mathfrak{N}(S)}(2^{1-d}\mathcal{H})^{mb}(\log(2^{1-d}\mathcal{H})+1)^{|S|-1} \le G^{(b)}_{m,\mathfrak{N}(S)}(2^{1-d}\mathcal{H})^{mb}(\log\mathcal{H}+2)^{|S|-1}$$

possibilities for h. Therefore, we have at most

$$H^{(n)}_{m,\mathfrak{N}(S)}\mathcal{H}^{mb}2^{md(a-b)}(\log\mathcal{H}+2)^{2(|S|-1)} \tag{4.7}$$

possibilities for gh with $M^k(gh) \le \mathcal{H}$ and $2^{d-1} \le M^k(g) < 2^d$, where $H^{(n)}_{m,\mathfrak{N}(S)}$ is a real constant depending on n, m and $\mathfrak{N}(S)$.

If $a = b = n/2$, then (4.7) is

$$H^{(n)}_{m,\mathfrak{N}(S)}\mathcal{H}^{mn/2}(\log\mathcal{H}+2)^{2(|S|-1)}.$$

Summing over all d, $1 \le d \le \lfloor 2\log\mathcal{H}\rfloor+1$ (recall (4.6)), gives an extra factor $2\log\mathcal{H}+1$. Therefore, when $a = b$, there are at most

$$H^{(n)}_{m,\mathfrak{N}(S)}\mathcal{H}^{mn/2}(2\log\mathcal{H}+2)^{2|S|-1}$$

possibilities for $f = gh$, with $M^k(f) \le \mathcal{H}$. If $|S| > 1$ or $(m,n) \ne (1,2)$, this has smaller order than the right hand side of (4.3), since $mn > 2$ implies $mn/2 < mn-1$. In the case $|S| = 1$ and $(m,n) = (1,2)$, we get $H^{(n)}_{m,\mathfrak{N}(S)}\mathcal{H}(2\log\mathcal{H}+2)$ and we need an additional logarithm factor.

For $a < b$, summing $2^{md(a-b)}$ over all d, $1 \le d \le \lfloor 2\log\mathcal{H}\rfloor+1 =: D$, we get

$$\sum_{d=1}^{D}(2^{m(a-b)})^d \le \sum_{d=1}^{D}2^{-d} \le 1.$$

Thus, recalling $b \le n-1$, if $a < b$ there are at most

$$H^{(n)}_{m,\mathfrak{N}(S)}\mathcal{H}^{m(n-1)}(\log\mathcal{H}+2)^{2(|S|-1)}$$

possibilities for $f = gh$ with $M^k(f) \le \mathcal{H}$. This is again not larger than the right hand side of (4.3). ∎

The last step of the proof links such irreducible polynomials with their roots, and M^k with the height of these roots. Recall that $\bar{S}$ is the set of places of $\overline{k}$ that lie above the places in S.

LEMMA 4.3. *An algebraic number $\beta \in \mathcal{O}_{\bar{S}}$ has degree e over k and $H(\beta) \le \mathcal{H}$ if and only if it is a root of a monic irreducible polynomial $f \in \mathcal{O}_S[X]$ of degree e with $M^k(f) \le \mathcal{H}^e$.*

Proof. If an algebraic number $\beta \in \mathcal{O}_{\bar{S}}$ has degree e over k, then it is clearly a root of a monic irreducible polynomial $f \in \mathcal{O}_S[X]$ of degree e, and vice versa. We claim that

$$H(\beta)^e = M^k(f).$$

The function M^k is independent of the choice of k since it is possible to define an absolute $M^{\bar{\mathbb{Q}}}$ over $\overline{\mathbb{Q}}[X]$ that, restricted to any $k[X]$, coincides with M^k. To see this one can simply imitate the proof of the fact that the Weil height is independent of the field containing the coordinates (see [4, Lemma 1.5.2]).

Suppose $f = (X-\alpha_1)\cdots(X-\alpha_e)$. By (4.5) we have

$$M^{\mathbb{Q}(\alpha_i)}(X-\alpha_i) = H(\alpha_i),$$

and the α_i have the same height because they are conjugate (see [4, Proposition 1.5.17]). Finally, by the multiplicativity of M^k we can see that

$$M^k(f) = M^{\bar{\mathbb{Q}}}(f) = \prod_{i=1}^{e} M^{\bar{\mathbb{Q}}}(X-\alpha_i) = H(\alpha_j)^e$$

for any α_j root of f. ∎

This implies that $|N(\mathcal{O}_S(1,e),\mathcal{H})| = e|\widetilde{\mathcal{M}}_{k,S}(e,\mathcal{H}^e)|$ because there are e different $\beta \in \mathcal{O}_{\bar{S}}$ with the same minimal polynomial over k. For every $\mathcal{H}_0 > 1$, there exists a positive $E_0 = E_0(m,e,\mathfrak{N}(S),\mathcal{H}_0)$ such that, for every $\mathcal{H} \geq \mathcal{H}_0$,

$$\begin{aligned}\left|N(\mathcal{O}_S(1,e),\mathcal{H}) - e^{|S|}C^r_{\mathbb{R},e}C^s_{\mathbb{C},e}B^{(e)}_{k,S}\mathcal{H}^{me^2}(\log\mathcal{H})^{|S|-1}\right| \\ \leq \begin{cases} E_0\mathcal{H}^{me^2}(\log\mathcal{H})^{|S|-2} & \text{if } |S|>1, \\ E_0\mathcal{H}^{e(me-1)}\mathcal{L} & \text{if } |S|=1, \end{cases}\end{aligned}$$

where $\mathcal{L} = \log\mathcal{H}$ if $(m,e) = (1,2)$ and $\mathcal{L} = 1$ otherwise. We obtain Theorem 1.2 by choosing $\mathcal{H}_0 = 2$.

5. Counting lattice points. We start this section by introducing the counting theorem that will be used to prove Theorem 3.2. The principle goes back to Davenport [7] and was developed by several authors. In a previous work [2], the author and Widmer formulated a counting theorem that relies on Davenport's Theorem and uses o-minimal structures. We do not need Theorem 1.3 of [2] in its full generality as we count lattice points in semialgebraic sets.

For a semialgebraic set $Z \subseteq \mathbb{R}^{n+n'}$, we call $Z_{\boldsymbol{t}} = \{\boldsymbol{x} \in \mathbb{R}^n : (\boldsymbol{x},\boldsymbol{t}) \in Z\}$ the *fiber* of Z lying above $\boldsymbol{t} \in \mathbb{R}^{n'}$ and Z a *semialgebraic family*. It is clear that the fibers $Z_{\boldsymbol{t}}$ are semialgebraic subsets of $\mathbb{R}^n$. Let Λ be a lattice of $\mathbb{R}^n$ with determinant $\det\Lambda$ and let $\lambda_i = \lambda_i(\Lambda)$, for $i = 1,\dots,n$, be the successive minima of Λ with respect to the unit ball $B_0(1)$, i.e.,

$$\lambda_i = \inf\{\lambda : B_0(\lambda) \cap \Lambda \text{ contains } i \text{ linearly independent vectors}\}.$$

The following theorem is a special case of [2, Theorem 1.3].

