DIOPHANTINE AVOIDANCE AND SMALL-HEIGHT PRIMITIVE ELEMENTS IN IDEALS OF NUMBER FIELDS

LENNY FUKSHANSKY AND SEHUN JEONG

Abstract. Let K be a number field of degree d. Then every ideal I in the ring of integers $\mathcal{O}_K$ contains infinitely many primitive elements, i.e. elements of degree d. A bound on the smallest height of such an element in I follows from some recent developments in the direction of a 1998 conjecture of W. Ruppert. We prove an explicit bound on the smallest height of such a primitive element in the case of quadratic fields. Further, we consider primitive elements in an ideal outside of a finite union of other ideals and prove a bound on the height of a smallest such element. Our main tool is a result on points of small norm in a lattice outside of an algebraic hypersurface and a finite union of sublattices of finite index, which we prove by blending two previous Diophantine avoidance results. We also obtain a bound for small-norm lattice points in the positive orthant in $\mathbb{R}^d$ with avoidance conditions and use it to obtain a small-height totally positive primitive element in an ideal of a totally real number field outside of a finite union of other ideals. Additionally, we use our avoidance method to prove a bound on the Mahler measure of a generating non-sparse polynomial for a given number field. Finally, we produce a bound on the height of a smallest primitive generator for a principal ideal in a quadratic number field.

Contents

1. Introduction and statement of main results

Diophantine avoidance has been studied by several authors in the recent years. This term refers to effective results on existence of points of bounded size (measured by norm or height, depending on the context) in a given algebraic set avoiding some specified subsets. In particular, there is a variety of Siegel's lemma-type results on

2020 *Mathematics Subject Classification.* Primary: 11H06, 11G50, 11R04, 11R11.
Key words and phrases. lattice, number field, small height, ideal, primitive element.
Fukshansky was partially supported by the Simons Foundation grant #519058.

small-size points in linear spaces and lattices with different avoidance conditions (e.g., [7], [8], [9], [10], [12], [13], [15], [16]). The application of avoidance conditions allows to understand how "well-distributed" points of bounded size are in a given set: if it is possible to find them outside of some prescribed collection of subsets of the set in question, then it suggests that they are evenly distributed, in some appropriate sense. More specifically, it is often interesting to understand how a prescribed avoidance condition affects the upper bound on the size of the "smallest" element in question. In this paper, we are interested in further investigating small-size points in lattices with avoidance conditions. The main application of our investigation is to small-height generators of number fields satisfying certain natural avoidance conditions.

To start, let $\mathbb{E}^d$ be a d-dimensional Euclidean space, $\Omega \subset \mathbb{E}^d$ be a lattice of rank $d \geq 2$. Let Δ be the determinant of Ω, i.e., volume of its fundamental domain, and $\Lambda_1, \dots, \Lambda_s \subset \Omega$ be sublattices of finite indices $D_1, \dots, D_s \geq 2$, $s \geq 1$, so $\det \Lambda_i = D_i \Delta$ for every $1 \leq i \leq s$. Assume that

$$\Omega \not\subseteq \bigcup_{i=1}^{s} \Lambda_i,$$

and let $\Lambda = \bigcap_{i=1}^{s} \Lambda_i$. Then Λ is a sublattice of Ω of index no larger than $D := D_1 \cdots D_s$; see [14] for detailed information on lattices and their properties.

For a vector $\boldsymbol{z} \in \mathbb{E}^d$, let

$$|\boldsymbol{z}| = \max_{1 \leq i \leq d} |z_i|$$

be its sup-norm, and define

$$C_d(T) = \left\{ \boldsymbol{z} \in \mathbb{E}^d : |\boldsymbol{z}| \leq T \right\}$$

be the cube of side-length $2T$ centered at the origin in $\mathbb{E}^d$, $T > 0$. For any full-rank lattice $L \subset \mathbb{E}^d$, define $\lambda_i(L)$, the i-th successive minimum of L with respect to $C_d(1)$ to be

$$\lambda_i(L) = \min \left\{ T > 0 : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}} (C_d(T) \cap L) \geq i \right\}, \tag{1}$$

for each $1 \leq i \leq d$. A theorem of Henk and Thiel [15, Theorem 1.2] guarantees that there exists $\boldsymbol{x} \in \Omega \setminus \bigcup_{i=1}^{s} \Lambda_i$ such that

$$|\boldsymbol{x}| < \frac{2^d D \Delta}{\lambda_1(\Lambda)^{d-1} \operatorname{Vol}_d(C_d(1))} \left(\sum_{i=1}^{s} \frac{1}{D_i} - \frac{s-1}{D} + \frac{\lambda_1(\Lambda)^d}{D\Delta} \right), \tag{2}$$

where Vol_d stands for the d-dimensional measure on $\mathbb{E}^d$. This result was obtained using a careful analysis and volume computations on the torus group $\mathbb{R}^d/\Lambda$.

