Dott. Mag. Fabrizio BARROERO

Counting lattice points, o-minimal structures and applications

DISSERTATION

zur Erlangung des akademischen Grades eines Doktors der technischen Wissenschaften

Doktoratsstudium der Technischen Wissenschaften im Rahmen der Doktoratsschule "Mathematik und Wissenschaftliches Rechnen"

Graz University of Technology

Technische Universität Graz

Betreuer:
Univ.-Prof. Dr.phil. Robert F. TICHY

Institut für Analysis und Computational Number Theory
(Math A)

Graz, im Oktober 2013

Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

....

date (signature)

Contents

Acknowledgments

First, I would like to thank my supervisor Prof. Robert Tichy, for his constant support and encouragement. I also thank Martin Widmer for sharing his ideas and his time and for his constant guidance.

I would like to thank the Austrian Science Fund (FWF) for funding the doctoral school DK "Discrete Mathematics", which I am part of, and Prof. Wolfgang Woess, Ecaterina Sava-Huss and Wilfried Huss as speaker and coordinators of the DK.

Many thanks go to all my colleagues and friends in Graz for all the great time spent together. In particular, I would like to thank Ante, Christian, Christoph, Christopher, Daniel K., Daniel S., Daniele, Dijana, Elisabetta, Elvira, Florian, Giulio, Jochen, Johannes, Maria Rita, Milton, Nina, Rosi, Tanja and Volker.

I shall also thank the Institute for Computational and Experimental Research in Mathematics (ICERM) and the department of Mathematics of the University of Texas at Austin for their hospitality during my staying there.

I would like to thank everybody who somehow influenced me in my, still ongoing, journey to mathematical maturity, in particular, Laura Capuano, Zoé Chatzidakis, Clemens Fuchs, Alfred Geroldinger, Peter Grabner, Vincenzo Mantova, Khoa Nguyen, Lukas Pottmeyer, Harry Schmidt, Tom Tucker and Jeffrey Vaaler.

Finally, I would like to thank my family, my girlfriend Ilaria and all my friends for their constant encouragement.

Introduction

Counting lattice points in bounded subsets of the Euclidean space $\mathbb{R}^n$ is a problem that arises frequently in number theory and other branches of mathematics. By a general principle, if the set S is "nice" one expects a good estimate for the number of points of a lattice Λ in S to be given by $\mathrm{Vol}(S)/\det\Lambda$, the ratio between the volume of S and the determinant of Λ. So, the problem is to find under what conditions we have good upper bounds for

$$E_{S,\Lambda} = \left| |S \cap \Lambda| - \frac{\mathrm{Vol}(S)}{\det \Lambda} \right|.$$

In the literature there are two different type of conditions for S. The first, associated to Lipschitz, requires the boundary of S to be parameterizable by finitely many maps satisfying a Lipschitz condition. The second dates back to Davenport and requires a bound on the number of connected components of the intersections of S, and its projections to coordinate subspaces, with lines. Moreover, the volumes of such projections need to be controlled.

Of course, to have a meaningful result we want the error $E_{S,\Lambda}$ to be small, but, regarding applications, it is also important that the dependence on the lattice is explicit, and that the conditions on S are not too restrictive and easily checkable.

Here and always in this thesis, a lattice in $\mathbb{R}^n$ is intended to be full rank, i.e., the $\mathbb{Z}$-span of n linearly independent vectors of $\mathbb{R}^n$.

As already mentioned, there are two different principles appearing in the literature. The older one dates back to Lipschitz and has been developed by several authors: Lang [15], Spain [25], Schmidt [24], Masser and Vaaler [16] and Widmer [29], who has the most refined version we are going to state below, after the following definitions.

A subset S of $\mathbb{R}^n$ is said to be in $\mathrm{Lip}(n, M, L)$ if there are M maps $\phi_1, \ldots, \phi_M : [0,1]^{n-1} \to \mathbb{R}^n$ satisfying the Lipschitz condition

$$|\phi_i(\boldsymbol{x}) - \phi_i(\boldsymbol{y})| \leq L|\boldsymbol{x} - \boldsymbol{y}| \text{ for } \boldsymbol{x}, \boldsymbol{y} \in [0,1]^{n-1},$$

such that S is covered by the images of the maps ϕ_i. Moreover, we write $\lambda_i = \lambda_i(\Lambda)$, for $i = 1, \ldots, n$, for the successive minima of Λ with respect to the zero-centered unit ball $B_0(1)$, i.e., for $i = 1, ..., n$,

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

THEOREM 1 (Widmer, [29], Theorem 5.4). *Let Λ be a lattice in $\mathbb{R}^n$ with successive minima $\lambda_1, \dots, \lambda_n$. Let S be a bounded set in $\mathbb{R}^n$ such that the boundary ∂S of S is in $Lip(n, M, L)$. Then S is measurable, and, moreover,*

$$\left| |S \cap \Lambda| - \frac{\mathrm{Vol}(S)}{\det \Lambda} \right| \leq c_2(n) M \max_{0 \leq i < n} \frac{L^i}{\lambda_1 \dots \lambda_i}.$$

For $i = 0$ the expression in the maximum is understood as 1. Furthermore one can choose $c_2(n) = n^{3n^2/2}$.

The Lipschitz parameterizability of the boundary is a rather mild condition and often easily checkable. However, if the volume of S is not much larger than its diameter, it might be difficult to get non-trivial estimates from the theorem above. Let us illustrate this phenomenon with the following example.

Suppose we want to estimate the number of points with integer coordinates in the set

$$S(T) = \left\{ (x_1, x_2, x_3) \in [0, +\infty)^3 : \prod_{i=1}^{3} \max\{1, x_i\} \leq T \right\}, \tag{1}$$

where T is a positive real parameter. The volume of $S(T)$ has order $T(\log T)^2$. The boundary of $S(T)$ is certainly Lipschitz parameterizable by a fixed number of maps but it is not clear how to avoid L to be of order T and thus the error term to be of order T^2. Therefore, Theorem 1 does not give an asymptotic formula, but only an inequality $|S(T) \cap \mathbb{Z}^n| \ll T^2$, which is far from being sharp since $|S(T) \cap \mathbb{Z}^n| \sim T(\log T)^2$, as we are going to see later.

The second and more recent principle dates back to Davenport.

THEOREM 2 (Davenport, [8]). *Let n be a positive integer, and let S be a compact set in $\mathbb{R}^n$ that satisfies the following conditions.*

1. *Any line parallel to one of the n coordinate axes intersects S in a set of points, which, if not empty, consists of at most h intervals.*
2. *The same is true (with j in place of n) for any of the j dimensional regions obtained by orthogonally projecting S on one of the coordinate spaces defined by equating a selection of $n-j$ of the coordinates to zero, and this condition is satisfied for all j from 1 to $n-1$.*

Then

$$||S \cap \mathbb{Z}^n| - \mathrm{Vol}(S)| \leq \sum_{j=0}^{n-1} h^{n-j} V_j(S),$$

where $V_j(S)$ is the sum of the j-dimensional volumes of the orthogonal projections of S on the various coordinate spaces obtained by equating any $n-j$ coordinates to zero, and $V_0(S) = 1$ by convention.

The first drawback of this theorem is that it is stated only for the standard lattice $\mathbb{Z}^n$ and for compact sets but, as we are going to see later, it is easy to deduce from it a more general counting theorem. Moreover, finding a bound for the constant h can be difficult.

On the other hand, Theorem 2 yields non-trivial estimates also for the set (1), despite the fact that its diameter is large. Indeed, the volumes of the projections of $S(T)$ onto any coordinate subspace have size at most $T \log T$. Therefore, since $S(T)$ satisfies condition 1. and 2. with $h = 1$, Davenport's theorem gives the asymptotic formula

$$|S(T) \cap \mathbb{Z}^n| = \frac{1}{2} T (\log T)^2 + O(T(\log T)).$$

At this point, it may be worthwhile pointing out that the conditions of these two counting principles are not totally unrelated. While the Lipschitz condition certainly does not imply the existence of a finite Davenport's h, the other implication might hold in some form, as pointed out by Masser and Vaaler in [16]. In [30], Widmer investigated this problem and proved results for convex sets and for sets in $\mathbb{R}^2$.

Theorem 2 has been generalized to arbitrary lattices by Thunder [26]. Schmidt ([23], Lemma 1) also proves a variant of Theorem 2 for arbitrary lattices in $\mathbb{R}^n$, but he assumes that the set S is contained in a zero centered ball of radius r, and gets an error term of order r^{n-1}. Hence, this result is also not directly applicable to get non-trivial estimates in sets of the form (1).

In applications, in stead of a single set S, one often deals with a parameterized family $Z \subseteq \mathbb{R}^{m+n}$ of subsets of $\mathbb{R}^n$, with fibers

$$Z_{\boldsymbol{t}} = \{\boldsymbol{x} \in \mathbb{R}^n : (\boldsymbol{t}, \boldsymbol{x}) \in Z\},$$

for $\boldsymbol{t} \in \mathbb{R}^m$, and is interested in getting an asymptotic formula as the parameters range through an unbounded set of $\mathbb{R}^m$, as, for instance, in example (1).

Let Z be a family with compact fibers. Using Minkowski's second Theorem, it is possible to deduce the following estimate from Thunder's work

$$\left| |Z_{\boldsymbol{t}} \cap \Lambda| - \frac{\mathrm{Vol}(Z_{\boldsymbol{t}})}{\det \Lambda} \right| \leq c_n \sum_{j=0}^{n-1} h'(Z_{\boldsymbol{t}})^{n-j} \frac{V_j'(Z_{\boldsymbol{t}})}{\lambda_1 \dots \lambda_j}, \tag{2}$$

where c_n is an explicit constant depending only on n, $V_j'(Z_{\boldsymbol{t}})$ is the supremum of the volumes of the orthogonal projections of $Z_{\boldsymbol{t}}$ to the j-dimensional linear subspaces, and h' is what we get instead of h when in Davenport's conditions *"line parallel to one of the n coordinate axes"* and *"orthogonally projecting $Z_{\boldsymbol{t}}$ on one of the coordinate spaces defined by equating a selection of $n-j$ of the coordinates to zero"* are replaced by *"line"* and *"any projection of $Z_{\boldsymbol{t}}$ on any j-dimensional subspace"*.

Now, the quantity $V_j'(Z_{\boldsymbol{t}})$ is definitely not so nice to work with as $V_j(Z_{\boldsymbol{t}})$. Moreover, proving the existence of a uniform upper bound

for $h'(Z_{\boldsymbol{t}})$ (i.e., independent of $\boldsymbol{t}$) is even more troublesome than for Davenport's h.

Therefore, it would be nice to have some general and mild conditions on the family Z that allow us to replace $h'(Z_{\boldsymbol{t}})$ by a uniform constant c_Z and $V_j'(Z_{\boldsymbol{t}})$ by $V_j(Z_{\boldsymbol{t}})$.

Note that, even if the sets $Z_{\boldsymbol{t}}$ are simply given by a finite number of squares in $\mathbb{R}^2$, we cannot expect that $V_j'(Z_{\boldsymbol{t}}) \leq cV_j(Z_{\boldsymbol{t}})$, for some constant c independent of $\boldsymbol{t}$. Example 2.67 of [1] gives an example of such phenomenon. Let C_1 be the unit interval. Suppose C_n is defined and is a finite union of intervals. Then C_{n+1} is obtained by dividing each of the intervals constituting C_n into 4 parts of the same length and dropping the second and the third intervals. Then $C_n \times C_n$ is a family of sets in $\mathbb{R}^2$, whose projection on one fixed line is constant, while the volumes of the projections on the two axes tend to zero as the parameter tends to infinity (see Figure 1).

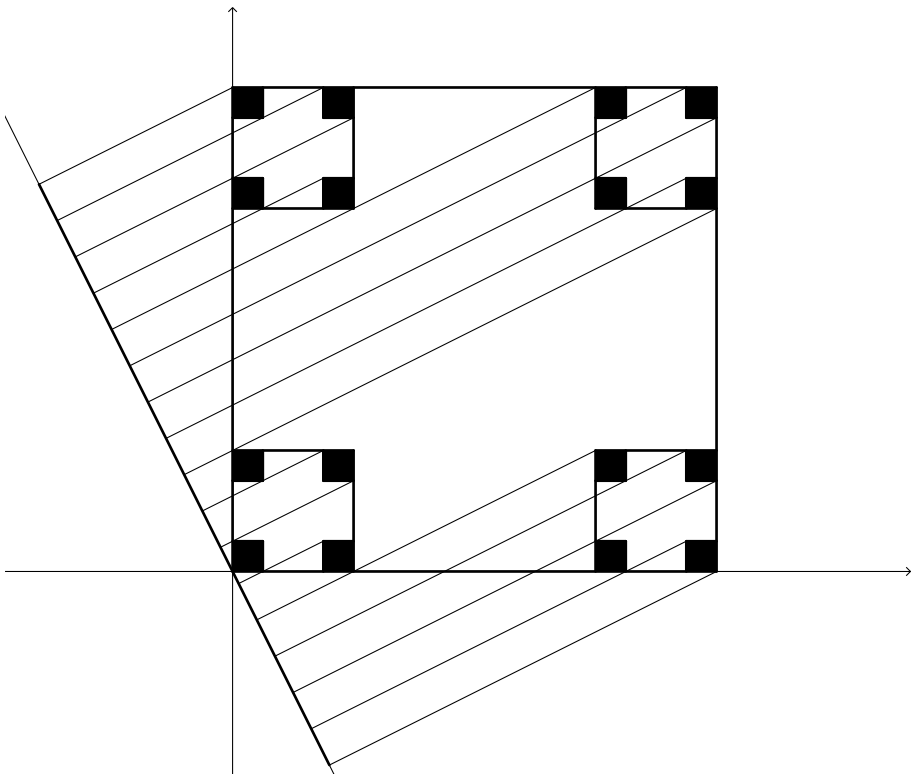

FIGURE 1. $C_3 \times C_3$

The latter example indicates that such an inequality would require a rather strong hypothesis on the family Z. Also, to handle h' we need that the number of connected components of a projection of $Z_{\boldsymbol{t}}$ when intersected with a line is uniformly bounded. Such a tameness in the topology of the family Z is delivered by o-minimality.

The theory of o-minimal structures comes from model theory and has been developed quite recently, starting from the '80s. Lately, after the work of Pila and Wilkie [18], o-minimality has given very important and promising applications to number theory, diophantine geometry in particular. For interesting and precise accounts on such applications we refer to the survey papers by Scanlon [19], [20], and to the book of Zannier [32].

Let us give the definition of an o-minimal structure.

DEFINITION 1. *An o-minimal structure is a sequence $\mathcal{S} = (\mathcal{S}_n)_{n\in\mathbb{N}}$ such that for each n:*

1) $\mathcal{S}_n$ is a boolean algebra of subsets of $\mathbb{R}^n$, that is, $\mathcal{S}_n$ is a collection of subsets of $\mathbb{R}^n$, $\emptyset \in \mathcal{S}_n$, and if $A, B \in \mathcal{S}_n$ then also $A \cup B \in \mathcal{S}_n$, and $\mathbb{R}^n \backslash A \in \mathcal{S}_n$.
2) If $A \in \mathcal{S}_n$ then $\mathbb{R} \times A \in \mathcal{S}_{n+1}$ and $A \times \mathbb{R} \in \mathcal{S}_{n+1}$.
3) $\{(x_1, \ldots, x_n) : x_i = x_j\} \in \mathcal{S}_n$ for $1 \leq i < j \leq n$.
4) If $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$ is the projection map on the first n coordinates and $A \in \mathcal{S}_{n+1}$ then $\pi(A) \in \mathcal{S}_n$.
5) $\{r\} \in \mathcal{S}_1$ for any $r \in \mathbb{R}$ and $\{(x, y) \in \mathbb{R}^2 : x < y\} \in \mathcal{S}_2$.
6) The only sets in $\mathcal{S}_1$ are the finite unions of intervals and points. ("Interval" always means "open interval" with infinite endpoints allowed.)

Following the usual convention, we say that a set $A \subseteq \mathbb{R}^n$ is definable (in $\mathcal{S}$) if it lies in $\mathcal{S}_n$. Moreover a function $f : A \to \mathbb{R}^m$ is said to be definable if its graph $\Gamma(f) \subseteq \mathbb{R}^{n+m}$ is a definable set.

Note that axiom 6) completely characterizes $\mathcal{S}_1$, which is the same for every o-minimal structure. Nonetheless, o-minimality is a rich and broad setting and we hope to convince the reader of this with the examples below, in which we follow the presentation of Scanlon in [19].

For each $n \in \mathbb{N}$, let F_n be a collection of functions $f : \mathbb{R}^n \to \mathbb{R}$ that we call distinguished functions. If $g, h : \mathbb{R}^n \to \mathbb{R}$ are built from the coordinate functions, constant functions and distinguished functions by appropriate composition, then we say that

$$\{\boldsymbol{x} \in \mathbb{R}^n : g(\boldsymbol{x}) < h(\boldsymbol{x})\},$$
$$\{\boldsymbol{x} \in \mathbb{R}^n : g(\boldsymbol{x}) = h(\boldsymbol{x})\}$$

are atomic sets. Now let us consider the smallest family of sets in $\mathbb{R}^n$ (for various n) that contains all atomic sets, and is closed under finite unions and complements, and images of the usual projection maps $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$ onto the first n coordinates. For the following choices of $F = \bigcup_n F_n$, the resulting family consists precisely of the definable sets in a particular o-minimal structure:

1. $F_{\text{alg}} = \{\text{polynomials defined over } \mathbb{R}\}$,
2. $F_{\text{an}} = F_{\text{alg}} \cup \{\text{restricted analytic functions}\}$,
3. $F_{\exp} = F_{\text{alg}} \cup \{\text{the exponential function } \exp : \mathbb{R} \to \mathbb{R}\}$,

4. $F_{\text{an,exp}} = F_{\text{an}} \cup F_{\text{exp}}$.

By a restricted analytic function we mean a function $f : \mathbb{R}^n \to \mathbb{R}$, which is zero outside of $[-1,1]^n$, and is the restriction to $[-1,1]^n$ of a function, which is real analytic on an open neighborhood of $[-1,1]^n$.

For the first example note that by the Tarski-Seidenberg Theorem every set in this family is a boolean combination of atomic sets, and thus is semialgebraic. This implies 6) in Definition 1, and 1)-5) are clear. The o-minimality of example 2. is due to Denef and van den Dries [9], who realized that it follows from results of Gabrielov [12], while 3. is due to Wilkie [31]. Van den Dries and Miller [11] proved the o-minimality of the fourth example.

Note that if the function $\sin x$, globally defined on $\mathbb{R}$, is in F_1 then we do not have an o-minimal structure. In fact, the set $\{x \in \mathbb{R} : \sin x = 0\}$ would be a definable set consisting of infinitely many isolated points, violating axiom 6) of Definition 1. On the other hand the function $\sin_{[a,b]} x$, which coincides with $\sin x$ on the interval $[a,b]$ (for $a, b \in \mathbb{R}$) and is 0 elsewhere, is definable in the o-minimal structure corresponding to the second example above.

Semialgebraic sets have been object of study for a long time and much is known about them. Many of the results in real algebraic geometry have been an inspiration for generalizations to the o-minimal setting. One of these results and probably the most important is the Cell Decomposition Theorem, which says that each definable set can be partitioned in a finite number of cells, particularly simple definable sets. It is hard to overestimate the strength and the importance of this result. In fact, in almost every proof of a non-trivial fact about definable sets in an o-minimal structure this theorem is invoked repeatedly. For instance, suppose $Z \in \mathbb{R}^{m+n}$ is a definable set. We call Z a definable family. Then the Cell Decomposition Theorem implies that there exists a uniform bound on the number of connected components of the fibers $Z_{\boldsymbol{t}}$.

The Cell Decomposition Theorem has many other consequences but most of the times the structure needs to be rich enough. In other words, many results require the structure to contain the semialgebraic sets. If this is the case then, for instance, the derivative of a definable function is definable and it is possible to prove an improved Cell Decomposition Theorem in which the cells are defined by C^1 functions. For details on this and other results we refer to the fundamental book [10] by van den Dries.

Let us go back to our setting. We fix an o-minimal structure containing the semialgebraic sets. Recall the definition of h' below (2). Then, the uniform bound on the number of connected components mentioned above implies that, if Z is a definable family, there exists a natural number M_Z, depending only on Z, such that $h'(Z_{\boldsymbol{t}}) \leq M_Z$ for

every $\boldsymbol{t} \in \mathbb{R}^m$. Therefore we can substitute the factor $h'(Z_{\boldsymbol{t}})^{n-j}$ in (2) with a constant depending on Z but independent of $\boldsymbol{t}$ and Λ.

Using deeper results from o-minimality combined with tools from geometric measure theory, it is also possible to prove the desired volume inequality and thus to substitute $V_j'(Z_{\boldsymbol{t}})$ with $V_j(Z_{\boldsymbol{t}})$ in (2). The strategy to deduce the inequality is, roughly speaking, as follows. For each $1 \leq j \leq n-1$ and any j-dimensional subspace Σ we construct a j-dimensional definable subset of $Z_{\boldsymbol{t}}$ that projects to Σ with maximal volume. Locally, the volume of the projection to Σ can be bounded by the sum of the volumes of the projections onto the j-dimensional coordinate spaces, so globally we only have to worry about these projections being non-injective. However, o-minimality provides a bound for the number of pre-images for each such projection, which is uniform in $\boldsymbol{t}$ and Σ, and this is sufficient.

Therefore, we obtain the following theorem.

THEOREM 3 ([5], Theorem 1.3). *Let m and n be positive integers, let $Z \subseteq \mathbb{R}^{m+n}$ be a definable 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 Z, such that*

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

where for $j = 0$ the term in the sum is to be understood as 1.

There are various advantages in using this theorem. First, the setting of o-minimal structures is broad and general and includes many classes of sets that appear in applications. Moreover, it is often easy to prove that a given family is definable in an o-minimal structure.

In addition, opposed to what mentioned before about the other counting theorems, $\mathrm{Vol}(Z_{\boldsymbol{t}})$ needs not be much larger than the diameter of $Z_{\boldsymbol{t}}$. For instance, recalling the example above, one can easily obtain a non-trivial estimate for the number of points of an arbitrary lattice in the sets $S(T)$ defined in (1).

Another feature of the theorem is the completely explicit dependence of the error term on the lattice. This is very important in certain applications as we are going to explain later.

We should also mention the fact that the error term is best-possible, up to the constant c_Z. To see this consider $\Lambda = \lambda_1 \boldsymbol{e}_1 \mathbb{Z} + \dots + \lambda_n \boldsymbol{e}_n \mathbb{Z}$ with $0 < \lambda_1 \leq \dots \leq \lambda_n$, where $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ is the standard basis of $\mathbb{R}^n$, and the semialgebraic set Z, defined as the union of $Z^{(j)} = \{(t, \boldsymbol{x}) \in \mathbb{R}^{1+n} : t \geq 0, \boldsymbol{x} \in ([0,t]^j \times \{0\}^{n-j} + \lambda_j \boldsymbol{e}_j)\}$ taken over $j = 1, \dots, n-1 > 0$. Hence, for $t \geq 0$ we get

$$\left| |Z_t \cap \Lambda| - \frac{\mathrm{Vol}(Z_t)}{\det \Lambda} \right| = \sum_{j=1}^{n-1} \prod_{p=1}^{j} \left(\left[\frac{t}{\lambda_p} \right] + 1 \right) \geq 2^{-n} \sum_{j=0}^{n-1} \frac{V_j(Z_t)}{\lambda_1 \dots \lambda_j}.$$

In what follows, we will apply Theorem 3 to count certain algebraic points of bounded height.

The simplest definition of the Weil height involves the Mahler measure of a polynomial. Let $f = z_0X^d + z_1X^{d-1} + \cdots + z_d \in \mathbb{C}[X]$ be a non-constant polynomial of degree d with roots $\alpha_1, \ldots, \alpha_d$. The Mahler measure of f is defined to be

$$M(f) = |z_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

Moreover, for $z \in \mathbb{C}$, we set $M(z) = |z|$.

Now, let α be an algebraic number. We can associate to it its minimal polynomial $a_0X^d + \cdots + a_d \in \mathbb{Z}[X]$, i.e., the non-zero polynomial of smallest degree vanishing at α with coprime coefficients and positive leading coefficient. Then the multiplicative Weil height of α, $H : \overline{\mathbb{Q}} \to [1, \infty)$, is defined to be

$$H(\alpha)^d = M(a_0X^d + \cdots + a_d).$$

There exists an equivalent definition of the Weil height in terms absolute values of a number field which naturally extends to vectors. 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 $\mathcal{O}_k$, the ring of integers of 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 $v \nmid \infty$,

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

for every $\alpha \in k \setminus \{0\}$, where $\mathfrak{N}(\mathfrak{p}_v)$ is the norm of $\mathfrak{p}_v$ from k to $\mathbb{Q}$ and $\mathrm{ord}_{\mathfrak{p}_v}(\alpha)$ is the power of $\mathfrak{p}_v$ in the factorization of the principal 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 multiplicative Weil height $H : k^n \to [1, \infty)$ is defined by

$$H(\alpha_1, \ldots, \alpha_n) = \prod_{v \in M_k} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{\frac{d_v}{m}}.$$

Note that for $\alpha \in k \setminus \{0\}$, $|\alpha|_v \neq 1$ for finitely many v so that the above is actually a finite product.

This definition is independent of the field containing the coordinates and therefore it can be extended to $\overline{k}^n$, where $\overline{k}$ is an algebraic closure

of k. For properties of the Weil height we refer to the first chapter of [6].

We set

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

where $k(\boldsymbol{\alpha})$ is the field obtained by adjoining all the coordinates of $\boldsymbol{\alpha}$ to k. By Northcott's Theorem [17], 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

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

Various results about this counting function appeared in the literature. One of the earliest is a result of Schanuel [21] who gave an asymptotic formula for $N(k(n,1),\mathcal{H})$. Schmidt was the first to consider the case $e > 1$. In [22], he found upper and lower bounds for $N(k(n,e),\mathcal{H})$ while in [23], he gave asymptotics for $N(\mathbb{Q}(n,2),\mathcal{H})$. Shortly afterwards, Gao [13] found the asymptotics for $N(\mathbb{Q}(n,e),\mathcal{H})$, provided $n > e$. Later Masser and Vaaler [16] established an asymptotic estimate for $N(k(1,e),\mathcal{H})$. Finally, Widmer [28] 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 thesis we investigate the asymptotics for certain sets of integral points.

Let $\mathcal{O}_k$ and $\mathcal{O}_{\overline{k}}$ be, respectively, the ring of algebraic integers of k and $\overline{k}$. We introduce

$$\mathcal{O}_k(n,e) = k(n,e) \cap \mathcal{O}_{\overline{k}}^n = \{\boldsymbol{\beta} \in \mathcal{O}_{\overline{k}}^n : [k(\boldsymbol{\beta}) : k] = e\}.$$

Possibly, the first asymptotic result (besides the trivial cases $\mathcal{O}_{\mathbb{Q}}(n,1) = \mathbb{Z}^n$) can be found in Lang's book [14]. Lang states, without proof,

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

where $m = [k : \mathbb{Q}]$, q is the rank of the unit group of $\mathcal{O}_k$, and γ_k is an unspecified positive constant, depending on k. More recently, Widmer [27] established the following asymptotic formula

$$N(\mathcal{O}_k(n,e),\mathcal{H}) = \sum_{i=0}^{t} D_i \mathcal{H}^{men} (\log \mathcal{H}^{men})^i + O(\mathcal{H}^{men-1} (\log \mathcal{H})^t), \tag{3}$$

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. Widmer's result is fairly specific in the sense that he works only with the absolute non-logarithmic Weil height H. On the other hand, the methods used in [27] are quite general and powerful, and can probably be applied to handle other heights (such as the heights used by Masser and Vaaler in [16] to deduce their main result). As mentioned in [27] this might lead to multiterm expansions as in (3) for $N(\mathcal{O}_k(1,e),\mathcal{H})$.

However, for the moment, such generalizations of (3) are not available, and thus the work [27] does not provide any results in the case $n = 1$ and $e > 1$.

But Chern and Vaaler in [7] proved an asymptotic formula for the number of monic polynomials in $\mathbb{Z}[X]$ of given degree and bounded Mahler measure. Theorem 6 of [7] immediately implies the following result

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

for some explicitly given positive real constant C_e.

Analogously, one can try to estimate $N(\mathcal{O}_k(1,e),\mathcal{H})$ by counting monic irreducible polynomials of degree e in $\mathcal{O}_k[X]$, that take bounded value under some function associated to the height of the roots. This is similar to the strategy of [16], in which the asymptotics for $N(k(1,e),\mathcal{H})$ is derived from an estimate for the number of monic irreducible polynomials f of degree e in $k[X]$ with $M_0(f) \leq \mathcal{H}$, where M_0 is some function $k[X] \to [0,\infty)$ related to the Mahler Measure. Using this approach it is possible to find an asymptotic formula for $N(\mathcal{O}_k(1,e),\mathcal{H})$.