THEOREM 5.1. *Let $Z \subset \mathbb{R}^{n+n'}$ be a semialgebraic family and suppose the fibers $Z_{\boldsymbol{t}}$ are bounded. Then there exists a constant $c_Z \in \mathbb{R}$, depending*

only on the family, such that

$$\left||Z_{\boldsymbol{t}} \cap \Lambda| - \frac{\mathrm{Vol}(Z_{\boldsymbol{t}})}{\det \Lambda}\right| \le \sum_{j=0}^{n-1} c_Z \frac{V_j(Z_{\boldsymbol{t}})}{\lambda_1 \cdots \lambda_j},$$

where $V_j(Z_{\boldsymbol{t}})$ for $j > 0$ is the sum of the j-dimensional volumes of the orthogonal projections of $Z_{\boldsymbol{t}}$ on every j-dimensional coordinate subspace of $\mathbb{R}^n$, and $V_0(Z_{\boldsymbol{t}}) = 1$.

Let us introduce the family we want to apply Theorem 5.1 to. We fix an (r,s)-system $\mathcal{N}$ of dimension n consisting of r real and s complex semialgebraic distance functions. Recall that we have defined $\widetilde{N}_i(\boldsymbol{z}) = N_i(1,\boldsymbol{z})$. Moreover, we see the complex $\widetilde{N}_i$ as functions from $\mathbb{R}^{2n}$, i.e.,

$$\widetilde{N}_i(x_1, x_2, \dots, x_{2n-1}, x_{2n}) = \widetilde{N}_i(z_1, \dots, z_n)$$

for $(x_1, x_2, \dots, x_{2n-1}, x_{2n}) = (\Re(z_1), \Im(z_1), \dots, \Re(z_n), \Im(z_n))$.

Recall that $d_i = 1$ for $i = 1, \dots, r$, and $d_i = 2$ for $i = r+1, \dots, r+s$, and $m = r + 2s$. Let

$$Z = \Big\{(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{r+s}, t) \in \mathbb{R}^{n(r+2s)+1} : \prod_{i=1}^{r+s} \widetilde{N}_i(\boldsymbol{x}_i)^{d_i} \le t\Big\}, \tag{5.1}$$

where $\boldsymbol{x}_i \in \mathbb{R}^{d_i n}$.

We need to show that Z is a semialgebraic family and that the fibers Z_t are bounded for every $t \in \mathbb{R}$.

Lemma 5.2. *The set Z defined in* (5.1) *is semialgebraic.*

Proof. First note that, since the N_i are semialgebraic functions, also the $\widetilde{N}_i$ are semialgebraic. Indeed, one can get $\Gamma(\widetilde{N}_i)$ by intersecting $\Gamma(N_i)$ with an appropriate affine subspace. Define

$$S^{(i)} = \{(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{r+s}, t, t_1, \dots, t_{r+s}) \in \mathbb{R}^{mn} \times \mathbb{R}^{1+r+s} : \widetilde{N}_i(\boldsymbol{x}_i) = t_i\}$$

for $i = 1, \dots, r+s$, and

$$A = \Big\{(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{r+s}, t, t_1, \dots, t_{r+s}) \in \mathbb{R}^{mn} \times \mathbb{R}^{1+r+s} : \prod_{i=1}^{r+s} t_i^{d_i} \le t\Big\}.$$

All these sets are clearly semialgebraic. Let π be the projection map of $\mathbb{R}^{mn+1+r+s}$ to the first $mn+1$ coordinates. By the Tarski–Seidenberg principle (Theorem 2.2) the set

$$B = \pi\Big(\bigcap_i S^{(i)} \cap A\Big)$$

is semialgebraic. A point $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{r+s}, t)$ belongs to B if and only if there are $t_1, \dots, t_{r+s}$ such that $\widetilde{N}_i(\boldsymbol{x}_i) = t_i$ for every i and $\prod_{i=1}^{r+s} t_i^{d_i} \le t$, i.e., $\prod_{i=1}^{r+s} \widetilde{N}_i(\boldsymbol{x}_i)^{d_i} \le t$. Therefore $B = Z$, and we have proved the claim. ∎

Since the N_i are bounded distance functions, there exist positive real constants δ_i such that

$$\delta_i|\boldsymbol{z}|_\infty \le N_i(\boldsymbol{z})$$

for every $\boldsymbol{z}$ in $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$ (see [5, Lemma 2, p. 108)]. We define $\gamma_i = \max\{\delta_i : \delta_i|\boldsymbol{z}|_\infty \le N_i(\boldsymbol{z})\}$ and $N_i'(\boldsymbol{z}) = \gamma_i|\boldsymbol{z}|_\infty$. As before, we use the notation $\widetilde{N}_i'(\boldsymbol{z})$ for $N_i'(1,\boldsymbol{z})$.

Let $\mathcal{N}'$ be the (r,s)-system consisting of $N_i'(\boldsymbol{z}) = \gamma_i|\boldsymbol{z}|_\infty$ for every $i = 1,\dots,r+s$. Each $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_{r+s},t)$ such that $\prod_{i=1}^{r+s}\widetilde{N}_i(\boldsymbol{x}_i)^{d_i} \le t$ satisfies $\prod_{i=1}^{r+s}\widetilde{N}_i'(\boldsymbol{x}_i)^{d_i} \le t$. Therefore, if

$$Z' = \Big\{(\boldsymbol{x}_1,\dots,\boldsymbol{x}_{r+s},t) \in \mathbb{R}^{mn+1} : \prod_{i=1}^{r+s}\widetilde{N}_i'(\boldsymbol{x}_i)^{d_i} \le t\Big\},$$

then $Z \subseteq Z'$. For every $\boldsymbol{x} \in \mathbb{R}^{d_i n}$ we have, by definition, $\widetilde{N}_i'(\boldsymbol{x}) \ge \gamma_i$ and therefore, for every $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_{r+s}) \in Z_t'$,

$$\widetilde{N}_i'(\boldsymbol{x}_i)^{d_i} \le \frac{t}{\prod_{j\ne i}\gamma_j^{d_j}}.$$

This implies

$$|\boldsymbol{x}_i|_\infty^{d_i} \le \frac{t}{\prod_j \gamma_j^{d_j}}$$

for every $i = 1,\dots,r+s$. We have just shown that the fibers Z_t', and therefore Z_t, are bounded.