On the other hand, let $P(x_1, \dots, x_d) \in \mathbb{R}[x_1, \dots, x_d]$ be a nonzero polynomial of degree m. Let $S_1, \dots, S_d$ be finite subsets of $\mathbb{Z}$ with $|S_i| \geq m+1$ for each $1 \leq i \leq d$ and let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_d$ be linearly independent vectors in our lattice Ω. Then Theorem 4.2 of [10] implies that there exist coefficients $\xi_i \in S_i$ for $1 \leq i \leq d$ so that

$$P\left(\sum_{i=1}^{d} \xi_i \boldsymbol{v}_i \right) \neq 0. \tag{3}$$

The proof of this theorem (Theorem 4.2 of [10]) is an application of Alon's Combinatorial Nullstellensatz [3]. Our first goal is to bridge the two above-mentioned avoidance results and prove the following theorem.

Theorem 1.1. *Let the notation be as above. Then there exists*

$$\boldsymbol{z} \in \Omega \setminus \left(\bigcup_{i=1}^{s} \Lambda_i \right),$$

such that $P(\boldsymbol{z}) \neq 0$ *and*

(4)
$$|\boldsymbol{z}| \leq \frac{d(D(m+2)+2)D\Delta}{2\lambda_1(\Lambda)^{d-1}} \max\left\{1, \frac{2^d}{\mathrm{Vol}_d(C_d(1))}\left(\sum_{i=1}^{s}\frac{1}{D_i} - \frac{s-1}{D} + \frac{\lambda_1(\Lambda)^d}{D\Delta}\right)\right\}.$$

We prove Theorem 1.1 in Section 2 using (2), (3) and Minkowski's Successive Minima Theorem.

We apply our Theorem 1.1 in the context of algebraic number fields. Let K be a number field of degree $d = [K : \mathbb{Q}] \geq 1$. Let $\sigma_1, \ldots, \sigma_d : K \hookrightarrow \mathbb{C}$ be the embeddings of K, ordered so that the first r_1 of them are real and the remaining $2r_2$ are conjugate pairs of complex embeddings so that $\sigma_{r_2+j} = \bar{\sigma}_j$ for

$$d = r_1 + 2r_2.$$

An element $\alpha \in K$ is called *primitive* if $K = \mathbb{Q}(\alpha)$. This is equivalent to the condition that $\deg_{\mathbb{Q}}(\alpha) = d$, and hence there are infinitely many primitive elements in K. A conjecture of Ruppert [20] asserts that there exists a primitive element $\alpha \in K$ such that

$$h(\alpha) \leq c(d)|\Delta_K|^{\frac{1}{2d}},$$

where h is the absolute Weil height, Δ_K is the discriminant of the number field K, and $c(d)$ is a constant depending only on the degree d; we review the height machinery in Section 3. Ruppert himself proved this conjecture for quadratic number fields and for totally real fields of prime degree. There has been quite a bit of later work on this conjecture; for instance, Vaaler and Widmer [23] proved the conjecture for number fields with at least one real embedding. More generally, a slightly weaker bound is obtained by Pazuki and Widmer in [19, Lemma 7.1]:

$$h(\alpha) \leq |\Delta_K|^{\frac{1}{d}}. \tag{5}$$

In fact, a more detailed result follows from Lemma 7.1 of [19]. Let $\mathcal{O}_K \subset K$ be the ring of integers of K and let $I \subseteq \mathcal{O}_K$ be an ideal in this ring. It is not difficult to see that I contains infinitely many primitive elements, and a straight-forward modification of the proof of Lemma 7.1 of [19] (replacing $\mathcal{O}_K$ by I) produces a primitive element $\alpha \in I$ with

$$h(\alpha) \leq \mathbb{N}_K(I)^{\frac{2}{d}}|\Delta_K|^{\frac{1}{d}}, \tag{6}$$

where $\mathbb{N}_K(I) = |\mathcal{O}_K/I|$ is the norm of the ideal I. To this end, we obtain a more concrete result in the case of quadratic number fields.

Theorem 1.2. *Let D be a squarefree integer and let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field. Let $I \subseteq \mathcal{O}_K$ be an ideal with the canonical basis $\{a, b + g\delta\}$, as described in* (16)*, so that $b < a$. Let*

$$h_{\min}(I) = \min\left\{h(\alpha) : \alpha \in I, K = \mathbb{Q}(\alpha)\right\}.$$

If $D \not\equiv 1 (\mathrm{mod}\, 4)$, then

$$\sqrt{ag} < h_{\min}(I) \leq g\left(\frac{2b + \sqrt{|\Delta_K|}}{2}\right),$$

and additionally $h_{\min}(I) > g\sqrt{|\Delta_K|}/2$ *if* $D < 0$.
If $D \equiv 1 (\mathrm{mod}\, 4)$, *then*

$$\sqrt{ag} < h_{\min}(I) \leq g\left(\frac{(2b+1)+\sqrt{|\Delta_K|}}{2}\right),$$

and additionally $h_{\min}(I) > g\sqrt{|\Delta_K|}/2$ *if* $D < 0$.