For positive rational integers e we define

$$C_{\mathbb{R},e} = 2^{e-M}\left(\prod_{l=1}^{M}\left(\frac{2l}{2l+1}\right)^{e-2l}\right)\frac{e^M}{M!}, \tag{4}$$

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

$$C_{\mathbb{C},e} = \pi^e\frac{e^e}{(e!)^2}. \tag{5}$$

And, finally, let

$$C_k^{(e)} = \frac{e^{2q+1}2^{se}m^q}{q!\left(\sqrt{|\Delta_k|}\right)^e}C_{\mathbb{R},e}^r C_{\mathbb{C},e}^s,$$

where $m = [k:\mathbb{Q}]$, r is the number of real embeddings of k, s the number of pairs of complex conjugate embeddings, $q = r + s - 1$, and Δ_k denotes the discriminant of k.

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 4 ([3], Theorem 1.1). *Let e be a positive integer, and let k be a number field of degree m over $\mathbb{Q}$. Then, as $\mathcal{H} \geq 2$ tends to infinity, we have*

$$N(\mathcal{O}_k(1,e),\mathcal{H}) = C_k^{(e)}\mathcal{H}^{me^2}(\log\mathcal{H})^q + \begin{cases} O\left(\mathcal{H}^{me^2}(\log\mathcal{H})^{q-1}\right), & \text{if } q \geq 1, \\ O\left(\mathcal{H}^{e(me-1)}\mathcal{L}\right), & \text{if } q = 0, \end{cases}$$

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

Let us mention two simple examples. The number of algebraic integers α quadratic over $\mathbb{Q}(\sqrt{2})$ with $H(\alpha) \leq \mathcal{H}$ is

$$32\mathcal{H}^8 \log \mathcal{H} + O(\mathcal{H}^8).$$

In case $e = 3$, we have

$$108\sqrt{2}\mathcal{H}^{18} \log \mathcal{H} + O(\mathcal{H}^{18})$$

algebraic integers α cubic over $\mathbb{Q}(\sqrt{2})$ with $H(\alpha) \leq \mathcal{H}$.

As mentioned above, the problem translates to counting the minimal polynomials over k of the elements of $\mathcal{O}_k(1, e)$. We define a function

$$\begin{array}{rccl} M^k: & k[X] & \to & [0, \infty) \\ & f & \mapsto & \prod_{i=1}^{r+s} M(\sigma_i(f))^{\frac{d_i}{m}}, \end{array}$$

where the σ_i are the embeddings of k into $\mathbb{C}$, acting on the coefficients of f, indexed in the usual way, i.e., $\sigma_1, \ldots, \sigma_r$ are the real embeddings and $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ are the complex ones, with $\sigma_{r+j} = \overline{\sigma}_{r+s+j}$, for $j = 1, \ldots, s$. Moreover, $d_1 = \cdots = d_r = 1$ and $d_{r+1} = \cdots = d_{r+s} = 2$.

One can prove that, if $\alpha \in \mathcal{O}_k(1, e)$ and f is its minimal polynomial over k, then $H(\alpha)^e = M^k(f)$. Therefore, if $\widetilde{\mathcal{M}}^k(e, \mathcal{H})$ is the the set of monic irreducible $f \in \mathcal{O}_k[X]$ of degree e and $M^k(f) \leq \mathcal{H}$, we have $N\left(\mathcal{O}_k(1, e), \mathcal{H}\right) = e \left|\widetilde{\mathcal{M}}^k(e, \mathcal{H}^e)\right|$. Now, after showing that the number of reducible polynomials is negligible, the problem finally translates to counting points of the lattice consisting of the embedding of $(\mathcal{O}_k)^n$ into $\mathbb{R}^{mn}$ inside

$$Z(T) = \left\{ (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{r+s}) \in (\mathbb{R}^n)^r \times \left(\mathbb{R}^{2n}\right)^s : \prod_{i=1}^{r+s} M_1(\boldsymbol{x}_i)^{d_i} \leq T \right\}, \tag{6}$$

where $M_1(\boldsymbol{x})$ is the Mahler measure of the monic polynomial with the entries of $\boldsymbol{x}$ as coefficients. Note that the set $S(T)$ defined in (1) coincides with $Z(T)$ if $n = 1$, $r = 3$ and $s = 0$.

Using results from [7] it is possible to calculate the volume of $Z(T)$ which has order $T^n(\log T)^{r+s-1}$. Whereas the diameter of $Z(T)$ has order T and, just as before for (1), a direct application of the Lipschitz counting method or of the counting theorem in [23] yields an error term of order $T^{n(r+2s)-1}$ if $r > 0$ and $T^{\frac{2sn-1}{2}}$ if $r = 0$, exceeding the main term, unless $r + s = 1$ or $(n, r, s) = (1, 2, 0)$.

On the other hand, one can prove that $V_j(Z(T)) \ll T^n(\log T)^{r+s-2}$. Therefore, Theorem 3 gives the desired estimate, provided the family Z, with fibers $Z(T)$, is definable in an o-minimal structure. This is ensured by the fact that Z is a semialgebraic family because the Mahler measure is actually a semialgebraic function.

It should be mentioned that the method developed in [27], which invokes the Lipschitz principle, can probably be used to establish precise estimates for the number of lattice points in (6), provided the lattice satisfies a certain gap principle, cf. [27], Theorem 4.1. Indeed, the embedding of $(\mathcal{O}_k)^n$ satisfies the required gap principle , but the method in [27] is rather technical and complicated. Thanks to Theorem 3 we have a simpler and more straightforward approach, although to the expense of getting a larger error term.

Note that the error term in the asymptotic formula of Theorem 4 depends only on e and the degree of k and not on the field itself. This is possible because of the completely explicit dependence on the lattice of the error term in Theorem 3.

Besides the work of Widmer [27] and Theorem 4, we are not aware of any result that deals with other choices of (n, e), therefore, the general problem of estimating $N(\mathcal{O}_k(n, e), \mathcal{H})$ remains open and not even the correct order of magnitude is known.

A further natural problem that can be investigated is to somehow generalize Theorem 4 in the direction of rings of S-integers. One naturally tries to apply the same method as before, i.e., count monic irreducible polynomials of fixed degree in $\mathcal{O}_S[X]$. Unfortunately, the image of $\mathcal{O}_S$ in $\mathbb{R}^{[k:\mathbb{Q}]}$ via the usual embedding is not a lattice, since it is dense, and thus the result cannot be obtained by a straightforward generalization of the strategy explained above. Nevertheless, it is possible to overcome these difficulties and finally obtain the desired result, which we are going to state after introducing some notation.

As before, fix a number field k of degree m over $\mathbb{Q}$. Let S be a finite set of places of k containing the archimedean ones. Let $\mathcal{O}_S$ be the ring of S-integers of k. Fix an algebraic closure $\overline{k}$ of k and let $\overline{S}$ be the set of places of $\overline{k}$ that lie above the places in S. Let $\mathcal{O}_{\overline{S}}$ be the ring of $\overline{S}$-integers of $\overline{k}$. Given n and e positive integers, we put

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

Let S_∞ be the set of archimedean places in S. If we choose $S = S_\infty$, then $\mathcal{O}_S = \mathcal{O}_k$ and clearly $\mathcal{O}_S(n, e) = \mathcal{O}_k(n, e)$.

Now, let S_{fin} be the set of non-archimedean places of S. Suppose that $v \in S_{\text{fin}}$ corresponds to the prime ideal $\mathfrak{p}_v$ of $\mathcal{O}_k$. Recall that $\mathfrak{N}(\mathfrak{p}_v)$ is the norm of $\mathfrak{p}_v$. We indicate by $\mathfrak{N}(S)$ the $|S_{\text{fin}}|$-tuple consisting of the norms of the $\mathfrak{p}_v$, for $v \in S_{\text{fin}}$. Let n be a positive integer, we put

$$B_{k,S}^{(n)} = \frac{n^{r+s-1} 2^{sn} m^{|S|-1}}{(|S|-1)! \left(\sqrt{|\Delta_k|}\right)^n} \prod_{v \in S_{\text{fin}}} \left(\frac{1}{\log \mathfrak{N}(\mathfrak{p}_v)} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p}_v)^n} \right) \right).$$

As usual, the empty product is understood to be 1. Moreover, recall the definitions (4) and (5) of $C_{\mathbb{R},e}$ and $C_{\mathbb{C},e}$ and set

$$C_{k,S}^{(e)} = e^{|S|} C_{\mathbb{R},e}^{r} C_{\mathbb{C},e}^{s} B_{k,S}^{(e)}.$$

THEOREM 5 ([2], 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,*

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

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

Note that, for S consisting of the archimedean places only, this is nothing but Theorem 4.

Theorem 5 is actually obtained from a more general result ([2], Theorem 3.1) that gives an estimate for the cardinality of $\mathcal{O}_S^n(\mathcal{H})$, the set of points $\boldsymbol{a} \in \mathcal{O}_S^n$ with $H_{\mathcal{N}}(1, \boldsymbol{a}) \leq \mathcal{H}$, where $H_{\mathcal{N}}$ is some height function on k^n.

The proof of this more general result relies again on Theorem 3 but it is not a straightforward application of it because, as mentioned above, $\mathcal{O}_S$ is not a lattice in $\mathbb{R}^m$. To overcome this problem one notices that any S-integer is contained in a non-zero fractional ideal of the form $\prod_{v \in S_{\mathrm{fin}}} \mathfrak{p}_v^{-g_v}$, for some non-negative integers g_v and that the embedding of a non-zero fractional ideal is a lattice in $\mathbb{R}^m$. One is therefore reduced to estimate the number of points of a lattice defined by some fractional ideal inside certain sets whose definition is similar to the one of $Z(T)$ in (6). This can be done using Theorem 3. Combining these estimates together and using the Möbius inversion formula, one manages to prove Theorem 3.1 of [2] and thus to derive Theorem 5.

At this point the importance of the shape of the error term of Theorem 3 should be mentioned. In fact, that explicit dependence on the lattice is essential for the combination of the estimates for different fractional ideals.

As another corollary of Theorem 3.1 of [2], one can prove the following.

THEOREM 6 ([2], 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,

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

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

Note that this is a generalization of the case $e = 1$ in (3), although with one explicit term only.

Finally, let us mention a few simple examples for both theorems. 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 $\mathbb{Z}\left[\frac{1}{p}\right]$ of height at most $\mathcal{H}$ is

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

Now, let d be a square-free positive integer with $d \equiv 3 \mod 4$. 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

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

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

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

We conclude this introduction with a summary of the four papers that constitute this thesis.

Counting lattice points and o-minimal structures

The article [5] constitute the first chapter of this thesis. This joint work with Martin Widmer has been accepted for publication by *International Mathematics Research Notices* and appeared online.

Counting algebraic integers of fixed degree and bounded height

The second chapter consists of [3], which is currently under review by a journal.

Algebraic S-integers of fixed degree and bounded height

The article [2] is the third chapter. This is a preprint and is soon going to be submitted to a journal.

Additive unit representations in global fields - A survey

Although quite unrelated to the other papers, the survey article [4] is included in this thesis as an appendix, since it has been written during my Ph.D. studies. This is joint work with Christopher Frei and Robert Tichy and offers an overview on the unit sum number problem. Special attention is given to rings of integers of algebraic number fields and matrix rings. This article is published in *Publicationes Mathematicae Debrecen*.

Bibliography

1. L. Ambrosio, N. Fusco, and D. Pallara, *Functions of Bounded Variation and Free Discontinuity problems*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 2000.
2. F. Barroero, *Algebraic S-integers of fixed degree and bounded height*, preprint.
3. ———, *Counting algebraic integers of fixed degree and bounded height*, submitted.
4. F. Barroero, C. Frei, and R. F. Tichy, *Additive unit representations in rings over global fields—a survey*, Publ. Math. Debrecen **79** (2011), no. 3-4, 291–307.
5. F. Barroero and M. Widmer, *Counting lattice points and o-minimal structures*, to appear in Int. Math. Res. Not. IMRN.
6. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.
7. S. Chern and J. D. Vaaler, *The distribution of values of Mahler's measure*, J. reine angew. Math. **540** (2001), 1–47.
8. H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.
9. J. Denef and L. van den Dries, *p-adic and real subanalytic sets*, Ann. of Math. (2) **128** (1988), no. 1, 79–138.
10. L. van den Dries, *Tame Topology and O-minimal Structures*, London Mathematical Society Lecture Note Series, vol. 248, Cambridge University Press, Cambridge, 1998. MR 1633348 (99j:03001)
11. L. van den Dries and C. Miller, *On the real exponential field with restricted analytic functions*, Israel J. Math. **85** (1994), no. 1-3, 19–56. MR 1264338 (95e:03099)
12. A. M. Gabrièlov, *Projections of semianalytic sets*, Funkcional. Anal. i Priložen. **2** (1968), no. 4, 18–30.
13. X. Gao, *On Northcott's Theorem*, Ph.D. Thesis, University of Colorado (1995).
14. S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.
15. ———, *Algebraic Number Theory*, Graduate texts in mathematics, Springer-Verlag, 1986.
16. D. Masser and J. D. Vaaler, *Counting algebraic numbers with large height. II*, Trans. Amer. Math. Soc. **359** (2007), no. 1, 427–445.
17. D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. **45** (1949), 502–509.
18. J. Pila and A. J. Wilkie, *The rational points of a definable set*, Duke Math. J. **133** (2006), no. 3, 591–616.
19. T. Scanlon, *A proof of the André-Oort conjecture using mathematical logic [after Pila, Wilkie and Zannier]*, Astérisque, Séminaire Bourbaki **1037** (2010).
20. ———, *Counting special points: logic, Diophantine geometry, and transcendence theory*, Bull. Amer. Math. Soc. (N.S.) **49** (2012), no. 1, 51–71.
21. S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), no. 4, 433–449.

22. W. M. Schmidt, *Northcott's theorem on heights. I. A general estimate*, Monatsh. Math. **115** (1993), no. 1-2, 169–181.
23. ———, *Northcott's theorem on heights II. The quadratic case*, Acta Arith. **LXX.4** (1995), 343–375.
24. ———, *The distribution of sublattices of* $\mathbf{Z}^m$, Monatsh. Math. **125** (1998), no. 1, 37–81.
25. P. G. Spain, *Lipschitz: a new version of an old principle*, Bull. London Math. Soc. **27** (1995), no. 6, 565–566.
26. J. L. Thunder, *The number of solutions of bounded height to a system of linear equations*, J. Number Theory **43** (1993), no. 2, 228–250.
27. M. Widmer, *Integral points of fixed degree and bounded height*, submitted.
28. ———, *Counting points of fixed degree and bounded height*, Acta Arith. **140** (2009), no. 2, 145–168.
29. ———, *Counting primitive points of bounded height*, Trans. Amer. Math. Soc. **362** (2010), 4793–4829.
30. ———, *Lipschitz class, narrow class, and counting lattice points*, Proc. Amer. Math. Soc. **140** (2012), no. 2, 677–689.
31. A. J. Wilkie, *Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function*, J. Amer. Math. Soc. **9** (1996), no. 4, 1051–1094.
32. U. Zannier, *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Annals of Mathematics Studies, vol. 181, Princeton University Press, 2012, With appendixes by David Masser.

COUNTING LATTICE POINTS AND O-MINIMAL STRUCTURES

FABRIZIO BARROERO AND MARTIN WIDMER

ABSTRACT. Let Λ be a lattice in $\mathbb{R}^n$, and let $Z \subseteq \mathbb{R}^{m+n}$ be a definable family in an o-minimal structure over $\mathbb{R}$. We give sharp estimates for the number of lattice points in the fibers $Z_T = \{x \in \mathbb{R}^n : (T, x) \in Z\}$. Along the way we show that for any subspace $\Sigma \subseteq \mathbb{R}^n$ of dimension $j > 0$ the j-volume of the orthogonal projection of Z_T to Σ is, up to a constant depending only on the family Z, bounded by the maximal j-dimensional volume of the orthogonal projections to the j-dimensional coordinate subspaces.

1. INTRODUCTION

Let Λ be a lattice in $\mathbb{R}^n$, and let Z be a subset of $\mathbb{R}^{m+n}$. We consider Z as a parameterized family of subsets $Z_T = \{x \subseteq \mathbb{R}^n : (T, x) \in Z\}$ of $\mathbb{R}^n$. One is often led to the problem of estimating the cardinality $|\Lambda \cap Z_T|$ as the parameter T ranges over an infinite set. According to a general principle one would expect that, if the sets Z_T are reasonably shaped, a good estimate for $|\Lambda \cap Z_T|$ is given by $\mathrm{Vol}(Z_T)/\det \Lambda$. The situation is relatively easy if $Z_T = TZ_1$ for some fixed subset Z_1 of $\mathbb{R}^n$ and as $T \in \mathbb{R}$ tends to infinity.[1] However, in many situations the family Z is more complicated, and typically described by inequalities such as

$$f_1(T_1, \dots, T_m, x_1, \dots, x_n) \leq 0, \dots, f_N(T_1, \dots, T_m, x_1, \dots, x_n) \leq 0, \tag{1.1}$$

where the f_i are certain real valued functions on $\mathbb{R}^{m+n}$, e.g., polynomials. Using the language of o-minimal structures from model theory we prove for fairly general families Z an estimate for $|\Lambda \cap Z_T|$, which is

2010 *Mathematics Subject Classification.* Primary 11H06, 03C98, 03C64; Secondary 11P21, 28A75, 52C07.

Key words and phrases. Lattice points, counting, o-minimal structure, volumes of projections, computational geometry.

F. Barroero is supported by the Austrian Science Foundation (FWF) project W1230-N13.

M. Widmer was supported in part by the Austrian Science Foundation (FWF) project M1222-N13 and ERC-Grant No. 267273.

[1]However, even if $Z_T = TZ_1$ is compact it is not necessarily true that $|\Lambda \cap Z_T| = \mathrm{Vol}(Z_1)T^n/\det \Lambda + O(T^{n-1})$, e.g., take $\Lambda = \mathbb{Z}^n$, and $Z_1 = \{0, 2^{-1}, 2^{-2}, 2^{-3}, \dots\} \times [0, 1]^{n-1}$. The latter is a counterexample to the claim in the first paragraph of [7].

quite precise in terms of the geometry of the sets Z_T, and the geometry of the lattice Λ.

A classical result, although restricted to $\Lambda = \mathbb{Z}^n$, was proven by Davenport [7, Theorem].

Theorem 1.1 (Davenport)**.** *Let n be a positive integer, and let Z_T be a compact set in $\mathbb{R}^n$ that satisfies the following conditions.*

(1) Any line parallel to one of the n coordinate axes intersects Z_T in a set of points, which, if not empty, consists of at most h intervals.

(2) The same is true (with j in place of n) for any of the j dimensional regions obtained by orthogonally projecting Z_T on one of the coordinate spaces defined by equating a selection of $n-j$ of the coordinates to zero, and this condition is satisfied for all j from 1 to $n-1$.

Then

$$||Z_T \cap \mathbb{Z}^n| - \mathrm{Vol}(Z_T)| \leq \sum_{j=0}^{n-1} h^{n-j} V_j(Z_T),$$

where $V_j(Z_T)$ is the sum of the j-dimensional volumes of the orthogonal projections of Z_T on the various coordinate spaces obtained by equating any $n-j$ coordinates to zero, and $V_0(Z_T) = 1$ by convention.

A drawback of Davenport's theorem is that the conditions (1) and (2) are often difficult to verify. Various authors have given similar estimates for general lattices with simpler, possibly milder, conditions on the set; see [33] for a discussion on that. Classical results are known for homogeneously expanding sets whose boundary is parameterizable by certain Lipschitz maps, see, e.g., [17, Theorem 5.1, Chap. 3], or [28, Theorem] for a refined version. Masser and Vaaler [18, Lemma 2] gave a counting result for sets satisfying the above Lipschitz condition but which are not necessarily homogeneously expanding, and moreover, the dependence on the lattice was made explicit. Masser and Vaaler's result was refined by the second author [31, Theorem 5.4] to get a sharp error term (for balls such sharp estimates have been obtained by Schmidt in [26, Lemma 2]). However, all these results for general lattices have one drawback in common: usually, a direct application yields nontrivial estimates only if the volume is much larger than the diameter; e.g., if $T \in \mathbb{R}$ tends to infinity we usually require $\mathrm{diam}(Z_T)^{n-1} = o(\mathrm{Vol}(Z_T))$. We shall illustrate this problem more explicitly after we have stated our theorem.

Of course, Davenport's theorem can easily be generalized to arbitrary lattices. With a bit care, using standard results from Geometry of Numbers, one gets the error term (ignoring a factor depending only on

n)

$$\sum_{j=0}^{n-1} h'(Z_T)^{n-j} \frac{V_j'(Z_T)}{\lambda_1 \cdots \lambda_j}, \tag{1.2}$$

where $\lambda_1, \ldots, \lambda_n$ are the successive minima of Λ (with respect to the zero-centered unit ball), $V_j'(Z_T)$ is the supremum of the volumes of the orthogonal projections of Z_T to the j-dimensional linear subspaces, and h' is what we get instead of h when in Davenport's conditions *"line parallel to one of the n coordinate axes"* and *"orthogonally projecting Z_T on one of the coordinate spaces defined by equating a selection of $n-j$ of the coordinates to zero"* are replaced by *"line"* and *"any projection of Z_T on any j-dimensional subspace"*.

Now the quantity $V_j'(Z_T)$ is definitely not so nice to work with as $V_j(Z_T)$. Moreover, proving the existence of uniform upper bounds for $h'(Z_T)$ (i.e., independent of T) is often troublesome and awkward. Therefore it would be nice to have some general but mild conditions on the family Z that allow us to replace $h'(Z_T)$ by a uniform constant c_Z and $V_j'(Z_T)$ by $V_j(Z_T)$.

At this point it might be worthwhile to emphasize that even if the sets Z_T are simply given by a finite number of squares in $\mathbb{R}^2$ we cannot expect that $V_j'(Z_T) \le cV_j(Z_T)$ for some absolute constant c; consider the sets $C_n \times C_n$ in [1, Example 2.67] for a simple counterexample. The latter example indicates that such an inequality would require a rather strong hypothesis on the family Z. Also, to handle h' we need that the number of connected components of a projection of Z_T when intersected with a line is uniformly bounded.

The setting of o-minimal structures delivers exactly the required topological properties, and therefore seems to be the natural framework suitable for our problem. Furthermore, it provides a rich and flexible structure, including many of the relevant examples.

We are using the notation of [9] and [7]. We write $\mathbb{N} = \{1, 2, 3, \ldots\}$ for the set of positive integers.

Definition 1.2. *An o-minimal structure is a sequence $\mathcal{S} = (\mathcal{S}_n)_{n\in\mathbb{N}}$ of families of subsets in $\mathbb{R}^n$ such that for each n:*

1. *$\mathcal{S}_n$ is a boolean algebra of subsets of $\mathbb{R}^n$, that is, $\mathcal{S}_n$ is a collection of subsets of $\mathbb{R}^n$, $\emptyset \in \mathcal{S}_n$, and if $A, B \in \mathcal{S}_n$ then also $A \cup B \in \mathcal{S}_n$, and $\mathbb{R}^n \setminus A \in \mathcal{S}_n$.*
2. *If $A \in \mathcal{S}_n$ then $\mathbb{R} \times A \in \mathcal{S}_{n+1}$ and $A \times \mathbb{R} \in \mathcal{S}_{n+1}$.*
3. *$\{(x_1, \ldots, x_n) : x_i = x_j\} \in \mathcal{S}_n$ for $1 \le i < j \le n$.*
4. *If $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$ is the projection map on the first n coordinates and $A \in \mathcal{S}_{n+1}$ then $\pi(A) \in \mathcal{S}_n$.*
5. *$\{r\} \in \mathcal{S}_1$ for any $r \in \mathbb{R}$ and $\{(x, y) \in \mathbb{R}^2 : x < y\} \in \mathcal{S}_2$.*

(6) *The only sets in $\mathcal{S}_1$ are the finite unions of intervals and points. ("Interval" always means "open interval" with infinite endpoints allowed.)*

Following the usual convention, we say a set A is definable (in $\mathcal{S}$) if it lies in some $\mathcal{S}_n$.

Next we give some important examples of o-minimal structures, following the presentation of Scanlon in [25]. For each $n \in \mathbb{N}$ let F_n be a collection of functions $f : \mathbb{R}^n \to \mathbb{R}$ that we call distinguished functions. If $g, h : \mathbb{R}^n \to \mathbb{R}$ are built from the coordinate functions, constant functions and distinguished functions by composition (provided it is defined), then we say

$$\{x \in \mathbb{R}^n : g(x) < h(x)\},$$
$$\{x \in \mathbb{R}^n : g(x) = h(x)\},$$

are atomic sets. Now let us consider the smallest family of sets in $\mathbb{R}^n$ (for various n) that contains all atomic sets, and is closed under finite unions and complements, and images of the usual projection maps $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$ onto the first n coordinates. For the following choices of $F = \bigcup_n F_n$, the resulting family consists precisely of the definable sets in a particular o-minimal structure:

(1) $F_{\text{alg}} = \{\text{polynomials defined over } \mathbb{R}\}$,
(2) $F_{\text{an}} = F_{\text{alg}} \cup \{\text{restricted analytic functions}\}$,
(3) $F_{\exp} = F_{\text{alg}} \cup \{\text{the exponential function } \exp : \mathbb{R} \to \mathbb{R}\}$,
(4) $F_{\text{an,exp}} = F_{\text{an}} \cup F_{\exp}$.

By a restricted analytic function we mean a function $f : \mathbb{R}^n \to \mathbb{R}$, which is zero outside of $[-1, 1]^n$, and is the restriction to $[-1, 1]^n$ of a function, which is real analytic on an open neighborhood of $[-1, 1]^n$.

For the first example note that by the Tarski-Seidenberg theorem every set in this family is a boolean combination of atomic sets, and thus is semialgebraic. This implies (6) in Definition 1.2, and (1)-(5) are clear. The o-minimality of example (2) is due to Denef and van den Dries [8], while (3) is due to Wilkie [34]. Van den Dries and Miller [11] proved the o-minimality of the fourth example.

From now on, and for the rest of the paper, we suppose that our o-minimal structure $\mathcal{S}$ contains the semialgebraic sets. Recall that a set A is definable if it lies in some $\mathcal{S}_n$. For a set $Z \subseteq \mathbb{R}^{m+n}$ we call $Z_T = \{x \in \mathbb{R}^n : (T, x) \in Z\}$ a fiber of Z. From this viewpoint it is natural to call Z a family. In particular, we call Z a definable family if Z is a definable set. We write $\lambda_i = \lambda_i(\Lambda)$ for $i = 1, \ldots, n$ for the successive minima of Λ with respect to the zero-centered unit ball $B_0(1)$, i.e., for $i = 1, ..., n$

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

Also 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 $\mathbb{R}^n$. We shall see that if Z is a definable family with bounded fibers Z_T then the j-dimensional volumes of the orthogonal projections of Z_T on any j-dimensional coordinate subspace of $\mathbb{R}^n$ exist and are finite, and also the volume $\mathrm{Vol}(Z_T)$ exists and is finite.

Theorem 1.3. *Let m and n be positive integers, let $Z \subseteq \mathbb{R}^{m+n}$ be a definable family, and suppose the fibers Z_T are bounded. Then there exists a constant $c_Z \in \mathbb{R}$, depending only on the family Z, such that*

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

where for $j = 0$ the term in the sum is to be understood as 1.

Up to the constant c_Z, our estimate is best-possible. To see this we take $\Lambda = \lambda_1 e_1 \mathbb{Z} + \cdots + \lambda_n e_n \mathbb{Z}$ with $0 < \lambda_1 \leq \cdots \leq \lambda_n$, and the semialgebraic set Z, defined as the union of $Z^{(j)} = \{(T, x) \in \mathbb{R}^{1+n} : T \geq 0, x \in ([0, T]^j \times \{0\}^{n-j} + \lambda_j e_j)\}$ taken over $j = 1, \ldots, n-1 > 0$. Hence, for $T \geq 0$ we get

$$\left| |Z_T \cap \Lambda| - \frac{\mathrm{Vol}(Z_T)}{\det \Lambda} \right| = \sum_{j=1}^{n-1} \prod_{p=1}^{j} \left(\left[\frac{T}{\lambda_p} \right] + 1 \right) \geq 2^{-n} \sum_{j=0}^{n-1} \frac{V_j(Z_T)}{\lambda_1 \cdots \lambda_j}.$$

Next let us consider a simple application. Suppose we want to count lattice points in the fibers Z_T of the family Z as defined in (1.1) by the 2^n polynomial functions $f_I(T, x) = \prod_I x_i^2 - T^2$, where I runs over all subsets of $\{1, 2, \ldots, n\}$, $n \geq 2$. This problem occurs if one counts algebraic integers in a totally real field k, and of bounded Weil height. Now we have $\mathrm{Vol}(Z_T) = 2^n T (\log T)^{n-1} + O(T(\log T)^{n-2})$, and moreover, $V_j(Z_T) = O(T(\log T)^{n-2})$. Obviously, our family Z is a semialgebraic set. Applying Theorem 1.3 we get an asymptotic formula.

Now suppose we want to derive a similar statement from the counting results in [18] or [31] ([17] cannot be applied as Z_T is not homogeneously expanding). Then we require to parameterize the boundary of Z_T by a finite number of Lipschitz maps $\phi : [0, 1]^{n-1} \to \mathbb{R}^n$. This can certainly be done, even with a single map. But the diameter of Z_T has size of order T, and thus the Lipschitz constant L of this map is necessarily of this size. This gives an error term of order T^{n-1} which exceeds the "main term", at least if $n > 2$. Possibly one can resolve this problem by using many parameterizing maps instead of just one. But even in this single case it is not obvious how to do this.