From now on we use the notation $Z(T)$ for Z_T. Recall that $V_j(Z(T))$ is the sum of the j-dimensional volumes of the orthogonal projections of $Z(T)$ on every j-dimensional coordinate subspace of $\mathbb{R}^n$ and $V_0(Z(T)) = 1$.

Since $Z \subseteq Z'$, we have $V_j(Z(T)) \le V_j(Z'(T))$. By Theorem 5.1 there exists a constant c_Z, depending only on Z, such that

$$\Big||Z(T)\cap\Lambda| - \frac{\mathrm{Vol}(Z(T))}{\det\Lambda}\Big| \le \sum_{j=0}^{mn-1} c_Z\frac{V_j(Z'(T))}{\lambda_1\cdots\lambda_j} \tag{5.2}$$

for every $T \in \mathbb{R}$.

We have to calculate $\mathrm{Vol}(Z(T))$ and we need upper bounds for $V_j(Z'(T))$.

Recall we have supposed that, for every $i = 1,\dots,r+s$, $\widetilde{N}_i(\boldsymbol{x}) \ge 1$ and the volume of the set $Z_i(T)$ defined in (3.2) is $p_i(T)$ for every $T \ge 1$, where p_i is a polynomial of degree $d_i n$ and leading coefficient C_i.

Lemma 5.3. *Let $q = r+s-1$. Under the hypotheses above we have, for every $T \ge 1$,*

$$\mathrm{Vol}(Z(T)) = Q(T^{1/2},\log T),$$

where $Q(X,Y) \in \mathbb{R}[X,Y]$, $\deg_X Q = 2n$, $\deg_Y Q = q$ *and the coefficient of* $X^{2n}Y^q$ *is* $(n^q/q!)\prod_{i=1}^{q+1} C_i$.

Proof. This is a special case of [1, Lemma 5.2]. ∎

The $V_j(Z'(T))$ were already computed in [1].

LEMMA 5.4. *For each* $j = 1, \dots, mn-1$, *there exists a polynomial* $P_j(X,Y)$ *in* $\mathbb{R}[X,Y]$, *with* $\deg_X P_j \le 2n$, $\deg_Y P_j \le q$ *and the coefficient of* $X^{2n}Y^q$ *being* 0, *such that, for every* $T \ge 1$, *we have*

$$V_j(Z'(T)) = P_j(T^{1/2}, \log T).$$

Proof. See [1, Lemma 5.4]. ∎

For an integer u, we will use the notation

$$X^{(u)} = \begin{cases} X^u & \text{for } u > 0, \\ 1 & \text{for } u \le 0, \end{cases}$$

in order to avoid possible appearances of 0^0, for instance in the following proposition, where we must consider $(\log T)^q$ for $T \ge 1$ and q can be 0.

Moreover, for Λ a lattice, we define

$$\mathfrak{D}(\Lambda) = \frac{1}{\det \Lambda} + \sum_{j=0}^{mn-1} \frac{1}{\lambda_1 \cdots \lambda_j}.$$

PROPOSITION 5.5. *Let* $\mathcal{N}$ *be an* (r,s)*-system of dimension* n *that satisfies the above hypotheses on the volumes of the sets* $Z_i(T)$ *and let* Λ *be a lattice. There exist two positive real constants* E *and* E', *depending only on* $\mathcal{N}$, *such that, for every* $T \ge 1$,

$$\left| |Z(T) \cap \Lambda| - \frac{n^q \prod_{i=1}^{q+1} C_i}{q! \det \Lambda} T^n (\log T)^{(q)} \right| \le \begin{cases} \mathfrak{D}(\Lambda)(ET^n(\log T)^{(q-1)} + E') & \text{if } q \ge 1, \\ \mathfrak{D}(\Lambda) E T^{n-1/m} & \text{if } q = 0. \end{cases}$$

Moreover, if $T < 1$, *then* $Z(T) = \emptyset$.

Proof. For $T < 1$, $Z(T) = \emptyset$ since we have supposed $\widetilde{N}_i(\boldsymbol{x}) \ge 1$ for every $\boldsymbol{x}$. Suppose $T \ge 1$.

We start with the case $q = 0$. In this case, our system $\mathcal{N}$ consists only of one function N_1 that can be either real ($d_1 = m = 1$) or complex ($d_1 = m = 2$). In any case, the volume of the set $Z(T) \subseteq \mathbb{R}^{mn}$ equals $p_1(T^{1/m})$ for every $T \ge 1$, where p_1 has degree mn and leading coefficient C_1.

Fix a j, $1 \le j \le mn-1$. Any projection of $Z'(T)$ to a j-dimensional coordinate subspace has volume at most $F_j T^{j/m}$ for some positive real con-

stant F_j. Therefore, there exists an E'' such that

$$V_j(Z'(T)) \le E'' T^{n-1/m}$$

for every $T \ge 1$, and by (5.2) we have the claim if $q = 0$.

Suppose $q > 0$. By (5.2) and Lemmas 5.3 and 5.4, we have the following inequality, for every $T \ge 1$:

$$\left| |Z(T) \cap \Lambda| - \frac{n^q \prod_{i=1}^{q+1} C_i}{q! \det \Lambda} T^n (\log T)^{(q)} \right| \le \mathfrak{D}(\Lambda) P(T^{1/2}, \log T)$$

for some polynomial $P(X, Y) \in \mathbb{R}[X, Y]$ with $\deg_X P \le 2n$, $\deg_Y P \le q$, whose coefficients depend on $\mathcal{N}$ and the coefficient of $X^{2n} Y^q$ is 0. Since P satisfies such conditions, there exists a positive E such that

$$P(T^{1/2}, \log T) \le E T^n (\log T)^{(q-1)}$$

for every $T \ge 3$. For $T \in [1, 3]$, the function of T given by $P(T^{1/2}, \log T)$ is bounded, say by E'. Then

$$P(T^{1/2}, \log T) \le E T^n (\log T)^{(q-1)} + E'$$

for every $T \ge 1$. Clearly, E and E' depend only on the coefficients of P and therefore only on $\mathcal{N}$. ∎

6. Proof of Theorem 3.2. Recall that we have fixed a number field k of degree m over $\mathbb{Q}$. Let $\sigma_1, \dots, \sigma_r$ be the real embeddings of k and $\sigma_{r+1}, \dots, \sigma_{r+2s}$ be the complex ones, indexed in such a way that $\sigma_i = \overline{\sigma_{i+s}}$ for every $i = r+1, \dots, r+s$. For $\boldsymbol{a} = (a_1, \dots, a_n) \in k^n$, we set $\sigma_i(\boldsymbol{a}) = (\sigma_i(a_1), \dots, \sigma_i(a_n)) \in \mathbb{R}^n$ for $i = 1, \dots, r$, and $\sigma_i(\boldsymbol{a}) = (\Re(\sigma_i(a_1)), \Im(\sigma_i(a_1)), \dots, \Re(\sigma_i(a_n)), \Im(\sigma_i(a_n))) \in \mathbb{R}^{2n}$ for $i = r+1, \dots, r+s$.