To compare the bounds of Theorem 1.2 to that of (6), notice that

$$bg < ag = \begin{cases} \mathbb{N}_K(I) & \text{if } D \not\equiv 1 (\mathrm{mod}\, 4), \\ 2\mathbb{N}_K(I) & \text{if } D \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

For example, in the case $D \not\equiv 1 (\mathrm{mod}\, 4)$, if $D > 4$ and $b > 2$, we obtain

$$h_{\min}(I) \leq g\left(\frac{2b+\sqrt{|\Delta_K|}}{2}\right) < \frac{bg\sqrt{|\Delta_K|}}{2} < \frac{\mathbb{N}_K(I)\sqrt{|\Delta_K|}}{2},$$

which is a slight improvement on (6), since $d = 2$; there is a similar comparison in the case $D \equiv 1 (\mathrm{mod}\, 4)$. We review all the necessary notation and prove Theorem 1.2 in Section 4.

To generalize the above setting, our next result produces a small-height primitive element in an ideal of a number field outside of a finite collection of other ideals.

Theorem 1.3. *Let* K *be a number field of degree* $d \geq 2$ *and let* $I \subset \mathcal{O}_K$ *be an ideal and* $J_1, \ldots, J_s \subsetneq I$ *be distinct ideals in* $\mathcal{O}_K$. *Let* $J = J_1 \cdots J_s$. *Then there exists an element* $\alpha \in I \setminus \bigcup_{i=1}^{s} J_i$ *such that* $K = \mathbb{Q}(\alpha)$ *and*

$$\begin{aligned} h(\alpha) \quad \leq \quad & \frac{d\ \mathbb{N}_K(J)|\Delta_K|^{1/2}\left((d^2-d+4)\ \mathbb{N}_K(J)+4\mathbb{N}_K(I)\right)}{4\mathbb{N}_K(I)} \times \\ & \times \max\left\{1, \left(\frac{2}{\pi}\right)^{r_2}\left(\sum_{i=1}^{s}\frac{\mathbb{N}_K(I)}{\mathbb{N}_K(J_i)} - \frac{(s-1)\mathbb{N}_K(I)}{\mathbb{N}_K(J)} + \frac{\mathbb{N}_K(J)^{d-1}}{|\Delta_K|^{1/2}}\right)\right\}. \end{aligned} \tag{7}$$

We want to emphasize that imposing an additional avoidance condition on an existence result for a primitive element is natural in the context of the Primitive Element Theorem, which asserts the existence of infinitely many primitive elements in a number field. The standard proof of this celebrated theorem (see, for instance, Theorem 2.2 of [22]) produces a primitive element for a number field K by constructing an element in K that avoids a finite collection of linear equations over $\mathbb{Q}$. In other words, the avoidance idea is already intrinsic to this construction. In fact, our avoidance argument produces, among other things, an alternate proof of the (effective version of the) Primitive Element Theorem.

Notice that the bound of (7) is explicit in terms of the invariants of K and norms of the ideals involved. To get a better grasp on its order of magnitude, it may be helpful to rewrite in a less explicit form as

$$h(\alpha) \ll_{K,s} \frac{\mathbb{N}_K(J)^{d+1}}{\mathbb{N}_K(I)}. \tag{8}$$

We prove Theorem 1.3 in Section 5, where our main tool is Theorem 1.1. In Section 6, we prove an analogous result for primitive totally positive elements in an ideal of a totally real number field outside of a finite union of other ideals (Corollary 6.2). This result follows as a consequence of a theorem we obtain on existence

of a small-norm positive point in a lattice avoiding a finite union of sublattices of the same rank and an algebraic set (Theorem 6.1). This theorem is proved by blending together the method of proof of Theorem 1.1 with the results on small-height lattice points in positive cones obtained in [11]. We also use our avoidance method in Section 7 to prove the existence of a monic polynomial $f(x) \in \mathbb{Z}[x]$ with bounded Mahler measure and all nonzero coefficients so that a given number field K is isomorphic to $\mathbb{Q}[x]/\langle f(x)\rangle$.

So far, we were concerned with small-height primitive elements, i.e. generators of number fields, contained in a prescribed ideal. Now we turn to small-height generators of ideals in number fields. It is well known that every ideal $I \subseteq \mathcal{O}_K$ can be generated by two elements (see, e.g., Theorem 5.20 of [22]), and principal ideals (i.e., ideals generated by a single element) correspond to the identity element in the class group of K. If $\mu \in \mathcal{O}_K$ is a generator for a principal ideal $I \subseteq \mathcal{O}_K$ and $\varepsilon \in \mathcal{O}_K^\times$ is a unit, then $\varepsilon\mu$ is another generator for I. Dirichlet units theorem states that the rank of the unit group $\mathcal{O}_K^\times$ is $r = r_1 + r_2 - 1$ (see, e.g., [22] for further details). In particular, $\mathcal{O}_K^\times$ is infinite unless K is an imaginary quadratic field. Hence, the same principal ideal I can have infinitely many generators, and while the norm of all of them is the same ($= \mathbb{N}_K(I)$), their heights can be very different and arbitrarily large. Theorem 1.1 of [1] by Akhtari and Vaaler then implies that there exists a generator μ for I such that