Now the aforementioned example of counting integers in k of bounded height is covered by more general and precise results in [32]. But in a subsequent paper [2] the first author will apply Theorem 1.3 to deduce the asymptotics of algebraic integers of bounded height and of fixed

degree over a given number field k. The special case $k = \mathbb{Q}$ follows from a result of Chern and Vaaler [6] but the general result appears to be new.

In an ongoing project we give a more elaborate application of Theorem 1.3, which, in conjunction with previous results of the second author, might lead to some new instances of Manin's conjecture on the number of k-rational points of bounded height on the symmetric square of $\mathbb{P}^n$, where k is an arbitrary number field. The special case $k = \mathbb{Q}$ follows easily from a theorem of Schmidt [27, Theorem 4a], which in turn follows from his results on the number of quadratic points of bounded height [27, Theorem 3a] and Davenport's theorem.

In recent times o-minimal structures have successfully been used for problems in number theory. Using ideas that date back to a paper by Bombieri and Pila [4], and were further developed in various articles of Pila, Pila and Wilkie [23] gave upper bounds for the number of rational points of bounded height on the transcendental part of definable sets. These results in turn have been applied to problems in Diophantine geometry (see [24], [22], [19], [20] and [16]). However, to the best of the authors' knowledge, o-minimal structures have not been used so far to establish asymptotic counting results.

The paper is organized as follows. In Section 2 we use Geometry of Numbers, and follow arguments of Thunder [29] to generalize Davenport's theorem to arbitrary lattices with an error term as in (1.2). In Section 3 we collect some basic facts about o-minimal structures, as well as some deeper results like the cell-decomposition Theorem, the Reparametrization Lemma (originally due to Yomdin [36], [35], and Gromov [15, p.232], and refined by Pila and Wilkie [23]), and the existence of definable Skolem functions. Then, in Section 4, we use the fact that there are uniform upper bounds for the number of connected components of fibers of definable sets, to establish a uniform upper bound for our quantity h'. In Section 6 we establish a geometric inequality that allows us to substitute $V_j'(Z_T)$ of (1.2) with $V_j(Z_T)$.

This is the core argument of the paper, and the strategy is, roughly speaking, as follows. For each $1 \leq j \leq n-1$ and any j-dimensional subspace Σ we construct a j-dimensional definable subset of Z_T that projects to Σ with maximal volume. Locally, the volume of the projection onto Σ can be bounded by the sum of the volumes of the projections onto the j-dimensional coordinate spaces, so globally we only have to worry about these projections being non-injective. However, o-minimality provides a bound for the number of pre-images for each such projection, which is uniform in T and Σ, and this is sufficient.

To carry out the aforementioned strategy we require some concepts and results from geometric measure theory such as rectifiability and

Hausdorff measure/dimension, which we derive and recall in Section 5. The Reparametrization Lemma implies the required rectifiability assumptions for bounded definable sets. Finally, in Section 7 we put all together to prove Theorem 1.3.

Some of the potential users of our theorem may not be familiar with o-minimality. Therefore, we have given definitions, and proofs or references, even for the most basic concepts, and results. For the same reason we also have restricted ourselves to the set-theoretic language instead of the model-theoretic approach, although the latter often leads to simpler and quicker proofs.

2. Geometry of numbers

By [5, Lemma 8 p.135] there exists a basis $v_1, \dots, v_n$ of the lattice Λ such that $|v_i| \leq i\lambda_i$ for $i = 1, \dots, n$. We let Ψ be the automorphism of $\mathbb{R}^n$ defined by $\Psi(v_i) = e_i$, where $e_1 = (1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$ is the standard basis of $\mathbb{R}^n$. Hence, we have $\Psi(\Lambda) = \mathbb{Z}^n$.

Lemma 2.1. *Let $D \subseteq \mathbb{R}^n$ be a compact set such that $\Psi(D)$ satisfies the hypothesis (1) and (2) of Theorem 1.1. Then*

$$\left| |D \cap \Lambda| - \frac{\mathrm{Vol}(D)}{\det \Lambda} \right| \leq \sum_{j=0}^{n-1} h^{n-j} V_j(\Psi(D)),$$

Proof. Clearly, we have

$$|D \cap \Lambda| = |\Psi(D) \cap \mathbb{Z}^n|,$$

and $\mathrm{Vol}(\Psi(D)) = |\det \Psi| \mathrm{Vol}(D)$. The inverse of Ψ corresponds to the matrix with columns $v_1, \dots, v_n$, and therefore $|\det \Psi|^{-1} = \det \Lambda$. As D is compact also $\Psi(D)$ is compact. Applying Theorem 1.1 yields the claim. □

In the next two lemmas we simply reproduce arguments of Thunder from [29] to obtain an error term as anticipated in (1.2).

Let $1 \leq j \leq n-1$, let I be any subset of $\{1, \dots, n\}$ of cardinality j, and let $\overline{I}$ be its complement. Let Σ_I and Λ_I be respectively the subspace of $\mathbb{R}^n$ and the sublattice of $v_1\mathbb{Z} + \cdots + v_n\mathbb{Z}$ generated by the vectors v_i, $i \in I$. For any set $D \subseteq \mathbb{R}^n$ we define

$$D^I = \{x \in \Sigma_I : x + y \in D \text{ for some } y \in \Sigma_{\overline{I}}\}.$$

This is nothing but the projection of D to Σ_I with respect to $\Sigma_{\overline{I}}$.

Lemma 2.2. *Suppose $D \subseteq \mathbb{R}^n$ is compact. Then, for every $j = 1, \dots, n-1$,*

$$V_j(\Psi(D)) \leq \sum_{|I|=j} \frac{2^j}{B_j} \frac{\mathrm{Vol}_j\left(D^I\right)}{\lambda_1 \cdots \lambda_j},$$

where B_j is the volume of the j-dimensional unit-ball.

Proof. The orthogonal projection of $\Psi(D)$ to the coordinate subspace spanned by e_i, $i \in I$ for some choice of I, corresponds to the projection D^I of D to Σ_I with respect to $\Sigma_{\overline{I}}$. Therefore we have that

$$V_j(\Psi(D)) = \sum_{|I|=j} \frac{\mathrm{Vol}_j\left(D^I\right)}{\det\Lambda_I}.$$

As $\lambda_i(\Lambda_I) \geq \lambda_i$ for $1 \leq i \leq j$ we deduce from Minkowski's second theorem

$$\det\Lambda_I \geq \frac{B_j}{2^j}\lambda_1 \cdots \lambda_j,$$

and this proves the lemma. □

Definition 2.3. *Suppose $D \subseteq \mathbb{R}^n$ is compact, and suppose $0 < j < n$. We define $V_j'(D)$ to be the supremum of the volumes of the orthogonal projections of D to any j-dimensional linear subspace of $\mathbb{R}^n$, and we set $V_0'(D) = 1$.*

Lemma 2.4. *Suppose $D \subseteq \mathbb{R}^n$ is compact. Then for any $j = 1, \ldots, n-1$ and any $I \subseteq \{1, \ldots, n\}$ with $|I| = j$ there exists a constant $c = c(n, j)$ such that*

$$\mathrm{Vol}_j\left(D^I\right) \leq cV_j'(D).$$

Proof. Let v_i' be the vectors defined by

$$v_i' = \frac{v_1 \wedge \cdots \wedge v_{i-1} \wedge v_{i+1} \wedge \cdots \wedge v_n}{|v_1 \wedge \cdots \wedge v_n|} = \frac{v_1 \wedge \cdots \wedge v_{i-1} \wedge v_{i+1} \wedge \cdots \wedge v_n}{\det\Lambda}.$$

Now let $\Sigma_{\overline{I}}^{\perp}$ be the linear subspace generated by v_i', $i \in I$ (and thus orthogonal to $\Sigma_{\overline{I}}$). Let $\widehat{D^I}$ be the orthogonal projection of D on $\Sigma_{\overline{I}}^{\perp}$. This means

$$\widehat{D^I} = \left\{x \in \Sigma_{\overline{I}}^{\perp} : x + y \in D \text{ for some } y \in \Sigma_{\overline{I}}\right\}.$$

There exists a linear transformation φ between Σ_I and $\Sigma_{\overline{I}}^{\perp}$ that maps a point of Σ_I to its orthogonal projection on $\Sigma_{\overline{I}}^{\perp}$. Note that $\varphi(D^I) \subseteq \widehat{D^I}$ because, for every $x \in D^I$, $x = z + y$ for some $z \in D$ and $y \in \Sigma_{\overline{I}}$, and $\varphi(x) = x + y'$ for some $y' \in \Sigma_{\overline{I}}$, and thus $\varphi(x) = z + (y + y') \in \widehat{D^I}$. Moreover, φ is an injective map. Indeed, suppose we had $x, y \in \Sigma_I$ with the same image, then $x - y \in \Sigma_{\overline{I}} \cap \Sigma_I$, which means $x = y$. Therefore we can see φ as an automorphism of $\mathbb{R}^j$. We want to bound the determinant of the inverse of φ. Let

$$x = \sum_{i \in I} a_i v_i \in \Sigma_I.$$

Since $x - \varphi(x) \in \Sigma_{\overline{I}}$ and by definition $v_p \cdot v_q' = \delta_{pq}$, we have, for every $i \in I$, $(x - \varphi(x)) \cdot v_i' = 0$ and $a_i = x \cdot v_i' = \varphi(x) \cdot v_i'$. Thus,

$$|x| \leq \sum_{i \in I} |a_i||v_i| \leq \sum_{i \in I} |\varphi(x)|\,|v_i'|\,|v_i|.$$

The condition $|v_i| \leq i\lambda_i$, the definition of v_i' and Minkowski's second Theorem imply that

$$|v_i'||v_i| \leq \frac{\prod_p |v_p|}{\det\Lambda} \leq \frac{n!\prod_p \lambda_p}{\det\Lambda} \leq \frac{n!2^n}{B_n}.$$

Thus,

$$|x| \leq j\frac{n!2^n}{B_n}|\varphi(x)|,$$

and this implies

$$\|\varphi^{-1}\|_{op} \leq j\frac{n!2^n}{B_n},$$

where $\|\cdot\|_{op}$ is the operator norm. Suppose φ^{-1} corresponds to the matrix $(a_{pq})_{p,q=1}^{j}$ then $\|\varphi^{-1}\|_{op} \geq \max_{p,q}\{|a_{pq}|\}$. By Hadamard's inequality

$$\left|\det\left(\varphi^{-1}\right)\right| \leq \prod_{p=1}^{j}\left(\sum_{q=1}^{j} a_{pq}^2\right)^{1/2} \leq \left(\sqrt{j}\|\varphi^{-1}\|_{op}\right)^j.$$

Finally, since $D^I \subseteq \varphi^{-1}\left(\widehat{D^I}\right)$,

$$\begin{aligned}\mathrm{Vol}_j\left(D^I\right) &\leq \mathrm{Vol}_j\left(\varphi^{-1}\left(\widehat{D^I}\right)\right) \leq \left(j^{3/2}\frac{n!2^n}{B_n}\right)^j \mathrm{Vol}_j\left(\widehat{D^I}\right)\\ &\leq \left(j^{3/2}\frac{n!2^n}{B_n}\right)^j V_j'(D).\end{aligned}$$

□

3. O-minimal structures

In this section we state the basic properties used later on. Most of the results are taken literally from [9].

We start with a list of simple facts that will be used in the sequel, sometimes without explicitly referring to them.

Lemma 3.1.

i) $A, B \in \mathcal{S}_n \Rightarrow A \cap B \in \mathcal{S}_n$;
ii) $A \in \mathcal{S}_n, B \in \mathcal{S}_m \Rightarrow A \times B \in \mathcal{S}_{n+m}$;
iii) $A \in \mathcal{S}_n, 1 \leq k \leq n \Rightarrow \{(x_1,\ldots,x_k,x_1,\ldots,x_n) : (x_1,\ldots,x_n) \in A\} \in \mathcal{S}_{k+n}$;
iv) $A \in \mathcal{S}_n$, σ *a permutation on* n *coordinates* $\Rightarrow \sigma A \in \mathcal{S}_n$;
v) $A \in \mathcal{S}_n \Rightarrow \pi_C(A) \in \mathcal{S}_n$, *where* C *is a coordinate subspace in* $\mathbb{R}^n$ *and* π_C *is the orthogonal projection to* C;
vi) $S \in \mathcal{S}_{m+n}, a \in \mathbb{R}^m \Rightarrow S_a = \{x \in \mathbb{R}^n : (a,x) \in S\} \in \mathcal{S}_n$.

Proof. The statement i) is obvious from Definition 1.2. For ii) we use that $A \times B = A \times \mathbb{R}^m \cap \mathbb{R}^n \times B$. Now iii) follows easily. For iv) we note that σA is the projection to the first n coordinates of the definable set $\cap_{i=1}^n \{(u,x) \in \mathbb{R}^n \times A : u_i = x_{\sigma(i)}\}$. Then, v) follows immediately. Finally, for vi) we note that $S_a = \pi(S \cap \{a\} \times \mathbb{R}^n)$, where π projects to the last n coordinates. □

Recall that a subset X of $\mathbb{R}^n$ is definable (in the o-minimal structure $\mathcal{S}$) if $X \in \mathcal{S}_n$. Also recall that our o-minimal structure $\mathcal{S}$ contains the semialgebraic sets.

Definition 3.2. *Suppose $X \subseteq \mathbb{R}^n$ is definable then we say that $f : X \to \mathbb{R}^m$ is a definable function (in $\mathcal{S}$) if its graph $\Gamma(f) = \{(x, f(x)) : x \in X\}$ is definable (in $\mathcal{S}$). We say that f is bounded if its graph is a bounded set.*

Let φ be an endomorphism of $\mathbb{R}^n$. Then we will identify φ with the vector $(\varphi(e_1), \dots, \varphi(e_n)) \in \mathbb{R}^{n^2}$, where $e_1, \dots, e_n$ is the standard basis of $\mathbb{R}^n$. A set of the form

$$\left\{(\varphi, x, y) \in \mathbb{R}^{n^2+2n} : y = \varphi(x)\right\}, \tag{3.1}$$

is defined by polynomial equalities, and hence is definable.

Now suppose X is a definable set, and let

$$C(X) = \{f : X \to \mathbb{R} : f \text{ is definable and continuous}\},$$

and

$$C_\infty(X) = C(X) \cup \{-\infty, \infty\}.$$

For f and g in $C_\infty(X)$ we write $f < g$ if $f(x) < g(x)$ for all $x \in X$. In this case we put

$$(f,g)_X = \{(x,r) \in X \times \mathbb{R} : f(x) < r < g(x)\}.$$

It is not difficult to see that $(f,g)_X$ is a definable subset of $\mathbb{R}^{n+1}$, e.g., $(-\infty, g)_X$ is a projection of the definable set $\{(x,z,y,z) \in \Gamma(g) \times \mathbb{R}^2 : y < z\}$.

We now come to the definition of cells which are particularly simple definable sets.

Definition 3.3. *Let $(i_1, \dots, i_n)$ be a sequence of zeros and ones of length n. A $(i_1, \dots, i_n)$-cell is a definable subset of $\mathbb{R}^n$ obtained by induction on n as follows:*

1. *A (0)-cell is a one-element set $\{r\} \subseteq \mathbb{R}$, a (1)-cell is a nonempty interval $(a,b) \subseteq \mathbb{R}$.*
2. *Suppose $(i_1, \dots, i_n)$-cells are already defined; then a $(i_1, \dots, i_n, 0)$-cell is the graph $\Gamma(f)$ of a function $f \in C(X)$, where X is a $(i_1, \dots, i_n)$-cell; further, a $(i_1, \dots, i_n, 1)$-cell is a set $(f,g)_X$, where X is a $(i_1, \dots, i_n)$-cell and $f, g \in C_\infty(X)$ with $f < g$.*

A cell in $\mathbb{R}^n$ is an $(i_1, \ldots, i_n)$-cell for some (necessarily unique) sequence $(i_1, \ldots, i_n)$.

Lemma 3.4. *Each cell is connected in the usual topological sense.*

Proof. This follows from [9, Exercise 7, p.59] combined with [9, Ch.3, (2.9) Proposition]. □

We need another definition.

Definition 3.5. *A decomposition of $\mathbb{R}^n$ is a special kind of partition into finitely many cells. Again the definition is by induction on n:*
(1) a decomposition of $\mathbb{R}$ is a collection

$$\{(-\infty, a_1), (a_1, a_2), \ldots, (a_k, \infty), \{a_1\}, \ldots, \{a_k\}\},$$

where $a_1 < \cdots < a_k$ are points in $\mathbb{R}$.
(2) a decomposition of $\mathbb{R}^{n+1}$ is a finite partition of $\mathbb{R}^{n+1}$ into cells A such that the set of projections $\pi(A)$ is a decomposition of $\mathbb{R}^n$. (Here $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$ is the usual projection map on the first n coordinates.)

A decomposition $\mathcal{D}$ of $\mathbb{R}^n$ is said to partition a set $S \subseteq \mathbb{R}^n$ if each cell in $\mathcal{D}$ is either part of S or disjoint from S. We can now state the following theorem, which is a special case of the cell decomposition theorem ([9, Ch.3, (2.11)] or [12, 4.2]).

Theorem 3.6. *Given a definable set $S \subseteq \mathbb{R}^n$ there is a decomposition of $\mathbb{R}^n$ partitioning S.*

Proof. This follows immediately from (I_n) in [9, Ch.3, (2.11)]. □

We recall the definition of dimension of a definable set from [9, Ch.4].

Definition 3.7. *Let $S \subseteq \mathbb{R}^n$ be nonempty and definable. The dimension of S is defined as*

$$\dim S = \max\{i_1 + \cdots + i_n : S \text{ contains an } (i_1, \ldots, i_n) - \text{cell}\}.$$

To the empty set we assign the dimension $-\infty$.

Note that a definable set of dimension zero is a finite collection of points. Next we collect some basic facts about definable functions. These will be used in the sequel, sometimes without further mention.

Lemma 3.8. *Suppose $f : A \to B$ is a definable function and suppose C is a nonempty definable subset of A. Then*

i) A and $f(A)$ are definable;
ii) The restriction $f\,|_C \colon C \to B$ is definable;
iii) If f is bijective then $f^{-1} : B \to A$ is definable;
iv) If f is bijective then $\dim A = \dim B$.

Proof. The claim *i)* follows immediately from the definition, similarly *ii)* by noting that $\Gamma(f\,|_C) = \Gamma(f) \cap (C \times f(A))$, and *iii)* is obvious. For *iv)* we refer to [9, Ch.4, (1.3) Proposition (ii)], □

Definition 3.9. *Let $S \subseteq \mathbb{R}^n$ be a definable set of dimension $d > 0$. Let $\mathcal{P}$ be a finite set of definable functions $\phi : (0,1)^d \to S$ such that $\bigcup_{\phi\in\mathcal{P}} \phi\left((0,1)^d\right) = S$. We call $\mathcal{P}$ a parametrization of S. Let $\alpha \in (\mathbb{N} \cup \{0\})^d$ be a multi index write $|\alpha| = \sum \alpha_i$ and, for $\phi = (\phi_1, \ldots, \phi_n) \in \mathcal{P}$,*

$$\phi^{(\alpha)} = \left(\frac{\partial^{|\alpha|}\phi_1}{\partial^{\alpha_1} x_1 \cdots \partial^{\alpha_d} x_d}, \cdots, \frac{\partial^{|\alpha|}\phi_n}{\partial^{\alpha_1} x_1 \cdots \partial^{\alpha_d} x_d} \right).$$

We call $\mathcal{P}$ a p-parametrization if every $\phi \in \mathcal{P}$ is of class $C^{(p)}$ and has the property that $\phi^{(\alpha)}$ is bounded for each $\alpha \in (\mathbb{N} \cup \{0\})^d$ with $|\alpha| \leq p$.

Theorem 3.10 (Pila, Wilkie)**.** *For any $p \in \mathbb{N}$, and any bounded definable set S of positive dimension, there exists a p-parametrization of S.*

Proof. This is a special case of [23, Theorem 2.3]. □

Let $D \subseteq \mathbb{R}^n$ be nonempty. We say $f : D \to \mathbb{R}^m$ is a Lipschitz map if there exists a real constant L such that

$$|f(x) - f(y)| \leq L|x - y| \text{ for all } x, y \in D.$$

Corollary 3.11. *Let $S \subseteq \mathbb{R}^n$ be bounded and definable, and suppose* $\dim S = d > 0$. *Then S can be parameterized by a finite number of Lipschitz maps $\phi : (0,1)^d \to S$.*

Proof. By Theorem 3.10 any bounded definable set S of dimension d can be parameterized by a finite number of maps $\phi : (0,1)^d \to S$ with uniformly bounded partial derivatives. This implies the claim (see also [9, Ch.7, (2.8) Lemma]). □

Proposition 3.12. [9, Ch.3, (3.5) Proposition] *Let $\pi : \mathbb{R}^{m+n} \to \mathbb{R}^m$ be the projection on the first m coordinates. If C is a cell in $\mathbb{R}^{m+n}$ and $a \in \pi(C)$, then C_a is a cell in $\mathbb{R}^n$. Moreover, if $\mathcal{D}$ is a decomposition of $\mathbb{R}^{m+n}$ and $a \in \mathbb{R}^m$ then the collection*

$$\mathcal{D}_a := \{C_a : C \in \mathcal{D}, a \in \pi(C)\}$$

is a decomposition of $\mathbb{R}^n$.

Corollary 3.13. *Let $S \subseteq \mathbb{R}^{m+n}$ be a definable family. Then there exists a number $M_S \in \mathbb{N}$ such that for each $a \in \mathbb{R}^m$ the set $S_a \subseteq \mathbb{R}^n$ can be partitioned into at most M_S cells. In particular, each fiber S_a has at most M_S connected components.*

Proof. By the cell decomposition theorem there exists a decomposition $\mathcal{D}$ of $\mathbb{R}^{m+n}$ partitioning S. Then for each $a \in \mathbb{R}^m$ the decomposition $\mathcal{D}_a$ of $\mathbb{R}^n$ consists of at most $|\mathcal{D}|$ cells and partitions S_a. So we can take $M_S = |\mathcal{D}|$. The last statement follows from Lemma 3.4. □

Another important property of o-minimal structures is the possibility of "lifting" projections. In model-theoretic terms this might be rephrased as existence of definable Skolem functions.

Proposition 3.14. [9, Ch.6, (1.2) Proposition] *If $S \subseteq \mathbb{R}^{m+n}$ is definable and $\pi : \mathbb{R}^{m+n} \to \mathbb{R}^m$ is the projection on the first m coordinates, then there is a definable map $f : \pi(S) \to \mathbb{R}^n$ such that $\Gamma(f) \subseteq S$.*

The proof of [9, Ch.6, (1.2) Proposition] actually shows that there is an algorithmic way to construct the Skolem function f. The construction of f is of no importance for us but we will use the fact that this choice of f is determined by S and π.

We write $\mathrm{cl}(A)$ and $\mathrm{int}(A)$ for the the topological closure and the interior of the set A respectively. Also recall that $\mathrm{bd}(A)$ denotes the topological boundary of A.

Lemma 3.15. *Suppose $Z \subseteq \mathbb{R}^{m+n}$ is definable. Then $\{(T,x) : x \in \mathrm{int}(Z_T)\}$, $\{(T,x) : x \in \mathrm{cl}(Z_T)\}$, and $\{(T,x) : x \in \mathrm{bd}(Z_T)\}$ are definable.*

Proof. The first statement is [9, Ch.1, (3.7) Exercise (ii)]. For the second set note that $x \in \mathrm{cl}(Z_T)$ is equivalent to $x \notin \mathrm{int}(\mathbb{R}^n \backslash Z_T)$, and, moreover, $\mathbb{R}^n \backslash Z_T = (\mathbb{R}^{m+n} \backslash Z)_T$. Hence, $\{(T,x) : x \in \mathrm{cl}(Z_T)\} = \mathbb{R}^{m+n} \backslash \{(T,x) : x \in \mathrm{int}((\mathbb{R}^{m+n} \backslash Z)_T)\}$, which is definable by our first statement. Finally, as $\{(T,x) : x \in \mathrm{bd}(Z_T)\} = \{(T,x) : x \in \mathrm{cl}(Z_T)\} \setminus \{(T,x) : x \in \mathrm{int}(Z_T)\}$ we get the last statement. □

4. The Davenport constant

If $D \subseteq \mathbb{R}^n$ satisfies the conditions (1) and (2) in Theorem 1.1 then we say h is a Davenport constant for D. Of course, this has nothing to do with the classical Davenport constant of a finite abelian group.

Lemma 4.1. *Let $Z \subseteq \mathbb{R}^{m+n}$ be a definable family. There exists a natural number $M = M_Z$, depending only on Z, such that for every $T \in \mathbb{R}^m$ and every endomorphism Ψ of $\mathbb{R}^n$ the number M is a Davenport constant for $\Psi(Z_T)$.*

Proof. Let I be a nonempty subset of $\{1, \ldots, n\}$ and let π_{C_I} be the orthogonal projection of $\mathbb{R}^n$ on the coordinate subspace C_I generated by the e_i, $i \in I$. Recall the notation of (3.1) in Section 3 and let W be the set

$$W = \left\{(\Psi, T, x) \in \mathbb{R}^{n^2+m+n} : x \in \Psi(Z_T)\right\}. \tag{4.1}$$

Note that, up to a coordinate permutation, W is the projection to the first $n^2 + m + n$ coordinates of the definable set

$$\left\{(\Psi, x, T, y) \in \mathbb{R}^{n^2+n+m+n} : x = \Psi(y)\right\} \cap \left(\mathbb{R}^{n^2+n} \times Z\right).$$

By Lemma 3.1 and the fact that semialgebraic sets are definable, this is a definable set. Moreover, note that

$$W_{(\Psi,T)} = \Psi(Z_T).$$

Let us set some notation we need. We indicate by π'_{C_I} the endomorphism of $\mathbb{R}^{n^2+m+n}$ defined by $(\Psi, T, x) \mapsto (\Psi, T, \pi_{C_I}(x))$. A line in C_I parallel to e_{i_0} is determined by $|I|-1$ reals and therefore we indicate it by $(l_i)_{i\in I\setminus\{i_0\}}$.

Let $I \subseteq \{1, \dots, n\}$ be nonempty and $i_0 \in I$, we consider the sets

$$B^{I,(i_0)} = \Big\{ \big((l_i)_{i\in I\setminus\{i_0\}}, \Psi, T, x\big) \in \mathbb{R}^{|I|-1} \times \mathbb{R}^{n^2+m+n} : \\ (\Psi, T, x) \in \pi'_{C_I}(W), l_i = x_i \text{ for } i \in I \setminus \{i_0\} \Big\}.$$

Again by elementary properties mentioned in Section 3, these are definable sets . A fiber $B^{I,(i_0)}_{((l_i),\Psi,T)}$ is exactly the intersection of $\pi'_{C_I}(W)_{(\Psi,T)} = \pi_{C_I}(W_{(\Psi,T)}) = \pi_{C_I}(\Psi(Z_T))$ and the line $(l_i)_{i\in I\setminus\{i_0\}}$ parallel to e_{i_0} in the subspace C_I.

Now we use Corollary 3.13 to find a uniform bound $M^{I,(i_0)}$ for the number of connected components of the fibers $B^{I,(i_0)}_{((l_i),\Psi,T)}$ of $B^{I,(i_0)}$. This means that $M^{I,(i_0)}$ is a bound on the number of connected components of the intersection of $\pi_{C_I}(\Psi(Z_T))$ with any line of C_I parallel to e_{i_0}, for any choice of Ψ and T. Finally, we can take M to be the maximum of the $M^{I,(i_0)}$ for all the possible choices of I and $i_0 \in I$. □

5. Hausdorff measure and rectifiability

We also require the j-Hausdorff measure $\mathcal{H}^j$. For the definition and properties of the Hausdorff measure we refer to [14] or [21].

Lemma 5.1. *Suppose $1 \le j \le n$, $A \subseteq \mathbb{R}^n$ and suppose A is j-Hausdorff measurable. Furthermore, let $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ be an endomorphism. Then $\mathcal{H}^j(\varphi(A)) \le \|\varphi\|^j_{op}\mathcal{H}^j(A)$. Moreover, if φ is an orthogonal projection we have $\mathcal{H}^j(\varphi(A)) \le \mathcal{H}^j(A)$. If φ is in the orthogonal group $O_n(\mathbb{R})$ then we have $\mathcal{H}^j(\varphi(A)) = \mathcal{H}^j(A)$.*

Proof. The first claim follows from [13, 2.4.1 Theorem 1]. If φ is in $O_n(\mathbb{R})$ or if φ is an orthogonal projection then $\|\varphi\|_{op} = 1$. If $\varphi \in O_n(\mathbb{R})$ then also $\varphi^{-1} \in O_n(\mathbb{R})$, and we apply the previous with φ^{-1} and $\varphi(A)$. □

Proposition 5.2. *Suppose $A \subseteq \mathbb{R}^n$ is nonempty and definable. Then* $\dim A$ *coincides with the Hausdorff dimension. Moreover, if* $\dim A = d$ *and A is bounded, then A is j-Hausdorff measurable for every j with $d \le j \le n$. Finally, $\mathcal{H}^d(A) < \infty$ and $\mathcal{H}^j(A) = 0$ for $j > d$.*

Proof. See [10, last paragraph on p.177]. The last claim follows from the definition of Hausdorff dimension. □

It is well known that on $\mathbb{R}^n$ the n-Hausdorff measure coincides with the Lebesgue measure (see [21, 2.8. Corollary]). This, together with Proposition 5.2, implies that a definable set in $\mathbb{R}^n$ of dimension $< n$ has

volume zero. Also recall that any bounded set that is open or closed is measurable and has finite volume.