Let $\mathfrak{A}$ be a non-zero fractional ideal of k. The image of $\mathfrak{A}$ via the embedding $\sigma : a \hookrightarrow (\sigma_1(a), \dots, \sigma_{r+s}(a))$ is a lattice in $\mathbb{R}^m$. If we set $\Lambda_{\mathfrak{A}} = \tau(\mathfrak{A}^n)$, where $\tau(\boldsymbol{a}) = (\sigma_1(\boldsymbol{a}), \dots, \sigma_{r+s}(\boldsymbol{a}))$ for $\boldsymbol{a} \in k^n$, then $\Lambda_{\mathfrak{A}}$ is a lattice in $\mathbb{R}^{mn}$. Recall that $\mathfrak{N}(\mathfrak{A})$ denotes the norm of $\mathfrak{A}$ and Δ_k the discriminant of k.

LEMMA 6.1. *We have*

$$\det \Lambda_{\mathfrak{A}} = (2^{-s} \mathfrak{N}(\mathfrak{A}) \sqrt{|\Delta_k|})^n,$$

and the first successive minimum of $\Lambda_{\mathfrak{A}}$ with respect to the Euclidean distance is $\lambda_1 \ge \mathfrak{N}(\mathfrak{A})^{1/m}$.

Proof. In [11] this lemma is stated for integral ideals [11, Lemma 5]. The same arguments work also for non-zero fractional ideals. ∎

To prove Theorem 3.2 we need an estimate for the cardinality of $\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})$, i.e., the set of points $\boldsymbol{a} \in \mathcal{O}_S^n$ such that $H_{\mathcal{N}}(1, \boldsymbol{a}) \le \mathcal{H}$.

Recall that we set $d_i = 1$ for $i = 1, \dots, r$, and $d_i = 2$ for $i = r+1, \dots, r+s$. As in Section 1, S_{fin} is the set of non-archimedean places in S.

First suppose $S_{\mathrm{fin}} = \emptyset$; then $\mathcal{O}_S = \mathcal{O}_k$ and $|S| = q+1 = r+s$. Note that, if $\boldsymbol{a}$ is a vector with integer coordinates, its non-archimedean absolute values are smaller than or equal to 1. Then

$$H_{\mathcal{N}}(1,\boldsymbol{a}) = \prod_{v\in M_k} N_v(1,\sigma_v(\boldsymbol{a}))^{d_v/m} = \prod_{i=1}^{r+s} \widetilde{N}_i(\sigma_i(\boldsymbol{a}))^{d_i/m}$$

for every $\boldsymbol{a}\in\mathcal{O}_k^n$. Therefore, the number of $\boldsymbol{a}\in\mathcal{O}_k^n$ such that $H_{\mathcal{N}}(1,\boldsymbol{a})\le\mathcal{H}$ is the number of lattice points of $\Lambda_{\mathcal{O}_k} = \tau(\mathcal{O}_k^n)$ in $Z(\mathcal{H}^m)$. By Lemma 6.1, $\det\Lambda_{\mathcal{O}_k} = (2^{-s}\sqrt{|\Delta_k|})^n$ and $\lambda_1\ge 1$. Thus, $\mathfrak{D}(\Lambda_{\mathcal{O}_k})\le mn+2^{sn}$. Moreover, for every $\mathcal{H}_0>1$ there exists a $C_0 = C_0(\mathcal{N},\mathcal{H}_0)$ such that, if $q\ge 1$,

$$(mn+2^{sn})(E\mathcal{H}^{mn}(\log\mathcal{H}^m)^{(q-1)} + E') \le C_0\mathcal{H}^{mn}(\log\mathcal{H})^{(q-1)}$$

for every $\mathcal{H}\ge\mathcal{H}_0$ and, in case $q=0$, $(mn+2^{sn})E\le C_0$. The claim of Theorem 3.2 follows by applying Proposition 5.5.

From now on, to avoid confusion between Cartesian powers and powers of an ideal with respect to ideal multiplication, we denote the latter by $\mathfrak{A}^{\star(d)}$ for a non-zero fractional ideal $\mathfrak{A}$ and an integer d.

Now, suppose $S_{\mathrm{fin}} = \{v_1,\dots,v_L\}$, with $L>0$. In this case we cannot apply Proposition 5.5 to $\tau(\mathcal{O}_S^n)$ directly because it is dense in $\mathbb{R}^{mn}$.

Recall that v_l corresponds to the prime ideal $\mathfrak{p}_l$ of $\mathcal{O}_k$. Let $\mathcal{I}_S$ be the set of non-zero integral ideals $\mathfrak{A}$ in $\mathcal{O}_k$ which are products of the prime ideals we fixed, i.e., $\mathfrak{A} = \mathfrak{p}_1^{\star(g_1)}\dots\mathfrak{p}_L^{\star(g_L)}$ for some non-negative integers $g_1,\dots,g_L$. An $\boldsymbol{a}\in k^n$ is in $\mathcal{O}_S^n$ if and only if there exists an ideal $\mathfrak{A}\in\mathcal{I}_S$ such that $a_u\in\mathfrak{A}^{\star(-1)}$ for every $u=1,\dots,n$, i.e., $\tau(\boldsymbol{a}) = (\sigma_1(\boldsymbol{a}),\dots,\sigma_{r+s}(\boldsymbol{a}))\in\Lambda_{\mathfrak{A}^{\star(-1)}}$, which is a lattice in $\mathbb{R}^{mn}$. We will therefore apply Proposition 5.5 to lattices of this form and then combine the estimates obtained.

We set

$$V_{k,\mathcal{N}} = \frac{n^q 2^{sn}}{q!(\sqrt{|\Delta_k|})^n}\prod_{i=1}^{q+1} C_i.$$

For a non-zero integral ideal $\mathfrak{A}$ and $T>0$, let $Z(\mathfrak{A},T)$ denote the set of $\boldsymbol{a}\in k^n$ such that $\tau(\boldsymbol{a})\in\Lambda_{\mathfrak{A}^{\star(-1)}}\cap Z(T^m)$.

LEMMA 6.2. *There exist positive constants F and F', depending only on $\mathcal{N}$, such that, for $T\ge 1$ and every non-zero integral ideal $\mathfrak{A}$, we have*

$$\big||Z(\mathfrak{A},T)| - V_{k,\mathcal{N}}\mathfrak{N}(\mathfrak{A})^n T^{mn}(\log T^m)^{(q)}\big| \le \begin{cases} \mathfrak{N}(\mathfrak{A})^n(FT^{mn}(\log T^m)^{(q-1)} + F') & \text{if } q\ge 1,\\ \mathfrak{N}(\mathfrak{A})^n F T^{mn-1} & \text{if } q=0.\end{cases}$$

Moreover, if $T<1$, then $Z(\mathfrak{A},T)=\emptyset$.