$$h(\mu) \le \mathbb{N}_K(I)^{1/d} \prod_{j=1}^{r} h(\varepsilon_j)^{1/2}, \tag{9}$$

where $\varepsilon_1, \dots, \varepsilon_r$ are multiplicatively independent units in $\mathcal{O}_K^\times$. In order to obtain a bound on $h(\mu)$ in terms of the invariants of I and K alone, we now need a result on existence of small-height multiplicatively independent units in $\mathcal{O}_K^\times$. Such a result has been obtained recently also by Akhtari and Vaaler in [2], but with a bound on the product of logarithmic heights of the units in question. Hence, using this bound in conjunction with (9) would essentially require reversing arithmetic-geometric mean inequality. On the other hand, we can obtain the following bound on $h(\mu)$ in the case of a quadratic number field using a different method.

Theorem 1.4. *Let D be a squarefree integer and let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field. Let $I \subseteq \mathcal{O}_K$ be a principal ideal with the canonical basis $\{a, b + g\delta\}$, as described in* (16)*. Define*

$$H(I) := \begin{cases} \max\left\{\frac{|a|}{g}, \frac{|2b|}{g}, \frac{|b^2-D|}{ag}\right\} & \text{if } D \not\equiv 1 \pmod 4 \\ \max\left\{\frac{|2a|}{g}, \frac{2|2b+g|}{g}, \frac{|4b^2+4b-Dg+g|}{2ag}\right\} & \text{if } D \equiv 1 \pmod 4, \end{cases} \tag{10}$$

Then there exists a primitive element $\mu \in I$ such that $I = \langle\mu\rangle$ and

$$h(\mu) \le \begin{cases} \left(a + b + g\sqrt{|D|}\right)(14H(I))^{5H(I)} & \text{if } D \not\equiv 1 \pmod 4 \\ \left(a + \frac{2b+g+g\sqrt{|D|}}{2}\right)(14H(I))^{5H(I)} & \text{if } D \equiv 1 \pmod 4, \end{cases}$$

Theorem 1.4 is essentially the quadratic case of a general difficult problem: given an infinite set of elements of fixed norm N in $\mathcal{O}_K$, prove the existence of an element of bounded height in this set with the bound depending only on N and invariants of the number field K. We prove Theorem 1.4 in Section 8. Our main tool is a result

of Kornhauser [17] on small-height zeros of integral binary quadratic equations with integer coefficients. We are now ready to proceed.

2. Avoiding sublattices and algebraic sets

The goal of this section is to prove Theorem 1.1, establishing an effective result on existence of a point in a lattice avoiding a union of full-rank sublattices and an algebraic hypersurface. Let the notation be as in the statement of the theorem. Then Minkowski's successive minima theorem (see, for instance, [14, Section 9.1, Theorem 1]) implies that $\prod_{i=1}^{d} \lambda_i(\Lambda) \le D\Delta$, and so

$$\lambda_d(\Lambda) \le \frac{D\Delta}{\lambda_1(\Lambda)^{d-1}}, \tag{11}$$

since $0 < \lambda_1(\Lambda) \le \cdots \le \lambda_{d-1}(\Lambda) \le \lambda_d(\Lambda)$.

Let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_d \in \Lambda$ be linearly independent vectors corresponding to these successive minima, so $|\boldsymbol{v}_i| = \lambda_i(\Lambda)$. Let $\boldsymbol{x} \in \Omega \setminus \bigcup_{i=1}^{s} \Lambda_i$ be a vector satisfying (2), then there is a subset of $d-1$ vectors among $\boldsymbol{v}_1, \dots, \boldsymbol{v}_d$ with which $\boldsymbol{x}$ is linearly independent, assume these are $\boldsymbol{v}_2, \dots, \boldsymbol{v}_d$, since they have larger norm. Notice that for any integer k and any vector $\boldsymbol{y} \in \Omega$, $Dk\boldsymbol{y} \in \Lambda_i$ for every $1 \le i \le s$, and hence the vector $(Dk+1)\boldsymbol{x} \notin \Lambda_i$ for every $1 \le i \le s$. Therefore, for all integers $k, n_2, \dots, n_d$, we have a collection of vectors

$$(Dk+1)\boldsymbol{x} + n_2\boldsymbol{v}_2 + \cdots + n_d\boldsymbol{v}_d \in \Omega \setminus \bigcup_{i=1}^{s} \Lambda_i. \tag{12}$$

Let $[\ ]$ denote the integer part function, and define the sets

$$\begin{aligned} S_1 &= \{Dk+1 : k \in \mathbb{Z}, -[m/2]-1 \le k \le [m/2]+1\}, \\ S_2 &= \{j \in \mathbb{Z} : -[m/2]-1 \le j \le [m/2]+1\}, \end{aligned} \tag{13}$$

consisting of $m+1$ integers each. Then (3) implies that there exists a vector

$$\boldsymbol{\xi} = (\xi_1, \xi_2, \dots, \xi_d) \in S_1 \times S_2 \times \cdots \times S_2$$

so that

$$P\left(\xi_1\boldsymbol{x} + \sum_{i=2}^{d} \xi_i \boldsymbol{v}_i\right) \neq 0.$$

