

COUNTING ALGEBRAIC NUMBERS WITH LARGE HEIGHT II

DAVID MASSER AND JEFFREY D. VAALER

ABSTRACT. We count algebraic numbers of fixed degree over a fixed algebraic number field. When the heights of the algebraic numbers are bounded above by a large parameter \mathcal{H} , we obtain asymptotic estimates for their cardinality as $\mathcal{H} \rightarrow \infty$.

1. INTRODUCTION

In this paper we count algebraic numbers of fixed degree over a fixed algebraic number field. When the heights of the algebraic numbers are bounded from above by a large parameter, we obtain asymptotic estimates for their cardinality. These generalize our recent work [10] over the rational field \mathbb{Q} .

There are several related asymptotic estimates in the literature. The earliest and best known is that of Schanuel [13]. Let K be a number field of degree d over \mathbb{Q} , let n be a positive integer, and let H denote the absolute height on K^n . In 1979 Schanuel proved that as $\mathcal{H} \rightarrow \infty$ there are asymptotically $S_K(n)\mathcal{H}^{d(n+1)}$ elements α of K^n with $H(\alpha) \leq \mathcal{H}$. Here $S_K(n) > 0$ is a certain constant depending only on K and n (see (1.4) below). Actually, Schanuel's result was proved for projective space $\mathbb{P}^n(K)$ instead of K^n , but it is easy to see that this is equivalent to the version for affine K^n .

Schmidt [15] was the first to consider what happens if we no longer restrict the co-ordinates of α to a fixed number field, but restrict only their degrees. In fact he combined this situation with Schanuel's situation by treating the subset of all vectors $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ in \overline{K}^n with relative degree

$$(1.1) \quad [K(\alpha_1, \alpha_2, \dots, \alpha_n) : K] = m,$$

where \overline{K} is an algebraic closure of K . It is well known that the absolute height function H extends to \overline{K}^n , and Northcott's Theorem [11] implies that for each m and \mathcal{H} the set of vectors α with relative degree m over K and $H(\alpha) \leq \mathcal{H}$ is finite. Let $\overline{K}_m^n(\mathcal{H})$ denote the cardinality of this set (actually Schmidt also worked projectively, but again this makes no real difference).

The asymptotics for estimating $\overline{K}_m^n(\mathcal{H})$ in general are still unknown. The case $m = 1$ in (1.1) corresponds to Schanuel's Theorem. For $m \geq 2$ there are results only when $K = \mathbb{Q}$. The quadratic case $m = 2$ was considered by Schmidt [16]. He showed that $\overline{\mathbb{Q}}_2^n(\mathcal{H})$ is asymptotic to $S(2, n)\mathcal{H}^{2(n+1)}$ if $n \geq 3$, to $S(2, 2)\mathcal{H}^6 \log \mathcal{H}$

Received by the editors December 14, 2004.

2000 *Mathematics Subject Classification*. Primary 11R04.

Key words and phrases. Mahler measure, height.

The research of the second author was supported in part by the National Science Foundation (DMS-00-88915).

if $n = 2$, and to $S(2, 1)\mathcal{H}^6$ if $n = 1$. Here $S(2, n) > 0$ depends only on n . For $m \geq 3$ the only asymptotic results known are due to Gao [5] (see also [17], p. 194) when $n \geq m$. The main term for $\overline{\mathbb{Q}}_m^n(\mathcal{H})$ is then $S(m, n)\mathcal{H}^{m(n+1)}$ for $S(m, n) > 0$ depending only on m and n . If $m \geq 3$ and $n < m$, Gao [5] also proved that the correct order of magnitude is $\mathcal{H}^{m(m+1)}$.

In a recent note [10] we were able to establish the asymptotic result in the case $n = 1$ for any m ; that is, for counting algebraic numbers of degree m over \mathbb{Q} .

Let us return to arbitrary K . If $m \geq 2$ or $n \geq 2$ even the correct order of magnitude for $\overline{K}_m^n(\mathcal{H})$ is still unknown. The case $m = 1$ is again covered by Schanuel. The case $n = 1$ is covered by [15], which implies that the correct order of magnitude for $\overline{K}_m^1(\mathcal{H})$ is $\mathcal{H}^{dm(m+1)}$.

In this paper we make modest progress by generalizing [10] to determine the asymptotics of $\overline{K}_m^1(\mathcal{H})$ which counts algebraic numbers of degree m over K with height at most \mathcal{H} . To state our result we need not only Schanuel’s constant $S_K(m)$, but also two constants $V_{\mathbb{R}}(m)$ and $V_{\mathbb{C}}(m)$ depending only on m . We define

$$(1.2) \quad V_{\mathbb{R}}(m) = (m + 1)^l \prod_{i=1}^l \frac{(2i)^{m-2i}}{(2i + 1)^{m+1-2i}},$$

where $l = \lceil (m - 1)/2 \rceil$ and an empty product is interpreted as 1, and

$$(1.3) \quad V_{\mathbb{C}}(m) = \frac{(m + 1)^{m+1}}{((m + 1)!)^2}.$$

We recall that

$$(1.4) \quad S_K(m) = (m + 1)^{r+s-1} \left(\frac{2^r (2\pi)^s}{\sqrt{|\Delta_K|}} \right)^{m+1} \frac{h_K R_K}{w_K \zeta_K(m + 1)}.$$

Here $r = r_K$ is the number of real embeddings of K , $s = s_K$ is the number of pairs of distinct complex conjugate embeddings of K , Δ_K is the discriminant, h_K the class number, R_K the regulator, w_K the number of roots of unity in K , and ζ_K is the Dedekind zeta-function of K .

Theorem. *Let K be an algebraic number field of degree d over \mathbb{Q} . Then as $\mathcal{H} \rightarrow \infty$, the number of β in \overline{K} such that*

$$[K(\beta) : K] = m \quad \text{and} \quad H(\beta) \leq \mathcal{H}$$

is

$$(1.5) \quad mV_{\mathbb{R}}(m)^r V_{\mathbb{C}}(m)^s S_K(m) \mathcal{H}^{dm(m+1)} + O(\mathcal{H}^{dm(m+1)-m\mathcal{L}}),$$

where $\mathcal{L} = 1$ unless $(d, m) = (1, 1)$ or $(d, m) = (1, 2)$ in which case $\mathcal{L} = \log \mathcal{H}$.

For $K = \mathbb{Q}$ this reduces to the main result of our note [10]. For any other K it is new; to take just one example, there are $c\mathcal{H}^{12} + O(\mathcal{H}^{10})$ algebraic numbers α , quadratic over the field $\mathbb{Q}(i)$, with $H(\alpha) \leq \mathcal{H}$; here

$$c = \frac{3\pi^3}{8\zeta_{\mathbb{Q}(i)}(3)} = \frac{12}{\zeta_{\mathbb{Q}}(3)}.$$

Our work sheds no light on the asymptotics of $\overline{K}_m^n(\mathcal{H})$ for $n > 1$. But it does suggest an interesting reciprocity relation regarding m and n . This becomes clearer

in Schmidt’s notation $Z(K, m, n, X)$, which counts the projective version of $\overline{K}_m^n(\mathcal{H})$ with $X = \mathcal{H}^{dm}$. It follows easily by comparing our Theorem with Schanuel’s that

$$(1.6) \quad \frac{Z(K, m, 1, X)}{Z(K, 1, m, X)}$$

tends to the rational number $mV_{\mathbb{R}}(m)^r V_{\mathbb{C}}(m)^s$ as $X \rightarrow \infty$. So one can ask more generally if

$$(1.7) \quad \frac{Z(K, m, n, X)}{Z(K, n, m, X)}$$

tends to a rational limit as $X \rightarrow \infty$. In view of the restriction $n \geq m$ in [5], this is not known for any $n \geq 2$ even if $K = \mathbb{Q}$. Moreover, even if the limit in (1.7) can be calculated, there may be difficulties in establishing its rationality. For example, the multiplying constant $S(2, n)$ in the above asymptotics for $Z(\mathbb{Q}, 2, n, X)$ or $\overline{\mathbb{Q}}_2^n(\mathcal{H})$ involve for $n \geq 3$ the (convergent) sum

$$\sum_K S_K(n)$$

of Schanuel’s (1.4) over all quadratic fields K , which does not look particularly summable. This is in contrast to the explicit constants

$$S(2, 1) = \frac{8}{\zeta_{\mathbb{Q}}(3)} \quad \text{and} \quad S(2, 2) = \frac{96 + 8\pi^2}{\zeta_{\mathbb{Q}}(3)^2}.$$

At any rate it is quickly checked for $K = \mathbb{Q}$ that the numerator and denominator in (1.7) have the same order of magnitude as $X \rightarrow \infty$.

The connection between the numerator and denominator arises naturally from our proof. Let β be in \overline{K} with $[K(\beta) : K] = m$. It satisfies an equation $f(\beta) = 0$ with a unique, monic polynomial

$$(1.8) \quad f(x) = x^m + \alpha_1 x^{m-1} + \alpha_2 x^{m-2} + \cdots + \alpha_m$$

in $K[x]$. So we obtain at once an element α in K^m . However, the height $H(\alpha)$ defined by

$$(1.9) \quad H(\alpha)^d = \prod_v \max\{1, |\alpha_1|_v, |\alpha_2|_v, \dots, |\alpha_m|_v\}^{d_v}$$

(see section 2 for the notation) has nothing to do with the height $H(\beta)$, which can be calculated in terms of certain local Mahler measures.