Proof. Note that, by Lemma 6.1, the first successive minimum of $\Lambda_{\mathfrak{A}^{\star(-1)}}$ is greater than or equal to $\mathfrak{N}(\mathfrak{A})^{-1/m}$. Since $\mathfrak{N}(\mathfrak{A})$ is a positive integer, we have

$$\prod_{i=1}^{j} \lambda_i \geq \mathfrak{N}(\mathfrak{A})^{-j/m} \geq \mathfrak{N}(\mathfrak{A})^{-(mn-1)/m} = \mathfrak{N}(\mathfrak{A})^{-n+1/m} \geq \mathfrak{N}(\mathfrak{A})^{-n}$$

for every $j = 1, \dots, mn-1$. Moreover, $|\Delta_k| \geq 1$. The claim follows from Proposition 5.5 and Lemma 6.1, after noting that

$$\mathfrak{D}(\Lambda_{\mathfrak{A}^{\star(-1)}}) \leq mn\mathfrak{N}(\mathfrak{A})^n + \frac{2^{sn}\mathfrak{N}(\mathfrak{A})^n}{(\sqrt{|\Delta_k|})^n} \leq \mathfrak{N}(\mathfrak{A})^n(mn + 2^{sn}). \ \blacksquare$$

We fix a $T \geq 1$. For a non-zero integral ideal $\mathfrak{A}$, let $Z^*(\mathfrak{A}, T)$ be the subset of $Z(\mathfrak{A}, T)$ consisting of the points $\boldsymbol{a}$ such that, for every $\mathfrak{B}$ strictly dividing $\mathfrak{A}$, there is a $u \in \{1, \dots, n\}$ such that $a_u \notin \mathfrak{B}^{\star(-1)}$. In other words, $\boldsymbol{a}$ corresponds to a lattice point of $\Lambda_{\mathfrak{A}^{\star(-1)}}$ that is not contained in any sublattice of the form $\Lambda_{\mathfrak{B}^{\star(-1)}}$ where $\mathfrak{B}$ is a strict divisor of $\mathfrak{A}$. We have

$$|Z(\mathfrak{A}, T)| = \sum_{\mathfrak{B}|\mathfrak{A}} |Z^*(\mathfrak{B}, T)|.$$

If μ_k is the Möbius function for the non-zero ideals of $\mathcal{O}_k$, the Möbius inversion formula implies that

$$|Z^*(\mathfrak{A}, T)| = \sum_{\mathfrak{B}|\mathfrak{A}} \mu_k(\mathfrak{B}) |Z(\mathfrak{A}\mathfrak{B}^{\star(-1)}, T)|.$$

Lemma 6.2 gives us an estimate for $|Z^*(\mathfrak{A}, T)|$, for every $T \geq 1$:

$$\begin{aligned} (6.1) \qquad & \Big| |Z^*(\mathfrak{A}, T)| - V_{k,\mathcal{N}} \sum_{\mathfrak{B}|\mathfrak{A}} \mu_k(\mathfrak{B}) \mathfrak{N}(\mathfrak{A}\mathfrak{B}^{\star(-1)})^n T^{mn} (\log T^m)^{(q)} \Big| \\ & \leq \begin{cases} \sum_{\mathfrak{B}|\mathfrak{A}} |\mu_k(\mathfrak{B})| \mathfrak{N}(\mathfrak{A}\mathfrak{B}^{\star(-1)})^n (F T^{mn} (\log T^m)^{(q-1)} + F') & \text{if } q \geq 1, \\ F \sum_{\mathfrak{B}|\mathfrak{A}} |\mu_k(\mathfrak{B})| \mathfrak{N}(\mathfrak{A}\mathfrak{B}^{\star(-1)})^n T^{mn-1} & \text{if } q = 0, \end{cases} \end{aligned}$$

and $Z^*(\mathfrak{A}, T) = \emptyset$ if $T < 1$.

Recall that $\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})$ is the set of points $\boldsymbol{a} \in \mathcal{O}_S^n$ with $H_{\mathcal{N}}(1, \boldsymbol{a}) \leq \mathcal{H}$.

LEMMA 6.3. *For every $\mathcal{H} \geq 1$ we have*

$$(6.2) \qquad |\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})| = \sum_{\substack{\mathfrak{A} \in \mathcal{I}_S, \\ \mathfrak{N}(\mathfrak{A})^{-1} \mathcal{H}^m \geq 1}} |Z^*(\mathfrak{A}, \mathfrak{N}(\mathfrak{A})^{-1/m} \mathcal{H})|.$$

Proof. Let $\mathfrak{A} = \mathfrak{p}_1^{\star(g_1)} \dots \mathfrak{p}_L^{\star(g_L)}$ and recall $d_{v_l} = [k_{v_l} : \mathbb{Q}_{v_l}]$ is the local degree of k at v_l. Every point $\boldsymbol{a} \in Z^*(\mathfrak{A}, T)$ is such that $\max_{u\in\{1,\dots,n\}} |a_u|_{v_l}^{d_{v_l}} = \mathfrak{N}(\mathfrak{p}_l)^{g_l}$ for every $l = 1, \dots, L$, and $\max_{u\in\{1,\dots,n\}} |a_u|_v \le 1$ for all $v \notin S$. This means that every $\boldsymbol{a} \in Z^*(\mathfrak{A}, T)$ satisfies

$$\prod_{v\nmid\infty} \max_u \{1, |a_u|_v\}^{d_v} = \mathfrak{N}(\mathfrak{A}),$$

and thus

$$H_{\mathcal{N}}(1, \boldsymbol{a}) = \mathfrak{N}(\mathfrak{A})^{1/m} \prod_{i=1}^{r+s} \widetilde{N}_i(\sigma_i(\boldsymbol{a}))^{d_i/m} \le \mathfrak{N}(\mathfrak{A})^{1/m} T.$$

Therefore, $\boldsymbol{a} \in \mathcal{O}_S^{\mathcal{N}}(\mathcal{H})$ if and only if there exists an $\mathfrak{A} \in \mathcal{I}_S$ such that $\boldsymbol{a} \in Z^*(\mathfrak{A}, \mathfrak{N}(\mathfrak{A})^{-1/m}\mathcal{H})$. Since such an $\mathfrak{A}$ is unique and recalling that, if $T < 1$, then $Z^*(\mathfrak{A}, T)$ is empty, we obtain the claim. ∎