Let $\boldsymbol{z} = \xi_1\boldsymbol{x} + \sum_{i=2}^{d} \xi_i\boldsymbol{v}_i$ for this choice of $\boldsymbol{\xi}$. We now need to estimate its sup-norm. Since

$$\lambda_1(\Lambda) = |\boldsymbol{v}_1| \le \lambda_2(\Lambda) = |\boldsymbol{v}_2| \le \cdots \le \lambda_d(\Lambda) = |\boldsymbol{v}_d|,$$

we can put together (2) and (11) to obtain

$$\begin{aligned} |\boldsymbol{z}| &\le d\left(\max_{1\le i\le d} |\xi_i|\right)(\max\{|\boldsymbol{x}|, \lambda_d(\Lambda)\}) \\ &\le \frac{d(D(m+2)+2)D\Delta}{2\lambda_1(\Lambda)^{d-1}} \max\left\{1, \frac{2^d}{\mathrm{Vol}_d(C_d(1))}\left(\sum_{i=1}^{s}\frac{1}{D_i} - \frac{s-1}{D} + \frac{\lambda_1(\Lambda)^d}{D\Delta}\right)\right\}. \end{aligned}$$

This completes the proof.

3. Heights and additional notation

In this section, we set up the notation needed for the proofs of our Theorems 1.2, 1.3 and 1.4. Notice that the space $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$ can be viewed as a subspace of

$$\left\{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : y_{r_2+j} = \bar{y}_j \ \forall\ 1 \le j \le r_2\right\} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \subset \mathbb{C}^d.$$

Here, in the containment

$$\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \mathbb{R} \times \cdots \times \mathbb{R} \times \mathbb{C} \times \cdots \times \mathbb{C} \subset \mathbb{C} \times \cdots \times \mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C} = \mathbb{C}^d$$

each copy of $\mathbb{R}$ is identified with the real part of the corresponding copy of $\mathbb{C}$ in which it is contained. Then $K_{\mathbb{R}}$ is a d-dimensional Euclidean space with the bilinear form induced by the trace form on K:

$$\langle \alpha, \beta \rangle := \mathrm{Tr}_K(\alpha\bar{\beta}) \in \mathbb{R},$$

for every $\alpha, \beta \in K$, where Tr_K is the number field trace on K. We also define the sup-norm on $K_{\mathbb{R}}$ by

$$|\boldsymbol{x}| := \max\{|x_1|, \ldots, |x_d|\},$$

for any $\boldsymbol{x} \in K_{\mathbb{R}}$, where $|x_j|$ stands for the usual absolute value of x_j on $\mathbb{C}$. Let $\Sigma_K = (\sigma_1, \ldots, \sigma_d) : K \hookrightarrow K_{\mathbb{R}}$ be the Minkowski embedding, then for any ideal $I \subseteq \mathcal{O}_K$ the image $\Sigma_K(I)$ is a lattice of full rank in $K_{\mathbb{R}}$. We define the determinant of a full-rank lattice to be the absolute value of the determinant of any basis matrix for the lattice, then

$$\det(\Sigma_K(I)) = \mathbb{N}_K(I)|\Delta_K|^{1/2}, \tag{14}$$

as follows, for instance, from Corollary 2.4 of [4].

Next we normalize absolute values and introduce the standard height function. Let us write $M(K)$ for the set of places of K. For each $v \in M(K)$ let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree, then for each $u \in M(\mathbb{Q})$, $\sum_{v|u} d_v = d$. We select the absolute values so that $|\ |_v$ extends the usual archimedean absolute value on $\mathbb{Q}$ when $v \mid \infty$, or the usual p-adic absolute value on $\mathbb{Q}$ when $v \nmid \infty$. With this choice, the product formula reads

$$\prod_{v \in M(K)} |\alpha|_v^{d_v} = 1,$$

for each nonzero $\alpha \in K$. We define the multiplicative Weil height on algebraic vectors $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in K^n$ as

$$h(\boldsymbol{\alpha}) = \prod_{v \in M(K)} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{\frac{d_v}{d}},$$

for all $n \ge 1$. This height is absolute, meaning that it is the same when computed over any number field K containing $\alpha_1, \ldots, \alpha_n$: this is due to the normalizing exponent $1/d$ in the definition. Hence we can compute height for points defined over $\overline{\mathbb{Q}}$.

We also review a couple useful well-known properties of heights. The first can be found, for instance, as Lemma 2.1 of [10].

Lemma 3.1. *Let $\xi_1, \ldots, \xi_m \in \overline{\mathbb{Q}}$ and $\boldsymbol{x}, \ldots, \boldsymbol{x}_m \in \overline{\mathbb{Q}}^n$ for $m, n \ge 1$. Then*

$$h\left(\sum_{j=1}^m \xi_j \boldsymbol{x}_j\right) \le m h(\boldsymbol{\xi}) \prod_{j=1}^m h(\boldsymbol{x}_j),$$

where $\boldsymbol{\xi} = (\xi_1, \dots, \xi_m)$.