For example, if $K = \mathbb{Q}$ and $v = \infty$, then any $f(x)$, as in (1.8), factors over \mathbb{C} as

$$(1.10) \quad f(x) = (x - \zeta_1)(x - \zeta_2) \cdots (x - \zeta_m).$$

It has a Mahler measure

$$(1.11) \quad M_{\infty}(f) = \max\{1, |\zeta_1|\} \max\{1, |\zeta_2|\} \cdots \max\{1, |\zeta_m|\}.$$

This can be considered as a function N_{∞} of the coefficients $1, \alpha_1, \alpha_2, \dots, \alpha_m$ of f in (1.8), and so one must be prepared to replace the maximum norm in (1.9) at $v = \infty$ with N_{∞} . In fact N_{∞} is a symmetric distance function on \mathbb{R}^m or \mathbb{C}^m in the sense of the geometry of numbers (as discussed in [1], Chapter IV), but it is not a norm because it fails to satisfy the triangle inequality.

Suppose for the sake of explanation that β is an algebraic integer. Then $f(x)$ is in $\mathbb{Z}[x]$ and one finds that $H(\beta) = M_{\infty}(f)^{1/m}$. Thus we have to count the monic f in $\mathbb{Z}[x]$ with degree m and $M_{\infty}(f) \leq \mathcal{H}^m$.

This type of problem was considered by Chern and the second author in [2], and they obtained asymptotic results. In our context we cannot afford the assumption that f is monic. They considered this case too, and they found the main term

$$\frac{V_{\mathbb{R}}(m)}{2^{m+1}} \mathcal{H}^{m(m+1)}.$$

In our discussion we can omit the integrality assumption by also taking into account the $v \neq \infty$. Still with $K = \mathbb{Q}$, let \mathbb{Q}_v be the corresponding topological completion. Then $f(x)$ in (1.8) factors in the algebraic closure $\overline{\mathbb{Q}_v}$ as in (1.10) and there is an analogue

$$M_v(f) = \max\{1, |\zeta_1|_v\} \max\{1, |\zeta_2|_v\} \cdots \max\{1, |\zeta_m|_v\}$$

of (1.11). However, Gauss's Lemma implies that

$$M_v(f) = \max\{1, |\alpha_1|_v, |\alpha_2|_v, \dots, |\alpha_m|_v\}$$

as in (1.9). So in this case N_v remains the maximum norm.

The strategy of our proof should now be clear. We have a natural collection \mathcal{N} of continuous functions N_v on the completions K_v^{m+1} , and using these we can define a height $H_{\mathcal{N}}$ in order to make $H_{\mathcal{N}}(\boldsymbol{\alpha}) = H(\beta)^m$ in the situation above. So all we have to do is imitate the Schanuel proof for K^n with $H_{\mathcal{N}}$ instead of H . If v corresponds to a complex embedding of K , then we can also appeal to the analogous results of [2] involving $V_{\mathbb{C}}(m)$, and in this way the main term in (1.5) appears. The additional extra factor m in (1.5) is explained simply by the fact that the polynomial f has m different zeros.

We are now rather close to the adelic formulations introduced by Peyre [12], and in fact it is just as easy to work with an arbitrary collection of N_v , provided that N_v is the maximum norm for all finite v (possibly with a finite number of exceptions). For example, this allows us to recover the version of Schanuel's Theorem for the l^2 norms $(1 + |\alpha_1|^2 + \cdots + |\alpha_m|^2)^{1/2}$ at infinity (already mentioned by Thunder in [19] and [20]). Way back in [14], Schmidt had defined heights H_F attached to an arbitrary distance function F , so we could also deduce counting results for these. See also Schmidt's height H^S defined in [16] for quadratic K , which depends on a suitable subset S of \mathbb{R}^{2m+2} .

It is conceivable that the main terms of all our asymptotic formulae could be guessed from the very general conjectures of [12], but it is unlikely that the latter would lead to comparable error terms. Such error terms arise from certain technical Lipschitz-type conditions on the sets defined by $N_v = 1$. We are particularly keen to obtain the precise error term in (1.5) so that for $m = 1$ we recover the full Schanuel Theorem. Another motivation comes from the possibility of summing (1.5) over K as Schmidt did. It is unclear if our error terms can come from considerations of the analytic continuation of a height zeta-function, as in the original investigation of Franke, Manin and Tschinkel [4].

Our programme is now as follows. In section 2 we describe the general heights set-up, state a Proposition, and deduce some consequences such as the Theorem above. We also reverse the situation to deduce something about the analytic continuation of the corresponding height zeta-function. The remainder of our paper is devoted to a proof of the Proposition. This could be considered as just an exercise, but it is one that we unashamedly carry out, as we consider that our proof simplifies the original exposition of Schanuel.

Since writing this paper we have been able to consult the unpublished work [5] of Gao Xia. He defines a height H_U generalizing Schmidt’s height H^S to arbitrary number fields K . Then in his Theorem 3.1 he proves a result resembling our Proposition (but with an explicit dependence on K). This opens a second approach to our Theorem; however along the way one would meet the problems with Davenport’s counting principle referred to in our section 3, as well as its extension to the situation of our Lemma 3.

We are very grateful to Gao Xia for showing us his work.

2. A GENERALIZATION

Here we give a detailed description of the general situation. Suppose that δ is an integer with $0 \leq \delta \leq D$. We say that a set in \mathbb{R}^D is Lipschitz parameterizable of codimension δ if there is a constant L and finitely many maps ϕ from the cube $[0, 1]^{D-\delta}$ to \mathbb{R}^D , whose images cover the set, each satisfying

$$(2.1) \quad |\phi(\mathbf{x}_1) - \phi(\mathbf{x}_2)| \leq L|\mathbf{x}_1 - \mathbf{x}_2|$$

with (for example) the Euclidean norms. If $\delta = D$ this is to be interpreted simply as the finiteness of the set.

Let n be a positive integer. We consider continuous functions N from \mathbb{R}^{n+1} or \mathbb{C}^{n+1} to the real interval $[0, \infty)$ satisfying the following conditions:

- (i) $N(\mathbf{z}) = 0$ if and only if \mathbf{z} is the zero vector,
- (ii) $N(w\mathbf{z}) = |w|N(\mathbf{z})$ for any scalar w in \mathbb{R} or \mathbb{C} ,
- (iii) the set $\{\mathbf{z} : N(\mathbf{z}) = 1\}$ in \mathbb{R}^{n+1} or $\mathbb{C}^{n+1} = \mathbb{R}^{2n+2}$ is Lipschitz parameterizable of codimension 1.

We call such functions *Lipschitz distance functions* (of dimension n).

The set defined in (iii) is the boundary of the set $B = \{\mathbf{z} : N(\mathbf{z}) < 1\}$, and it follows (as in [1], Chapter IV, section 2) that B is a bounded, symmetric, open star-body in \mathbb{R}^{n+1} or \mathbb{C}^{n+1} . In particular the set B has a finite volume V_N .

Let r and s be nonnegative integers not both zero. We will consider a system \mathcal{N} of $r + s$ such Lipschitz distance functions N , one for each of the factors in the product $\mathbb{R}^r \times \mathbb{C}^s$. We call such a system an (r, s) -Lipschitz system (of dimension n). We define its volume $V_{\mathcal{N}}$ to be the product of the $r + s$ volumes V_N .

Next let K be a number field with r real embeddings and s pairs of complex conjugate embeddings. These induce $r + s$ infinite places of K . If v is any one of these, then we can choose an identification of the completion K_v with \mathbb{R} or \mathbb{C} . Thus an (r, s) -Lipschitz system \mathcal{N} gives a system of distance functions N_v on each K_v^{n+1} . We are now rather close to the adelic situation of [12] (p. 107), except for two things: first we have an extra condition (iii), and second we are restricted to the infinite places v . This second restriction can be lifted simply by defining

$$(2.2) \quad N_v(\mathbf{z}) = \max\{|z_0|_v, |z_1|_v, \dots, |z_n|_v\}$$

for $\mathbf{z} = (z_0, z_1, \dots, z_n)$ in K_v^{n+1} and v a finite place of K . If $v|p$, then the absolute value is the unique one extending the standard p -adic absolute value on \mathbb{Q}_p . Note, however, that [12] allows a finite number of exceptions v to (2.2).

We define now for $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_n)$ in K^{n+1} the corresponding absolute height $H_{\mathcal{N}}$ by

$$(2.3) \quad H_{\mathcal{N}}(\boldsymbol{\alpha})^d = \prod_v N_v(\sigma_v(\boldsymbol{\alpha}))^{d_v}$$

taken over all places v , infinite and finite, where σ_v is the canonical embedding of K in K_v extended componentwise to K^{n+1} , $d = [K : \mathbb{Q}]$ and $d_v = [K_v : \mathbb{Q}_v]$ is the local degree. We have the product formula

$$\prod_v |\sigma_v(\alpha)|_v^{d_v} = 1$$

for any $\alpha \neq 0$ in K , where the absolute values are as in (ii) for infinite v and as in (2.2) for finite v . This implies that (2.3) defines a height on $\mathbb{P}^n(K)$ satisfying $H_{\mathcal{N}}(\alpha) \geq 1$.