Lemma 5.3. *Let $A \subseteq \mathbb{R}^n$ be a bounded definable set. Then,* $\mathrm{Vol}(\mathrm{bd}(A)) = 0$. *In particular, A is measurable and* $\mathrm{Vol}(\mathrm{int}(A)) = \mathrm{Vol}(A) = \mathrm{Vol}(\mathrm{cl}(A))$.

Proof. By [9, Ch.4, (1.10) Corollary] we have $\dim \mathrm{bd}(A) < n$. This, combined with the previous observation yields $\mathrm{Vol}(\mathrm{bd}(A)) = 0$. □

Berarducci and Otero [3] have proven measurability results for more general o-minimal structures expanding a field, not necessarily $\mathbb{R}$. E.g., [3, 2.5 Theorem] implies that any bounded definable set is measurable.

Lemma 5.4. *Let $Z \subseteq \mathbb{R}^{m+n}$ be a definable family and suppose the fibers Z_T are bounded. Then for $1 \leq j \leq n-1$ the j-dimensional volumes of the orthogonal projections of Z_T on every j-dimensional coordinate subspace of $\mathbb{R}^n$ exist and are finite. Moreover, we have $V_j(Z_T) = V_j(\mathrm{cl}(Z_T))$.*

Proof. Let C be a coordinate space of dimension j, and let π_C be the orthogonal projection from $\mathbb{R}^n$ to C. Recall that the Lebesgue measure on C is denoted by Vol_j. Using the continuity of π_C we get $\pi_C(\mathrm{cl}(Z_T)) = \mathrm{cl}(\pi_C(Z_T))$. In particular, $\pi_C(\mathrm{cl}(Z_T))$ is measurable, and $\mathrm{Vol}_j(\pi_C(\mathrm{cl}(Z_T))) = \mathrm{Vol}_j(\mathrm{cl}(\pi_C(Z_T)))$. Next we apply Lemma 5.3 with $A = \pi_C(Z_T)$ in the coordinate space C to get $\mathrm{Vol}_j(\mathrm{cl}(\pi_C(Z_T))) = \mathrm{Vol}_j(\pi_C(Z_T))$, and this proves the claim. □

Next we recall the definition of j-rectifiability from [14, Ch.3, 3.2.14].

Definition 5.5. *Let $A \subseteq \mathbb{R}^n$ and let j be a positive integer. We say A is j-rectifiable if there exists a Lipschitz function mapping some bounded subset of $\mathbb{R}^j$ onto A. Moreover, A is $(\mathcal{H}^j, j)$-rectifiable if there exist countably many j-rectifiable sets whose union is $\mathcal{H}^j$-almost A and $\mathcal{H}^j(A) < \infty$.*

Proposition 5.6. *Let $A \subseteq \mathbb{R}^n$ be bounded and definable, and suppose* $\dim A = d > 0$. *Then A is $(\mathcal{H}^j, j)$-rectifiable for every j such that $d \leq j \leq n$.*

Proof. By Corollary 3.11 we can cover A by the images of finitely many Lipschitz maps $\phi : (0,1)^d \to \mathbb{R}^n$ whose domain can clearly be extended to $(0,1)^j$ for every $j = d+1, \ldots, n$ without loosing the Lipschitz condition. The finiteness of $\mathcal{H}^j(A)$ comes from Proposition 5.2. □

We fix an integer $j \in \{1, \ldots, n-1\}$. Let I be a subset of $\{1, \ldots, n\}$ of cardinality j and let $\pi_I : \mathbb{R}^n \to \mathbb{R}^j$ be the projection map such that $\pi_I(x_1, \ldots, x_n) = (x_i)_{i \in I}$. For $y \in \mathbb{R}^j$ let

$$N(\pi_I \mid A, y) = |\{x \in A : \pi_I(x) = y\}| = |\pi_I^{-1}(y) \cap A|. \tag{5.1}$$

A priori, $N(\pi_I \mid A, y)$ could be infinite, even for every $y \in \pi_I(A)$. The following theorem ([14, 3.2.27 Theorem]) tells us that if A is $(\mathcal{H}^j, j)$-rectifiable then we can integrate $N(\pi_I \mid A, y)$ and obtain a finite value. Unless specified otherwise, the domain of integration is always $\mathbb{R}^j$.

Theorem 5.7. [14, 3.2.27 Theorem] *If $1 \leq j \leq n$, and if A is a $(\mathcal{H}^j, j)$-rectifiable subset of $\mathbb{R}^n$, then*

$$\left(\sum_{|I|=j} a_I(A)^2\right)^{\frac{1}{2}} \leq \mathcal{H}^j(A) \leq \sum_{|I|=j} a_I(A),$$

where

$$a_I(A) = \int N(\pi_I \mid A, y)\, d\mathcal{L}^j y.$$

To conclude this section we apply Theorem 5.7 to fibers of definable families.

Lemma 5.8. *Let $S \subseteq \mathbb{R}^{p+n}$ be a definable family whose fibers $S_a \subseteq \mathbb{R}^n$ are bounded and of dimension at most $j \geq 1$. Then there exists a real constant $E_I = E_I(S)$ such that*

$$\mathcal{H}^j(S_a) \leq \sum_{|I|=j} E_I \mathrm{Vol}_j\left(\pi_I\left(S_a\right)\right),$$

for every $a \in \mathbb{R}^p$.

Proof. If $S = \emptyset$, the claim is trivially true. For those a such that $S_a = \emptyset$ or $\dim S_a = 0$ we have from Proposition 5.2 that $\mathcal{H}^j\left(S_a\right) = 0$, and so in this case again the claim is trivially true. Therefore, we can assume that $\dim S_a > 0$, and so we get from Proposition 5.6 that S_a is $(\mathcal{H}^j, j)$-rectifiable. Hence, we can apply Theorem 5.7, and we get

$$\mathcal{H}^j\left(S_a\right) \leq \sum_{|I|=j} \int N\left(\pi_I \mid S_a, y\right) \mathrm{d}\mathcal{L}^j y,$$

for every $a \in \mathbb{R}^p$ such that $\dim S_a > 0$. Therefore, we are left to prove that for any $I \subseteq \{1, \ldots, n\}$ of cardinality j there exists a real $E_I = E_I(S)$ such that

$$\int N\left(\pi_I \mid S_a, y\right) \mathrm{d}\mathcal{L}^j y \leq E_I \mathrm{Vol}_j\left(\pi_I\left(S_a\right)\right),$$

for every $a \in \mathbb{R}^p$.

Let R be the definable family

$$R = \left\{(a, y, x) \in \mathbb{R}^{p+j+n} : (a, x) \in S, y = \pi_I(x)\right\}.$$

Note that $R_{(a,y)} = \pi_I^{-1}(y) \cap S_a$. Thus, for every $(a, y) \in \mathbb{R}^{p+j}$ we have $N\left(\pi_I \mid S_a, y\right) = |R_{(a,y)}|$. Moreover, by Corollary 3.13 there is a uniform upper bound E_I for the number of connected components of the fibers $R_{(a,y)}$. In particular, if $\dim R_{(a,y)} = 0$ we get $|R_{(a,y)}| \leq E_I$.

Now fix an $a \in \mathbb{R}^p$. The restriction $\pi_{I|S_a} : S_a \to \mathbb{R}^j$ is a definable map. Thus, by [9, Ch. 4, (1.6) Corollary (ii)], we obtain

$$P = \left\{ y \in \mathbb{R}^j : \dim \left(\pi_I^{-1}(y) \cap S_a \right) \geq 1 \right\}$$

is definable, and, moreover,

$$\dim P \leq \dim S_a - 1 \leq j - 1.$$

Hence P has measure zero in $\mathbb{R}^j$. Let Q be its complement in $\pi_I(S_a)$, i.e., $Q = \pi_I(S_a) \setminus P = \left\{ y \in \pi_I(S_a) : \dim \left(\pi_I^{-1}(y) \cap S_a \right) = 0 \right\}$. This set is definable, and it is exactly the set of y such that $R_{(a,y)}$ has dimension zero. Therefore

$$\begin{aligned} \int N\left(\pi_I \mid S_a, y\right) \mathrm{d}\mathcal{L}^j y &= \int_Q |R_{(a,y)}| \mathrm{d}\mathcal{L}^j y \\ &\leq \int_Q E_I \mathrm{d}\mathcal{L}^j y = E_I \mathrm{Vol}_j\left(\pi_I\left(S_a\right)\right). \end{aligned}$$

□

6. A geometric inequality

In this section we are going to prove the following proposition. Recall the definition of $V_j'(\cdot)$ from Definition 2.3, and also that $\mathrm{cl}(Z_T)$ denotes the topological closure of Z_T.

Proposition 6.1. *Let $Z \subseteq \mathbb{R}^{m+n}$ be a definable family such that the fibers Z_T are bounded, and let j be an integer such that $0 \leq j \leq n-1$. Then there exists a constant B_Z, depending only on the family and on j, such that*

$$V_j'(\mathrm{cl}(Z_T)) \leq B_Z V_j(Z_T),$$

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

If $Z = \emptyset$ or $j = 0$ the inequality is trivially true. For the remainder of this section we assume that Z is nonempty, and we fix an integer j satisfying $1 \leq j \leq n-1$. By Lemma 5.4 we have $V_j(Z_T) = V_j(\mathrm{cl}(Z_T))$. Hence, for the rest of this section we can and will also assume

$$\mathrm{cl}(Z_T) = Z_T.$$

Let $O_n(\mathbb{R})$ be the orthogonal group. It embeds into $\mathbb{R}^{n^2}$ if we identify, as already done before, a linear function φ with the image vector of the standard basis. So $O_n(\mathbb{R})$ is a semialgebraic set, as it is defined by polynomial equalities.

Lemma 6.2. *There exists a definable set $Z' \subseteq \mathbb{R}^{n^2+m+n}$ depending only on Z such that*

$$\dim Z'_{(\varphi,T)} \leq j, \tag{6.1}$$

and

$$Z'_{(\varphi,T)} \subseteq Z_T, \tag{6.2}$$

for every $(\varphi, T) \in \mathbb{R}^{n^2+m}$*, and*

$$V_j'(Z_T) \leq \sup_{\varphi \in O_n(\mathbb{R})} \mathcal{H}^j\left(Z'_{(\varphi,T)}\right), \tag{6.3}$$

for every $T \in \mathbb{R}^m$*.*

Proof. Let

$$S = \{(\varphi, T, y) \in \mathbb{R}^{n^2+m+n} : \varphi \in O_n(\mathbb{R}), y \in \varphi(Z_T)\}.$$

This set is nothing but the set W in (4.1) intersected with $O_n(\mathbb{R}) \times \mathbb{R}^{m+n}$ and is therefore definable. Note that

$$S_{(\varphi,T)} = \varphi(Z_T), \tag{6.4}$$

for every $(\varphi, T) \in O_n(\mathbb{R}) \times \mathbb{R}^m$. Let $\pi : \mathbb{R}^{n^2+m+n} \to \mathbb{R}^{n^2+m+j}$ be the projection that cancels the last $n - j$ coordinates. We use the fact that o-minimal structures have definable Skolem functions (Proposition 3.14, see also the observation after Proposition 3.14). There exists an explicit construction of a definable function

$$f : \pi(S) \subseteq \mathbb{R}^{n^2+m+j} \to \mathbb{R}^{n-j},$$

such that the graph of f

$$\Gamma(f) = \{(\varphi, T, z, f(\varphi, T, z)) : (\varphi, T, z) \in \pi(S)\} \subseteq \pi(S) \times \mathbb{R}^{n-j},$$

is contained in S. Therefore

$$\Gamma(f)_{(\varphi,T)} \subseteq S_{(\varphi,T)}, \tag{6.5}$$

for every $(\varphi, T) \in \mathbb{R}^{n^2+m}$. Moreover, since $\pi(S) = \pi(\Gamma(f))$ we have

$$\pi(S)_{(\varphi,T)} = \pi(\Gamma(f))_{(\varphi,T)}, \tag{6.6}$$

for every $(\varphi, T) \in \mathbb{R}^{n^2+m}$. The function

$$\begin{array}{rccc} F: & \pi(S) & \to & \Gamma(f) \\ & (\varphi, T, z) & \mapsto & (\varphi, T, z, f(\varphi, T, z)) \end{array}$$

is definable because its graph is the definable set

$$\{(\varphi, T, z, \varphi, T, z, f(\varphi, T, z)) : (\varphi, T, z) \in \pi(S)\} \subseteq \pi(S) \times \Gamma(f).$$

Moreover, F is a bijection with inverse $\pi_{|\Gamma(f)}$. Now fix any (φ, T), suppose $\pi(S)_{(\varphi,T)}$ is nonempty, and consider the bijection $g : \pi(S)_{(\varphi,T)} \to \Gamma(f)_{(\varphi,T)}$ defined by $g(z) = (z, f(\varphi, T, z))$. Using the elementary properties we see that $\Gamma(g)$ is definable. Hence, by Lemma 3.8, we conclude that

$$\dim \pi(S)_{(\varphi,T)} = \dim \Gamma(f)_{(\varphi,T)}, \tag{6.7}$$

for every $(\varphi, T) \in \mathbb{R}^{n^2+m}$. Note that $\pi(S)_{(\varphi,T)} = \emptyset$ implies $\Gamma(f)_{(\varphi,T)} = \emptyset$, and hence (6.7) remains true for $\pi(S)_{(\varphi,T)} = \emptyset$.

Again by the elementary properties, the set

$$Z' = \left\{(\varphi, T, x) \in \mathbb{R}^{n^2+m+n} : \varphi \in O_n(\mathbb{R}), \varphi(x) \in \Gamma(f)_{(\varphi,T)}\right\},$$

is definable. Note that

$$\varphi\left(Z'_{(\varphi,T)}\right) = \Gamma(f)_{(\varphi,T)} \tag{6.8}$$

for every $(\varphi, T) \in O_n(\mathbb{R}) \times \mathbb{R}^m$. Moreover, if $\varphi \in \mathbb{R}^{n^2} \setminus O_n(\mathbb{R})$, we have $Z'_{(\varphi,T)} = \emptyset$ and (6.1), (6.2) are satisfied.

Now fix $(\varphi, T) \in O_n(\mathbb{R}) \times \mathbb{R}^m$. As $\varphi \in O_n(\mathbb{R})$ we can apply Lemma 3.8 to get

$$\dim Z'_{(\varphi,T)} = \dim \Gamma(f)_{(\varphi,T)}. \tag{6.9}$$

By (6.4), (6.5) and (6.8) we have that

$$\varphi\left(Z'_{(\varphi,T)}\right) = \Gamma(f)_{(\varphi,T)} \subseteq S_{(\varphi,T)} = \varphi(Z_T),$$

and this proves (6.2). Moreover, since $\pi(S)_{(\varphi,T)} \subseteq \mathbb{R}^j$ and by (6.7) and (6.9), we have

$$j \geq \dim \pi(S)_{(\varphi,T)} = \dim Z'_{(\varphi,T)},$$

that is exactly (6.1).

We now prove the volume inequality (6.3). Let Σ be any j-dimensional linear subspace of $\mathbb{R}^n$. Fix an orthonormal basis $\{u_1, \ldots, u_j\}$ of Σ. Suppose φ is in $O_n(\mathbb{R})$ and such that $\varphi(u_i) = e_i$ for $i = 1, \ldots, j$. Let π_Σ be the orthogonal projection map from $\mathbb{R}^n$ to Σ and $\widetilde{\pi}$ the projection from $\mathbb{R}^n$ to the coordinate subspace spanned by $e_1, \ldots, e_j$. Note that $\varphi \circ \pi_\Sigma$ and $\widetilde{\pi} \circ \varphi$ coincide on Σ and their kernel is the orthogonal complement $\Sigma^\perp$. Hence, $\varphi \circ \pi_\Sigma = \widetilde{\pi} \circ \varphi$. Recalling that $\mathcal{H}^j = \mathrm{Vol}_j$ on Σ and $\varphi(\Sigma)$, and using (6.4) and Lemma 5.1, we obtain

$$\begin{aligned}\mathrm{Vol}_j\left(\pi_\Sigma(Z_T)\right) &= \mathrm{Vol}_j\left(\varphi\left(\pi_\Sigma(Z_T)\right)\right) \\ &= \mathrm{Vol}_j\left(\widetilde{\pi}\left(\varphi\left(Z_T\right)\right)\right) = \mathrm{Vol}_j\left(\widetilde{\pi}\left(S_{(\varphi,T)}\right)\right).\end{aligned}$$

Then

$$V'_j(Z_T) = \sup_\Sigma \mathrm{Vol}_j(\pi_\Sigma(Z_T)) \leq \sup_{\varphi \in O_n(\mathbb{R})} \mathrm{Vol}_j\left(\widetilde{\pi}\left(S_{(\varphi,T)}\right)\right). \tag{6.10}$$

Fix $(\varphi, T) \in O_n(\mathbb{R}) \times \mathbb{R}^m$. Note that for any set $A \subseteq \mathbb{R}^{n^2+m+n}$ we have $\widetilde{\pi}\left(A_{(\varphi,T)}\right) = \{(x_1, \ldots, x_j, 0, \ldots, 0) : (\varphi, T, x_1, \ldots, x_n) \in A\}$ and $\pi(A)_{(\varphi,T)} = \{(x_1, \ldots, x_j) : (\varphi, T, x_1, \ldots, x_n) \in A\}$. The latter in conjunction with (6.6) gives

$$\widetilde{\pi}\left(S_{(\varphi,T)}\right) = \widetilde{\pi}\left(\Gamma(f)_{(\varphi,T)}\right).$$

By this and Lemma 5.1 we get

$$\mathrm{Vol}_j\left(\widetilde{\pi}\left(S_{(\varphi,T)}\right)\right) = \mathcal{H}^j\left(\widetilde{\pi}\left(S_{(\varphi,T)}\right)\right) \leq \mathcal{H}^j\left(\Gamma(f)_{(\varphi,T)}\right). \tag{6.11}$$

Again by (6.8) and Lemma 5.1 we have

$$\mathcal{H}^j\left(\Gamma(f)_{(\varphi,T)}\right) = \mathcal{H}^j\left(Z'_{(\varphi,T)}\right), \tag{6.12}$$

for every $(\varphi, T) \in O_n(\mathbb{R}) \times \mathbb{R}^m$. Combining (6.10), (6.11) and (6.12) proves (6.3), and thereby completes the proof of Lemma 6.2. □

As in Section 5, I indicates a nonempty proper subset of $\{1,\dots,n\}$ and π_I is the projection map such that $\pi_I(x_1,\dots,x_n)=(x_i)_{i\in I}$.

Applying Lemma 5.8 to the family Z' we conclude that there exist E_I such that

$$\mathcal{H}^j\left(Z'_{(\varphi,T)}\right) \le \sum_{|I|=j} E_I \mathrm{Vol}_j\left(\pi_I\left(Z'_{(\varphi,T)}\right)\right),$$

for every $(\varphi,T)\in\mathbb{R}^{n^2+m}$.

Let π_{C_I} be the orthogonal projection map from $\mathbb{R}^n$ to the coordinate subspace C_I spanned by e_i, $i\in I$. We have

$$\mathrm{Vol}_j\left(\pi_I\left(Z'_{(\varphi,T)}\right)\right) = \mathrm{Vol}_j\left(\pi_{C_I}\left(Z'_{(\varphi,T)}\right)\right).$$

Therefore, recalling (6.2),

$$\mathcal{H}^j\left(Z'_{(\varphi,T)}\right) \le \sum_{|I|=j} E_I \mathrm{Vol}_j\left(\pi_{C_I}\left(Z'_{(\varphi,T)}\right)\right) \le B_Z V_j\left(Z'_{(\varphi,T)}\right) \le B_Z V_j\left(Z_T\right),$$

where

$$B_Z = \max_j \binom{n}{j} \max_I E_I.$$

Finally, combining this with (6.3) from Lemma 6.2, completes the proof of Proposition 6.1.

7. Proof of Theorem 1.3

First we assume Z is such that $Z_T=\mathrm{cl}(Z_T)$ for all T. By assumption the fibers Z_T are also bounded, and so they are compact. Thanks to Lemma 4.1 we can apply Lemma 2.1 with a Davenport constant $h=M_Z$ depending only on Z. Then we use Lemmas 2.2, 2.4, and Proposition 6.1 to bound $V_j(\Psi(Z_T))$, and this proves the estimate of Theorem 1.3 when $Z_T=\mathrm{cl}(Z_T)$. From this special case of the theorem we will deduce the general case.

To this end we first note that

$$\left||\Lambda\cap Z_T| - |\Lambda\cap \mathrm{cl}(Z_T)|\right| \le |\Lambda\cap \mathrm{bd}(Z_T)|.$$

By Lemma 3.15 we see that $C=C(Z)=\{(T,x) : x\in \mathrm{cl}(Z_T)\}$ and $B=B(Z)=\{(T,x) : x\in \mathrm{bd}(Z_T)\}$ are definable. Clearly, $C_T=\mathrm{cl}(Z_T)$, and $B_T=\mathrm{bd}(Z_T)$, and these sets are closed and bounded as the sets Z_T are bounded. Hence, we can apply our theorem with $Z=C$ and then with $Z=B$. For C we obtain

$$\left||\Lambda\cap \mathrm{cl}(Z_T)| - \frac{\mathrm{Vol}(\mathrm{cl}(Z_T))}{\det\Lambda}\right| \le c_C \sum_{j=0}^{n-1} \frac{V_j(\mathrm{cl}(Z_T))}{\lambda_1\cdots\lambda_j}.$$

Note that the constant c_C depends only on the family C, and thus only on the family Z. Moreover, $\mathrm{Vol}(\mathrm{cl}(Z_T))=\mathrm{Vol}(Z_T)$ by Lemma 5.3 and

$V_j(\mathrm{cl}(Z_T)) = V_j(Z_T)$ by Lemma 5.4. Using also $\mathrm{Vol}(\mathrm{bd}(Z_T)) = 0$ by Lemma 5.3, and $\mathrm{bd}(Z_T) \subseteq \mathrm{cl}(Z_T)$, we get similarly that

$$|\Lambda \cap \mathrm{bd}(Z_T)| \leq c_B \sum_{j=0}^{n-1} \frac{V_j(Z_T)}{\lambda_1 \cdots \lambda_j},$$

again with a constant c_B depending only on the family Z. Combining these estimates concludes the proof of Theorem 1.3 in the general case.

Acknowledgements

It is our pleasure to thank Alessandro Berarducci, Zoé Chatzidakis, Marcello Mamino, and Vincenzo Mantova for answering many questions about o-minimal structures. We thank Francesco Ghiraldin for pointing out the example [1, Example 2.67] mentioned in the introduction, and Andrea Mondino for helpful discussions on rectifiability. We also thank Robert Tichy, Johannes Wallner, and Umberto Zannier for interesting discussions and encouragement. We are grateful to the referees for providing valuable suggestions that simplified the proof of Lemma 5.8 and improved the exposition of the paper. Parts of this project have been done while the second author was visiting Graz University of Technology. He is grateful for the invitation and the financial support. The first author would like to thank Centro de Giorgi for the hospitality during his visit in Pisa.

References

[1] L. Ambrosio, N. Fusco and D. Pallara, *Functions of Bounded Variation and Free Discontinuity Problems*, Oxford University Press, 2000.
[2] F. Barroero, *Counting algebraic integers of fixed degree and bounded height*, submitted.
[3] A. Berarducci and M. Otero, *An additive measure in o-minimal expansions of fields*, Quart. J. Math. **55** (2004), no. 4, 411-419.
[4] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. **59** (1989), no. 2, 337-357.
[5] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, 1997.
[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.
[8] J. Denef and L. van den Dries, *p-adic and real subanalytic sets*, Ann. of Math. (2) **128** (1988), no. 1, 79-138.
[9] L. van den Dries, *Tame Topology and O-minimal Structures*, Cambridge University Press, 1998.
[10] L. van den Dries, *Limit sets in o-minimal structures*, Proceedings of the Real Algebraic and Analytic Geometry Summer School Lisbon 2003: O-Minimal Structures, Cuvillier Göttingen (2005), 172-215.
[11] L. van den Dries and C. Miller, *On the real exponential field with restricted analytic functions*, Israel J. Math. **85** (1994), no. 1-3, 19-56.
[12] L. van den Dries and C. Miller, *Geometric categories and o-minimal structures*, Duke Math. J. **84** (1993), no. 2, 497-540.

[13] L. C. Evans and R. F. Gariepy, *Measure Theory and Fine Properties of Functions*, Studies in Advanced Mathematics, CRC Press, Boca Raton, FL, 1992.
[14] H. Federer, *Geometric Measure Theory*, Die Grundlehren der mathematischen Wissenschaften, Band 153, Springer-Verlag New York Inc., New York, 1969.
[15] M. Gromov, *Entropy, homology and semialgebraic geometry*, Séminaire Bourbaki, Vol. 1985/86, exposé 663, Astérisque **145-146** (1987), 225-240.
[16] P. Habegger and J. Pila, *Some unlikely intersections beyond André-Oort*, Compos. Math. **148** (2012), no. 1, 1-27.
[17] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.
[18] D. Masser and J. D. Vaaler, *Counting algebraic numbers with large height II*, Trans. Amer. Math. Soc. **359** (2007), no. 1, 427-445.
[19] D. Masser and U. Zannier, *Torsion anomalous points and families of elliptic curves*, C. R. Math. Acad. Sci. Paris **346** (2008), no. 9-10, 491-494.
[20] D. Masser and U. Zannier, *Torsion anomalous points and families of elliptic curves*, Amer. J. Math. **132** (2010), no. 6, 1677-1691.
[21] F. Morgan, *Geometric Measure Theory. A Beginner's Guide*, Fourth ed., Elsevier/Academic Press, Amsterdam, 2009.
[22] J. Pila, *O-minimality and the André-Oort conjecture for* $\mathbb{C}^n$, Ann. of Math. (2) **173** (2011), no. 3, 1779-1840.
[23] J. Pila and A. J. Wilkie, *The rational points of a definable set*, Duke Math. J. **133** (2006), no. 3, 591-616.
[24] J. Pila and U. Zannier, *Rational points in periodic analytic sets and the Manin-Mumford conjecture*, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **19** (2008), no. 2, 149-162.
[25] T. Scanlon, *A proof of the André-Oort conjecture using mathematical logic [after Pila, Wilkie and Zannier]*, Astérisque, Séminaire Bourbaki, Exposé 1037, (2010-2011).
[26] W. M. Schmidt, *Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height*, Duke Math. J. **35** (1968), 327-339.
[27] W. M. Schmidt, *Northcott's Theorem on heights II. The quadratic case*, Acta Arith. **70** (1995), no. 4, 343-375.
[28] P. G. Spain, *Lipschitz: A new version of an old principle*, Bull. London Math. Soc. **27** (1995), no. 6, 565-566.
[29] J. L. Thunder, *The number of solutions of Bounded Height to a System of Linear Equations*, J. Number Theory **43** (1993), no. 2, 228-250.
[30] M. Widmer, *Counting points of fixed degree and bounded height*, Acta Arith. **140** (2009), no. 2, 145-168.
[31] M. Widmer, *Counting primitive points of bounded height*, Trans. Amer. Math. Soc. **362** (2010), no. 9, 4793-4829.
[32] M. Widmer, *Integral points of fixed degree and bounded height*, submitted.
[33] M. Widmer, *Lipschitz class, narrow class, and counting lattice points*, Proc. Amer. Math. Soc. **140** (2012), no. 2, 677-689.
[34] A. J. Wilkie, *Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function*, J. Amer. Math. Soc. **9** (1996), no. 4, 1051-1094.
[35] Y. Yomdin, *C^k-resolutions of semialgebraic mappings. Addendum to: Volume growth and entropy*, Israel J. Math. **57** (1987), no. 3, 301-317.
[36] Y. Yomdin, *Volume growth and entropy*, Israel J. Math. **57** (1987), no. 3, 285-300.

Institute of Analysis and Computational Number Theory (Math A), Graz University of Technology, Steyrergasse 30, A-8010 Graz, Austria
E-mail address: barroero@math.tugraz.at

Scuola Normale Superiore di Pisa, 56126 Pisa, Italy
E-mail address: martin.widmer@sns.it

COUNTING ALGEBRAIC INTEGERS OF FIXED DEGREE AND BOUNDED HEIGHT

FABRIZIO BARROERO

Abstract. Let k be a number field. For $\mathcal{H} \to \infty$, we give an asymptotic formula for the number of algebraic integers of absolute Weil height bounded by $\mathcal{H}$ and fixed degree over k.

1. Introduction

Let k be a number field of degree m over $\mathbb{Q}$. We count the number of algebraic integers β of degree e over k and bounded height. Here and in the rest of the article, by height we mean the multiplicative height H on the affine space $\overline{\mathbb{Q}}^n$ (see [3], 1.5.6).