Next is Lemma 4.1 of [11]: while in that paper the lemma is stated for totally real fields, its proof holds verbatim for any number field with our definition of Minkowski embedding Σ_K.

Lemma 3.2. *For any* $\alpha \in \mathcal{O}_K$,

$$1 \le h(\alpha) \le |\Sigma_K(\alpha)|,$$

where $|\ |$ *stands for the sup-norm on* $K_{\mathbb{R}}$, *as above.*

4. Quadratic fields

In this section we review the additional necessary notation specific to Theorem 1.2 and prove this theorem. First notice that for any number field K and $\alpha \in \mathcal{O}_K$,

$$h(\alpha) = \prod_{v|\infty} \max\{1, |\alpha|_v\}^{\frac{d_v}{d}} \ge \left(\prod_{v|\infty} |\alpha|_v^{d_v} \right)^{\frac{1}{d}} = \left(\prod_{j=1}^{d} |\sigma_j(\alpha)| \right)^{\frac{1}{d}} = \mathbb{N}_K(\alpha)^{\frac{1}{d}}.$$

Now let D be a squarefree integer and $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field. Let $I \subseteq \mathcal{O}_K$ be an ideal. Then there exists a unique integral basis $a, b + g\delta$ for I, called the canonical basis, where

$$\delta = \begin{cases} -\sqrt{D} & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \not\equiv 1 (\mathrm{mod}\, 4) \\ \frac{1-\sqrt{D}}{2} & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \equiv 1 (\mathrm{mod}\, 4), \end{cases} \tag{15}$$

and $a, b, g \in \mathbb{Z}_{\ge 0}$ such that

$$b < a,\ g \mid a, b, \text{ and } ag \mid \mathbb{N}_K(b + g\delta), \tag{16}$$

see Section 6.3 of [5] for further details. The embeddings $\sigma_1, \sigma_2 : K \to \mathbb{C}$ are given by

$$\sigma_1(x + y\sqrt{D}) = x + y\sqrt{D},\ \sigma_2(x + y\sqrt{D}) = x - y\sqrt{D}$$

for each $x + y\sqrt{D} \in K$, where D is positive for real quadratic field K and negative for imaginary quadratic field K. The number field norm on K is given by

$$\mathbb{N}_K(x + y\sqrt{D}) = \sigma_1(x + y\sqrt{D})\sigma_2(x + y\sqrt{D}) = \left(x + y\sqrt{D}\right)\left(x - y\sqrt{D}\right).$$

The discriminant of K is

$$\Delta_K = \begin{cases} 4D & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \not\equiv 1 (\mathrm{mod}\, 4) \\ D & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \equiv 1 (\mathrm{mod}\, 4), \end{cases} \tag{17}$$

and the norm of the ideal I with the canonical basis as in (16) above is

$$\mathbb{N}_K(I) = \begin{cases} ag & \text{if } D \not\equiv 1 (\mathrm{mod}\, 4), \\ ag/2 & \text{if } D \equiv 1 (\mathrm{mod}\, 4). \end{cases} \tag{18}$$

Observe that an ideal I with the canonical basis as in (16) above can be written as $I = gJ$ for the corresponding ideal $J = \frac{1}{g} I \subseteq \mathcal{O}_K$, since $g \mid a, b$. Hence we start by restricting our consideration to ideals with $g = 1$. Then the bound in (6) in the case of a quadratic field can be written as

$$\sqrt{\mathbb{N}_K(\alpha)} \le h(\alpha) \ll a\sqrt{|D|}. \tag{19}$$

We will show that in this case the power on $\sqrt{D}$ cannot in general be reduced. First observe that an element $\alpha \in I$ is primitive if and only if it is of the form

$$\alpha = xa + y(b + \delta)$$

with $x, y \in \mathbb{Z}$ and $y \neq 0$.

Case 1: Suppose $D \in \mathbb{Z}$ is squarefree, $D \not\equiv 1 \pmod 4$ and $K = \mathbb{Q}(\sqrt{D})$. Then K is a real quadratic if $D > 0$ and K is an imaginary quadratic if $D < 0$. Take an ideal

$$I = \mathrm{span}_{\mathbb{Z}}\{a, b - \sqrt{D}\} \subseteq \mathcal{O}_K$$

with $a \mid \mathbb{N}_K(b - \sqrt{D}) = |b^2 - D|$. Then

$$\begin{aligned} \mathbb{N}_K(\alpha) &= \left|\left(xa + y(b - \sqrt{D})\right)\left(xa + y(b + \sqrt{D})\right)\right| \\ &= \left|x^2a^2 + 2xyab + y^2(b^2 - D)\right| = a\left|x^2a + 2xyb + y^2\left(\frac{b^2 - D}{a}\right)\right| > a, \end{aligned} \tag{20}$$