This definition is slightly more general than Schmidt’s H_F in [14] (p. 432), which takes F on \mathbb{R}^{n+1} and then uses

$$N_v(\mathbf{z}) = F(|z_0|, |z_1|, \dots, |z_n|).$$

But we need to allow genuine functions on \mathbb{C}^{n+1} as well in order to deduce our Theorem. This is because when $n \geq 2$ the Mahler measure of $z_0x^n + z_1x^{n-1} + \dots + z_n$ is not a function of $|z_0|, |z_1|, \dots, |z_n|$ alone (even if z_0, z_1, \dots, z_n are real). For example,

$$M(x^2 + 2x + 1) = 1 < 1 + \sqrt{2} = M(x^2 + 2x - 1).$$

Proposition. *Let K be a number field with r real embeddings and s pairs of complex conjugate embeddings, and for $n \geq 1$ let \mathcal{N} be an (r, s) -Lipschitz system of dimension n . Then for any $\mathcal{H} \geq 1$ there are only finitely many α in $\mathbb{P}^n(K)$ with $H_{\mathcal{N}}(\alpha) \leq \mathcal{H}$, and as $\mathcal{H} \rightarrow \infty$ their number is*

$$2^{-r(n+1)}\pi^{-s(n+1)}V_{\mathcal{N}}S_K(n)\mathcal{H}^{d(n+1)} + O(\mathcal{H}^{d(n+1)-1}\mathcal{L}),$$

where $\mathcal{L} = 1$ unless $(d, n) = (1, 1)$ in which case $\mathcal{L} = \log \mathcal{H}$.

Note that Schmidt [16] in Theorem 2a (p. 358) already proved a similar result for his height $H^S(\alpha)$ when K is quadratic, with an especially good explicit error term if the points of $\mathbb{P}^n(\mathbb{Q})$ are excluded from the counting.

We will prove our result in subsequent sections. But for now we list and prove some consequences.

If we choose (2.2) for all v , then clearly $V_{\mathcal{N}} = 2^{r(n+1)}\pi^{s(n+1)}$. The boundary of a cube in \mathbb{R}^{n+1} is clearly Lipschitz parameterizable (most naturally with $2n + 2$ linear maps), and the complex analogue can also be parameterized (for example, with $n + 1$ trigonometrical maps). So we recover Schanuel’s Theorem, with in fact the same error term.

If we choose

$$N_v(\mathbf{z}) = (|z_0|^2 + |z_1|^2 + \dots + |z_n|^2)^{1/2}$$

for all infinite v , then $V_{\mathcal{N}}$ may be calculated in terms of the volume

$$V_D = \frac{\pi^{D/2}}{\Gamma(1 + D/2)}$$

of the D -dimensional unit ball as $V_{n+1}^r V_{2n+2}^s$. The boundary of such a ball is well known to be Lipschitz parameterizable (for example, with a single trigonometrical map). Thus with the corresponding height $H_{\mathcal{N}} = H_2$ we find the main term

$$2^{-r(n+1)}\pi^{-s(n+1)}V_{n+1}^r V_{2n+2}^s S_K(n)\mathcal{H}^{d(n+1)}$$

for the number of α in $\mathbb{P}^n(K)$ with $H_2(\alpha) \leq \mathcal{H}$. If we interpret these α as one-dimensional subspaces of K^{n+1} , then this agrees with special cases of Theorem 1 of [19] (p. 395) or Theorem 1 of [20] (p. 229).

In [11] Northcott used l^1 norms at all infinite v , so that

$$N_v(\mathbf{z}) = |z_0| + |z_1| + \dots + |z_n|,$$

and so we find the main term

$$\frac{(2^{2n}n!)^s S_K(n) \mathcal{H}^{d(n+1)}}{((n+1)!)^r ((2n+1)!)^s}.$$

More generally, if the set defined by Schmidt's $F(|z_0|, |z_1|, \dots, |z_n|) = 1$ is Lipschitz parameterizable of codimension 1 in \mathbb{R}^{n+1} , then we find the main term

$$2^{-r(n+1)} \pi^{-s(n+1)} V_{F, \mathbb{R}}^r V_{F, \mathbb{C}}^s S_K(n) \mathcal{H}^{d(n+1)}$$

counting points α with $H_F(\alpha) \leq \mathcal{H}$, where $V_{F, \mathbb{R}}$ and $V_{F, \mathbb{C}}$ are the volumes of the sets defined by $F(|z_0|, |z_1|, \dots, |z_n|) \leq 1$ in \mathbb{R}^{n+1} and \mathbb{C}^{n+1} , respectively.

Here we may also deduce the counting results on algebraic subgroups G of the multiplicative group \mathbb{G}_m^{n+1} referred to in [10]. Any such subgroup has a degree $\deg G$ which can be interpreted, for example, as the degree of the Zariski closure in $\mathbb{P}^{n+1}(\mathbb{C})$.

If G is of dimension n , then it is defined by an equation

$$(2.4) \quad x_0^{\alpha_0} x_1^{\alpha_1} \dots x_n^{\alpha_n} = 1$$

for non-zero $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_n)$ in \mathbb{Z}^{n+1} . One sees immediately by homogenizing that $\deg G = N(\alpha)$, where

$$(2.5) \quad N(\mathbf{z}) = \max \left\{ \sum_{i \in \mathcal{I}} z_i, \sum_{j \in \mathcal{J}} (-z_j) \right\} = \max_{\mathcal{K}} \left\{ \left| \sum_{k \in \mathcal{K}} z_k \right| \right\}$$

on \mathbb{R}^{n+1} ; here $\mathcal{I} = \mathcal{I}(\mathbf{z})$ is the set of i with $z_i > 0$, $\mathcal{J} = \mathcal{J}(\mathbf{z})$ is the set of j with $z_j < 0$, and \mathcal{K} runs over all nonempty subsets of $\{0, 1, \dots, n\}$. Further G is connected if and only if $\alpha_0, \alpha_1, \dots, \alpha_n$ are coprime. Thus in this case $\deg G = H_{\mathcal{N}}(\alpha)$, where \mathcal{N} (for $r = 1, s = 0$) is defined by N in (2.5). It is an easy exercise to prove that N is a Lipschitz distance function (even convex). Also, if \mathcal{I} has cardinality I in (2.5), we find that

$$\begin{aligned} V_{\mathcal{N}} &= \sum_{I=0}^{n+1} \binom{n+1}{I} \frac{1}{I!(n-I+1)!} \\ &= \frac{1}{(n+1)!} \sum_{I=0}^{n+1} \binom{n+1}{I}^2 = \frac{(2n+2)!}{((n+1)!)^3}. \end{aligned}$$

Thus the number of connected G of dimension n in \mathbb{G}_m^{n+1} with $\deg G \leq \mathcal{H}$ is $c_{n+1,n} \mathcal{H}^{n+1} + O(\mathcal{H}^n \mathcal{L})$ as $\mathcal{H} \rightarrow \infty$, where

$$c_{n+1,n} = \frac{(2n+2)!}{2((n+1)!)^3 \zeta_{\mathbb{Q}}(n+1)}.$$

If G is connected of dimension 1, then it is defined by parametric equations

$$x_0 = t^{\alpha_0}, \quad x_1 = t^{\alpha_1}, \quad \dots, \quad x_n = t^{\alpha_n}$$

with $\alpha_0, \alpha_1, \dots, \alpha_n$ coprime. One sees by intersecting with a generic hyperplane that $\deg G = N(\alpha)$, where now

$$N(\mathbf{z}) = \max_{i \in \mathcal{I}} z_i + \max_{j \in \mathcal{J}} (-z_j) = \max \left\{ \max_{0 \leq k \leq n} |z_k|, \max_{0 \leq p, q \leq n} |z_p - z_q| \right\}$$

with \mathcal{I} and \mathcal{J} as above. This time we find that

$$\begin{aligned} V_{\mathcal{N}} &= 1 + \sum_{I=0}^{n+1} \binom{n+1}{I} \int_0^1 It^{I-1}(1-t)^{n-I+1} dt \\ &= \sum_{I=0}^{n+1} \binom{n+1}{I} \frac{I!(n-I+1)!}{(n+1)!} = n+1. \end{aligned}$$

Thus the number of connected G of dimension 1 in \mathbb{G}_m^{n+1} with $\deg G \leq \mathcal{H}$ is $c_{n+1,1}\mathcal{H}^{n+1} + O(\mathcal{H}^n\mathcal{L})$ as $\mathcal{H} \rightarrow \infty$, where

$$c_{n+1,1} = \frac{n+1}{2\zeta_{\mathbb{Q}}(n+1)}.$$

Similar results may be obtained when the multiplicative group \mathbb{G}_m is replaced by a suitable abelian variety. But then it is usually the l^2 -norm that turns up. For example, if E is an elliptic curve whose endomorphism algebra K is either \mathbb{Q} or an imaginary quadratic field, and the endomorphism ring is maximal, then the degree of a connected algebraic subgroup of dimension 1 or n in E^{n+1} is given by $CH_2(\boldsymbol{\alpha})^2$ as above, where $\boldsymbol{\alpha}$ is in K^{n+1} and C depends only on n and a polarization on E . See Appendix B of [8].