For positive rational integers n and e, and a fixed algebraic closure $\overline{k}$ of k, let

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

where $k(\boldsymbol{\beta})$ is the field obtained by adjoining all the coordinates of $\boldsymbol{\beta}$ to k. By Northcott's Theorem [10] any subset of $k(n,e)$ of uniformly bounded height is finite. Therefore, for any subset S of $k(n,e)$ and $\mathcal{H} > 0$, we may introduce the following counting function

$$N(S,\mathcal{H}) = |\,\{\boldsymbol{\beta} \in S : H(\boldsymbol{\beta}) \leq \mathcal{H}\}\,|.$$

The counting function $N(k(n,e),\mathcal{H})$ has been investigated by various people. The best known and one of the earliest is a result of Schanuel [12] who gave an asymptotic formula for $N(k(n,1),\mathcal{H})$. The first who dropped the restriction of the coordinates to lie in a fix number field was Schmidt. In [13], he found upper and lower bounds for $N(k(n,e),\mathcal{H})$ and in [14] he gave an asymptotic formula for $N(\mathbb{Q}(n,2),\mathcal{H})$. Shortly afterwards, Gao [6] found the asymptotics for $N(\mathbb{Q}(n,e),\mathcal{H})$, provided $n > e$. Later Masser and Vaaler [9] established an asymptotic estimate for $N(k(1,e),\mathcal{H})$. Finally, Widmer [16] proved an asymptotic formula for $N(k(n,e),\mathcal{H})$ for arbitrary number fields k, 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.

2010 *Mathematics Subject Classification.* Primary 11G50, 11R04.

Key words and phrases. Heights, algebraic integers, counting.

F. Barroero is supported by the Austrian Science Foundation (FWF) project W1230-N13.

In this article we are interested in counting integral points, i.e., points $\boldsymbol{\beta} \in \overline{k}^n$, whose coordinates are algebraic integers. Let $\mathcal{O}_k$ and $\mathcal{O}_{\overline{k}}$ be, respectively, the ring of algebraic integers in k and $\overline{k}$. We introduce

$$\mathcal{O}_k(n,e) = k(n,e) \cap \mathcal{O}_{\overline{k}}^n = \{\boldsymbol{\beta} \in \mathcal{O}_{\overline{k}}^n : [k(\boldsymbol{\beta}) : k] = e\}.$$

Possibly, the first asymptotic result (besides the trivial cases $\mathcal{O}_{\mathbb{Q}}(n,1) = \mathbb{Z}^n$) can be found in Lang's book [7]. Lang states, without proof,

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

where $m = [k : \mathbb{Q}]$, q is the rank of the unit group of the ring of integers $\mathcal{O}_k$, and γ_k is an unspecified positive constant, depending on k. More recently, Widmer [15] established the following asymptotic formula

(1.1)

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

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. Widmer's result is fairly specific in the sense that he works only with the absolute non-logarithmic Weil height H. On the other hand, the methods used in [15] are quite general and powerful, and can probably be applied to handle other heights (such as the heights used by Masser and Vaaler in [9] to deduce their main result). As mentioned in [15] this might lead to multiterm expansions as in (1.1) for $N(\mathcal{O}_k(1,e), \mathcal{H})$.

However, for the moment, such generalizations of (1.1) are not available, and thus the work [15] does not provide any results in the case $n = 1$ and $e > 1$.

But Chern and Vaaler in [4], proved an asymptotic formula for the number of monic polynomials in $\mathbb{Z}[x]$ of given degree and bounded Mahler measure. Theorem 6 of [4] immediately implies the following result

$$N(\mathcal{O}_{\mathbb{Q}}(1,e), \mathcal{H}) = C_e \mathcal{H}^{e^2} + O\left(\mathcal{H}^{e^2-1}\right), \tag{1.2}$$

for some explicitly given positive real constant C_e. Theorem 1.1 extends Chern and Vaaler's result to arbitrary ground fields k.

For positive rational integers e we define

$$C_{\mathbb{R},e} = 2^{e-M} \left(\prod_{l=1}^{M} \left(\frac{2l}{2l+1} \right)^{e-2l} \right) \frac{e^M}{M!},$$

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

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

And, finally, let

$$C_k^{(e)} = \frac{e^{2q+1}2^{se}m^q}{q!\left(\sqrt{|\Delta_k|}\right)^e} C_{\mathbb{R},e}^r C_{\mathbb{C},e}^s, \tag{1.3}$$

where $m = [k : \mathbb{Q}]$, r is the number of real embeddings of k, s the number of pairs of complex conjugate embeddings, $q = r + s - 1$, and Δ_k denotes the discriminant of k. As usual, here and in the rest of this article, the empty product is 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 e be a positive integer, and let k be a number field. Then, as $\mathcal{H} \geq 2$ tends to infinity, we have*

$$N(\mathcal{O}_k(1,e),\mathcal{H}) = C_k^{(e)}\mathcal{H}^{me^2}(\log\mathcal{H})^q + \begin{cases} O\left(\mathcal{H}^{me^2}(\log\mathcal{H})^{q-1}\right), & \text{if } q \geq 1, \\ O\left(\mathcal{H}^{e(me-1)}\mathcal{L}\right), & \text{if } q = 0, \end{cases}$$

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

Let us mention two simple examples. The number of algebraic integers α quadratic over $\mathbb{Q}(\sqrt{2})$ with $H(\alpha) \leq \mathcal{H}$ is

$$32\mathcal{H}^8\log\mathcal{H} + O(\mathcal{H}^8).$$

In case $e = 3$, we have

$$108\sqrt{2}\mathcal{H}^{18}\log\mathcal{H} + O(\mathcal{H}^{18})$$

algebraic integers α cubic over $\mathbb{Q}(\sqrt{2})$ with $H(\alpha) \leq \mathcal{H}$.

Our approach is similar to the one used to obtain (1.2) above, because we count monic polynomials in $\mathcal{O}_k[X]$, but this is not a straightforward generalization of Theorem 6 of [4]. In fact, in [4] the estimate on the number of monic polynomials in $\mathbb{Z}[x]$ is obtained from a counting lattice points theorem, which is formulated only for the standard lattice $\mathbb{Z}^n$ ([4], Lemma 24). Our proof relies on a new counting theorem for points of an arbitrary lattice in definable sets in an o-minimal structure [1]. Moreover, our proof is fairly short, and more straightforward than the approach of [15], but to the expense that we do not get a multiterm expansion.

In [9], Masser and Vaaler observed that the limit for $\mathcal{H} \to \infty$ of

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

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

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

If we consider only the first term in (1.1), and combine it with Theorem 1.1 we see that

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

is a rational number depending only on e, r and s. As Masser and Vaaler did, one can ask again whether

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

2. Counting monic polynomials

In this section we see how our problem translates to counting monic polynomials of fixed degree that assume a uniformly bounded value under a certain real valued function called M^k, defined using the Mahler measure.

Recall we fixed a number field k of degree m over $\mathbb{Q}$ and $\mathcal{O}_k$ is its ring of integers. Let $\sigma_1,\dots,\sigma_r$ be the real embeddings of k and $\sigma_{r+1},\dots,\sigma_m$ be the strictly complex ones, indexed in such a way that $\sigma_j = \overline{\sigma}_{j+s}$ for $j = r+1,\dots,r+s$. Therefore, r and s are, respectively, the number of real and pairs of conjugate complex embeddings of k and $m = r+2s$. We put $d_i = 1$ for $i = 1,\dots,r$ and $d_i = 2$ for $i = r+1,\dots,r+s$ and fix a positive integer e. Let us recall the definition of the Mahler measure.

Definition 2.1. *If $f = z_0X^d + z_1X^{d-1} + \cdots + z_d \in \mathbb{C}[X]$ is a non-zero polynomial of degree d with roots $\alpha_1,\dots,\alpha_d$, the Mahler measure of f is defined to be*

$$M(f) = |z_0| \prod_{i=1}^{d} \max\{1,|\alpha_i|\}.$$

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

We see M as a function $\mathbb{C}[X] \to [0,\infty)$ and define

$$\begin{array}{rccc} M^k: & k[X] & \to & [0,\infty) \\ & f & \mapsto & \prod_{i=1}^{r+s} M(\sigma_i(f))^{\frac{d_i}{m}}, \end{array}$$

where σ_i acts on the coefficients of f. Note that, for every $\alpha \in \mathcal{O}_k$,

$$M^k(X-\alpha) = \prod_{i=1}^{r+s} \max\{1,|\sigma_i(\alpha)|\}^{\frac{d_i}{m}} = H(\alpha). \tag{2.1}$$

In fact, if $\alpha \in \mathcal{O}_k$ then $|\alpha|_v \le 1$ for every non-archimedean place v of k.

Moreover, the Mahler measure is multiplicative by definition, i.e.,

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

and one can see that

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

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

For some positive integer e and some $\mathcal{H} > 0$, we define $\mathcal{M}^k(e, \mathcal{H})$ to be the set of monic $f \in \mathcal{O}_k[X]$ of degree e and $M^k(f) \leq \mathcal{H}$. It is easy to see that $\mathcal{M}^k(e, \mathcal{H})$ is finite for all $\mathcal{H}$. The following theorem gives an estimate for its cardinality.

Theorem 2.1. *For every $\mathcal{H}_0 > 1$ there exists a D_0 such that, for every $\mathcal{H} \geq \mathcal{H}_0$,*

(2.2)
$$\left| \left|\mathcal{M}^k(e, \mathcal{H})\right| - \frac{C_k^{(e)}}{e^{q+1}} \mathcal{H}^{me} (\log \mathcal{H})^q \right| \leq \begin{cases} D_0 \mathcal{H}^{me} (\log \mathcal{H})^{q-1}, & \text{if } q \geq 1, \\ D_0 \mathcal{H}^{me-1}, & \text{if } q = 0, \end{cases}$$

where $q = r + s - 1$. The constant D_0 depends only on $\mathcal{H}_0$, m and e.

Note that our constant $C_k^{(e)}$ defined in (1.3), is bounded if we fix m and e and we let k vary among all number fields of degree m. This implies that there exists a real constant $C^{(m,e)}$, depending only on m and e, such that $\left|\mathcal{M}^k(e, \mathcal{H})\right|$ is bounded from above by

$$C^{(m,e)} \mathcal{H}^{me} (\log \mathcal{H} + 1)^q, \tag{2.3}$$

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

We prove Theorem 2.1 later and for the rest of this section we derive Theorem 1.1 from Theorem 2.1. We follow the line of Masser and Vaaler [9].

Now we want to restrict to monic f irreducible over k. Let $\widetilde{\mathcal{M}}^k(e, \mathcal{H})$ be the set of polynomials in $\mathcal{M}^k(e, \mathcal{H})$ that are irreducible over k.

Corollary 2.2. *For every $\mathcal{H}_0 > 1$ there exists an F_0 such that, for every $\mathcal{H} \geq \mathcal{H}_0$,*

(2.4)
$$\left| \left|\widetilde{\mathcal{M}}^k(e, \mathcal{H})\right| - \frac{C_k^{(e)}}{e^{q+1}} \mathcal{H}^{me} (\log \mathcal{H})^q \right| \leq \begin{cases} F_0 \mathcal{H}^{me} (\log \mathcal{H})^{q-1}, & \text{if } q \geq 1, \\ F_0 \mathcal{H}^{me-1} \mathcal{L}, & \text{if } q = 0, \end{cases}$$

where $\mathcal{L} = \log \mathcal{H}$ if $(m, e) = (1, 2)$ and 1 otherwise. The constant F_0 depends again only on $\mathcal{H}_0$, m and e.

Proof. For $e = 1$ there is nothing to prove. Suppose $e > 1$. We show that, up to a constant, the number of all monic reducible $f \in \mathcal{O}_k[X]$ of degree e with $M^k(f) \leq \mathcal{H}$ is not larger than the right hand side of (2.2), except for the case $(m, e) = (1, 2)$.

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

$$1 \leq l \leq \frac{\log \mathcal{H}}{\log 2} + 1 \leq 2 \log \mathcal{H} + 1. \tag{2.5}$$

Since M^k is multiplicative,

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

Using (2.3) and noting that $2^l \leq 2\mathcal{H}$, we can say that there are at most

$$C^{(m,a)} \left(2^l\right)^{ma} \left(\log 2^l + 1\right)^q \leq C^{(m,a)} \left(2^l\right)^{ma} (\log \mathcal{H} + 2)^q$$

possibilities for g and

$$C^{(m,b)} \left(2^{1-l}\mathcal{H}\right)^{mb} \left(\log\left(2^{1-l}\mathcal{H}\right) + 1\right)^q \leq C^{(m,b)} \left(2^{1-l}\mathcal{H}\right)^{mb} (\log \mathcal{H} + 2)^q$$

possibilities for h. Therefore, we have at most

$$C'\mathcal{H}^{mb} 2^{ml(a-b)} (\log \mathcal{H} + 2)^{2q} \tag{2.6}$$

possibilities for gh with $M^k(gh) \leq \mathcal{H}$ and $2^{l-1} \leq M^k(g) < 2^l$, where C' is a real constant. Since there are only finitely many choices for a and b we can take C' to depend only on m and e.

If $a = b = \frac{e}{2}$ then (2.6) is

$$C'\mathcal{H}^{m\frac{e}{2}} (\log \mathcal{H} + 2)^{2q}.$$

Summing over all l, $1 \leq l \leq \lfloor 2 \log \mathcal{H} \rfloor + 1$ (recall (2.5)), gives an extra factor $2 \log \mathcal{H} + 1$. Therefore, when $a = b$, there are at most

$$C'\mathcal{H}^{\frac{me}{2}} (2 \log \mathcal{H} + 2)^{2q+1}$$

possibilities for $f = gh$, with $M^k(f) \leq \mathcal{H}$. If $(m, e) \neq (1, 2)$, this has smaller order than the right hand side of (2.2), since $me > 2$ implies $\frac{me}{2} < me - 1$. In the case $(m, e) = (1, 2)$ we get $C'\mathcal{H}(2 \log \mathcal{H} + 2)$ and we need an additional logarithm factor.

In the case $a < b$, summing $2^{ml(a-b)}$ over all l, $1 \leq l \leq \lfloor 2 \log \mathcal{H} \rfloor + 1 = L$, we get

$$\sum_{l=1}^{L} \left(2^{m(a-b)}\right)^l \leq \sum_{l=1}^{L} 2^{-l} \leq 1.$$

Thus, recalling $b \leq e - 1$, when $a < b$, there are at most

$$C''\mathcal{H}^{m(e-1)} (\log \mathcal{H} + 2)^{2q}$$

possibilities for $f = gh$, with $M^k(f) \leq \mathcal{H}$, where again C'' depends only on m and e. This is again not larger than the right hand side of (2.2). □

For the last step of the proof we link such monic irreducible polynomials with their roots.

Lemma 2.3. *An algebraic integer β has degree e over k and $H(\beta) \leq \mathcal{H}$ if and only if it is a root of a monic irreducible polynomial $f \in \mathcal{O}_k[X]$ of degree e with $M^k(f) \leq \mathcal{H}^e$*

Proof. Suppose $f \in \mathcal{O}_k[X]$ is a monic irreducible polynomial of degree e and β is one of its roots, i.e., β is an algebraic integer with $[k(\beta) : k] = e$ and minimal polynomial f over k. We claim that

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

The function M^k is independent of the field k and we can define an absolute $M^{\overline{\mathbb{Q}}}$ over $\overline{\mathbb{Q}}[X]$ that, restricted to any $k[X]$, equals 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 [3], Lemma 1.5.2).

Suppose $f = (X-\alpha_1)\cdots(X-\alpha_e)$. Since the α_i are algebraic integers, by (2.1), we have

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

and the α_i have the same height because they are conjugate (see [3], Proposition 1.5.17). Moreover, by the multiplicativity of M^k we can see that

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

for any α_j root of f. □

Lemma 2.3 implies that $N(\mathcal{O}_k(1,e),\mathcal{H}) = e\left|\widetilde{\mathcal{M}}^k(e,\mathcal{H}^e)\right|$ because there are e different β with the same minimal polynomial f over k. Therefore, by (2.4), we have that for every $\mathcal{H}_0 > 1$ there exists a C_0, depending only on $\mathcal{H}_0$, m and e, such that for every $\mathcal{H} \geq \mathcal{H}_0$,

$$\left|N(\mathcal{O}_k(1,e),\mathcal{H}) - C_k^{(e)}\mathcal{H}^{me^2}(\log\mathcal{H})^q\right| \leq \begin{cases} C_0\mathcal{H}^{me^2}(\log\mathcal{H})^{q-1}, & \text{if } q \geq 1, \\ C_0\mathcal{H}^{e(me-1)}\mathcal{L}, & \text{if } q = 0, \end{cases}$$

where $\mathcal{L} = \log\mathcal{H}$ if $(m,e) = (1,2)$ and 1 otherwise. We get Theorem 1.1 by choosing $\mathcal{H}_0 = 2$.

3. A counting principle

In this section we introduce the counting theorem that will be used to prove Theorem 2.1. The principle dates back to Davenport [5] and was developed by several authors. In a previous work [1] the author and Widmer formulated a counting theorem that relies on Davenport's

result and uses o-minimal structures. The full generality of Theorem 1.3 of [1] is not needed here as we are going to count lattice points in semialgebraic sets.

Definition 3.1. *Let N, 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 $=$.

A very important feature of semialgebraic sets is the fact that this collection of subsets of the Euclidean spaces is closed under projections. This is the well known Tarski-Seidenberg principle.

Theorem 3.1 ([2], 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.*

Let $S \subseteq \mathbb{R}^{n+n'}$, for a $\boldsymbol{t} \in \mathbb{R}^{n'}$ we call $S_{\boldsymbol{t}} = \{\boldsymbol{x} \in \mathbb{R}^n : (\boldsymbol{x}, \boldsymbol{t}) \in S\}$ the fiber of S above $\boldsymbol{t}$. Clearly, if S is semialgebraic also the fibers $S_{\boldsymbol{t}}$ are semialgebraic. If so, we call S a semialgebraic family.

Let Λ be a lattice of $\mathbb{R}^n$, i.e., the $\mathbb{Z}$-span of n linearly independent vectors of $\mathbb{R}^n$. Let $\lambda_i = \lambda_i(\Lambda)$ for $i = 1, \dots, n$ be the successive minima of Λ with respect to the zero centered unit ball $B_0(1)$, i.e., for $i = 1, ..., n$

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

The following theorem is a special case of Theorem 1.3 of [1].

Theorem 3.2. *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, for every $\boldsymbol{t} \in \mathbb{R}^{n'}$,*

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

where $V_j(Z_{\boldsymbol{t}})$ 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 $V_0(Z_{\boldsymbol{t}}) = 1$.

4. A semialgebraic family

In this section we introduce the family we want to apply Theorem 3.2 to.

We see the Mahler measure as a function of the coefficients of the polynomial. We fix $n > 0$ and define $M : \mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1} \to [0, \infty)$ such that

$$M(z_0, \dots, z_n) = M(z_0 X^n + \cdots + z_n).$$

These two functions satisfy the definition of bounded distance function in the sense of the geometry of numbers, i.e.,

(1) M is continuous;
(2) $M(\boldsymbol{z}) = 0$ if and only if $\boldsymbol{z} = \mathbf{0}$;
(3) $M(w\boldsymbol{z}) = |w|M(\boldsymbol{z})$, for any scalar $w \in \mathbb{R}$ or $\mathbb{C}$.

Properties (2) and (3) are obvious from the definition, while continuity was proved already by Mahler (see [8], Lemma 1).

Let M_1 be the monic Mahler measure function, i.e., $M_1(\boldsymbol{z}) = M(1, \boldsymbol{z})$ for $\boldsymbol{z} \in \mathbb{R}^n$ or $\mathbb{C}^n$.

In the following we consider the complex monic Mahler measure as a function M_1

$$\begin{array}{ccc} \mathbb{R}^{2n} & \to & \mathbb{R} \\ (x_1, \dots, x_{2n}) & \mapsto & M\left(X^n + (x_1 + ix_2)X^{n-1} + \cdots + x_{2n-1} + ix_{2n}\right). \end{array}$$

We fix positive integers n, m, r, s with $m = r + 2s$ and $d_1, \dots d_{r+s}$ such that $d_i = 1$ for $i = 1, \dots, r$ and $d_i = 2$ for $i = r+1, \dots, r+s$.

We define

(4.1)

$$Z = \left\{ (\boldsymbol{x}_1, \dots, \boldsymbol{x}_{r+s}, t) \in (\mathbb{R}^n)^r \times \left(\mathbb{R}^{2n}\right)^s \times \mathbb{R} : \prod_{i=1}^{r+s} M_1(\boldsymbol{x}_i)^{d_i} \le t \right\}.$$

Here $\boldsymbol{x}_i \in \mathbb{R}^{d_i n}$ and $M_1(\boldsymbol{x}_i)$ is the real or the complex monic Mahler measure respectively if $i = 1, \dots, r$ or $i = r+1, \dots, r+s$.

We want to count lattice points in the fibers $Z_t \subseteq \mathbb{R}^{mn}$ using Theorem 3.2, therefore we need to show that Z is a semialgebraic set and that the fibers Z_t are bounded.

Lemma 4.1. *The set Z defined in (4.1) is semialgebraic.*

Proof. Recall the definition of Z. To each $\boldsymbol{x}_i \in \mathbb{R}^{d_i n}$ corresponds a monic polynomial f_i of degree n with real (for $i = 1, \dots r$) or complex (for $i = r+1, \dots r+s$) coefficients. Let S be the set of points

$$\left(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{r+s}, t, t_1, \dots, t_{r+s}, \boldsymbol{\alpha}^{(1)}, \boldsymbol{\beta}^{(1)}, \dots, \boldsymbol{\alpha}^{(r+s)}, \boldsymbol{\beta}^{(r+s)}\right)$$

in $\mathbb{R}^{n(r+2s)+1+r+s+2n(r+s)}$, with $\boldsymbol{\alpha}^{(i)}, \boldsymbol{\beta}^{(i)} \in \mathbb{R}^n$, such that

- $\boldsymbol{\alpha}^{(i)}$ and $\boldsymbol{\beta}^{(i)}$ are, respectively, the vectors of the real and the imaginary parts of the n roots of f_i, for every $i = 1, \dots, r+s$;
- $\prod_{l=1}^{n} \max\left\{1, \left(\alpha_l^{(i)}\right)^2 + \left(\beta_l^{(i)}\right)^2\right\} = t_i^2$ and $t_i \ge 0$, for every $i = 1, \dots, r+s$;
- $\prod_{i=1}^{r+s} t_i^{d_i} \le t$.

It is clear that the set S is defined by polynomial equalities and inequalities. In fact, the first condition is enforced by the fact that the coordinates of $\boldsymbol{x}_i$ are the images of $\boldsymbol{\alpha}^{(i)}$ and $\boldsymbol{\beta}^{(i)}$ under the appropriate symmetric functions, which are polynomials. The second and the

third conditions are also clearly obtained by polynomial equalities and inequalities. Therefore, S is a semialgebraic set. The claim follows after noting that Z is nothing but the projection of S on the first $n(r+2s)+1$ coordinates and applying the Tarski-Seidenberg principle (Theorem 3.1). □

By Lemma 1.6.7 of [3], there exists a positive real constant $\gamma \leq 1$ such that

$$\gamma|\boldsymbol{z}|_\infty \leq M(\boldsymbol{z}), \text{ for every } \boldsymbol{z} \in \mathbb{R}^{n+1} \text{ or } \mathbb{C}^{n+1},$$

where, if $\boldsymbol{z} = (z_0, \dots, z_n) \in \mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$, $|\boldsymbol{z}|_\infty = \max\{|z_0|, \dots, |z_n|\}$ is the usual max norm. Clearly we have, for $\boldsymbol{x} \in \mathbb{R}^n$

$$N(\boldsymbol{x}) := \gamma|(1, \boldsymbol{x})|_\infty \leq M_1(\boldsymbol{x}) \tag{4.2}$$

in the real case and, for the complex case,

$$N(\boldsymbol{x}) := \gamma|(1, \boldsymbol{x})|_\infty \leq \gamma|(1, \boldsymbol{z})|_\infty \leq M_1(\boldsymbol{z}) = M_1(\boldsymbol{x}), \tag{4.3}$$

where $\boldsymbol{x} = (x_1, \dots, x_{2n}) \in \mathbb{R}^{2n}$ and $\boldsymbol{z} = (x_1 + ix_2, \dots, x_{2n-1} + ix_{2n})$.

Recall that, by the definition, the monic Mahler measure function assumes values greater than or equal to 1, therefore, if $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{r+s}) \in Z_t$ then $M_1(\boldsymbol{x}_i)^{d_i} \leq t$ for every i. Thus, $|\boldsymbol{x}_i|_\infty^{d_i} \leq \frac{t}{\gamma^{d_i}}$ and this means that Z_t is bounded for every $t \in \mathbb{R}$.

Now we can apply Theorem 3.2 to the family Z. If we set $Z(T) = Z_T$, we have

$$\left| |Z(T) \cap \Lambda| - \frac{\mathrm{Vol}(Z(T))}{\det \Lambda} \right| \leq \sum_{j=0}^{mn-1} C \frac{V_j(Z(T))}{\lambda_1 \cdots \lambda_j}, \tag{4.4}$$

for every $T \in \mathbb{R}$, where Λ is a lattice in $\mathbb{R}^{mn}$ and C is a real constant independent of Λ and 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 $\mathbb{R}^{mn}$ and $V_0(Z(T)) = 1$.

5. Proof of Theorem 2.1

We fix a number field k of degree m over $\mathbb{Q}$. The ring of integers $\mathcal{O}_k$ of k, embedded into $\mathbb{R}^{r+2s}$ via $\sigma = (\sigma_1, \dots, \sigma_{r+s})$, is a lattice of full rank. We embed $(\mathcal{O}_k)^n$ in $\mathbb{R}^{mn}$ via $\boldsymbol{a} \mapsto (\sigma_1(\boldsymbol{a}), \dots, \sigma_{r+s}(\boldsymbol{a}))$, where the σ_i are extended to k^n. We want to count lattice points of $\Lambda = (\mathcal{O}_k)^n$ inside $Z(T)$.

Lemma 5.1. *We have*

$$\det \Lambda = \left(2^{-s}\sqrt{|\Delta_k|}\right)^n,$$

and its first successive minimum is $\lambda_1 \geq 1$.

Proof. This is a special case of Lemma 5 of [9]. □

Now we need to calculate the volume of $Z(T)$. We do something more general. Suppose we have $r+s$ continuous functions $f_i : \mathbb{R}^{n_i} \to [1,\infty)$, $i = 1,\dots,r+s$ where $1 \leq n_i \leq d_i n$ for every i. We define

$$Z_i(T) = \{\boldsymbol{x} \in \mathbb{R}^{n_i} : f_i(\boldsymbol{x}) \leq T\}, \tag{5.1}$$

for every $i = 1,\dots,r+s$. Suppose that, for every i, there exists a polynomial $p_i(X) \in \mathbb{R}[X]$ of degree n_i such that the volume of $Z_i(T)$ is $p_i(T)$ for every $T \geq 1$. Let C_i be the leading coefficient of p_i. Moreover, let

$$\widetilde{Z}(T) = \left\{ (\boldsymbol{x}_1,\dots,\boldsymbol{x}_{r+s}) \in \mathbb{R}^{\sum n_i} : \prod_{i=1}^{r+s} f_i(\boldsymbol{x}_i)^{d_i} \leq T \right\}.$$

Note that, since $f_i(\boldsymbol{x}_i) \geq 1$ for every i, $\widetilde{Z}(T)$ is bounded for every T.

Lemma 5.2. *Let $q = r+s-1$. Under the hypotheses and the notation from above, for every $T \geq 1$, we have*

$$\mathrm{Vol}\left(\widetilde{Z}(T)\right) = \widetilde{p}\left(T^{\frac{1}{2}}, \log T\right),$$

where $\widetilde{p}(X,Y) \in \mathbb{R}[X,Y]$, $\deg_X \widetilde{p} \leq 2n$, $\deg_Y \widetilde{p} \leq q$. In the case $n_i = d_i n$ for every $i = 1,\dots,r+s$, the coefficient of $X^{2n}Y^q$ is $\frac{n^q}{q!}\prod_{i=1}^{q+1} C_i$. If $n_i < d_i n$ for some i then the monomial $X^{2n}Y^q$ does not appear in $\widetilde{p}$.