where $(b^2 - D)/a \in \mathbb{Z}$. Further,

$$\mathbb{N}_K(\alpha) = \left|x^2a^2 + 2xyab + y^2(b^2 - D)\right| = \left|(xa + yb)^2 - y^2D\right| > |D|, \tag{21}$$

if $D < 0$. On the other hand,

$$\begin{aligned} h(\alpha) &= \prod_{v \in M(K)} \max\{1, |\alpha|_v\}^{\frac{d_v}{2}} = \prod_{v|\infty} \max\{1, |\alpha|_v\}^{\frac{d_v}{2}} = \left(\prod_{j=1}^{2} \max\{1, |\sigma_i(\alpha)|\}\right)^{\frac{1}{2}} \\ &\leq \frac{1}{2}\left(\max\{1, |\sigma_1(\alpha)|\} + \max\{1, |\sigma_2(\alpha)|\}\right) \leq \frac{1}{2}\left(2 \cdot \max\{|\sigma_1(\alpha)|, |\sigma_2(\alpha)|\}\right) \\ &= \max\{|\sigma_1(\alpha)|, |\sigma_2(\alpha)|\} = \max\left\{\left|(xa + yb) - y\sqrt{D}\right|, \left|(xa + yb) + y\sqrt{D}\right|\right\} \\ &\leq |x|a + |y|b + |y|\sqrt{|D|}. \end{aligned} \tag{22}$$

Taking the minimum over all primitive elements $\alpha \in I$, we see that

$$\begin{aligned} \min\{h(\alpha) : \alpha \in I, K = \mathbb{Q}(\alpha)\} &\leq \min\{|x|a + |y|b + |y|\sqrt{|D|} : x, y \in \mathbb{Z}, y \neq 0\} \\ &\leq b + \sqrt{|D|}, \end{aligned} \tag{23}$$

where the last inequality is obtained by taking $x = 0$, $y = 1$. Putting together (19), (20), (21) and (23), we obtain the $D \not\equiv 1 (\mathrm{mod}\, 4)$ case of Theorem 1.2 in case $g = 1$.

Case 2: Suppose $D \in \mathbb{Z}$ is squarefree, $D \equiv 1 \pmod 4$ and $K = \mathbb{Q}(\sqrt{D})$. Again, K is a real quadratic if $D > 0$ and K is an imaginary quadratic if $D < 0$. Take an ideal

$$I = \mathrm{span}_{\mathbb{Z}}\left\{a, b + \frac{1 - \sqrt{D}}{2}\right\} \subseteq \mathcal{O}_K$$

with $a \mid \mathbb{N}_K\left(\frac{(2b+1)-\sqrt{D}}{2}\right) = \frac{|(2b+1)^2-D|}{4} = \left|b^2+b-\frac{D-1}{4}\right|$. Then

$$\begin{aligned}
\mathbb{N}_K(\alpha) &= \left|\left(xa+y\left(b+\frac{1-\sqrt{D}}{2}\right)\right)\left(xa+y\left(b+\frac{1+\sqrt{D}}{2}\right)\right)\right| \\
&= \left|x^2a^2+(2b+1)axy+y^2\left(b^2+b-\frac{D-1}{4}\right)\right| \\
&= a\left|x^2a+(2b+1)xy+\frac{y^2}{a}\left(b^2+b-\frac{D-1}{4}\right)\right| > a, \qquad (24)
\end{aligned}$$

where $\frac{1}{a}\left(b^2+b-\frac{D-1}{4}\right) \in \mathbb{Z}$. Further,

$$\mathbb{N}_K(\alpha) = \left|x^2a^2+(2b+1)axy+y^2(b^2+b+1/4)-y^2D/4\right| > |D|/4, \qquad (25)$$

if $D<0$. On the other hand,

$$\begin{aligned}
h(\alpha) &\leq \max\{|\sigma_1(\alpha)|, |\sigma_2(\alpha)|\} \\
&= \max\left\{\left|xa+y\left(b+\frac{1-\sqrt{D}}{2}\right)\right|, \left|xa+y\left(b+\frac{1+\sqrt{D}}{2}\right)\right|\right\} \\
&\leq |x|a+\frac{|y|(2b+1)}{2}+\frac{|y|\sqrt{|D|}}{2}. \qquad (26)
\end{aligned}$$

Taking the minimum over all primitive elements $\alpha \in I$, we see that

$$\min\{h(\alpha) : \alpha \in I, K=\mathbb{Q}(\alpha)\} \leq \frac{(2b+1)+\sqrt{|D|}}{2}, \qquad (27)$$

where the inequality is obtained by taking $x=0$, $y=1$. Putting together (19), (24), (25) and (27), we obtain the $D \equiv 1 (\mathrm{mod}\, 4)$ case of Theorem 1.2 in case $g=1$.