The rest of this section is devoted to deducing our Theorem from our Proposition, and to pointing out a simple consequence for height zeta-functions.

We choose \mathcal{N} as explained in section 1. Any polynomial f in $\mathbb{C}[x]$ has a Mahler measure $M(f)$. The simplest definition is analytic using the integral

$$m(f) = \int_0^1 \log |f(e^{2\pi it})| dt$$

if $f \neq 0$; then $M(f) = \exp m(f)$ and $M(0) = 0$. Algebraically, $M(f) = |f|$ if f is constant, and if $f \neq 0$ factors over $\mathbb{C}[x]$ as

$$f(x) = z_0(x - \zeta_1)(x - \zeta_2) \cdots (x - \zeta_m) \quad \text{with } m \geq 1,$$

then

$$M(f) = |z_0| \max\{1, |\zeta_1|\} \max\{1, |\zeta_2|\} \cdots \max\{1, |\zeta_m|\}.$$

The continuity of M as a function of the coefficients was proved by Mahler as Lemma 1 (p. 146) of [9]; see also Theorem 4 (p. 6) of [2], for a Lipschitz-type strengthening which, however, has nothing to do with our (iii) above.

Clearly

$$(2.6) \quad M(f_1f_2) = M(f_1)M(f_2).$$

If we define

$$(2.7) \quad N(\mathbf{z}) = M(z_0x^n + z_1x^{n-1} + \cdots + z_n),$$

then the properties (i) and (ii) above are clear.

Property (iii) is not so clear, but it is implied by the following result.

Lemma 1. *The subsets of \mathbb{R}^{n+1} and $\mathbb{C}^{n+1} = \mathbb{R}^{2n+2}$ defined by*

$$M(z_0x^n + z_1x^{n-1} + \cdots + z_n) = 1$$

are Lipschitz parameterizable of codimension 1.

Proof. This is proved in detail for \mathbb{R}^{n+1} as Theorem 20 (p. 35) of [2]. A similar argument works in the complex case, so we content ourselves here with a sketch. Let

$$f(x) = z_0x^n + z_1x^{n-1} + \dots + z_n$$

be in $\mathbb{C}[x]$ with $M(f) = 1$.

If f is constant, then $|z_n| = 1$ and there is an obvious parameterization coming from $z_n = e^{2\pi iw}$ with w in $[0, 1]$.

Next suppose f is nonconstant and that all its zeros are in the closed unit disc. Then $f(x) = z_{n-p}g(x)$ for

$$g(x) = x^p + u_1x^{p-1} + \dots + u_p$$

with $1 \leq p \leq n$, $|z_{n-p}| = 1$, and $M(g) = 1$. This implies that $|u_1|, |u_2|, \dots, |u_p|$ are bounded by functions of n . So f can be parameterized using $z_{n-p} = e^{2\pi iw}$ and the real and imaginary parts of u_1, u_2, \dots, u_p suitably scaled; this gives a map from $[0, 1]^{2p+1}$. So we obtain a ϕ in (2.1) for each p .

Next suppose f is still nonconstant but that all its zeros are outside the closed unit disc. Now $f = h$ for

$$h(x) = v_0x^q + v_1x^{q-1} + \dots + v_{q-1}x + z_n$$

with $1 \leq q \leq n$ and $|z_n| = 1$ and $M(h) = 1$. We get similar parameterizations on $[0, 1]^{2q+1}$ using $z_n = e^{2\pi iw}$ and the real and imaginary parts of v_0, v_2, \dots, v_{q-1} .

Finally, if f is nonconstant with zeros both inside and outside the closed unit disc, then we can factor f as $f = gh$ with

$$g(x) = x^p + u_1x^{p-1} + \dots + u_p, \quad h(x) = v_0x^q + v_1x^{q-1} + \dots + v_{q-1}x + v_q,$$

and $p \geq 1, q \geq 1, p + q \leq n, M(g) = M(h) = 1$, and $|v_q| = 1$. For each p and q we obtain parameterizations linear in each of the real and imaginary parts of $u_1, u_2, \dots, u_p, v_0, v_1, \dots, v_{q-1}$ and also involving w with $v_q = e^{2\pi iw}$. The total number of variables is $2p + 2q + 1 \leq 2n + 1$, and we are finished.

Therefore we have a Lipschitz distance function N . The volume V_N was also computed in [2]. From Corollary 2 (p. 4) we find that the volume is either $2^{n+1}V_{\mathbb{R}}(n)$ or $\pi^{n+1}V_{\mathbb{C}}(n)$. Thus taking the (r, s) -Lipschitz system \mathcal{N} to consist of copies of N , we deduce

$$V_{\mathcal{N}} = 2^{r(n+1)}\pi^{s(n+1)}V_{\mathbb{R}}(n)^rV_{\mathbb{C}}(n)^s,$$

supporting the main term in (1.5). We conclude from the Proposition that there are

$$(2.8) \quad V_{\mathbb{R}}(n)^rV_{\mathbb{C}}(n)^sS_K(n)\mathcal{H}_0^{d(n+1)} + O(\mathcal{H}_0^{d(n+1)-1}\mathcal{L}_0)$$

elements α of $\mathbb{P}^n(K)$ with $H_{\mathcal{N}}(\alpha) \leq \mathcal{H}_0$, where $\mathcal{L}_0 = 1$ unless $(d, n) = (1, 1)$ in which case $\mathcal{L}_0 = \log \mathcal{H}_0$.

We proceed to reformulate this in terms of polynomials. For $f \neq 0$ in $K[x]$ of degree at most n we can define

$$(2.9) \quad M_0(f) = H_{\mathcal{N}}(\alpha)$$

for the vector α of coefficients. This could be referred to as the global absolute Mahler measure; like $H_{\mathcal{N}}$ it is projective in the sense that $M_0(\gamma f) = M_0(f)$ for any $\gamma \neq 0$ in K . So (2.8) counts all such f , up to proportionality, with

$$(2.10) \quad M_0(f) \leq \mathcal{H}_0.$$

We also note from (2.6) that

$$(2.11) \quad M_0(f_1 f_2) = M_0(f_1) M_0(f_2)$$

if $f_1 f_2$ has degree at most n .

Clearly if we now restrict to f of degree exactly n , then the estimate (2.8) continues to hold, because we only have to remove the f of smaller degree. Any such f is proportional to a unique monic polynomial of degree n , and so (2.8) counts the number of these with (2.10).

We wish, however, further to restrict to f irreducible over K . This can be achieved by removing $f = gh$ with g, h monic of degrees $p < n, q < n$, respectively (see also [16], p. 363). By symmetry we can assume $q \geq n/2$. Since $M_0(g) \geq 1$ there is an integer $k \geq 1$ with $2^{k-1} < M_0(g) < 2^k$. Now the multiplicativity (2.11) gives $M_0(h) \leq 2^{1-k} \mathcal{H}_0$. For each fixed k the estimate (2.8) implies that there are at most $c(2^k)^{d(p+1)}$ possibilities for g and at most $c(2^{1-k} \mathcal{H}_0)^{d(q+1)}$ possibilities for h , where c depends only on K and n . If $q < n - 1$ we have

$$(2.12) \quad (2^k)^{p+1} (2^{1-k} \mathcal{H}_0)^{q+1} = (2 \mathcal{H}_0)^{q+1} 2^{k(n-2q)} \leq (2 \mathcal{H}_0)^{n-1},$$

and summing the d -th powers over all $k \geq 1$ with $2^{k-1} \leq \mathcal{H}_0$ gives an extra factor $2 \log \mathcal{H}_0$ (if say $\mathcal{H}_0 \geq 8$). So for $q < n - 1$ there are at most

$$(2.13) \quad 2c^2(2 \mathcal{H}_0)^{d(n-1)} \log \mathcal{H}_0$$

possibilities for $gh = f$. This is smaller than the error term allowed in (2.8).

If $q = n - 1$ and $n > 2$, then $q > n/2$, and so summing the d -th powers of the middle terms in (2.12) over all $k \geq 1$ in \mathbb{Z} gives at most $c^2(2 \mathcal{H}_0)^{dn}$ possibilities for f . This is still no larger than the error term in (2.8).

Finally if $q = n - 1$ and $n = 2$ we get at most $2c^2(2 \mathcal{H}_0)^{2d} \log \mathcal{H}_0$ possibilities for f . This is covered by (2.8) unless $d = 1$. So in the case $(d, n) = (1, 2)$ we have to include the logarithm.