Let $\mathcal{I}_S(T)$ be the set of ideals in $\mathcal{I}_S$ with norm not exceeding T and recall that the norm is multiplicative. Combining (6.2) with (6.1), we see that

$$\left| |\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})| - V_{k,\mathcal{N}} \sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)} \sum_{\mathfrak{B}|\mathfrak{A}} \frac{\mu_k(\mathfrak{B})}{\mathfrak{N}(\mathfrak{B})^n} \mathcal{H}^{mn} \left(\log\left(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{A})} \right) \right)^{(q)} \right|$$

is smaller than or equal to

$$\sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)} \sum_{\mathfrak{B}|\mathfrak{A}} \frac{|\mu_k(\mathfrak{B})|}{\mathfrak{N}(\mathfrak{B})^n} \left(F\mathcal{H}^{mn} \left(\log\left(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{A})} \right) \right)^{(q-1)} + F'\mathfrak{N}(\mathfrak{A})^n \right)$$

if $q \ge 1$, and

$$F \sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)} \sum_{\mathfrak{B}|\mathfrak{A}} \frac{|\mu_k(\mathfrak{B})|}{\mathfrak{N}(\mathfrak{B})^n} \mathfrak{N}(\mathfrak{A})^{1/m} \mathcal{H}^{mn-1}$$

if $q = 0$, for every $\mathcal{H} \ge 1$.

Now, let

$$\Psi^{(1)}(\mathfrak{A}) = \sum_{\mathfrak{B}|\mathfrak{A}} \frac{\mu_k(\mathfrak{B})}{\mathfrak{N}(\mathfrak{B})^n} \quad \text{and} \quad \Psi^{(2)}(\mathfrak{A}) = \sum_{\mathfrak{B}|\mathfrak{A}} \frac{|\mu_k(\mathfrak{B})|}{\mathfrak{N}(\mathfrak{B})^n}.$$

Then

$$\left| |\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})| - V_{k,\mathcal{N}} \mathcal{H}^{mn} \sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)} \Psi^{(1)}(\mathfrak{A}) \left(\log\left(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{A})} \right) \right)^{(q)} \right| \tag{6.3}$$

$$\le \begin{cases} \displaystyle\sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)} \Psi^{(2)}(\mathfrak{A}) \left(F\mathcal{H}^{mn} \left(\log\left(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{A})} \right) \right)^{(q-1)} + F'\mathfrak{N}(\mathfrak{A})^n \right) & \text{if } q \ge 1, \\ F\mathcal{H}^{mn-1} \sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)} \Psi^{(2)}(\mathfrak{A}) \mathfrak{N}(\mathfrak{A})^{1/m} & \text{if } q = 0. \end{cases}$$

Let K be a non-negative integer. We set

$$\mathcal{L}_S^{(h)}(\mathcal{H},K)=\sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)}\Psi^{(h)}(\mathfrak{A})\left(\log\left(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{A})}\right)\right)^{(K)}$$

for $h=1,2$. Recall that we have defined $\mathfrak{N}(S)=(\mathfrak{N}(\mathfrak{p}_1),\dots,\mathfrak{N}(\mathfrak{p}_L))$, and let

$$F_l^{(h)}=\frac{\Psi^{(h)}(\mathfrak{p}_l)}{\log\mathfrak{N}(\mathfrak{p}_l)}.$$

In the next lemma we allow S_{fin} to be empty as the base step of induction.

LEMMA 6.4. *For every non-negative integer K, there exists a positive constant $U_{K,\mathfrak{N}(S)}$, depending only on K and $\mathfrak{N}(S)$, such that for $h=1,2$ and for every $\mathcal{H}\geq 1$,*

$$\left|\mathcal{L}_S^{(h)}(\mathcal{H},K)-\Big(\prod_{l=1}^{L}F_l^{(h)}\Big)\Big(\prod_{i=K+1}^{K+L}\frac{1}{i}\Big)(\log\mathcal{H}^m)^{(K+L)}\right|\leq U_{K,\mathfrak{N}(S)}(\log\mathcal{H}^m+1)^{(K+L-1)}.$$

Proof. We proceed by induction on the cardinality of S_{fin}. Clearly, we can define $\mathcal{L}_{S'}^{(h)}(\mathcal{H},K)$ and $\mathcal{I}_{S'}$ for $S'=S\setminus\{v_L\}$.

If S_{fin} is empty, i.e. $L=0$, then $\mathcal{I}_S(\mathcal{H}^m)=\{\mathcal{O}_k\}$ and $\mathcal{L}_S^{(h)}(\mathcal{H},K)=(\log\mathcal{H}^m)^{(K)}$ for every $\mathcal{H}\geq 1$.

Now suppose S_{fin} has cardinality $L>0$. The sum over all $\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)$ can be viewed as consisting of two sums: the first over all $\mathfrak{B}\in\mathcal{I}_{S'}(\mathcal{H}^m)$, and the second over all non-negative integers g_L with $\mathfrak{N}(\mathfrak{p}_L^{\star(g_L)})\leq\mathcal{H}^m\mathfrak{N}(\mathfrak{B})^{-1}$. For typographical convenience we set

$$A(\mathfrak{B})=\left\lfloor\frac{\log(\mathcal{H}^m\mathfrak{N}(\mathfrak{B})^{-1})}{\log\mathfrak{N}(\mathfrak{p}_L)}\right\rfloor\quad\text{and}\quad R=\mathcal{I}_{S'}(\mathcal{H}^m).$$

We have

$$\begin{aligned}\mathcal{L}_S^{(h)}(\mathcal{H},K)&=\sum_{\mathfrak{B}\in R}\sum_{g_L=0}^{A(\mathfrak{B})}\Psi^{(h)}(\mathfrak{B}\mathfrak{p}_L^{\star(g_L)})\left(\log\left(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{B})}\right)-g_L\log\mathfrak{N}(\mathfrak{p}_L)\right)^{(K)}\\&=\sum_{\mathfrak{B}\in R}\sum_{g_L=1}^{A(\mathfrak{B})}\Bigg[\Psi^{(h)}(\mathfrak{B}\mathfrak{p}_L^{\star(g_L)})\\&\quad\times\sum_{i=0}^{K}(-1)^i\binom{K}{i}(\log\mathfrak{N}(\mathfrak{p}_L))^i g_L^i\left(\log\left(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{B})}\right)\right)^{(K-i)}\Bigg]+\mathcal{L}_{S'}^{(h)}(\mathcal{H},K).\end{aligned}$$

Using the definitions of $\Psi^{(h)}$, it is easy to see that $1/2\leq\Psi^{(h)}(\mathfrak{p}_l)\leq 3/2$ for

every l and, if $g_L \geq 1$,

$$\Psi^{(h)}(\mathfrak{B}\mathfrak{p}_L^{\star(g_L)}) = \Psi^{(h)}(\mathfrak{B}\mathfrak{p}_L) = \Psi^{(h)}(\mathfrak{B})\Psi^{(h)}(\mathfrak{p}_L) > 0. \tag{6.4}$$