Proof. We have

$$V(T) := \mathrm{Vol}\left(\widetilde{Z}(T)\right) = \int_{\widetilde{Z}(T)} \mathrm{d}\boldsymbol{x}_1 \dots \mathrm{d}\boldsymbol{x}_{q+1}.$$

We proceed by induction on q. If $q = 0$ there is nothing to prove. Suppose $q > 0$ and let

$$\widetilde{Z}^{(q)}(T) = \left\{ (\boldsymbol{x}_1,\dots,\boldsymbol{x}_q) \in \mathbb{R}^{n_1+\dots+n_q} : \prod_{i=1}^{q} f_i(\boldsymbol{x}_i)^{d_i} \leq T \right\}.$$

Then

$$V(T) = \int_{Z_{q+1}\left(T^{\frac{1}{d_{q+1}}}\right)} \left(\int_{\widetilde{Z}^{(q)}\left(T f_{q+1}(\boldsymbol{x}_{q+1})^{-d_{q+1}}\right)} \mathrm{d}\boldsymbol{x}_1 \dots \mathrm{d}\boldsymbol{x}_q \right) \mathrm{d}\boldsymbol{x}_{q+1}.$$

By the inductive hypothesis there exists $\widetilde{p}_q(X,Y) \in \mathbb{R}[X,Y]$ such that $V(T)$ equals

$$\int_{Z_{q+1}\left(T^{\frac{1}{d_{q+1}}}\right)} \widetilde{p}_q\left(\left(\frac{T}{f_{q+1}(\boldsymbol{x}_{q+1})^{d_{q+1}}} \right)^{\frac{1}{2}}, \log\left(\frac{T}{f_{q+1}(\boldsymbol{x}_{q+1})^{d_{q+1}}} \right) \right) \mathrm{d}\boldsymbol{x}_{q+1},$$

where $\widetilde{p}_q(X,Y) \in \mathbb{R}[X,Y]$, $\deg_X \widetilde{p}_q \leq 2n$, $\deg_Y \widetilde{p}_q \leq q-1$ and, if $n_i = d_i n$ for every $i = 1,\dots,q$, the coefficient of $X^{2n}Y^{q-1}$ is $\frac{n^{q-1}}{(q-1)!}\prod_{i=1}^{q} C_i$. If not, that monomial does not appear.

By $\mathcal{L}^n$, we indicate the Lebesgue measure on $\mathbb{R}^n$. Since f_{q+1} is a measurable function, we get

$$V(T) = \int_{\left[1,T^{\frac{1}{d_{q+1}}}\right]} \widetilde{p}_q \left(\left(\frac{T}{X^{d_{q+1}}} \right)^{\frac{1}{2}}, \log \left(\frac{T}{X^{d_{q+1}}} \right) \right) \mathrm{d} \left(\mathcal{L}^{n_{q+1}} \circ f_{q+1}^{-1} \right)(X),$$

where we consider $\mathcal{L}^{n_{q+1}} \circ f_{q+1}^{-1}$ as a measure on $\left[1, T^{\frac{1}{d_{q+1}}}\right]$. In particular for $(u,v] \subseteq \left[1, T^{\frac{1}{d_{q+1}}}\right]$,

$$\left(\mathcal{L}^{n_{q+1}} \circ f_{q+1}^{-1} \right)((u,v]) = p_{q+1}(v) - p_{q+1}(u),$$

and $\left(\mathcal{L}^{n_{q+1}} \circ f_{q+1}^{-1} \right)(\{1\}) = p_{q+1}(1)$. Using 1.29 Theorem of [11], we get

$$\begin{aligned} V(T) = & \int_{\left(1,T^{\frac{1}{d_{q+1}}}\right]} \widetilde{p}_q \left(\left(\frac{T}{X^{d_{q+1}}} \right)^{\frac{1}{2}}, \log \left(\frac{T}{X^{d_{q+1}}} \right) \right) p'_{q+1}(X) \mathrm{d}\mathcal{L}^1(X) \\ & + \widetilde{p}_q \left(T^{\frac{1}{2}}, \log T \right) p_{q+1}(1), \end{aligned}$$

where p'_{q+1} is the derivative of p_{q+1}.

For some integer $c \geq 0$ we put $L(X,c) = X^c$ in case $c > 0$ and $L(X,0) = 1$. Because of the linearity of the integral we are reduced to calculate

$$\begin{aligned} \mathcal{I}(a,b,c) &= \int_1^{T^{\frac{1}{d_{q+1}}}} X^a \left(\frac{T}{X^{d_{q+1}}} \right)^{\frac{b}{2}} L \left(\log \frac{T}{X^{d_{q+1}}}, c \right) \mathrm{d}X \\ &= T^{\frac{b}{2}} \int_1^{T^{\frac{1}{d_{q+1}}}} X^{a - \frac{b}{2} d_{q+1}} L \left(\log T - \log \left(X^{d_{q+1}} \right), c \right) \mathrm{d}X, \end{aligned}$$

for some integers a, b, c, with $0 \leq a \leq n_{q+1} - 1$, $0 \leq b \leq 2n$ and $0 \leq c \leq q-1$. We have three possibilities. If $a - \frac{b}{2} d_{q+1} = -1$, then

$$\begin{aligned} \mathcal{I}(a,b,c) &= T^{\frac{b}{2}} \int_1^{T^{\frac{1}{d_{q+1}}}} X^{-1} L \left(\log T - \log \left(X^{d_{q+1}} \right), c \right) \mathrm{d}X \\ &= \frac{1}{(c+1) d_{q+1}} T^{\frac{b}{2}} \left(\log T \right)^{c+1}. \end{aligned}$$

If $a - \frac{b}{2} d_{q+1} \neq -1$ and $c = 0$,

$$\mathcal{I}(a,b,0) = \frac{T^{\frac{b}{2}}}{a - \frac{b}{2} d_{q+1} + 1} \left(T^{\frac{a - \frac{b}{2} d_{q+1} + 1}{d_{q+1}}} - 1 \right) = \frac{T^{\frac{a+1}{d_{q+1}}} - T^{\frac{b}{2}}}{a - \frac{b}{2} d_{q+1} + 1}.$$

If $a - \frac{b}{2} d_{q+1} \neq -1$ and $c \neq 0$, then

$$\mathcal{I}(a,b,c) = -\frac{T^{\frac{b}{2}} \left(\log T \right)^c}{a - \frac{b}{2} d_{q+1} + 1} + \frac{c d_{q+1}}{a - \frac{b}{2} d_{q+1} + 1} \mathcal{I}(a,b,c-1).$$

Therefore, one can see that $\mathcal{I}(a,b,c)$ is a polynomial in $T^{\frac{1}{2}}$ and $\log T$. In particular $\mathcal{I}(a,b,c) = \widehat{p}(T^{\frac{1}{2}}, \log T)$, where $\widehat{p}(X,Y) \in \mathbb{R}[X,Y]$, with $\deg_X \widehat{p} \leq 2n$ and $\deg_Y \widehat{p} \leq q$. Note that in the case $a = d_{q+1}n - 1$, $b = 2n$ and $c = q-1$, the coefficient of $X^{2n}Y^q$ is $\frac{1}{qd_{q+1}}$ and 0 for any other choice of a, b and c. Therefore, the monomial $X^{2n}Y^q$ does not appear in $\widehat{p}$ if either $n_{q+1} < d_{q+1}n$ or $X^{2n}Y^{q-1}$ does not appear in $\widetilde{p}_q$, i.e., if $n_i < d_i n$ for some i. To conclude, recall that, in the case $n_i = d_i n$ for every $i = 1, \ldots, r+s$, p'_{q+1} has leading coefficient $nd_{q+1}C_{q+1}$ and the coefficient of $X^{2n}Y^{q-1}$ in $\widetilde{p}_q$ is $\frac{n^{q-1}}{(q-1)!}\prod_{i=1}^{q} C_i$, thus, the coefficient in front of $\mathcal{I}(d_{q+1}n-1, 2n, q-1)$ in $V(T)$ is $\frac{n^q d_{q+1}}{(q-1)!}\prod_{i=1}^{q+1} C_i$. □

The volumes of the sets

$$\{(z_1, \ldots, z_n) \in \mathbb{R}^n : M(1, z_1, \ldots, z_n) \leq T\} \tag{5.2}$$

and

$$\{(z_1, \ldots, z_n) \in \mathbb{C}^n : M(1, z_1, \ldots, z_n)^2 \leq T\} \tag{5.3}$$

were computed by Chern and Vaaler in [4]. By (1.16) and (1.17) of [4], these volumes are, for every $T \geq 1$, polynomials $p_{\mathbb{R}}(T)$ and $p_{\mathbb{C}}(T)$ of degree n and leading coefficients, respectively,

$$C_{\mathbb{R},n} = 2^{n-M}\left(\prod_{l=1}^{M}\left(\frac{2l}{2l+1}\right)^{n-2l}\right)\frac{n^M}{M!},$$ [1]

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

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

Suppose $q = 0$ and recall Lemma 5.1. In this case $Z(T)$ corresponds to (5.2) if $m = 1$ or to (5.3) if $m = 2$. We have

$$\frac{\mathrm{Vol}(Z(T))}{\det \Lambda} = \frac{2^{sn}}{\left(\sqrt{|\Delta_k|}\right)^n} C_{\mathbb{R},n}^r C_{\mathbb{C},n}^s T^n + \frac{P(T)}{\left(\sqrt{|\Delta_k|}\right)^n}, \tag{5.4}$$

for every $T > 1$, where $P(X) \in \mathbb{R}[X]$ depends only on n, r and s and has degree at most $n-1$.

Corollary 5.3. *Suppose $q > 0$. We have, for $T > 1$,*

(5.5)

$$\frac{\mathrm{Vol}(Z(T))}{\det \Lambda} = \frac{n^q 2^{sn}}{q!\left(\sqrt{|\Delta_k|}\right)^n} C_{\mathbb{R},n}^r C_{\mathbb{C},n}^s T^n (\log T)^q + \frac{P\left(T^{\frac{1}{2}}, \log T\right)}{\left(\sqrt{|\Delta_k|}\right)^n},$$

where $P(X,Y) \in \mathbb{R}[X,Y]$ depends on n, r and s, $\deg_X P \leq 2n$, $\deg_Y P \leq q$ and the coefficient of $X^{2n}Y^q$ is 0.

[1] There is a misprint in (1.16) of [4], 2^{-N} should read 2^{-M}.

Proof. By Lemma 5.2 and the result of Chern and Vaaler about the volumes of the sets defined in (5.2) and (5.3), the volume of $Z(T)$ is $p(T^{\frac{1}{2}}, \log T)$ where $p(X,Y) \in \mathbb{R}[X,Y]$, $\deg_X p \leq 2n$, $\deg_Y p \leq q$ and the coefficient of $X^{2n}Y^q$ is $\frac{n^q}{q!} C^r_{\mathbb{R},n} C^s_{\mathbb{C},n}$. □

Therefore, recalling $|\Delta_k|$ and $\lambda_1, \dots, \lambda_{mn}$ are greater than or equal to 1, by (5.4) and Corollary 5.3, (4.4) becomes

$$\left| |Z(T) \cap \Lambda| - \frac{n^q 2^{sn}}{q! \left(\sqrt{|\Delta_k|}\right)^n} C^r_{\mathbb{R},n} C^s_{\mathbb{C},n} T^n (\log T)^q \right| \leq \sum_{j=0}^{mn-1} C V_j(Z(T)) + Q(T), \tag{5.6}$$

for every $T > 1$, where $Q(T)$ is the function of T obtained from the polynomial P of (5.4) or (5.5) substituting the coefficients with their absolute values. Note that Q depends only on m and n.

Now we want to find a bound for $V_j(Z(T))$. Recall that in (4.2) and (4.3) we have defined a function $N(\boldsymbol{x}) = \gamma |(1, \boldsymbol{x})|_\infty$ such that $N(\boldsymbol{x}) \leq M_1(\boldsymbol{x})$. Let

$$Z'(T) = \left\{ (\boldsymbol{x}_1, \dots, \boldsymbol{x}_{r+s}) \in \mathbb{R}^{mn} : \prod_{i=1}^{r+s} N(\boldsymbol{x}_i)^{d_i} \leq T \right\}.$$

Each $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{r+s})$ with $\prod_{i=1}^{r+s} M_1(\boldsymbol{x}_i)^{d_i} \leq T$ satisfies $\prod_{i=1}^{r+s} N(\boldsymbol{x}_i)^{d_i} \leq T$. Therefore, we have $Z(T) \subseteq Z'(T)$ and $V_j(Z(T)) \leq V_j(Z'(T))$.

Suppose $q = 0$. This means that k is either $\mathbb{Q}$ ($m = 1$) or an imaginary quadratic field ($m = 2$). In any case any projection of $Z'(T)$ to a j-dimensional coordinate subspace has volume $\left(\frac{2}{\gamma}\right)^j T^{\frac{j}{m}}$ if $T \geq \gamma^m$, for every $j = 1, \dots mn - 1$. Therefore we obtain

$$V_j(Z(T)) \leq V_j\left(Z'(T)\right) \leq E T^{n - \frac{1}{m}}, \tag{5.7}$$

for some real constant E depending only on n and m. This holds for every $T > 1$ since $\gamma \leq 1$.

Now suppose $q > 0$.

Lemma 5.4. *For every $j = 1, \dots, mn - 1$, there exists a polynomial $P_j(X,Y) \in \mathbb{R}[X,Y]$ whose coefficients depend only on m and n, with $\deg_X P_j \leq 2n$, $\deg_Y P_j \leq q$, and the coefficient of $X^{2n}Y^q$ is 0, such that, for every $T > 1$, we have*

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

Proof. By definition, the projection of $Z'(T)$ on a j-dimensional coordinate subspace is just the intersection of $Z'(T)$ with such subspace. To each such subspace Σ we can associate integers $n_1, \dots, n_{r+s}$ with

$0 \leq n_i \leq d_i n$ such that Σ is defined by setting $d_i n - n_i$ coordinates of each $\boldsymbol{x}_i$ to 0. Therefore we are in the situation of Lemma 5.2 because, after dividing by γ, we have, for every i such that $n_i > 0$, a continuous function $f_i : \mathbb{R}^{n_i} \to [1, \infty)$, with $\sum n_i = j$. This gives rise to sets of the form (5.1), whose volumes are $2^{n_i} T^{n_i}$. Since $j < mn$, not all n_i can be equal to $d_i n$. Therefore, by Lemma 5.2, the volume of any such projection equals a polynomial with the desired property and we have the claim. □

Recall the definition of $\mathcal{M}^k(e, \mathcal{H})$ that was given in Section 2. Clearly $\left|\mathcal{M}^k(e, \mathcal{H})\right|$ is the number of $\boldsymbol{a} \in \mathcal{O}_k^e$ with $\prod_{i=1}^{r+s} M_1\left(\sigma_i(\boldsymbol{a})\right)^{d_i} \leq \mathcal{H}^m$, i.e., $|Z(\mathcal{H}^m) \cap \mathcal{O}_k^e|$.

By (5.6), (5.7) and Lemma 5.4 we have, for every $\mathcal{H} > 1$,

$$\left| \left|\mathcal{M}^k(e, \mathcal{H})\right| - \frac{e^q m^q 2^{se}}{q! \left(\sqrt{|\Delta_k|}\right)^e} C_{\mathbb{R},e}^r C_{\mathbb{C},e}^s \mathcal{H}^{me} \left(\log \mathcal{H}\right)^q \right| \leq E(\mathcal{H}),$$

with

$$E(\mathcal{H}) = \begin{cases} \sum_{i=0}^{2e} \sum_{j=0}^{q} E_{i,j} \mathcal{H}^{\frac{mi}{2}} (\log \mathcal{H})^j, & \text{if } q \geq 1, \\ \sum_{i=0}^{me-1} E_i \mathcal{H}^i, & \text{if } q = 0, \end{cases}$$

where $E_{2e,q} = 0$ and all the coefficients depend on m and e.

Finally, it is clear that for every $\mathcal{H}_0 > 1$ one can find a D_0 such that, for every $\mathcal{H} \geq \mathcal{H}_0$,

$$E(\mathcal{H}) \leq \begin{cases} D_0 \mathcal{H}^{me} \left(\log \mathcal{H}\right)^{q-1}, & \text{if } q \geq 1, \\ D_0 \mathcal{H}^{me-1}, & \text{if } q = 0, \end{cases}$$

and we derive the claim of Theorem 2.1.

Acknowledgments

The author would like to thank Martin Widmer for sharing his ideas, for his constant encouragement and advice, Giulio Peruginelli, Robert Tichy and Jeffrey Vaaler for many useful discussions and the anonymous referee for providing valuable suggestions.

References

1. F. Barroero and M. Widmer, *Counting lattice points and o-minimal structures*, to appear in Int. Math. Res. Not. IMRN.
2. E. Bierstone and P. D. Milman, *Semianalytic and subanalytic sets*, Inst. Hautes Études Sci. Publ. Math. (1988), no. 67, 5–42.
3. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.
4. S. Chern and J. D. Vaaler, *The distribution of values of Mahler's measure*, J. reine angew. Math. **540** (2001), 1–47.
5. H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.
6. X. Gao, *On Northcott's Theorem*, Ph.D. Thesis, University of Colorado (1995).

7. S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.
8. K. Mahler, *On the zeros of the derivative of a polynomial*, Proc. Roy. Soc. Ser. A **264** (1961), 145–154.
9. D. Masser and J. D. Vaaler, *Counting algebraic numbers with large height. II*, Trans. Amer. Math. Soc. **359** (2007), no. 1, 427–445.
10. D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. **45** (1949), 502–509.
11. W. Rudin, *Real and Complex Analysis*, McGraw-Hill Book Co., New York, 1966.
12. S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), no. 4, 433–449.
13. W. M. Schmidt, *Northcott's theorem on heights. I. A general estimate*, Monatsh. Math. **115** (1993), no. 1-2, 169–181.
14. ———, *Northcott's theorem on heights II. The quadratic case*, Acta Arith. **LXX.4** (1995), 343–375.
15. M. Widmer, *Integral points of fixed degree and bounded height*, submitted.
16. ———, *Counting points of fixed degree and bounded height*, Acta Arith. **140** (2009), no. 2, 145–168.

E-mail address: barroero@math.tugraz.at

Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, A-8010 Graz, Austria

ALGEBRAIC S-INTEGERS OF FIXED DEGREE AND BOUNDED HEIGHT

FABRIZIO BARROERO

ABSTRACT. Let k be a number field of degree m over $\mathbb{Q}$ and S a finite set of places of k containing the archimedean ones. We count the number of algebraic points of bounded height whose coordinates lie in the ring of S-integers of k. Moreover, we give an asymptotic formula for the number of $\overline{S}$-integers of bounded height and fixed degree over k, where $\overline{S}$ is the set of places of $\overline{k}$ lying above the ones in S.

1. INTRODUCTION

In this article we give asymptotic estimates for the cardinality of certain subsets of $\overline{\mathbb{Q}}^n$ of bounded height. Here and in the rest of the article, by height we mean the multiplicative absolute Weil height H on the affine space $\overline{\mathbb{Q}}^n$, that will be defined 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

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

where $k(\boldsymbol{\alpha})$ is the field obtained by adjoining all the coordinates of $\boldsymbol{\alpha}$ to k. By Northcott's Theorem [13], 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

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

Various results about this counting function appeared in the literature. One of the earliest is a result of Schanuel [14], who gave an asymptotic formula for $N(k(n,1),\mathcal{H})$. Schmidt was the first to consider the case $e > 1$. In [15], he found upper and lower bounds for $N(k(n,e),\mathcal{H})$ while in [16], 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 [18] proved an asymptotic formula for $N(k(n,e),\mathcal{H})$, provided $n > 5e/2 + 5 + 2/me$. However, for general n

2010 *Mathematics Subject Classification.* Primary 11G50, 11R04.

Key words and phrases. Heights, algebraic S-integers, counting.

F. Barroero is supported by the Austrian Science Foundation (FWF) project W1230-N13.

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. Let $\mathcal{O}_S$ be the ring of S-integers of k. Let $\overline{S}$ be the set of places of $\overline{k}$ that lie above the places in S. Let $\mathcal{O}_{\overline{S}}$ be the ring of $\overline{S}$-integers of $\overline{k}$. Given n and e positive integers, we put

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

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,

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

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

(1.1)

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

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, in [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

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

This was extended by the author in [1], where an asymptotic estimate is given for $N(\mathcal{O}_k(1,e),\mathcal{H})$. Our Theorem 1.2 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 indicate 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 and pairs of conjugate complex embeddings of k. Moreover, we indicate by Δ_k the discriminant of k.

Let n be a positive integer, we put

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

and

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

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

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

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

We set

$$C_{k,S}^{(e)} = e^{|S|}C_{\mathbb{R},e}^r C_{\mathbb{C},e}^s B_{k,S}^{(e)}.$$

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,*

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

where $\mathcal{L} = \log\mathcal{H}$ if $(m,e) = (1,2)$ and 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 $S_\infty \neq S$ the results appear to be new.

As in [1], our proof relies on a 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 in 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 $\mathbb{Z}\left[\frac{1}{p}\right]$ of height at most $\mathcal{H}$ is

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

Now, let d be a square-free positive integer with $d \equiv 3 \mod 4$. 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

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

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

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

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

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

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

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

Analogously we notice that

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

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

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

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 $v \nmid \infty$,

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

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 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

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

Note that for $\alpha \in k \setminus \{0\}$, $|\alpha|_v \neq 1$ for finitely many v. Therefore, the product above is actually finite. 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 introducing semialgebraic sets and stating The Tarski-Seidenberg principle.

Definition 2.1. *Let N and M_i, for $i = 1, \ldots, N$, 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 $f_{i,j} \in \mathbb{R}[X_1, \ldots, X_n]$ 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 are going to need the following theorem which is usually known as the Tarski-Seidenberg principle.

Theorem 2.1 ([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 integers. 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 (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 put $d_i = 1$, for $i = 1, \dots, r$, and $d_i = 2$ for $i = r + 1, \dots, r + s$. For the non-archimedean places we set

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

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

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

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

Now let $\widetilde{N}_v(\boldsymbol{z}) = N_v(1, \boldsymbol{z})$ for $\boldsymbol{z} \in k_v$. Suppose that, for every $i = 1, \dots, r + s$, $\widetilde{N}_i(\boldsymbol{z}) \geq 1$ for every $\boldsymbol{z} \in \mathbb{R}^n$ or $\mathbb{C}^n$ and that the sets

$$Z_i(T) = \left\{\boldsymbol{z} : \widetilde{N}_i(\boldsymbol{z}) \leq T\right\} \tag{3.1}$$

have volume $p_i(T)$ for every $T \geq 1$, where $p_i(X) \in \mathbb{R}[X]$ is a polynomial of degree $d_i n$ and leading coefficient C_i. Let $\mathcal{O}_S^n(\mathcal{H})$ be the set of $\boldsymbol{a} \in (\mathcal{O}_S)^n$ with $H_{\mathcal{N}}(1, \boldsymbol{a}) \leq \mathcal{H}$.

Theorem 3.1. *Let $\mathcal{N}$ be a (r, s)-system of dimension n on k satisfying the above hypothesis about the volumes of the sets $Z_i(T)$. Moreover,*

suppose S is a finite set of places of k as fixed in Section 1. 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 $\mathcal{H} \geq \mathcal{H}_0$

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

where

(3.2)

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

4. Proof of Theorems 1.1 and 1.2

In this section we apply Theorem 3.1 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

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

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 (3.1) have volume $(2T)^n$ for $i = 1, \ldots, r$ and $\pi^n T^{2n}$ for $i = r+1, \ldots, r+s$, for every $T \geq 1$. Therefore, the hypotheses of Theorem 3.1 are satisfied.

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

$$H_{\mathcal{N}}(1, \boldsymbol{a}) = \prod_v \widetilde{N}_v(\sigma_v(\boldsymbol{a}))^{\frac{d_v}{m}} = \prod_v \max\left\{1, |a_1|_v, \ldots, |a_n|_v\right\}^{\frac{d_v}{m}} = H(\boldsymbol{a}).$$

Therefore $H_{\mathcal{N}}$ is the usual absolute Weil height defined in (2.1). The claim of Theorem 1.1 follows applying Theorem 3.1 with $\mathcal{H}_0 = 2$.

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

$$N_v(z_0, \ldots, z_n) = M(z_0X^n + z_1X^{n-1} + \cdots + z_n),$$

for every $v \mid \infty$. Let us recall its definition. If $f = z_0X^n + z_1X^{n-1} + \cdots + z_n$ is a non-zero polynomial of degree n with complex coefficients and roots $\alpha_1, \ldots \alpha_n$, the Mahler measure of f is defined to be:

$$M(f) = |z_0|\prod_{i=1}^{n}\max\left\{1, |\alpha_i|\right\}. \tag{4.1}$$

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

Mahler ([10], Lemma 1) proved that M is continuous as a function of the coefficients 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 prove that, for every positive integer n, the function

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

is semialgebraic, i.e., its graph

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

is a semialgebraic set.

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

$$\Gamma_1(M)=\left\{(x_0,x_1,x_2,x_3,t)\in\mathbb{R}^5 : \max\left\{x_0^2+x_1^2,x_2^2+x_3^2\right\}=t^2, t\geq 0\right\}$$

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

$$A=\left\{(x_0,\dots,x_{2n+1},t)\in\Gamma_n(M) : x_0^2+x_1^2\neq 0\right\},$$

and

$$B=\left\{(x_0,\dots,x_{2n+1},t)\in\Gamma_n(M) : x_0=x_1=0\right\}.$$

By the inductive hypothesis, B is semialgebraic since $B=\{(0,0)\}\times\Gamma_{n-1}(M)$. 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

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

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 2.1). 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

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

□

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 (3.1), where $\widetilde{N}$ is the real and the complex monic Mahler measure.

Recall the notation of (3.1). By (1.16) and (1.17) of [6], for every $T\geq 1$ the volumes of the sets

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

and

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

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

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

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

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

We just showed that $\mathcal{N}$ satisfies the hypothesis of Theorem 3.1 and we have that 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 $\mathcal{H}\ge\mathcal{H}_0$,

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

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 as done in Section 2 of [1]. 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

$$\begin{array}{rccc} M^k: & k[X] & \to & [0,\infty)\\ & a_0X^n+a_1X^{n-1}+\cdots+a_n & \mapsto & H_{\mathcal{N}_n}(a_0,a_1,\dots,a_n).\end{array}$$

Let $\mathcal{M}_{k,S}(n,\mathcal{H})$ be the set of of monic polynomials $f\in\mathcal{O}_S[X]$ of degree n with $M^k(f)\le\mathcal{H}$. Clearly $|\mathcal{O}_S^n(\mathcal{H})|=|\mathcal{M}_{k,S}(n,\mathcal{H})|$ and (4.3) is an estimate for such cardinality. Fixing m and n and letting k vary among number fields of degree m, $B_{k,S}^{(n)}$ is bounded and therefore there exists a constant $G_{m,\mathfrak{N}(S)}^{(n)}$, depending on n, m and $\mathfrak{N}(S)$, such that

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

for every $\mathcal{H}\ge1$.

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

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

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

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

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

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

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

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

Now we 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 $M^k(f) \leq \mathcal{H}$, 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 $\mathcal{H} \geq \mathcal{H}_0$ we have*

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

where $\mathcal{L} = \log \mathcal{H}$ if $(m,n) = (1,2)$ and 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 $M^k(f) \leq \mathcal{H}$ 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 $0 < a \leq b < n$ and $a + b = n$. We have $1 \leq M^k(g), M^k(h) \leq \mathcal{H}$ because g and h are monic. Thus, there exists a positive integer d such that $2^{d-1} \leq M^k(g) < 2^d$. Note that d must satisfy

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

Since M^k is multiplicative,

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

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

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

possibilities for g and

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

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

If $a = b = \frac{n}{2}$, then (4.7) is

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

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

$$H_{m,\mathfrak{N}(S)}^{(n)} \mathcal{H}^{\frac{mn}{2}} \left(2\log \mathcal{H} + 2\right)^{2|S|-1}$$

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 $\frac{mn}{2} < mn - 1$. In the case $|S| = 1$ and $(m,n) = (1,2)$, we get $H_{m,\mathfrak{N}(S)}^{(n)} \mathcal{H} \left(2\log \mathcal{H} + 2\right)$ and we need an additional logarithm factor.

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

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

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

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

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 $\overline{S}$ is the set of places of $\overline{k}$ that extend the places in S.

Lemma 4.3. *An algebraic number $\beta \in \mathcal{O}_{\overline{S}}$ has degree n 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 n with $M^k(f) \le \mathcal{H}^n$.*

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

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

We show that it is possible to define an absolute $M^{\overline{\mathbb{Q}}} : \overline{\mathbb{Q}}[X] \to [0,\infty)$ such that, if $f \in k[X]$, then $M^{\overline{\mathbb{Q}}}(f) = M^k(f)$. In fact, let k' be a finite extension of k with $[k' : \mathbb{Q}] = m'$. Recall (see [12], Ch.II, (8.4) Corollary) that for any $w \in M_k$

$$\sum_{\substack{v \in M_{k'} \\ v|w}} d_v = d_w [k' : k] = d_w \frac{m'}{m}.$$

For any $f = a_0X^n + \cdots + a_n \in k'[X]$, we use the notation $M_v(f) = M(f)$ for $v \mid \infty$ and $M_v(f) = \max\{|a_0|_v, \dots, |a_n|_v\}$ for $v \nmid \infty$. We have

$$M^{k'}(f) = \prod_{v \in M_{k'}} M_v(\sigma_v(f))^{\frac{d_v}{m'}} = \prod_{w \in M_k} \prod_{\substack{v \in M_{k'} \\ v \mid w}} M_v(\sigma_v(f))^{\frac{d_v}{m'}}$$

$$= \prod_{w \in M_k} M_w(\sigma_w(f))^{\sum_{\substack{v \in M_{k'} \\ v \mid w}} \frac{d_v}{m'}} = \prod_{w \in M_k} M_w(\sigma_w(f))^{\frac{d_w}{m}} = M^k(f).$$

Suppose $f = (X - \alpha_1) \cdots (X - \alpha_n)$. 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). Moreover, by the multiplicativity of M^k we can see that

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

for any α_j root of f. □

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

$$\left| N\left(\mathcal{O}_S(1,n), \mathcal{H}\right) - n^{|S|} C^r_{\mathbb{R},n} C^s_{\mathbb{C},n} B^{(n)}_{k,S} \mathcal{H}^{mn^2} \left(\log \mathcal{H}\right)^{|S|-1} \right|$$

$$\leq \begin{cases} E_0 \mathcal{H}^{mn^2} \left(\log \mathcal{H}\right)^{|S|-2}, & \text{if } |S| > 1, \\ E_0 \mathcal{H}^{n(mn-1)} \mathcal{L}, & \text{if } |S| = 1, \end{cases}$$

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

5. Counting lattice points

We start this section introducing the counting theorem that will be used to prove Theorem 3.1. The principle dates 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 $\mathbb{R}^n$ 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 Theorem 1.3 of [2].