Summing up, we have shown that the number of monic f in $K[x]$ of degree n , irreducible over K with (2.10), is

$$(2.14) \quad V_{\mathbb{R}}(n)^r V_{\mathbb{C}}(n)^s S_K(n) \mathcal{H}_0^{d(n+1)} + O(\mathcal{H}_0^{d(n+1)-1} \mathcal{L}'_0),$$

where $\mathcal{L}'_0 = 1$ unless $(d, n) = (1, 1)$ or $(d, n) = (1, 2)$, in which case $\mathcal{L}'_0 = \log \mathcal{H}_0$.

The last step to the Theorem is relatively easy. Here we wish to count β in \overline{K} with $[K(\beta) : K] = n$. Any such β is the zero of a unique f as above, and in fact

$$(2.15) \quad M_0(f) = H(\beta)^n.$$

This can be seen as follows. The equations (2.3), (2.7) and (2.9) define $M_0(f)$ on $K[x]$. But it is easy to verify that they are independent of the field K , and so they provide a definition on $\overline{\mathbb{Q}}[x]$. Further, $M_0(x - \zeta) = H(\zeta)$, the standard absolute height. Now (2.15) follows after factoring f over $\overline{\mathbb{Q}}$, using (2.11), and noting that all the zeroes of f have the same height $H(\beta)$.

If now $H(\beta) \leq \mathcal{H}$, then (2.15) implies that this is equivalent to $M_0(f) \leq \mathcal{H}^n$. So in view of (2.10), to obtain our Theorem all we have to do is substitute $\mathcal{H}_0 = \mathcal{H}^n$ in (2.14) and multiply by n to take account of the fact that precisely n different β in \overline{K} give rise to the same f . This completes the proof.

Incidentally the expression $M_v(f) = M(\sigma_v(f))$ (where σ_v acts on the coefficients) could be termed the local Mahler measure, so that (2.3) yields

$$M_0(f)^d = \prod_v M_v(f)^{d_v}.$$

Finally, we add some remarks about height zeta-functions. Let \mathcal{N} be an arbitrary Lipschitz system on a number field K . We may formally define

$$\zeta_{\mathcal{N}}(s) = \sum_{\alpha} H_{\mathcal{N}}(\alpha)^{-s}$$

taken over all α in $\mathbb{P}^n(K)$. The upper bound of order $\mathcal{H}^{d(n+1)}$ in the Proposition implies that $\zeta_{\mathcal{N}}(s)$ converges for all complex s with real part $\Re(s) > d(n+1)$. The full asymptotic result with error term implies that $\zeta_{\mathcal{N}}(s)$ has an analytic continuation to $\Re(s) > d(n+1) - 1$, with a simple pole at $s = d(n+1)$ whose residue is

$$d(n+1)2^{-r\kappa(n+1)}\pi^{-s\kappa(n+1)}V_{\mathcal{N}}S_K(n).$$

It would be interesting to know if this can be deduced from the Langlands theory invoked in [4].

3. COUNTING PRINCIPLES

Traditionally the counting is carried out with the help of the well-known principle that a reasonable set S in \mathbb{R}^D contains about V/Δ points of a lattice Λ , where V is the volume of S and Δ is the determinant of Λ . In fact it usually suffices to take S as a large multiple tS_1 of a fixed set S_1 and Λ also as fixed. But some of the details of the present proofs can be simplified if the dependence on Λ is made explicit. This we do in the following result; recall that the first successive minimum of Λ with respect to the Euclidean distance function is simply the smallest length of any nonzero element of Λ .

Lemma 2. *Let S in \mathbb{R}^D be a bounded set whose boundary ∂S can be covered by the images of at most W maps ϕ from $[0, 1]^{D-1}$ to \mathbb{R}^D satisfying Lipschitz conditions*

$$(3.1) \quad |\phi(\mathbf{x}_1) - \phi(\mathbf{x}_2)| \leq L|\mathbf{x}_1 - \mathbf{x}_2|$$

for the Euclidean norms. Then S is measurable. Further let Λ in \mathbb{R}^D be a lattice with first successive minimum λ_1 . Then the number Z of points in $S \cap \Lambda$ satisfies

$$(3.2) \quad |Z - V/\Delta| \leq cW \left(\frac{L}{\lambda_1} + 1 \right)^{D-1}$$

for some $c = c(D)$ depending only on D .

Proof. The versions in [6] (p. 128) or [7] (p. 294) can easily be made to yield explicit constants, and in [18] this is efficiently carried out for $\Lambda = \mathbb{Z}^D$. But in these proofs there is the danger of bringing in also the last successive minimum λ_D of Λ .

The measurability of S has already been observed in [7] and [18]. For the estimate (3.2) we start with the case $\Lambda = \mathbb{Z}^D$, using various constants c which depend only on D .

A standard argument shows that the left-hand side of (3.2) is at most the number of lattice points \mathbf{y} such that $C_{\mathbf{y}} = \mathbf{y} + [0, 1]^D$ intersects ∂S . We can split $[0, 1]^{D-1}$ into L_1^{D-1} subcubes of side $1/L_1$, where $L_1 = 1 + [L]$, and the images of these subcubes under each ϕ in (3.1) have diameters at most $cL/L_1 \leq c$. Clearly no more

than c of the $C_{\mathbf{y}}$ can meet a single such image, and the result (3.2) follows from the covering property, at least for $\Lambda = \mathbb{Z}^D$ with $\lambda_1 = 1$.

In general Λ has basis elements $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_D$ satisfying $|\mathbf{y}_i| \leq c\lambda_i$ ($1 \leq i \leq D$) for the successive minima $\lambda_1, \lambda_2, \dots, \lambda_D$ of Λ . See for example Lemma 8 (p. 135) of [1]. If η^{-1} is the automorphism of \mathbb{R}^D whose matrix has the columns $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_D$, then $\eta(\Lambda) = \mathbb{Z}^D$ and we can apply the result above to $\eta(S)$. The boundary of this latter set can be parameterized by finitely many maps $\psi(\mathbf{x}) = \eta(\phi(\mathbf{x}))$, and from (3.1) we obtain

$$(3.3) \quad |\psi(\mathbf{x}_1) - \psi(\mathbf{x}_2)| \leq L\|\eta\|\|\mathbf{x}_1 - \mathbf{x}_2\|,$$

where $\|\eta\|$ is the (Euclidean) operator norm of η .

Finally the entries of row i of the matrix of η have the shape $\Delta^{-1}\mu$, where μ is a minor of the matrix with columns $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_D$ omitting \mathbf{y}_i . For these

$$|\mu| \leq c \frac{|\mathbf{y}_1||\mathbf{y}_2| \cdots |\mathbf{y}_D|}{|\mathbf{y}_i|} \leq c \frac{\lambda_1 \lambda_2 \cdots \lambda_D}{\lambda_i}.$$

As $\lambda_1 \lambda_2 \cdots \lambda_D \leq c\Delta$ by Minkowski's Second Theorem, we see that each entry of the matrix of η has absolute value at most c/λ_1 . It follows easily that $\|\eta\| \leq c/\lambda_1$. Now (3.2) comes out because the L in (3.1) has been replaced by $L\|\eta\|$ in (3.3).

Note that this result is not restricted to homogeneously expanding domains $S = tS_1$.

An alternative counting principle was proved by Davenport [3], but formulated only for $\Lambda = \mathbb{Z}^D$. It was adapted to arbitrary Λ using the geometry of numbers by Thunder [19], [20], and Schmidt [16]. This works very well if we know enough about the intersections of lines with suitable projections of S . The situation is optimal if S is convex, and controllable if S is defined by inequalities such as $|x_1 x_2 \cdots x_D| \leq C$. But to prove our Theorem we have to consider inequalities of the form $F(\mathbf{x}_1)F(\mathbf{x}_2) \cdots F(\mathbf{x}_d) \leq C$ in d sets of variables with

$$F(\mathbf{x}) = F(x_0, x_1, \dots, x_n) = M(x_0 z^n + x_1 z^{n-1} + \cdots + x_n)$$

defined using a Mahler measure. It is known (see below) that the individual sets defined by $M(x_0 z^n + x_1 z^{n-1} + \cdots + x_n) \leq C$ are not convex if $n \geq 2$. There is a good substitute for convexity in Theorem 4 (p. 6) of [2], but it says nothing about intersections with lines.

Further the versions in [19], [20] use "co-ordinate domains" S defined by the property that \mathbf{x} in S and $|y_1| \leq |x_1|, |y_2| \leq |x_2|, \dots, |y_D| \leq |x_D|$ imply \mathbf{y} in S . This too fails for the Mahler measure; a simple example follows from the observation

$$M(4x^2 + 10x + 4) = 8 < 9 = M(3x^2 + 10x + 3).$$

(Here one can also see the lack of convexity—dividing by 8 and 9 we get f_1, f_2 with $M(f_1) = M(f_2) = 1$, and one checks that

$$M\left(\frac{1}{2}f_1 + \frac{1}{2}f_2\right) = \frac{85 + \sqrt{3625}}{144} > 1.)$$

Probably it is not too difficult to overcome these problems, but then the Proposition would have to involve "(r, s)-Davenport systems" which we prefer not to meet in the dark. It may be worth pointing out that the Davenport property might well imply the Lipschitz property (for example a convex set probably has a parameterizable boundary), but certainly not conversely (for counterexamples a biscuit with crinkly edges or a cubical golf ball).