Therefore,

$$\mathcal{L}_S^{(h)}(\mathcal{H}, K) = \Psi^{(h)}(\mathfrak{p}_L) \sum_{i=0}^{K} \Bigg[(-1)^i \binom{K}{i} (\log \mathfrak{N}(\mathfrak{p}_L))^i \times \sum_{\mathfrak{B}\in R} \Psi^{(h)}(\mathfrak{B}) \bigg(\log\bigg(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{B})} \bigg) \bigg)^{(K-i)} \sum_{g_L=1}^{A(\mathfrak{B})} g_L^i \Bigg] + \mathcal{L}_{S'}^{(h)}(\mathcal{H}, K). \tag{6.5}$$

By Faulhaber's formula, for every $i = 0, \ldots, K$, we have

$$\sum_{g_L=1}^{A(\mathfrak{B})} g_L^i - \frac{1}{i+1} \bigg\lfloor \frac{\log(\mathcal{H}^m \mathfrak{N}(\mathfrak{B})^{-1})}{\log \mathfrak{N}(\mathfrak{p}_L)} \bigg\rfloor^{i+1} = Q_i \bigg(\bigg\lfloor \frac{\log(\mathcal{H}^m \mathfrak{N}(\mathfrak{B})^{-1})}{\log \mathfrak{N}(\mathfrak{p}_L)} \bigg\rfloor \bigg),$$

where Q_i is a polynomial of degree i (except $Q_0 = 0$) whose coefficients depend only on i. Then

$$\bigg| \sum_{g_L=1}^{A(\mathfrak{B})} g_L^i - \frac{1}{i+1} \bigg(\frac{\log(\mathcal{H}^m \mathfrak{N}(\mathfrak{B})^{-1})}{\log \mathfrak{N}(\mathfrak{p}_L)} \bigg)^{i+1} \bigg| \leq Q_i' \bigg(\log\bigg(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{B})} \bigg) \bigg),$$

where Q_i' is a polynomial of degree at most i whose coefficients depend on i and $\mathfrak{N}(\mathfrak{p}_L)$. Finally, after noting that

$$\sum_{i=0}^{K} (-1)^i \binom{K}{i} \frac{1}{i+1} = \frac{1}{K+1},$$

by (6.5), we can derive the following inequality:

$$\bigg| \mathcal{L}_S^{(h)}(\mathcal{H}, K) - \frac{F_L^{(h)}}{K+1} \sum_{\mathfrak{B}\in R} \Psi^{(h)}(\mathfrak{B}) \bigg(\log\bigg(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{B})} \bigg) \bigg)^{(K+1)} \bigg| \leq \mathcal{L}_{S'}^{(h)}(\mathcal{H}, K) + \sum_{\mathfrak{B}\in R} \Psi^{(h)}(\mathfrak{B}) Q \bigg(\log\bigg(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{B})} \bigg) \bigg),$$

where Q is a polynomial of degree at most K whose coefficients depend only on K and $\mathfrak{N}(\mathfrak{p}_L)$. Therefore, we have

$$\bigg| \mathcal{L}_S^{(h)}(\mathcal{H}, K) - \frac{F_L^{(h)}}{K+1} \mathcal{L}_{S'}^{(h)}(\mathcal{H}, K+1) \bigg| \leq \sum_{i=0}^{K} b_i \mathcal{L}_{S'}^{(h)}(\mathcal{H}, i),$$

where the b_i are real coefficients again depending on K and $\mathfrak{N}(\mathfrak{p}_L)$. Now, by the inductive hypothesis, there exist $U_{K+1,\mathfrak{N}(S')}$ and $U'_{i,\mathfrak{N}(S')}$ for $i = 0, \ldots, K$,

such that

$$\left|\mathcal{L}^{(h)}_{S'}(\mathcal{H},K+1)-\Big(\prod_{l=1}^{L-1}F_l^{(h)}\Big)\Big(\prod_{i=K+2}^{K+L}\frac{1}{i}\Big)(\log\mathcal{H}^m)^{(K+L)}\right| \le U_{K+1,\mathfrak{N}(S')}(\log\mathcal{H}^m+1)^{(K+L-1)}$$

and

$$\mathcal{L}^{(h)}_{S'}(\mathcal{H},i)\le U'_{i,\mathfrak{N}(S')}(\log\mathcal{H}^m+1)^{(i+L-1)}$$

for every $i=0,\dots,K$. The claim follows easily. ∎

LEMMA 6.5. *There exists a real constant $V_{m,\mathfrak{N}(S)}$, depending only on m and $\mathfrak{N}(S)$, such that*

$$\sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)}\Psi^{(2)}(\mathfrak{A})\mathfrak{N}(\mathfrak{A})^{1/m}\le V_{m,\mathfrak{N}(S)}\mathcal{H}(\log\mathcal{H}+1)^{(L-1)}$$

for every $\mathcal{H}\ge 1$.

Proof. We proceed by induction on the cardinality of S_{fin}, as before. If S_{fin} is empty, then $\sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)}\Psi^{(2)}(\mathfrak{A})\mathfrak{N}(\mathfrak{A})^{1/m}=1$ and the claim holds. Now suppose $S_{\mathrm{fin}}=\{v_1,\dots,v_L\}$ with $L>0$, and again $\mathfrak{p}_1,\dots,\mathfrak{p}_L$ are the prime ideals associated to the places in S_{fin}. Let $S'=S\setminus\{v_L\}$ and again

$$A(\mathfrak{B})=\left\lfloor\frac{\log(\mathcal{H}^m\mathfrak{N}(\mathfrak{B})^{-1})}{\log\mathfrak{N}(\mathfrak{p}_L)}\right\rfloor.$$