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*

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

where $V_j(Z_{\boldsymbol{t}})$ 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 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

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

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. In fact, one can get $\Gamma\left(\widetilde{N}_i\right)$ by intersecting $\Gamma(N_i)$ with an appropriate affine subspace. Let us define the following sets:

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

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

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

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 2.1) the set

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

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 $\prod_{i=1}^{r+s} t_i^{d_i} \leq t$, i.e., $\prod_{i=1}^{r+s} \widetilde{N}_i(\boldsymbol{x}_i)^{d_i} \leq t$. Therefore $B = Z$, and we proved the claim. □

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

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

for every $\boldsymbol{z}$ in $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$ (see [5], Lemma 2, p. 108). We define $\gamma_i = \max\{\delta_i : \delta_i |\boldsymbol{z}|_\infty \leq N_i(\boldsymbol{z})\}$ 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 $\prod_{i=1}^{r+s} \widetilde{N}_i(\boldsymbol{x}_i)^{d_i} \leq t$ satisfies $\prod_{i=1}^{r+s} \widetilde{N}_i'(\boldsymbol{x}_i)^{d_i} \leq t$. Therefore, if

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

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

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

holds. This implies

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

for every $i = 1, \dots, r+s$. We have just showed 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 $V_j(Z(T)) \leq V_j(Z'(T))$. By Theorem 5.1 there exists a constant c_Z, depending only on Z, such that

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

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 supposed that, for every $i = 1, \dots, r+s$, $\widetilde{N}_i(\boldsymbol{x}) \geq 1$ and the volume of the set $Z_i(T)$ defined in (3.1) is $p_i(T)$ for every $T \geq 1$, 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 that, for every $T \geq 1$,*

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

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 $\frac{n^q}{q!}\prod_{i=1}^{q+1} C_i$.

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

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 $\deg_X P_j \leq 2n$, $\deg_Y P_j \leq q$, and the coefficient of $X^{2n}Y^q$ is 0, such that, for every $T \geq 1$, we have*

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

Proof. See [1], Lemma 5.4. □

For an integer u, we will use the notation

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

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

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

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

where $\mathfrak{D}(\Lambda) = \sum_{j=0}^{mn-1} \frac{1}{\lambda_1 \dots \lambda_j} + \frac{1}{\det \Lambda}$. Moreover, if $T < 1$, then $Z(T) = \emptyset$.

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

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 $p_1\left(T^{\frac{1}{m}}\right)$ for every $T \geq 1$, where p_1 has degree mn and leading coefficient C_1.

Fix a j, $1 \leq j \leq mn-1$. Any projection of $Z'(T)$ to a j-dimensional coordinate subspace has volume at most $F_j T^{\frac{j}{m}}$, for some positive real constant F_j. Therefore, there exists an E'' such that

$$V_j(Z'(T)) \leq E'' T^{n-\frac{1}{m}},$$

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

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

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

for some polynomial $P(X, Y) \in \mathbb{R}[X, Y]$ with $\deg_X P \leq 2n$, $\deg_Y P \leq q$, 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

$$P\left(T^{\frac{1}{2}}, \log T\right) \leq E T^n (\log T)^{(q-1)},$$

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

$$P\left(T^{\frac{1}{2}}, \log T\right) \leq E T^n (\log T)^{(q-1)} + E',$$

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

6. Proof of Theorem 3.1

Recall that we fixed a number field k of degree m over $\mathbb{Q}$. Recall that $\sigma_1, \ldots, \sigma_{r+s}$ are the real and complex embeddings of k indexed in the usual way. Moreover, $d_i = 1$, for $i = 1, \ldots, r$, and $d_i = 2$, for $i = r+1, \ldots, r+s$. Let $\mathfrak{A}$ be a non-zero fractional ideal of k. The image of $\mathfrak{A}$ via the embedding $\sigma : a \hookrightarrow (\sigma_1(a), \ldots, \sigma_{r+s}(a))$ is a lattice in $\mathbb{R}^m$ and we call the cartesian product of n copies of it $\Lambda_{\mathfrak{A}} = \sigma(\mathfrak{A})^n$. Recall that with $\mathfrak{N}(\mathfrak{A})$ we denote the norm of $\mathfrak{A}$.

Lemma 6.1. *We have*

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

and its first successive minimum with respect to the Euclidean distance is $\lambda_1 \geq \mathfrak{N}(\mathfrak{A})^{\frac{1}{m}}$.

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

Now, recall that we fixed a finite set of places S of k containing the archimedean ones and $\mathcal{O}_S$ is the ring of S-integers of k. As in Section 1, we call S_{fin} the set of non-archimedean places in S. To prove Theorem 3.1 we need an estimate for the cardinality of $\mathcal{O}_S^n(\mathcal{H})$, i.e., the set of points $\boldsymbol{a} \in \mathcal{O}_S^n$ such that $H_{\mathcal{N}}(1, \boldsymbol{a}) \leq \mathcal{H}$.

First suppose $S_{\text{fin}} = \emptyset$, then $\mathcal{O}_S = \mathcal{O}_k$ and $|S| = q + 1 = r + s$. Note that, in this case,

$$H_{\mathcal{N}}(1, \boldsymbol{a}) = \prod_{i=1}^{r+s} \widetilde{N}_i(\sigma_i(\boldsymbol{a}))^{\frac{d_i}{m}},$$

because $\boldsymbol{a}$ is a vector with integer coordinates whose non-archimedean absolute values are smaller than or equal to 1. Therefore, the number of $\boldsymbol{a} \in \mathcal{O}_k^n$ such that $H_{\mathcal{N}}(1, \boldsymbol{a}) \leq \mathcal{H}$ is the number of lattice points of $\Lambda_{\mathcal{O}_k} = \sigma(\mathcal{O}_k)^n$ in $Z(\mathcal{H}^m)$. By Lemma 6.1, $\det \Lambda_{\mathcal{O}_k} = \left(2^{-s}\sqrt{|\Delta_k|}\right)^n$ and $\lambda_1 \geq 1$. Thus, $\mathfrak{D}(\Lambda) \leq mn + 2^{sn}$. Moreover, for every $\mathcal{H}_0 > 1$ there exists a $C_0 = C_0(\mathcal{N}, \mathcal{H}_0)$ such that

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

for every $\mathcal{H} \geq \mathcal{H}_0$, in case $q \geq 1$ and $(mn + 2^{sn})E \leq C_0$ in case $q = 0$. The claim of Theorem 3.1 follows applying Proposition 5.5.

Now, suppose $S_{\text{fin}} = \{v_1, \ldots, v_L\}$, with $L > 0$ and 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., $\mathfrak{A} = \mathfrak{p}_1^{g_1} \ldots \mathfrak{p}_L^{g_L}$ for some non-negative integers $g_1, \ldots, g_L$. 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 $a_u \in \mathfrak{A}^{-1}$ for every $u = 1, \ldots, n$, i.e., $\sigma(\boldsymbol{a}) = (\sigma_1(\boldsymbol{a}), \ldots, \sigma_{r+s}(\boldsymbol{a})) \in \Lambda_{\mathfrak{A}^{-1}}$.

From now on we put

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

For a non-zero integral ideal $\mathfrak{A}$, by $Z(\mathfrak{A}, T)$ we indicate the set of $\boldsymbol{a} \in k^n$ such that $\sigma(\boldsymbol{a}) \in \Lambda_{\mathfrak{A}^{-1}} \cap Z(T^m)$.

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

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

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

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

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

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

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

□

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 $a_u \notin \mathfrak{B}^{-1}$. In other words, $\boldsymbol{a}$ corresponds to a lattice point of $\Lambda_{\mathfrak{A}^{-1}}$ that is not contained in any sublattice of the form $\Lambda_{\mathfrak{B}^{-1}}$ 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 of k, the Möbius inversion formula implies that

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

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

$$\left||Z^*(\mathfrak{A}, T)| - V_{k,\mathcal{N}} \sum_{\mathfrak{B}|\mathfrak{A}} \mu_k(\mathfrak{B})\mathfrak{N}(\mathfrak{A}\mathfrak{B}^{-1})^n T^{mn}\left(\log T^m\right)^{(q)}\right| \tag{6.1}$$

$$\leq \begin{cases} \sum_{\mathfrak{B}|\mathfrak{A}} |\mu_k(\mathfrak{B})|\mathfrak{N}(\mathfrak{A}\mathfrak{B}^{-1})^n \left(FT^{mn}\left(\log T^m\right)^{(q-1)} + F'\right), & \text{if } q \geq 1, \\ F\sum_{\mathfrak{B}|\mathfrak{A}} |\mu_k(\mathfrak{B})|\mathfrak{N}(\mathfrak{A}\mathfrak{B}^{-1})^n T^{mn-1}, & \text{if } q = 0. \end{cases}$$

Recall that $\mathcal{O}_S^n(\mathcal{H})$ 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. *We have*

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

Proof. Let $\mathfrak{A} = \mathfrak{p}_1^{g_1} \dots \mathfrak{p}_L^{g_L}$ and recall $d_{v_l} = [k_{v_l} : \mathbb{Q}_{v_l}]$. Every point $\boldsymbol{a} \in Z^*(\mathfrak{A}, T)$ is such that $\max_u |a_u|_{v_l}^{d_{v_l}} = \mathfrak{N}\left(\mathfrak{p}_l\right)^{g_l}$, for every $l = 1, \dots, L$, and $\max_u |a_u|_v \leq 1$ 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

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

Therefore, $\boldsymbol{a} \in \mathcal{O}_S^n(\mathcal{H})$ if and only if there exists an $\mathfrak{A} \in \mathcal{I}_S$ such that $\boldsymbol{a} \in Z^*(\mathfrak{A}, \mathfrak{N}(\mathfrak{A})^{-\frac{1}{m}}\mathcal{H})$. Since such an $\mathfrak{A}$ is unique and recalling that, if $T < 1$, then $Z(\mathfrak{A}, T)$, and therefore $Z^*(\mathfrak{A}, T)$, are 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 have that

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

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 $q \geq 1$ and

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

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

Now, let $\Psi^{(1)}(\mathfrak{A}) = \sum_{\mathfrak{B}|\mathfrak{A}} \frac{\mu_k(\mathfrak{B})}{\mathfrak{N}(\mathfrak{B})^n}$ and $\Psi^{(2)}(\mathfrak{A}) = \sum_{\mathfrak{B}|\mathfrak{A}} \frac{|\mu_k(\mathfrak{B})|}{\mathfrak{N}(\mathfrak{B})^n}$. The left hand side becomes

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

while the right hand side is

$$\begin{cases} \sum_{\mathfrak{A} \in \mathcal{I}_S(\mathcal{H}^m)} \Psi^{(2)}(\mathfrak{A}) \left(F\mathcal{H}^{mn} \left(\log \left(\frac{\mathcal{H}^m}{\mathfrak{N}(\mathfrak{A})} \right) \right)^{(q-1)} + F' \mathfrak{N}(\mathfrak{A})^n \right), & \text{if } q \geq 1, \\ F\mathcal{H}^{mn-1} \sum_{\mathfrak{A} \in \mathcal{I}_S(\mathcal{H}^m)} \Psi^{(2)}(\mathfrak{A}) \mathfrak{N}(\mathfrak{A})^{\frac{1}{m}}, & \text{if } q = 0. \end{cases} \tag{6.4}$$

Let K be a non-negative integer, we put

$$\mathcal{L}_S^{(h)}(\mathcal{H}, K) = \sum_{\mathfrak{A} \in \mathcal{I}_S(\mathcal{H}^m)} \Psi^{(h)}(\mathfrak{A}) \left(\log \left(\mathfrak{N}(\mathfrak{A})^{-1} \mathcal{H}^m \right) \right)^{(K)},$$

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

Lemma 6.4. *For every non-negative integer K and for $h = 1, 2$, there exist positive constants $U^{(1)}_{K,\mathfrak{N}(S)}$ and $U^{(2)}_{K,\mathfrak{N}(S)}$, depending only on K and $\mathfrak{N}(S)$, such that*

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

for every $\mathcal{H} \geq 1$, where

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

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

$$\mathfrak{N}(\mathfrak{p}_L^{g_L}) \leq \mathcal{H}^m \mathfrak{N}(\mathfrak{B})^{-1}.$$

For typographical convenience we set

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

and

$$R = \mathcal{I}_{S'}(\mathcal{H}^m).$$

We have

$$\mathcal{L}^{(h)}_S(\mathcal{H}, K) = \sum_{\mathfrak{B}\in R}\sum_{g_L=0}^{A(\mathfrak{B})} \Psi^{(h)}\left(\mathfrak{B}\mathfrak{p}_L^{g_L}\right)\left(\log\left(\mathcal{H}^m\mathfrak{N}(\mathfrak{B})^{-1}\right) - g_L \log \mathfrak{N}(\mathfrak{p}_L)\right)^{(K)}$$

$$= \sum_{\mathfrak{B}\in R}\sum_{g_L=1}^{A(\mathfrak{B})} \Psi^{(h)}\left(\mathfrak{B}\mathfrak{p}_L^{g_L}\right)\sum_{i=0}^{K}(-1)^i\binom{K}{i}(\log \mathfrak{N}(\mathfrak{p}_L))^i g_L^i\left(\log\left(\mathcal{H}^m\mathfrak{N}(\mathfrak{B})^{-1}\right)\right)^{(K-i)} + \mathcal{L}^{(h)}_{S'}(\mathcal{H}, K).$$

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 $g_L \geq 1$,

$$\Psi^{(h)}(\mathfrak{B}\mathfrak{p}_L^{g_L}) = \Psi^{(h)}(\mathfrak{B}\mathfrak{p}_L) = \Psi^{(h)}(\mathfrak{B})\Psi^{(h)}(\mathfrak{p}_L) > 0. \tag{6.5}$$

Therefore,

$$\left(\mathcal{L}_S^{(h)}(\mathcal{H},K)-\mathcal{L}_{S'}^{(h)}(\mathcal{H},K)\right)\left(\Psi^{(h)}(\mathfrak{p}_L)\right)^{-1} \tag{6.6}$$
$$=\sum_{i=0}^{K}(-1)^i\binom{K}{i}\left(\log\mathfrak{N}\left(\mathfrak{p}_L\right)\right)^i\sum_{\mathfrak{B}\in R}\Psi^{(h)}(\mathfrak{B})\left(\log\left(\mathcal{H}^m\mathfrak{N}(\mathfrak{B})^{-1}\right)\right)^{(K-i)}\sum_{g_L=1}^{A(\mathfrak{B})}g_L^i.$$

Using Faulhaber's formula, for every $i=0,\dots,K$, we get

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

where Q_i is a polynomial of degree i whose coefficients depend only on i. Then

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

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

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

by (6.6), we can derive the following inequality:

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

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

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

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

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

and

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

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

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

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

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

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

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

Note that $\Psi^{(2)}(\mathfrak{p}_L)\leq 2$ and then, by (6.5), $\Psi^{(2)}(\mathfrak{B}\mathfrak{p}_L^{g_L}) \leq 2\Psi^{(2)}(\mathfrak{B})$. Then

$$\begin{aligned}
\sum_{\mathfrak{A}\in\mathcal{I}_S(\mathcal{H}^m)} \Psi^{(2)}(\mathfrak{A})\mathfrak{N}(\mathfrak{A})^{\frac{1}{m}} &\leq \sum_{\mathfrak{B}\in\mathcal{I}_{S'}(\mathcal{H}^m)} 2\Psi^{(2)}(\mathfrak{B})\mathfrak{N}(\mathfrak{B})^{\frac{1}{m}} \sum_{g_L=0}^{A(\mathfrak{B})} \mathfrak{N}(\mathfrak{p}_L)^{\frac{g_L}{m}} \\
&= 2\sum_{\mathfrak{B}\in\mathcal{I}_{S'}(\mathcal{H}^m)} \Psi^{(2)}(\mathfrak{B})\mathfrak{N}(\mathfrak{B})^{\frac{1}{m}} \frac{\mathfrak{N}(\mathfrak{p}_L)^{\frac{1}{m}(A(\mathfrak{B})+1)}-1}{\mathfrak{N}(\mathfrak{p}_L)^{\frac{1}{m}}-1} \\
&\leq \frac{2}{\mathfrak{N}(\mathfrak{p}_L)^{\frac{1}{m}}-1} \sum_{\mathfrak{B}\in\mathcal{I}_{S'}(\mathcal{H}^m)} \Psi^{(2)}(\mathfrak{B})\mathfrak{N}(\mathfrak{B})^{\frac{1}{m}}\mathfrak{N}(\mathfrak{p}_L)^{\frac{1}{m}(A(\mathfrak{B})+1)} \\
\leq \frac{2}{\mathfrak{N}(\mathfrak{p}_L)^{\frac{1}{m}}-1} \sum_{\mathfrak{B}\in\mathcal{I}_{S'}(\mathcal{H}^m)} \Psi^{(2)}(\mathfrak{B})\mathfrak{N}(\mathfrak{B})^{\frac{1}{m}} &\left(\mathfrak{N}(\mathfrak{p}_L)\mathfrak{N}(\mathfrak{p}_L)^{\frac{\log\left(\mathcal{H}^m\mathfrak{N}(\mathfrak{B})^{-1}\right)}{\log\mathfrak{N}(\mathfrak{p}_L)}}\right)^{\frac{1}{m}} \\
&= \frac{2\mathfrak{N}(\mathfrak{p}_L)^{\frac{1}{m}}}{\mathfrak{N}(\mathfrak{p}_L)^{\frac{1}{m}}-1} \sum_{\mathfrak{B}\in\mathcal{I}_{S'}(\mathcal{H}^m)} \Psi^{(2)}(\mathfrak{B})\mathfrak{N}(\mathfrak{B})^{\frac{1}{m}} \left(\mathcal{H}^m\mathfrak{N}(\mathfrak{B})^{-1}\right)^{\frac{1}{m}} \\
&= 4\mathcal{H}\mathcal{L}_{S'}^{(2)}(\mathcal{H},0).
\end{aligned}$$

The claim follows applying Lemma 6.4. □

Now we are ready prove Theorem 3.1.

We already dealt with the case $S_{\text{fin}}=\emptyset$. Suppose $S_{\text{fin}}\neq\emptyset$. By (6.3) and (6.4), we have

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

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

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

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

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

for every $\mathcal{H} \geq 1$, where $C_{\mathcal{N},k,S}$ was defined in (3.2).

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 3.1

Acknowledgements

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 his advice that significantly improved this article.

References

1. F. Barroero, *Counting algebraic integers of fixed degree and bounded height*, submitted.
2. F. Barroero and M. Widmer, *Counting lattice points and o-minimal structures*, to appear in Int. Math. Res. Not. IMRN.
3. E. Bierstone and P. D. Milman, *Semianalytic and subanalytic sets*, Inst. Hautes Études Sci. Publ. Math. (1988), no. 67, 5–42.
4. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.
5. J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Grundlehren der mathematischen Wissenschaften, Springer-Verlag, 1971.
6. S. 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.
8. X. Gao, *On Northcott's Theorem*, Ph.D. Thesis, University of Colorado (1995).
9. S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, 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), no. 1, 427–445.
12. J. Neukirch, *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999.
13. D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. **45** (1949), 502–509.

14. S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), no. 4, 433–449.
15. W. M. Schmidt, *Northcott's theorem on heights. I. A general estimate*, Monatsh. Math. **115** (1993), no. 1-2, 169–181.
16. ———, *Northcott's theorem on heights II. The quadratic case*, Acta Arith. **LXX.4** (1995), 343–375.
17. M. Widmer, *Integral points of fixed degree and bounded height*, submitted.
18. ———, *Counting points of fixed degree and bounded height*, Acta Arith. **140** (2009), no. 2, 145–168.

Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, A-8010 Graz, Austria

E-mail address: barroero@math.tugraz.at

ADDITIVE UNIT REPRESENTATIONS IN GLOBAL FIELDS – A SURVEY

FABRIZIO BARROERO, CHRISTOPHER FREI, AND ROBERT F. TICHY

Dedicated to Kálmán Győry, Attila Pethő, János Pintz and András Sarközy.

Abstract. We give an overview on recent results concerning additive unit representations. Furthermore the solutions of some open questions are included. The central problem is whether and how certain rings are (additively) generated by their units. This has been investigated for several types of rings related to global fields, most importantly rings of algebraic integers. We also state some open problems and conjectures which we consider to be important in this field.

1. The unit sum number

In 1954, Zelinsky [37] proved that every endomorphism of a vector space V over a division ring D is a sum of two automorphisms, except if $D = \mathbb{Z}/2\mathbb{Z}$ and $\dim V = 1$. This was motivated by investigations of Dieudonné on Galois theory of simple and semisimple rings [6] and was probably the first result about the additive unit structure of a ring.

Using the terminology of Vámos [34], we say that an element r of a ring R (with unity 1) is *k-good* if r is a sum of exactly k units of R. If every element of R has this property then we call R *k-good*. By Zelinsky's result, the endomorphism ring of a vector space with more than two elements is 2-good. Clearly, if R is k-good then it is also l-good for every integer $l > k$. Indeed, we can write any element of R as

$$r = (r - (l-k)\cdot 1) + (l-k)\cdot 1,$$

and expressing $r - (l-k)\cdot 1$ as a sum of k units gives a representation of r as a sum of l units.

Goldsmith, Pabst and Scott [17] defined the *unit sum number* $u(R)$ of a ring R to be the minimal integer k such that R is k-good, if such an integer exists. If R is not k-good for any k then we put $u(R) := \omega$

1991 *Mathematics Subject Classification.* 00-02, 11R27, 16U60.

Key words and phrases. global fields, sums of units, unit sum number, additive unit representations.

F. Barroero is supported by the Austrian Science Foundation (FWF) project W1230-N13.

C. Frei is supported by the Austrian Science Foundation (FWF) project S9611-N23.

if every element of R is a sum of units, and $u(R) := \infty$ if not. We use the convention $k < \omega < \infty$ for all integers k.

Clearly, $u(R) \leq \omega$ if and only if R is generated by its units. Here are some easy examples from [17]:

- $u(\mathbb{Z}) = \omega$,
- $u(K[X]) = \infty$, for any field K,
- $u(K) = 2$, for any field K with more than 2 elements, and
- $u(\mathbb{Z}/2\mathbb{Z}) = \omega$.

Goldsmith, Pabst and Scott [17] were mainly interested in endomorphism rings of modules. For example, they proved independently from Zelinsky that the endomorphism ring of a vector space with more than two elements has unit sum number 2, though they mentioned that this result can hardly be new.

Henriksen [21] proved that the ring $M_n(R)$ of $n \times n$-matrices ($n \geq 2$) over any ring R is 3-good.

Herwig and Ziegler [22] proved that for every integer $n \geq 2$ there exists a factorial domain R such that every element of R is a sum of at most n units, but there is an element of R that is no sum of $n-1$ units.

The introductory section of [34] contains a historical overview of the subject with some references. We also mention the survey article [31] by Srivastava.

In the following sections, we are going to focus on rings of ($S-$)integers in global fields.

2. Rings of integers

The central result regarding rings of integers in number fields, or more generally, rings of S-integers in global fields ($S \neq \emptyset$ finite), is that they are not k-good for any k, thus their unit sum number is ω or ∞. This was first proved by Ashrafi and Vámos [2] for rings of integers of quadratic and complex cubic number fields, and of cyclotomic number fields generated by a primitive 2^n-th root of unity. They conjectured, however, that it holds true for the rings of integers of all algebraic number fields (finite extensions of $\mathbb{Q}$). The proof of an even stronger version of this was given by Jarden and Narkiewicz [24] for a much more general class of rings:

Theorem 1. [24, Theorem 1] *If R is a finitely generated integral domain of zero characteristic then there is no integer n such that every element of R is a sum of at most n units.*

In particular, we have $u(R) \geq \omega$, for any ring R of integers of an algebraic number field.

This theorem is an immediate consequence of the following lemma, which Jarden and Narkiewicz proved by means of Evertse and Győry's

[10] bound on the number of solutions of S-unit equations combined with van der Waerden's theorem [36] on arithmetic progressions.

Lemma 2. [24, Lemma 4] *If R is a finitely generated integral domain of zero characteristic and $n \geq 1$ is an integer then there exists a constant $A_n(R)$ such that every arithmetic progression in R having more than $A_n(R)$ elements contains an element which is not a sum of n units.*

Lemma 2 is a special case of a theorem independently found by Hajdu [20]. Hajdu's result provides a bound for the length of arithmetic progressions in linear combinations of elements from a finitely generated multiplicative subgroup of a field of zero characteristic. Here the linear combinations are of fixed length and only a given finite set of coefficient-tuples is allowed. Hajdu used his result to negatively answer the following question by Pohst: Is it true that every prime can be written in the form $2^u \pm 3^v$, with non-negative integers u, v?

Using results by Mason [27, 28] on S-unit equations in function fields, Frei [14] proved the function field analogue of Theorem 1. It holds in zero characteristic as well as in positive characteristic.

Theorem 3. *Let R be the ring of S-integers of an algebraic function field in one variable over a perfect field, where $S \neq \emptyset$ is a finite set of places. Then, for each positive integer n, there exists an element of R that can not be written as a sum of at most n units of R. In particular, we have $u(R) \geq \omega$.*

We will later discuss criteria which show that in the number field case as well as in the function field case, both possibilities $u(R) = \omega$ and $u(R) = \infty$ occur.

3. The qualitative problem

Problem A. [24, Problem A] *Give a criterion for an algebraic extension K of the rationals to have the property that its ring of integers R has unit sum number $u(R) \leq \omega$.*

Jarden and Narkiewicz provided some easy examples of infinite extensions of $\mathbb{Q}$ with $u(R) \leq \omega$: By the Kronecker-Weber theorem, the maximal Abelian extension of $\mathbb{Q}$ has this property. Further examples are the fields of all algebraic numbers and all real algebraic numbers.

More criteria are known for algebraic number fields of small degree. Here, the only possibilities for $u(R)$ are ω and ∞, by Theorem 1. For quadratic number fields, Belcher [3], and later Ashrafi and Vámos [2], proved the following result:

Theorem 4. [3, Lemma 1][2, Theorems 7, 8] *Let $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ squarefree, be a quadratic number field with ring of integers R. Then $u(R) = \omega$ if and only if*

1. $d \in \{-1, -3\}$, or

2. $d > 0$, $d \not\equiv 1 \mod 4$, *and* $d+1$ *or* $d-1$ *is a perfect square, or*
3. $d > 0$, $d \equiv 1 \mod 4$, *and* $d+4$ *or* $d-4$ *is a perfect square.*

A similar result for purely cubic fields was found by Tichy and Ziegler [33].

Theorem 5. [33, Theorem 2] *Let d be a cubefree integer and R the ring of integers of the purely cubic field $\mathbb{Q}(\sqrt[3]{d})$. Then $u(R) = \omega$ if and only if*

1. d is squarefree, $d \not\equiv \pm 1 \mod 9$, and $d+1$ or $d-1$ is a perfect cube, or
2. $d = 28$.

Filipin, Tichy and Ziegler used similar methods to handle purely quartic complex fields $\mathbb{Q}(\sqrt[4]{d})$. Their criterion [11, Theorem 1.1] states that $u(R) = \omega$ if and only if d is contained in one of six explicitly given sets.

As a first guess, one could hope to get information about the unit sum number of the ring of integers of a number field K by comparing the regulator and the discriminant of K. In personal communication with the authors, Martin Widmer pointed out the following sufficient criterion for the simple case of complex cubic fields:

Proposition 6. *(Widmer) If R is the ring of integers of a complex cubic number field K then $u(R) = \omega$ whenever the inequality*

$$|\Delta_K| > (e^{\frac{3}{4}R_K} + e^{-\frac{3}{4}R_K})^4 \tag{1}$$

holds. Here, Δ_K is the discriminant and R_K is the regulator of K.