4. PRELIMINARIES

Here we do no counting, but we define and investigate the sets to which Lemma 2 will be applied.

For nonnegative integers r and s not both zero write $q = r + s - 1 \geq 0$. Denote by Σ the hyperplane in \mathbb{R}^{q+1} defined by $x_1 + x_2 + \dots + x_{q+1} = 0$, and write $\delta = (d_1, d_2, \dots, d_{q+1})$, where $d_i = 1$ for $1 \leq i \leq r$ (if $r \geq 1$) and $d_i = 2$ for $r + 1 \leq i \leq r + s = q + 1$ (if $s \geq 1$). Let F be a bounded set in Σ , and for real $T > 0$ denote by $F(T)$ in \mathbb{R}^{q+1} the vector sum

$$(4.1) \quad F(T) = F + (-\infty, \log T] \delta.$$

Write \exp for the diagonal exponential map from \mathbb{R}^{q+1} to $[0, \infty)^{q+1}$ in \mathbb{R}^{q+1} .

Let n be a positive integer, and let \mathcal{N} be a fixed (r, s) -Lipschitz system of dimension n . So we have Lipschitz distance functions N_1, N_2, \dots, N_{q+1} on each of the $q + 1$ factors of $\mathbb{R}^r \times \mathbb{C}^s$. We use corresponding variables z_1, z_2, \dots, z_{q+1} ; thus z_i is in $\mathbb{R}^{d_i(n+1)}$ according to the above definition of d_i for $1 \leq i \leq q + 1$. Write $d = r + 2s$. We define $S_F(T)$ in \mathbb{R}^D for

$$D = \sum_{i=1}^{q+1} d_i(n + 1) = d(n + 1)$$

as the set of all $(z_1, z_2, \dots, z_{q+1})$ with

$$(N_1(z_1)^{d_1}, N_2(z_2)^{d_2}, \dots, N_{q+1}(z_{q+1})^{d_{q+1}}) \text{ in } \exp F(T).$$

Using (ii) of section 2 together with (4.1) and the observation

$$\exp((\log |w|) \delta) = (|w|^{d_1}, |w|^{d_2}, \dots, |w|^{d_{q+1}})$$

for real w , it is easy to see that

$$(4.2) \quad S_F(T) = TS_F(1)$$

is homogeneously expanding and bounded.

Lemma 3. *Suppose $q \geq 1$ and F has a boundary ∂F that is Lipschitz parameterizable of codimension 2 in \mathbb{R}^{q+1} . Then the boundary of $S_F(1)$ is Lipschitz parameterizable of codimension 1 in \mathbb{R}^D .*

Proof. Consider to begin with the boundary $\partial F(1)$ in (4.1). Because F is in the hyperplane Σ and δ is not, we see that $\partial F(1)$ is contained in two parts: the closure of F together with $\partial F + (-\infty, 0] \delta$. As F is bounded the first part is clearly Lipschitz parameterizable of codimension 1 in \mathbb{R}^{q+1} ; for example one can project to any q coordinates, say x_1, x_2, \dots, x_q , and use the inverse map $\phi = (\phi_1, \phi_2, \dots, \phi_{q+1})$ suitably scaled to $[0, 1]^q$.

To parameterize the second part $\partial F + (-\infty, 0] \delta$, at least if $q \geq 2$, we simply let $\psi = (\psi_1, \psi_2, \dots, \psi_{q+1})$ be one of the Lipschitz parameterizing maps for ∂F on $[0, 1]^{q-1}$ and use $\psi + t \delta$ ($-\infty < t \leq 0$). Of course this region for t is not compact, but we deduce that $\exp \partial F(1)$ can be covered by the images of maps

$$(4.3) \quad \Phi = \exp \phi = (e^{\phi_1}, e^{\phi_2}, \dots, e^{\phi_{q+1}})$$

on $[0, 1]^q$ or maps

$$(4.4) \quad \begin{aligned} \Phi &= \exp(\psi + t\delta) = (e^{\psi_1+td_1}, e^{\psi_2+td_2}, \dots, e^{\psi_{q+1}+td_{q+1}}) \\ &= (e^{\psi_1}u^{d_1}, e^{\psi_2}u^{d_2}, \dots, e^{\psi_{q+1}}u^{d_{q+1}}) \end{aligned}$$

on $[0, 1]^{q-1} \times [0, 1]$, with $u = e^t$ in $(0, 1]$.

It is not difficult to check that these maps satisfy the Lipschitz conditions (3.1). By hypothesis this is certainly true of the functions $\phi_1, \phi_2, \dots, \phi_{q+1}, \psi_1, \psi_2, \dots, \psi_{q+1}$. Also, it is well known that the class of functions from $[0, 1]^q$ to \mathbb{R} satisfying (3.1) is closed under addition, multiplication, and exponentiation (or more generally composition suitably formulated). Thus $\exp \partial F(1)$ is Lipschitz parameterizable of codimension 1 in \mathbb{R}^{q+1} , at least if $q \geq 2$; and it is easy to check this also for $q = 1$ (when F is just a finite set).

Next, since F is bounded we see from (4.1) that $\partial(\exp F(1))$ consists of $\exp \partial F(1)$ together with the origin. So this too is Lipschitz parameterizable of codimension 1 in \mathbb{R}^{q+1} ; one only has to extend the range of u to $[0, 1]$. Let

$$\Phi = (\Phi_1(\mathbf{t}), \Phi_2(\mathbf{t}), \dots, \Phi_{q+1}(\mathbf{t}))$$

be a typical parameterizing map as in (4.3) or (4.4), defined for \mathbf{t} in $[0, 1]^q$.

Now $\partial S_F(1)$ is the set of all $(\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_{q+1})$ with

$$(4.5) \quad (N_1(\mathbf{z}_1)^{d_1}, N_2(\mathbf{z}_2)^{d_2}, \dots, N_{q+1}(\mathbf{z}_{q+1})^{d_{q+1}})$$

in $\partial(\exp F(1))$, because N_1, N_2, \dots, N_{q+1} are continuous. So the part of it covered by Φ is contained in the set of all $(\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_{q+1})$ for which there exists \mathbf{t} in $[0, 1]^q$ with $N_i(\mathbf{z}_i)^{d_i} = \Phi_i(\mathbf{t})$ ($1 \leq i \leq q+1$). By (iii) of section 2 the boundaries defined by $N_i(\mathbf{z}) = 1$ are parameterized by maps $\Psi_i(\mathbf{t}_i)$ for \mathbf{t}_i in $[0, 1]^{e_i}$ with $e_i = d_i(n+1) - 1$ ($1 \leq i \leq q+1$). So the set $N_i(\mathbf{z}) = \zeta$ (for $\zeta \geq 0$) is parameterized by $\zeta \Psi_i$, by (ii) of section 2. Thus $\partial S_F(1)$ can be parameterized by

$$(\Phi_1(\mathbf{t})^{1/d_1} \Psi_1(\mathbf{t}_1), \Phi_2(\mathbf{t})^{1/d_2} \Psi_2(\mathbf{t}_2), \dots, \Phi_{q+1}(\mathbf{t})^{1/d_{q+1}} \Psi_{q+1}(\mathbf{t}_{q+1})).$$

From (4.3) and (4.4) we see that $\Phi_i(\mathbf{t})^{1/d_i}$ is e^{ϕ_i/d_i} or $e^{\psi_i/d_i}u$ ($1 \leq i \leq q+1$), and so the foregoing remarks about multiplication and exponentiation show that the above maps continue to satisfy the Lipschitz conditions. The total number of variables is

$$q + \sum_{i=1}^{q+1} e_i = D - 1,$$

and therefore $\partial S_F(1)$ is parameterizable of codimension 1 as required.

In the sequel the set F will be a fundamental domain for a lattice. In practice this can be taken as a parallelepiped and so is easily parameterizable, e.g., by continuously differentiable maps. In this case the proof of Lemma 3 simplifies considerably.