Note that $\Psi^{(2)}(\mathfrak{p}_L)\le 2$ and then, by (6.4), $\Psi^{(2)}(\mathfrak{B}\mathfrak{p}_L^{\star(g_L)})\le 2\Psi^{(2)}(\mathfrak{B})$. Hence

$$\begin{aligned}
\sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)}\Psi^{(2)}(\mathfrak{A})\mathfrak{N}(\mathfrak{A})^{1/m} &\le \sum_{\mathfrak{B}\in\mathcal{I}_{S'}(\mathcal{H}^m)}2\Psi^{(2)}(\mathfrak{B})\mathfrak{N}(\mathfrak{B})^{1/m}\sum_{g_L=0}^{A(\mathfrak{B})}\mathfrak{N}(\mathfrak{p}_L)^{g_L/m}\\
&= 2\sum_{\mathfrak{B}\in\mathcal{I}_{S'}(\mathcal{H}^m)}\Psi^{(2)}(\mathfrak{B})\mathfrak{N}(\mathfrak{B})^{1/m}\,\frac{\mathfrak{N}(\mathfrak{p}_L)^{(A(\mathfrak{B})+1)/m}-1}{\mathfrak{N}(\mathfrak{p}_L)^{1/m}-1}\\
&\le \frac{2\mathfrak{N}(\mathfrak{p}_L)^{1/m}}{\mathfrak{N}(\mathfrak{p}_L)^{1/m}-1}\sum_{\mathfrak{B}\in\mathcal{I}_{S'}(\mathcal{H}^m)}\Psi^{(2)}(\mathfrak{B})\mathfrak{N}(\mathfrak{B})^{1/m}\big(\mathfrak{N}(\mathfrak{p}_L)^{\frac{\log(\mathcal{H}^m\mathfrak{N}(\mathfrak{B})^{-1})}{\log\mathfrak{N}(\mathfrak{p}_L)}}\big)^{1/m}\\
&= \frac{2\mathfrak{N}(\mathfrak{p}_L)^{1/m}}{\mathfrak{N}(\mathfrak{p}_L)^{1/m}-1}\sum_{\mathfrak{B}\in\mathcal{I}_{S'}(\mathcal{H}^m)}\Psi^{(2)}(\mathfrak{B})\mathfrak{N}(\mathfrak{B})^{1/m}\left(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{B})}\right)^{1/m}\\
&\le \frac{2\mathfrak{N}(\mathfrak{p}_L)^{1/m}}{\mathfrak{N}(\mathfrak{p}_L)^{1/m}-1}\mathcal{H}\mathcal{L}^{(2)}_{S'}(\mathcal{H},0).
\end{aligned}$$

The claim follows by applying Lemma 6.4. ∎

Now we are ready to prove Theorem 3.2.

We already dealt with the case $S_{\mathrm{fin}} = \emptyset$. Suppose $S_{\mathrm{fin}} \neq \emptyset$. By (6.3) we have

$$\begin{aligned}\big||\mathcal{O}_S^{\mathcal{N}}(\mathcal{H})| - V_{k,\mathcal{N}}\mathcal{H}^{mn}\mathcal{L}_S^{(1)}(\mathcal{H},q)\big| \\ \leq \begin{cases} F\mathcal{H}^{mn}\mathcal{L}_S^{(2)}(\mathcal{H},q-1) + F'\mathcal{H}^{mn}\mathcal{L}_S^{(2)}(\mathcal{H},0) & \text{if } q \geq 1, \\ F\mathcal{H}^{mn-1}\sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)} \Psi^{(2)}(\mathfrak{A})\mathfrak{N}(\mathfrak{A})^{1/m} & \text{if } q = 0. \end{cases}\end{aligned}$$

Note that $L \leq |S| - 1$, and if $q \geq 1$, then $L \leq |S| - 2$. Moreover,

$$F_l^{(1)} = \frac{\Psi^{(1)}(\mathfrak{p}_l)}{\log \mathfrak{N}(\mathfrak{p}_l)} = \frac{1}{\log \mathfrak{N}(\mathfrak{p}_l)}\bigg(1 - \frac{1}{\mathfrak{N}(\mathfrak{p}_l)^n}\bigg).$$

We apply Lemmas 6.4 and 6.5 to conclude that there exists a positive $G = G(\mathcal{N}, \mathfrak{N}(S))$ such that

$$\big||\mathcal{O}_S^n(\mathcal{H})| - C_{\mathcal{N},k,S}\mathcal{H}^{mn}(\log \mathcal{H})^{|S|-1}\big| \leq G\mathcal{H}^{mn}(\log \mathcal{H} + 1)^{|S|-2}$$

for every $\mathcal{H} \geq 1$, where $C_{\mathcal{N},k,S}$ was defined in (3.4).

Now, for every $\mathcal{H}_0 > 1$, there exists a positive C_0, clearly depending on $\mathcal{N}$, $\mathfrak{N}(S)$ and $\mathcal{H}_0$, such that

$$G\mathcal{H}^{mn}(\log \mathcal{H} + 1)^{|S|-2} \leq C_0\mathcal{H}^{mn}(\log \mathcal{H})^{|S|-2},$$

and we have the claim of Theorem 3.2.

Acknowledgments. The author would like to thank Jeffrey Vaaler for many useful discussions and the hospitality at the Department of Mathematics at UT Austin, and Martin Widmer for his encouragement and advice that significantly improved this article. The author is supported by the Austrian Science Foundation (FWF) project W1230-N13 and ERC-Grant No. 267273.

References

[1] F. Barroero, *Counting algebraic integers of fixed degree and bounded height*, Monatsh. Math. 175 (2014), 25–41.

[2] F. Barroero and M. Widmer, *Counting lattice points and o-minimal structures*, Int. Math. Res. Notices 2014, no. 18, 4932–4957.

[3] E. Bierstone and P. D. Milman, *Semianalytic and subanalytic sets*, Inst. Hautes Études Sci. Publ. Math. 67 (1988), 5–42.

[4] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge Univ. Press, Cambridge, 2006.

[5] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, Berlin, 1971.

[6] S.-J. Chern and J. D. Vaaler, *The distribution of values of Mahler's measure*, J. Reine Angew. Math. 540 (2001), 1–47.

[7] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. 26 (1951), 179–183; Corrigendum, ibid. 39 (1964), 580.

[8] X. Gao, *On Northcott's Theorem*, Ph.D. thesis, Univ. of Colorado, 1995.
[9] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, New York, 1983.
[10] K. Mahler, *On the zeros of the derivative of a polynomial*, Proc. Roy. Soc. Ser. A 264 (1961), 145–154.
[11] D. Masser and J. D. Vaaler, *Counting algebraic numbers with large height. II*, Trans. Amer. Math. Soc. 359 (2007), 427–445.
[12] D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. 45 (1949), 502–509.
[13] S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France 107 (1979), 433–449.
[14] W. M. Schmidt, *Northcott's theorem on heights. I. A general estimate*, Monatsh. Math. 115 (1993), 169–181.
[15] W. M. Schmidt, *Northcott's theorem on heights. II. The quadratic case*, Acta Arith. 70 (1995), 343–375.
[16] M. Widmer, *Counting points of fixed degree and bounded height*, Acta Arith. 140 (2009), 145–168.
[17] M. Widmer, *Integral points of fixed degree and bounded height*, arXiv:1309.1944 (2013).

Fabrizio Barroero
Scuola Normale Superiore
Piazza dei Cavalieri 7
56126 Pisa, Italy
E-mail: fbarroero@gmail.com

Received on 28.3.2014
and in revised form on 11.9.2014 (7765)