Proof. Regard K as a subfield of the reals, and let $\eta > 1$ be a fundamental unit, so $R_K = \log \eta$. Since K contains no roots of unity except ± 1, the ring of integers R is generated by its units if and only if $R = \mathbb{Z}[\eta]$. By the standard embedding $K \to \mathbb{R} \times \mathbb{C} \simeq \mathbb{R}^3$, we can regard R and $\mathbb{Z}[\eta]$ as lattices in $\mathbb{R}^3$ and compare their determinants. Let $\eta' = x+iy$ be one of the non-real conjugates of η. We get $u(R) = \omega$ if and only if

$$2^{-1}\sqrt{|\Delta_K|} = \left| \det \begin{pmatrix} 1 & \eta & \eta^2 \\ 1 & x & x^2 - y^2 \\ 0 & y & 2xy \end{pmatrix} \right|.$$

Since the right-hand side of the above equality is always a multiple of the left-hand side, we have $u(R) = \omega$ if and only if

$$\sqrt{|\Delta_K|} > \left| \det \begin{pmatrix} 1 & \eta & \eta^2 \\ 1 & x & x^2 - y^2 \\ 0 & y & 2xy \end{pmatrix} \right|.$$

Clearly, $\eta^{-1} = \eta'\overline{\eta'} = x^2 + y^2$, whence $|x|$, $|y| \leq \eta^{-1/2}$. With this in mind, a simple computation shows that the right-hand side of the above inequality is at most $\eta^{-3/2} + 2 + \eta^{3/2}$, so (1) implies that $u(R) = \omega$. $\square$

To see that condition (1) is satisfied in infinitely many cases, we consider the complex cubic fields $K_N = \mathbb{Q}(\alpha_N)$, where α_N is a root of the polynomial

$$f_N = X^3 + NX + 1, \tag{2}$$

with a positive integer N such that $4N^3 + 27$ is squarefree. By [7], infinitely many such N exist. We may assume that $\alpha_N \in \mathbb{R}$. From (2), we get

$$\frac{N^2}{N^3+1} < -\alpha_N = \frac{1}{\alpha_N^2 + N} < 1/N.$$

Since $-1/\alpha_N$ is a unit of the ring of integers of K_N, and $N < -1/\alpha_N < N + 1/N^2$, we have $R_K \leq \log(N + 1/N^2)$. The discriminant $-4N^3 - 27$ of f_N is squarefree by hypothesis, so $|\Delta_K| = 4N^3 + 27$. Now we see by a simple computation that (1) holds.

In the function field case, Frei [14] investigated quadratic extensions of rational global function fields.

Theorem 7. [14, Theorem 2] *Let K be a finite field, and F a quadratic extension field of the rational function field $K(x)$ over K. Denote the integral closure of $K[x]$ in F by R. Then the following two statements are equivalent.*

1. *$u(R) = \omega$*
2. *The function field $F|K$ has full constant field K and genus 0, and the infinite place of $K(x)$ splits into two places of $F|K$.*

This criterion can also be phrased in terms of an element generating F over $K(x)$. If, for example, K is the full constant field of F and of odd characteristic then we can write $F = K(x, y)$, where $y^2 = f(x)$ for some separable polynomial $f \in K[x] \setminus K$. Then we get $u(R) = \omega$ if and only if f is of degree 2 and its leading coefficient is a square in K ([14, Corollary 1]).

Theorem 7 holds in fact for arbitrary perfect base fields K. An alternative proof given at the end of [14] implies the following stronger version:

Theorem 8. *Let $F|K$ be an algebraic function field in one variable over a perfect field K. Let S be a set of two places of $F|K$ of degree one, and denote by R the ring of S-integers of $F|K$. Then $u(R) = \omega$ if and only if $F|K$ is rational.*

All of the rings R investigated above have in common that their unit groups are of rank at most one. Currently, there are no known nontrivial criteria for families of number fields (or function fields) whose rings of integers have unit groups of higher rank. We consider it an important direction to find such criteria.

Pethő and Ziegler investigated a modified version of Problem A, where one asks whether a ring of integers has a power basis consisting of units [39, 29]. For example, Ziegler proved the following:

Theorem 9. [39, Theorem 1] *Let $m > 1$ be an integer which is not a square. Then the order $\mathbb{Z}[\sqrt[4]{m}]$ admits a power basis consisting of units if and only if $m = a^4 \pm 1$, for some integer a.*

Since analogous results are already known for negative m [40] and for the rings $\mathbb{Z}[\sqrt[d]{m}]$, $d < 4$ [3, 33], Theorem 9 motivates the following conjecture:

Conjecture. [39, Conjecture 1] *Let $d \geq 2$ be an integer and $m \in \mathbb{Z} \setminus \{0\}$, and assume that $\sqrt[d]{m}$ is an algebraic number of degree d. Then $\mathbb{Z}[\sqrt[d]{m}]$ admits a power basis consisting of units if and only if $m = a^d \pm 1$, for some integer a.*

For rings R with $u(R) = \omega$, Ashrafi [1] investigated the stronger property that every element of R can be written as a sum of k units for all sufficiently large integers k. Ashrafi proved that this is the case if and only if R does not have $\mathbb{Z}/2\mathbb{Z}$ as a factor, and applied this result to rings of integers of quadratic and complex cubic number fields.

Let R be an order in a quadratic number field. Ziegler [38] found various results about representations of elements of R as sums of S-units in R, where S is a finite set of places containing all Archimedean places.

Another variant of Problem A asks for representations of algebraic integers as sums of distinct units. Jacobson [23] proved that in the rings of integers of the number fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, every element is a sum of distinct units. His conjecture that these are the only quadratic number fields with that property was proved by Śliwa [30]. Belcher [3, 4] investigated cubic and quartic number fields. A recent article by Thuswaldner and Ziegler [32] puts these results into a more general framework: they apply methods from the theory of arithmetic dynamical systems to additive unit representations.

4. The extension problem

Problem B. [24, Problem B] *Is it true that each number field has a finite extension L such that the ring of integers of L is generated by its units?*

If K is an Abelian number field, that is, $K|\mathbb{Q}$ is a Galois extension with Abelian Galois group, then we know by the Kronecker-Weber theorem that K is contained in a cyclotomic number field $\mathbb{Q}(\zeta)$, where ζ is a primitive root of unity. The ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$, which is obviously generated by its units. Problem B was completely solved by Frei [13]:

Theorem 10. [13, Theorem 1] *For any number field K, there exists a number field L containing K, such that the ring of integers of L is generated by its units.*

The proof relies on finding elements of the ring of integers of K with certain properties via asymptotic counting arguments, and then using these properties to generate easily manageable quadratic extensions of K in which those elements are sums of units of the respective rings of integers. The field L is then taken as the compositum of all these quadratic extensions.

Prior to this, with an easier but conceptually similar argument, Frei [15] answered the function field version of Problem B:

Theorem 11. [15, Theorem 2] *Let $F|K$ be an algebraic function field over a perfect field K, and R the ring of S-integers of F, for some finite set $S \neq \emptyset$ of places. Then there exists a finite extension field F' of F such that the integral closure of R in F' is generated by its units.*

5. The quantitative problem

Problem C. [24, Problem C] *Let K be an algebraic number field. Obtain an asymptotical bound for the number $N_k(x)$ of positive rational integers $n \leq x$ which are sums of at most k units of the ring of integers of K.*

As Jarden and Narkiewicz noticed, Lemma 2 and Szemerédi's theorem (see [19]) imply that

$$\lim_{x\to\infty} \frac{N_k(x)}{x} = 0,$$

for any fixed k. Aside from this, the problem still remains open.

A similar question has been investigated by Filipin, Fuchs, Tichy, and Ziegler [11, 12, 16]. We state here the most general result [16]. Let R be the ring of S-integers of a number field K, where S is a finite set of places containing all Archimedean places. Two S-integers α, β are *associated*, if there exists a unit ε of R such that $\alpha = \beta\varepsilon$. For any $\alpha \in R$, we write

$$N(\alpha) := \prod_{\nu\in S} |\alpha|_\nu.$$

Fuchs, Tichy and Ziegler investigated the counting function $u_{K,S}(n, x)$ which denotes the number of all classes $[\alpha]$ of associated elements α of R with $N(\alpha) \leq x$ such that α can be written as a sum

$$\alpha = \sum_{i=1}^{n} \varepsilon_i,$$

where the ε_i are units of R and no subsum of $\varepsilon_1 + \cdots + \varepsilon_n$ vanishes. The proof uses ideas of Everest [8], see also Everest and Shparlinski [9].

Theorem 12. [16, Theorem 1] *Let $\varepsilon > 0$. Then*

$$u_{K,S}(n,x) = \frac{c_{n-1,s}}{n!}\left(\frac{\omega_K(\log x)^s}{\mathrm{Reg}_{K,S}}\right)^{n-1} + o((\log x)^{(n-1)s-1+\varepsilon}),$$

as $x \to \infty$. Here, ω_K is the number of roots of unity of K, $\mathrm{Reg}_{K,S}$ is the S-regulator of K, and $s = |S| - 1$. The constant $c_{n,s}$ is the volume of the polyhedron

$$\{(x_{11}, \dots, x_{ns}) \in \mathbb{R}^{ns} \mid g(x_{11}, \dots, x_{ns}) < 1\},$$

with

$$g(x_{11}, \dots, x_{ns}) = \sum_{i=1}^{s} \max\{0, x_{1i}, \dots, x_{ni}\} + \max\left\{0, -\sum_{i=1}^{s} x_{1i}, \dots, -\sum_{i=1}^{s} x_{ni}\right\}.$$

The values of the constant $c_{n,s}$ are known in special cases from [16]:

	n				
s	1	2	3	4	5
1	2	3	4	5	6
2	3	15/4	7/2	45/16	
3	10/3	7/3	55/54		
4	35/12	275/32			
5	21/10				

Furthermore, $c_{n,1} = n + 1$ and $c_{1,s} = \frac{1}{s!}\binom{2s}{s}$.

In the following we calculate the constant $c_{n,s}$ for $n > 1$ and $s = 2$. This constant is the volume of the polyhedron

$$V = \{(x,y) \in \mathbb{R}^n \times \mathbb{R}^n : g(x,y) < 1\},$$

with

$$g(x,y) = \max_i \{0, x_i\} + \max_i \{0, y_i\} + \max_i \{0, -x_i - y_i\},$$

where $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$.

For any K, L, $M \in \{1, \dots, n\}$ we consider the sets

$$V_{K,L,M} = \big\{(x,y) \in \mathbb{R}^{2n} : x_i \le x_K,\ y_i \le y_L,\ x_M + y_M \le x_i + y_i,\ g(x,y) < 1\big\}.$$

Clearly the union of these sets is V and the intersection of any two of them has volume zero. Thus

$$c_{n,2} = \sum_{K=1}^{n}\sum_{L=1}^{n}\sum_{M=1}^{n} I_{K,L,M},$$

where $I_{K,L,M}$ is the volume of $V_{K,L,M}$. For the values of $I_{K,L,M}$ we distinguish three cases:

(i) K, L, M are pairwise distinct;

(ii) exactly two of the indices K, L, M are equal;
(iii) $K = L = M$.

The third case is simple. Since $x_i \leq x_K$, $y_i \leq y_K$ implies $x_i + y_i \leq x_K + y_K$ we obtain $x_i + y_i = x_K + y_K$. Thus $V_{K,K,K}$ has volume zero.

We only have to consider the remaining cases (i) and (ii). Clearly,

$$c_{n,2} = n(n-1)(n-2)I_{1,2,3} + 3n(n-1)I_{1,1,2}.$$

5.i. **Calculation of $I_{1,2,3}$.** This case can only happen if $n \geq 3$. The inequalities $x_3 + y_3 \leq x_i + y_i$ give us lower bounds for x_i and y_i and we always have the upper bounds $x_i \leq x_1$ and $y_i \leq y_2$. Hence we have

$$x_3 + y_3 - x_i \leq y_i \leq y_2$$

and

$$x_i \leq x_1.$$

Note that

$$g(x,y) = \max\{0, x_1\} + \max\{0, y_2\} + \max\{0, -x_3 - y_3\}.$$

We integrate with respect to the y_i's, $i \neq 2, 3$ and obtain

$$I_{1,2,3} = \int\cdots\int_{\substack{x_3+y_3-x_i\leq y_i\leq y_2\\ x_i\leq x_1,\, g(x,y)<1}} dxdy = \int\cdots\int_{\substack{x_3+y_3\leq x_2+y_2\\ x_3+y_3-y_2\leq x_i\leq x_1\\ y_3\leq y_2,\, g(x,y)<1}} \prod_{j\neq 2,3} (y_2 - x_3 - y_3 + x_j)\, dxdy_2dy_3.$$

Next we integrate over the x_i's, $i \neq 1, 2, 3$ and obtain

$$I_{1,2,3} = \int\cdots\int_{\substack{x_2,x_3\leq x_1,\, y_3\leq y_2\\ x_3+y_3\leq x_2+y_2\\ g(x,y)<1}} \frac{1}{2^{n-3}} \left(y_2 - x_3 - y_3 + x_1\right)^{2n-5} dx_1dx_2dx_3dy_2dy_3.$$

For the values of $g(x, y)$ we consider the following cases depending on the signs of x_1, y_2 and $-x_3 - y_3$:

r	x_1	y_2	$-x_3 - y_3$	$g(x,y)$
1	≥ 0	< 0	< 0	x_1
2	< 0	≥ 0	< 0	y_2
3	< 0	< 0	≥ 0	$-x_3 - y_3$
4	≥ 0	≥ 0	< 0	$x_1 + y_2$
5	≥ 0	< 0	≥ 0	$x_1 - x_3 - y_3$
6	< 0	≥ 0	≥ 0	$y_2 - x_3 - y_3$
7	≥ 0	≥ 0	≥ 0	$x_1 + y_2 - x_3 - y_3$

According to the table we split the integral into seven parts:

$$I_{1,2,3} = \sum_{r=1}^{7} I_{1,2,3}^{(r)}.$$

One can calculate these integrals with the help of a computer algebra system. We just give the final expressions:

$$\begin{aligned} I^{(1)}_{1,2,3} = I^{(2)}_{1,2,3} = I^{(3)}_{1,2,3} &= \frac{2}{n(2n-1)(n-1)2^n}, \\ I^{(4)}_{1,2,3} = I^{(5)}_{1,2,3} = I^{(6)}_{1,2,3} &= \frac{2}{n(n-1)2^n}, \\ I^{(7)}_{1,2,3} &= \frac{2}{n2^n}. \end{aligned}$$

In conclusion we have

$$I_{1,2,3} = \frac{2(n+1)(2n+1)}{n(2n-1)(n-1)2^n}.$$

5.ii. **Calculation of $I_{1,1,2}$.** We proceed in the same way as in the other case. We have the same bounds

$$x_2 + y_2 - x_i \leq y_i \leq y_1$$

and

$$x_i \leq x_1.$$

We integrate first with respect to the y_i's and then with respect to the x_i's, $i \neq 1, 2$, and obtain

$$\begin{aligned} I_{1,1,2} &= \int \cdots \int_{\substack{x_2+y_2-y_1 \leq x_i \leq x_1 \\ y_2 \leq y_1,\ g(x,y)<1}} \prod_{j \neq 1,2} (y_1 - x_2 - y_2 + x_j) dx dy_1 dy_2 \\ &= \int \cdots \int_{\substack{x_2 \leq x_1,\ y_2 \leq y_1 \\ g(x,y)<1}} \frac{1}{2^{n-2}} \left(y_1 - x_2 - y_2 + x_1\right)^{2n-4} dx_1 dx_2 dy_1 dy_2. \end{aligned}$$

Proceeding as in the previous section we again split the integral into seven parts $I^{(r)}_{1,1,2}$, $r = 1, \ldots, 7$, and obtain:

$$\begin{aligned} I^{(1)}_{1,1,2} = I^{(2)}_{1,1,2} = I^{(3)}_{1,1,2} &= \frac{1}{n(2n-1)(n-1)2^n}, \\ I^{(4)}_{1,1,2} = I^{(5)}_{1,1,2} = I^{(6)}_{1,1,2} &= \frac{1}{n(n-1)2^n}, \\ I^{(7)}_{1,1,2} &= \frac{1}{n2^n}. \end{aligned}$$

Hence

$$I_{1,1,2} = \frac{(n+1)(2n+1)}{n(2n-1)(n-1)2^n}.$$

Conclusion. *The value of $c_{n,2}$ is*

$$\frac{(n+1)(2n+1)}{2^n}.$$

Remark. *The computation of $c_{n,s}$ for $s > 2$ seems to be more difficult and might be considered later.*

6. Matrix rings

6.1. **Matrix rings over arbitrary rings.** Let R be any ring with 1. We say that two elements $a, b \in R$ are equivalent ($a \sim b$) if there exist two units $u, v \in R^\times$ such that $b = uav$. Vámos [34, Lemma 1] already noticed the following simple fact.

Lemma 13. *Let R be a ring and $a, b \in R$. If $a \sim b$ then, for all $k \geq 1$, a is k-good if and only if b is k-good.*

We consider the ring $M_n(R)$ of $n \times n$ matrices, with $n \geq 2$, over an arbitrary ring R with 1. As usual $GL_n(R)$ denotes the group of units of $M_n(R)$.

For $a \in R$ the matrix $E_n(a, i, j)$, $i, j \in \{1, \ldots, n\}$, $i \neq j$, is the $n \times n$ matrix with 1 entries on the main diagonal, a as the entry at position (i, j) and 0 elsewhere. We call this kind of matrices *elementary matrices* and denote by $E_n(R)$ the subgroup of $GL_n(R)$ generated by elementary matrices, permutation matrices and $-I$, where I is the identity matrix of $M_n(R)$.

Let us consider a more specific kind of k-goodness introduced by Vámos [34].

Definition. *A square matrix of size n over R is strongly k-good if it can be written as a sum of k elements of $E_n(R)$. The ring $M_n(R)$ is strongly k-good if every element is strongly k-good.*

The following lemma is Lemma 1 from [21] and Lemma 5 from [34].

Lemma 14. *Let R be a ring and $n \geq 2$. Then any diagonal matrix in $M_n(R)$ is strongly 2-good.*

A ring R is called an *elementary divisor ring* (see [25]) if every matrix in $M_n(R)$, $n \geq 2$, can be diagonalized. Lemma 14 implies that, in this case, $M_n(R)$ is 2-good. In particular, if any matrix in $M_n(R)$ can be diagonalized using only matrices in $E_n(R)$ then $M_n(R)$ is strongly 2-good.

The following two remarks can be deduced without much effort from the proof of Lemma 14 that is given in [34].

Remark. *If R is an elementary divisor ring and $1 \neq -1$ then the representation of a matrix in $M_n(R)$ as a sum of two units is never unique.*

Remark. *If R is an elementary divisor ring and $1 \neq -1$ then every element of $M_n(R)$ has a representation as a sum of two distinct units.*

As we have already mentioned, Henriksen [21] proved that $M_n(R)$, where R is any ring, is 3-good. Henriksen's result was generalized by Vámos [34] to arbitrary dimension:

Theorem 15. [34, Theorem 11] *Let R be a ring and let F be a free R-module of rank α, where $\alpha \geq 2$ is a cardinal number. Then the ring of endomorphisms E of F is 3-good.*

If α is finite and R is 2-good or an elementary divisor ring then E is 2-good. If R is any one of the rings $\mathbb{Z}[X]$, $K[X,Y]$, $K\langle X,Y\rangle$, where K is a field, then $u(E) = 3$. Here $K\langle X,Y\rangle$ is the free associative algebra generated by X, Y over K.

To prove that a matrix ring over a certain ring has unit sum number 3, Vámos used the following proposition.

Proposition 16. [34, Proposition 10] *Let R be a ring, $n \geq 2$ an integer and let $L = Ra_1 + \cdots + Ra_n$ be the left ideal generated by the elements $a_1, \ldots, a_n \in R$. Let A be the $n \times n$ matrix whose entries are all zero except for the first column which is $(a_1, \ldots, a_n)^T$. Suppose that*

1. L cannot be generated by fewer than n elements, and
2. zero is the only 2-good element in L.

Then A is not 2-good.

We now apply Lemma 14 to a special case. Let R be a ring and suppose there exists a function

$$f : R \setminus \{0\} \to \mathbb{Z}_{\geq 0},$$

with the following property: for every $a, b \in R$, $b \neq 0$, there exist $q_1, q_2, r_1, r_2 \in R$ such that

$$\begin{aligned} a &= q_1 b + r_1, \quad \text{where} \quad r_1 = 0 \text{ or } f(r_1) < f(b), \\ a &= b q_2 + r_2, \quad \text{where} \quad r_2 = 0 \text{ or } f(r_2) < f(b). \end{aligned}$$

Then we say that R has *left and right Euclidean division.*

The next theorem is a generalization of the well known fact that every square matrix over a Euclidean domain is diagonalizable. The proof strictly follows the line of the one in the commutative case (see Section 3.5 of [18]), hence it is omitted.

Theorem 17. *Let R be a ring with left and right Euclidean division and $n \geq 2$. For every $A \in M_n(R)$ there exist two matrices $U, V \in E_n(R)$ such that*

$$UAV = D,$$

where D is a diagonal matrix.

Corollary. *Let R be a ring with left and right Euclidean division and $n \geq 2$. Then $M_n(R)$ is strongly 2-good.*

We apply the previous result to the special case of quaternions. Consider the quaternion algebra

$$Q = \left\{ a + bi + cj + dk \mid a,\, b,\, c,\, d \in \mathbb{Q},\, i^2 = -1,\, j^2 = -1,\, k = ij = -ji \right\}.$$

Definition. *The ring of Hurwitz quaternions is defined as the set*

$$H = \left\{ a + bi + cj + dk \in Q \mid \ a, b, c, d \in \mathbb{Z} \ \ or \ \ a, b, c, d \in \mathbb{Z} + \frac{1}{2} \right\}.$$

For basic properties about Hurwitz quaternions see [5, Chapter 5].

In Q the ring of Hurwitz quaternions plays a similar role as maximal orders in number fields.

The units of H are the 24 elements ± 1, $\pm i$, $\pm j$, $\pm k$ and $(\pm 1 \pm i \pm j \pm k)/2$, so $u(H) = \omega$.

It is well known that H has left and right Euclidean division. Therefore, we get the following corollary.

Corollary. *For $n \geq 2$, $M_n(H)$ is strongly 2-good.*

6.2. **Matrix rings over Dedekind domains.** Let R be a ring and A an $r \times c$ matrix. The *type* of A is the pair (r, c) and the *size* of A is $\max(r, c)$. Let A_1 and A_2 be matrices of type (r_1, c_1) and (r_2, c_2), respectively. The *block diagonal sum* of A_1 and A_2 is the block diagonal matrix

$$diag(A_1, A_2) = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix},$$

of type $(r_1 + r_2, c_1 + c_2)$. A matrix of positive size is *indecomposable* if it is not equivalent to the block diagonal sum of two matrices of positive size.

In 1972 Levy [26] proved that, for a Dedekind domain R, the class number, when it is finite, is an upper bound to the number of rows and columns in every indecomposable matrix over R. Vámos and Wiegand [35] generalized Levy's result to Prüfer domains (under some technical conditions) and applied it to the unit sum problem.

Theorem 18. *(see* [35, Theorem 4.7]*) Let R be a Dedekind domain with finite class number c. For every $n \geq 2c$, $M_n(R)$ is 2-good.*

Unfortunately we do not know a criterion. The only sufficient condition we know for a matrix not to be 2-good is given by Proposition 16. For rings R of algebraic integers this proposition is of limited use. Since ideals in Dedekind domains need at most 2 generators, condition (1) can be fulfilled only for $n = 2$. Concerning condition (2) it is not hard to see that, if the unit group is infinite, there is a nonzero sum of two units in every nonzero ideal in a ring of algebraic integers. Therefore we can apply Proposition 16 only to the non-PID complex quadratic case.

Corollary. [35, Example 4.11] *Let R be the ring of integers of $\mathbb{Q}(\sqrt{-d})$, where $d > 0$ is squarefree and R has class number $c > 1$. Then $u(M_2(R)) = 3$ and $u(M_n(R)) = 2$ for every integer $n \geq 2c$.*

Question A. [35, Example 4.11] *With the hypotheses of the previous corollary, what is the value of $u(M_n(R))$ for $3 \leq n < 2c$?*

Question B. [35, Question 4.12] *If R is any ring of algebraic integers with class number c, what is the value of $u(M_n(R))$ for $2 \leq n < 2c$?*

References

1. N. Ashrafi, *A finer classification of the unit sum number of the ring of integers of quadratic fields and complex cubic fields*, Proc. Indian Acad. Sci. Math. Sci. **119** (2009), no. 3, 267–274.
2. N. Ashrafi and P. Vámos, *On the unit sum number of some rings*, Q. J. Math. **56** (2005), no. 1, 1–12.
3. P. Belcher, *Integers expressible as sums of distinct units*, Bull. Lond. Math. Soc. **6** (1974), 66–68.
4. ———, *A test for integers being sums of distinct units applied to cubic fields*, J. Lond. Math. Soc. (2) **12** (1975/76), no. 2, 141–148.
5. J. H. Conway and D. A. Smith, *On quaternions and octonions: their geometry, arithmetic and symmetry*, A K Peters, Natick, Massachusetts, 2003.
6. J. Dieudonné, *La théorie de Galois des anneux simples et semi-simples*, Comment. Math. Helv. **21** (1948), 154–184.
7. P. Erdös, *Arithmetical properties of polynomials*, J. London Math. Soc. **28** (1953), 416–425.
8. G. R. Everest, *Counting the values taken by sums of S-units*, J. Number Theory **35** (1990), no. 3, 269–286.
9. G. R. Everest and I. E. Shparlinski, *Counting the values taken by algebraic exponential polynomials*, Proc. Amer. Math. Soc. **127** (1999), no. 3, 665–675.
10. J.-H. Evertse and K. Győry, *On the numbers of solutions of weighted unit equations*, Compositio Math. **66** (1988), no. 3, 329–354.
11. A. Filipin, R. F. Tichy, and V. Ziegler, *The additive unit structure of pure quartic complex fields*, Funct. Approx. Comment. Math. **39** (2008), no. 1, 113–131.
12. ———, *On the quantitative unit sum number problem—an application of the subspace theorem*, Acta Arith. **133** (2008), no. 4, 297–308.
13. C. Frei, *On rings of integers generated by their units*, submitted.
14. ———, *Sums of units in function fields*, Monatsh. Math., DOI: 10.1007/s00605-010-0219-7.
15. ———, *Sums of units in function fields II - The extension problem*, to appear in Acta Arith.
16. C. Fuchs, R. F. Tichy, and V. Ziegler, *On quantitative aspects of the unit sum number problem*, Arch. Math. **93** (2009), 259–268.
17. B. Goldsmith, S. Pabst, and A. Scott, *Unit sum numbers of rings and modules*, Q. J. Math. **49** (1998), no. 195, 331–344.
18. F. M. Goodman, *Algebra: abstract and concrete*, SemiSimple Press, Iowa City, IA, 1998.
19. W. T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), no. 3, 465–588.
20. L. Hajdu, *Arithmetic progressions in linear combinations of S-units*, Period. Math. Hung. **54** (2007), no. 2, 175–181.
21. M. Henriksen, *Two classes of rings generated by their units*, J. Algebra **31** (1974), 182–193.
22. B. Herwig and M. Ziegler, *A remark on sums of units*, Arch. Math. (Basel) **79** (2002), no. 6, 430–431.
23. B. Jacobson, *Sums of distinct divisors and sums of distinct units*, Proc. Am. Math. Soc. **15** (1964), 179–183.

24. M. Jarden and W. Narkiewicz, *On sums of units*, Monatsh. Math. **150** (2007), no. 4, 327–332.
25. I. Kaplansky, *Elementary divisors and modules*, Trans. Amer. Math. Soc. **66** (1949), 464–491.
26. L. S. Levy, *Almost diagonal matrices over Dedekind domains*, Math. Z. **124** (1972), 89–99.
27. R. C. Mason, *Norm form equations. I*, J. Number Theory **22** (1986), no. 2, 190–207.
28. ———, *Norm form equations. III. Positive characteristic*, Math. Proc. Camb. Philos. Soc. **99** (1986), no. 3, 409–423.
29. A. Pethő and V. Ziegler, *On biquadratic fields that admit unit power integral basis,*, submitted.
30. J. Śliwa, *Sums of distinct units*, Bull. Acad. Pol. Sci. **22** (1974), 11–13.
31. A. K. Srivastava, *A survey of rings generated by units*, Ann. Fac. Sci. Toulouse Math. (6) **19** (2010).
32. J. Thuswaldner and V. Ziegler, *On linear combinations of units with bounded coefficients*, preprint.
33. R. F. Tichy and V. Ziegler, *Units generating the ring of integers of complex cubic fields*, Colloq. Math. **109** (2007), no. 1, 71–83.
34. P. Vámos, *2-good rings*, Q. J. Math. **56** (2005), no. 3, 417–430.
35. P. Vámos and S. Wiegand, *Block diagonalization and 2-unit sums of matrices over Prüfer domains*, to appear in Trans. Amer. Math. Soc.
36. B. L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Arch. Wisk (2) **15** (1927), 212–216.
37. D. Zelinsky, *Every linear transformation is a sum of nonsingular ones*, Proc. Am. Math. Soc. **5** (1954), 627–630.
38. V. Ziegler, *The additive S-unit structure of quadratic fields*, to appear in Int. J. Number Theory.
39. ———, *On unit power integral bases of $\mathbb{Z}[\sqrt[4]{m}]$*, to appear in Period. Math. Hung.
40. ———, *The additive unit structure of complex biquadratic fields*, Glas. Mat. **43(63)** (2008), no. 2, 293–307.

Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, A-8010 Graz, Austria

E-mail address: barroero@math.tugraz.at

E-mail address: frei@math.tugraz.at

E-mail address: tichy@tugraz.at