Lemma 4. *Suppose that F is measurable with volume V_F . Then $S_F(1)$ is measurable with volume*

$$(n+1)^q (q+1)^{-1/2} V_F V_{\mathcal{N}}.$$

Proof. The set $S_F(1)$ is the inverse image of $\exp F(1)$ under the continuous map N taking $(z_1, z_2, \dots, z_{q+1})$ in \mathbb{R}^D to (4.5). So its volume V is

$$\int_{\exp F(1)} d\rho(\mathbf{X}),$$

where $\rho(\mathbf{X}) = \rho(X_1, X_2, \dots, X_{q+1})$ is the corresponding distribution function; that is, the measure of the set defined by $N_i(z_i)^{d_i} \leq X_i$ ($1 \leq i \leq q + 1$). But we noted that the sets with $N_i(z_i) \leq 1$ are measurable, with volume say V_i ($1 \leq i \leq q + 1$). By (ii) of section 2 it follows that

$$\rho(\mathbf{X}) = V_1 V_2 \cdots V_{q+1} X_1^{n+1} X_2^{n+1} \cdots X_{q+1}^{n+1}.$$

Thus

$$V = (n + 1)^{q+1} V_{\mathcal{N}} \int_{\exp F(1)} X_1^n X_2^n \cdots X_{q+1}^n dX_1 dX_2 \cdots dX_{q+1}.$$

Let us use for definiteness x_1, x_2, \dots, x_q as co-ordinates on F (with $x_{q+1} = -x_1 - x_2 - \cdots - x_q$), and then $X_i = e^{x_i + td_i}$ ($1 \leq i \leq q + 1$) for the corresponding co-ordinates on $\exp F(1) = \exp(F + (-\infty, 0] \delta)$. The Jacobian determinant

$$\frac{\partial(X_1, X_2, \dots, X_{q+1})}{\partial(x_1, x_2, \dots, x_q, t)}$$

is readily calculated as

$$(d_1 + d_2 + \cdots + d_{q+1}) X_1 X_2 \cdots X_{q+1} = dX_1 X_2 \cdots X_{q+1},$$

and it follows that

$$V = d(n + 1)^{q+1} V_{\mathcal{N}} \int_{-\infty}^0 e^{td(n+1)} dt \int_F dx_1 dx_2 \cdots dx_q.$$

The lemma comes out after noting that the above integral over F is $(q + 1)^{-1/2} V_F$.

5. PROOF OF THE PROPOSITION

Let K be a number field of degree d with r embeddings $\sigma_1, \sigma_2, \dots, \sigma_r$ into \mathbb{R} and s pairs $\sigma_{r+1}, \bar{\sigma}_{r+1}, \sigma_{r+2}, \bar{\sigma}_{r+2}, \dots, \sigma_{r+s}, \bar{\sigma}_{r+s}$ of complex conjugate embeddings into \mathbb{C} . Then $\sigma = (\sigma_1, \dots, \sigma_{r+s})$ defines a map from K into \mathbb{R}^d . As in section 4 write $q = r + s - 1$.

Let \mathfrak{A} be a nonzero ideal in the ring of integers $\mathfrak{O} = \mathfrak{O}_K$ of K , with norm $[\mathfrak{O} : \mathfrak{A}]$ abbreviated to $[\mathfrak{A}]$ for convenience. For a positive integer n write $D = d(n + 1)$, also as in section 4.

Lemma 5. *The product $\Lambda(\mathfrak{A}) = \sigma(\mathfrak{A})^{n+1}$ is a lattice in \mathbb{R}^D with determinant*

$$\Delta = (2^{-s} [\mathfrak{A}] \sqrt{|\Delta_K|})^{n+1},$$

and its first successive minimum with respect to the Euclidean distance is $\lambda_1 \geq [\mathfrak{A}]^{1/d}$.

Proof. That $\Lambda(\mathfrak{A})$ is a lattice with the desired determinant is classical; see for example Lemma 2 (p. 115) of [6]. Clearly λ_1 is also the first minimum of the lattice $\sigma(\mathfrak{A})$. An element $\sigma(\alpha)$ of this lattice has squared length

$$\sum_{i=1}^{q+1} |\sigma_i(\alpha)|^2 \geq \frac{1}{2} \sum_{i=1}^{q+1} d_i |\sigma_i(\alpha)|^2$$

with d_1, d_2, \dots, d_{q+1} as in section 4; here the fraction $\frac{1}{2}$ can be omitted if $d = 1$. Using the weighted arithmetic mean we see that this is at least $\frac{1}{2}d \prod_{i=1}^{q+1} |\sigma_i(\alpha)|^{2d_i/d}$. Here $\prod_{i=1}^{q+1} |\sigma_i(\alpha)|^{d_i}$ is the absolute value of the norm of α from K to \mathbb{Q} , which if $\alpha \neq 0$ is at least $[\mathfrak{A}]$; the result follows.

Now let \mathcal{N} be an (r, s) -Lipschitz system of dimension n . In what follows we will often suppress the dependence on K and \mathcal{N} . Let Σ be the hyperplane in \mathbb{R}^{q+1} defined as in section 4 by $x_1 + x_2 + \dots + x_{q+1} = 0$. With F, T, δ and $S_F(T)$ as in section 4 and $\Lambda(\mathfrak{A})$ as above, we consider the intersection $S_F(T) \cap \Lambda(\mathfrak{A})$. As $S_F(T)$ is bounded and $\Lambda(\mathfrak{A})$ is a lattice, this intersection is a finite set; let $Z_F(\mathfrak{A}, T)$ denote the number of its nonzero points.

Lemma 6. *There is a positive constant c , depending only on K and \mathcal{N} , with the following property. Let F be bounded measurable with volume V_F such that ∂F is Lipschitz parameterizable of codimension 2. If $T < c[\mathfrak{A}]^{1/d}$, then $Z_F(\mathfrak{A}, T) = 0$. If $T \geq c[\mathfrak{A}]^{1/d}$, then*

$$\left| Z_F(\mathfrak{A}, T) - C_F \frac{T^{d(n+1)}}{[\mathfrak{A}]^{n+1}} \right| \leq c_F \frac{T^{d(n+1)-1}}{[\mathfrak{A}]^{n+1-1/d}}$$

for c_F depending only on K, \mathcal{N} and F , and

$$(5.1) \quad C_F = \frac{(n+1)^q}{\sqrt{q+1}} \frac{2^{s(n+1)}}{\sqrt{|\Delta_K|^{n+1}}} V_F V_{\mathcal{N}}.$$

Proof. The set $S_F(T)$ consists of all $(z_1, z_2, \dots, z_{q+1})$, with z_i in $\mathbb{R}^{d_i(n+1)}$ ($1 \leq i \leq q+1$), such that (4.5) lies in

$$\exp F(T) = \exp(F + (-\infty, \log T] \delta).$$

Thanks to $-\infty$ this set contains the origin, which we exclude from the counting. Thanks to $\log T$ we deduce

$$(5.2) \quad \prod_{i=1}^{q+1} N_i(\mathbf{z}_i)^{d_i} \leq T^d$$

on this set. Because of (i) of section 2 (see also [1], p. 108) there are positive constants c_i with

$$(5.3) \quad N_i(\mathbf{z}) \geq c_i \max\{|z_0|, |z_1|, \dots, |z_n|\}$$

for all $\mathbf{z} = (z_0, z_1, \dots, z_n)$ in $\mathbb{R}^{d_i(n+1)}$ ($1 \leq i \leq q+1$).

Our lattice points have the shape $\mathbf{z}_i = \sigma_i(\alpha)$ for some $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_n)$ in \mathfrak{A}^{n+1} . If α is not zero, then some $\alpha_j \neq 0$ and (5.3) implies

$$\prod_{i=1}^{q+1} N_i(\mathbf{z}_i)^{d_i} \geq c^d \prod_{i=1}^{q+1} |\sigma_i(\alpha_j)|^{d_i} \geq c^d [\mathfrak{A}] \quad \text{with} \quad c = \prod_{i=1}^{q+1} c_i^{d_i/d}.$$

Comparing with (5.2) gives the first assertion of the present lemma.

Next, recall from (4.2) that $S_F(T) = T S_F(1)$. By Lemma 4 the volume of $S_F(T)$ is

$$V = (n+1)^q (q+1)^{-1/2} V_F V_{\mathcal{N}} T^{d(n+1)}.$$

It follows from Lemma 3 that $\partial S_F(1)$ is Lipschitz parameterizable of codimension 1, and so we deduce the same for $\partial S_F(T)$; in Lemma 3 the number W of maps

depends only on K, \mathcal{N} and F . We also get $L \leq c'_F T$ with c'_F also depending only on K, \mathcal{N} and F .

Finally $\Lambda(\mathfrak{A})$ has determinant

$$\Delta = (2^{-s}[\mathfrak{A}]\sqrt{|\Delta_K|})^{n+1}$$

with first successive minimum $\lambda_1 \geq [\mathfrak{A}]^{1/d}$ thanks to Lemma 5. The main estimate of the present lemma comes from applying Lemma 2 and adjusting for the origin. This completes the proof.

The points of $S_F(T) \cap \Lambda(\mathfrak{A})$ correspond to $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_n)$ in \mathfrak{A}^{n+1} , which is equivalent to

$$(5.4) \quad \alpha_0\mathfrak{D} + \alpha_1\mathfrak{D} + \dots + \alpha_n\mathfrak{D} \subseteq \mathfrak{A}.$$

We now use Möbius inversion to count the subset with $\alpha_0\mathfrak{D} + \alpha_1\mathfrak{D} + \dots + \alpha_n\mathfrak{D} = \mathfrak{A}$. Write $Z_F^*(\mathfrak{A}, T)$ for the cardinality of this subset.

Lemma 7. *Let F be bounded measurable with volume V_F such that ∂F is Lipschitz parameterizable of codimension 2. Then for any $T \geq e$ we have*

$$\left| Z_F^*(\mathfrak{A}, T) - C_F^* \frac{T^{d(n+1)}}{[\mathfrak{A}]^{n+1}} \right| \leq c_F^* T^{d(n+1)-1} \mathcal{L}_0$$

for c_F^* depending only on K, \mathcal{N} and F and $C_F^* = C_F/\zeta_K(n+1)$. Here $\mathcal{L}_0 = 1$ unless $(d, n) = (1, 1)$ in which case $\mathcal{L}_0 = \log T$.

Proof. As the inclusion (5.4) for nonzero α is equivalent to $\alpha_0\mathfrak{D} + \alpha_1\mathfrak{D} + \dots + \alpha_n\mathfrak{D} = \mathfrak{A}\mathfrak{B}$ for some nonzero integral ideal \mathfrak{B} , using the Möbius function μ_K of K shows that

$$Z_F^*(\mathfrak{A}, T) = \sum_{\mathfrak{B}} \mu_K(\mathfrak{B}) Z_F(\mathfrak{A}\mathfrak{B}, T),$$

and we may restrict here to \mathfrak{B} with $[\mathfrak{B}] \leq c^{-d}T^d$. The present lemma then follows after a short calculation from Lemma 6 on recalling that

$$\sum_{\mathfrak{B}} \mu_K(\mathfrak{B}) [\mathfrak{B}]^{-s} = 1/\zeta_K(s)$$

for $s > 1$ (here $s = n + 1$). The error terms arise because

$$\sum_{[\mathfrak{B}] > X} [\mathfrak{B}]^{-s}$$

has order at most X^{1-s} as $X \rightarrow \infty$ if $s > 1$ (here $s = n + 1$), and because

$$\sum_{[\mathfrak{B}] \leq X} [\mathfrak{B}]^{-s}$$

has order at most 1 as $X \rightarrow \infty$ if $s > 1$, with an extra logarithm if $s = 1$ (here $s = n + 1 - 1/d$). For references see [6] (pp. 155–162) or [13] (p. 446).

In our Proposition we are considering $(\alpha_0, \alpha_1, \dots, \alpha_n)$ in $\mathbb{P}^n(K)$ with

$$H_{\mathcal{N}}(\alpha_0, \alpha_1, \dots, \alpha_n) \leq \mathcal{H}.$$

It is not difficult to see that this is a finite set. For example the definition (2.3) together with (2.2) and (5.3) show that

$$H_{\mathcal{N}}(\alpha_0, \alpha_1, \dots, \alpha_n) \geq cH(\alpha_0, \alpha_1, \dots, \alpha_n)$$

for

$$c = \prod_{i=1}^{q+1} c_i^{d_i/d}$$

and the conventional height. Denoting the cardinality of this finite set by $Z(\mathcal{H})$, we may formulate the final step in the proof as follows.

Recall the standard logarithmic map l from K^\times to \mathbb{R}^{q+1} taking η to

$$(5.5) \quad l(\eta) = (d_1 \log |\sigma_1(\eta)|, d_2 \log |\sigma_2(\eta)|, \dots, d_{q+1} \log |\sigma_{q+1}(\eta)|).$$

If U is the unit group of K , then $l(U)$ is a lattice in the hyperplane Σ .

Lemma 8. *If F is a bounded measurable fundamental domain for $l(U)$ with volume V_F and ∂F Lipschitz parameterizable of codimension 2, then for any $\mathcal{H} \geq 1$*

$$(5.6) \quad Z(\mathcal{H}) = w_K^{-1} \sum_{\mathfrak{A}} Z_F^*(\mathfrak{A}, [\mathfrak{A}]^{1/d} \mathcal{H}),$$

where the sum is taken over any set of integral ideal class representatives of K .

Proof. Any $(\alpha_0, \alpha_1, \dots, \alpha_n)$ in $\mathbb{P}^n(K)$ corresponds to a unique ideal class, that of $\alpha_0\mathfrak{D} + \alpha_1\mathfrak{D} + \dots + \alpha_n\mathfrak{D}$, and so there is \mathfrak{A} in the sum (5.6) such that we can take a representative α in K^{n+1} with

$$(5.7) \quad \alpha_0\mathfrak{D} + \alpha_1\mathfrak{D} + \dots + \alpha_n\mathfrak{D} = \mathfrak{A}.$$

This representative is unique up to units η . Now the set $F(\infty) = F + \mathbb{R}\delta$ is a fundamental domain for \mathbb{R}^{q+1} under the additive action of $l(U)$. From the identities

$$\log N_i(\sigma_i(\eta\alpha))^{d_i} = \log N_i(\sigma_i(\alpha))^{d_i} + d_i \log |\sigma_i(\eta)| \quad (1 \leq i \leq q+1)$$

arising from (ii) of section 2, we see that there is exactly one unit, up to roots of unity, such that

$$(d_1 \log N_1(\sigma_1(\alpha)), d_2 \log N_2(\sigma_2(\alpha)), \dots, d_{q+1} \log N_{q+1}(\sigma_{q+1}(\alpha)))$$

lies in $F(\infty)$. This is equivalent to

$$(N_1(\sigma_1(\alpha))^{d_1}, N_2(\sigma_2(\alpha))^{d_2}, \dots, N_{q+1}(\sigma_{q+1}(\alpha))^{d_{q+1}})$$

lying in $\exp F(\infty)$.

Now $\exp F(T)$ is the set of $(X_1, X_2, \dots, X_{q+1})$ with $X_1 X_2 \dots X_{q+1} \leq T^d$ and for $X_i = N_i(\sigma_i(\alpha))^{d_i}$ ($1 \leq i \leq q+1$), this is equivalent to $H_{\mathcal{N}}(\alpha) \leq T/H_{fin}(\alpha)$, where

$$H_{fin}(\alpha)^d = \prod_{v \nmid \infty} N_v(\sigma_v(\alpha))^{d_v}$$

is the product over all finite places. In view of (2.2) and (5.7) this product is exactly $[\mathfrak{A}]^{-1}$. The present lemma follows at once.

Finally our Proposition drops out using the estimates of Lemma 7. We just have to remember that the regulator R_K is the absolute value of any maximal subdeterminant of the matrix with q rows and $q+1$ columns formed with the map (5.5) evaluated on basis elements of U , while the volume V_F of the fundamental domain is the square root of the sums of the squares of these same subdeterminants. This completes the proof.

REFERENCES

1. J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, New York, 1959. MR0157947 (28:1175)
2. S.-J. Chern and J. D. Vaaler, *The distribution of values of Mahler's measure*, J. reine angew. Math. **540** (2001), 1–47. MR1868596 (2003a:11137)
3. H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183. MR0043821 (13:323d)
4. J. Franke, Y. I. Manin and Y. Tschinkel, *Rational points of bounded height on Fano varieties*, Invent. Math. **95** (1989), 421–435. MR0974910 (89m:11060)
5. X. Gao, *On Northcott's Theorem*, Ph.D. Thesis, University of Colorado (1995).
6. S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1970. MR0282947 (44:181)
7. A. Leutbecher, *Zahlentheorie*, Springer-Verlag, Berlin, 1996.
8. C. Liebendörfer, *Linear equations and heights over division algebras*, Ph.D. Thesis, Basel (2002).
9. K. Mahler, *On the zeros of the derivative of a polynomial*, Proc. Royal Soc. London, Ser. A **264** (1961), 145–154. MR0133437 (24:A3271)
10. D. Masser and J. D. Vaaler, *Counting algebraic numbers with large height I*, submitted for publication.
11. D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Phil. Soc. **45** (1949), 502–509 and 510–518. MR0033094 (11:390a)
12. E. Peyre, *Hauteurs et mesures de Tamagawa sur les variétés de Fano*, Duke Math. J. **79** (1995), 101–218. MR1340296 (96h:11062)
13. S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), 433–449. MR0557080 (81c:12025)
14. W. M. Schmidt, *On heights of algebraic subspaces and diophantine approximations*, Ann. Math. **85** (1967), 430–472. MR0213301 (35:4165)
15. W. M. Schmidt, *Northcott's theorem on heights I. A general estimate*, Monatsh. Math. **115** (1993), 169–181. MR1223249 (94b:11054)
16. W. M. Schmidt, *Northcott's theorem on heights II. The quadratic case*, Acta Arith. **LXX.4** (1995), 343–375. MR1330740 (96a:11059)
17. W. M. Schmidt, *Heights of algebraic points*, Number Theory and its Applications (C. Y. Yildirim and S. A. Stepanov, eds.), Marcel Dekker, 1999, pp. 185–225. MR1661668 (2000b:11076)
18. P. G. Spain, *Lipschitz: a new version of an old principle*, Bull. London Math. Soc. **27** (1995), 565–566. MR1348710 (96g:11072)
19. J. L. Thunder, *An asymptotic estimate for heights of algebraic subspaces*, Trans. Amer. Math. Soc. **331** (1992), 395–424. MR1072102 (92g:11062)
20. J. L. Thunder, *The number of solutions of bounded height to a system of linear equations*, J. Number Theory **43** (1993), 228–250. MR1207503 (94a:11045)

MATHEMATISCHES INSTITUT, UNIVERSITÄT BASEL, RHEINSPRUNG 21, 4051 BASEL, SWITZERLAND

E-mail address: David.Masser@unibas.ch

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS AT AUSTIN, 1 UNIVERSITY STATION C1200, AUSTIN, TEXAS 78712

E-mail address: vaaler@math.utexas.edu