Proof of Theorem 1.2. Let I be an ideal with the canonical basis $\{a, b+g\delta\}$ and $J=\frac{1}{g}I$. Then for any $\alpha \in J$ and the corresponding $g\alpha \in I$,

$$h(g\alpha) = \left(\prod_{j=1}^{2}\max\{1,|\sigma_i(g\alpha)|\}\right)^{\frac{1}{2}} \leq g\left(\prod_{j=1}^{2}\max\{1,|\sigma_i(\alpha)|\}\right)^{\frac{1}{2}} = gh(\alpha). \qquad (28)$$

Further, $\mathbb{N}_K(I) = g\mathbb{N}_K(J)$. Take $\alpha \in J$ be a primitive element of bounded height as obtained above in Cases 1 and 2, then $g\alpha \in I$ is also a primitive element and the result follows. □

5. Primitive elements with avoidance conditions

The goal of this section is to prove Theorem 1.3. Our main tool is Theorem 1.1, so we will set things up to apply it. First recall that a union of ideals $\bigcup_{i=1}^{s} J_k$ is an ideal if and only if there exists some $1 \leq i \leq s$ such that $J_1, \dots, J_s \subseteq J_i$: if this is not the case, the union would not be closed under addition. Since they are all properly contained in I, we conclude that $I \neq \bigcup_{i=1}^{s} J_i$, and so there exists $\alpha \in I \setminus \bigcup_{i=1}^{s} J_i$. Let us then define lattices

$$\Omega = \Sigma_K(I),\ \Lambda_i = \Sigma_K(J_i)\ \forall\ 1 \leq i \leq s,\ \Lambda = \Sigma_K(J)$$

in the Euclidean space $K_{\mathbb{R}}$. Let

$$P(x_1,\dots,x_d)=\prod_{1\le i<j\le d}(x_i-x_j)\in\mathbb{Z}[x_1,\dots,x_d], \tag{29}$$

and notice that an element $\alpha\in K$ is primitive if and only if $P(\Sigma_K(\alpha))\neq 0$. Indeed, an element $\alpha\in K$ is primitive if and only if all of its algebraic conjugates $\sigma_1(\alpha),\dots,\sigma_d(\alpha)$ are distinct, but these are precisely the coordinates of the vector $\Sigma_K(\alpha)$ in $K_{\mathbb{R}}$. Degree of this polynomial P is $m=\binom{d}{2}$, and so Theorem 1.1 guarantees the existence of a point $\boldsymbol{z}\in\Omega\setminus(\bigcup_{i=1}^s\Lambda_i)$ such that $P(\boldsymbol{z})\neq 0$ and (4) is satisfied. Let $\alpha\in I$ be such that $\boldsymbol{z}=\Sigma_K(\alpha)$. We now want to rewrite the inequality (4) in terms of the invariants of the ideals and the number field K and use it to estimate $h(\alpha)$.

Since D_i and D are indices of Λ_i and Λ, respectively, in Ω, we have

$$D_i=\frac{\det\Lambda_i}{\det\Omega}=\frac{\mathbb{N}_K(J_i)}{\mathbb{N}_K(I)},\ D=\frac{\det\Lambda}{\det\Omega}=\frac{\mathbb{N}_K(J)}{\mathbb{N}_K(I)},$$

by (14), and $\Delta=\det\Omega=\mathbb{N}_K(I)|\Delta_K|^{1/2}$. Now, the "cube"

$$C_d(1)=\{\boldsymbol{x}\in K_{\mathbb{R}}:|\boldsymbol{x}|\le 1\}$$

is the Cartesian product of r_1 intervals $[-1,1]$ and r_2 circles of radius 1. Hence, $C_d(1)$ is a convex $\mathbf{0}$-symmetric set with d-dimensional volume

$$\mathrm{Vol}_d(C_d(1))=2^{r_1}\pi^{r_2}.$$

Finally, notice that

$$\begin{aligned}1 &= \min\left\{\left(\prod_{v|\infty}|\beta|_v\right)^{1/d}:\beta\in\mathcal{O}_K\right\}\\ &\le \min\left\{\max_{1\le j\le d}|\sigma_j(\beta)|:\beta\in J\setminus\{0\}\right\}=\lambda_1(\Lambda)\le\mathbb{N}_K(J),\end{aligned}$$

since $\mathbb{N}_K(J)\in J\cap\mathbb{Z}_{>0}$, and so $|\sigma_j(\mathbb{N}_K(J))|=\mathbb{N}_K(J)$ for every $1\le j\le d$. Putting all of the above observations together with Lemma 3.2, we obtain (7). This completes the proof of Theorem 1.3.

6. Positive points with avoidance conditions

In this section, we let our Euclidean space $\mathbb{E}^d$ to be just $\mathbb{R}^d$. We consider "small" *positive* points in a lattice outside of a union of sublattices, at which a given polynomial does not vanish. A previous result in [11] provided a bound on the smallest norm of a nonzero positive point in a lattice, i.e., a point in the intersection of a lattice with the positive orthant in $\mathbb{R}^d$. Here, we extend this result to include additional avoidance conditions. Specifically, we prove the following theorem.

Theorem 6.1. *Let $\Omega\subseteq\mathbb{R}^d$ be a lattice of full rank and determinant Δ, $\Lambda_1,\dots,\Lambda_s\subseteq\Omega$ its sublattices with indices $[\Omega:\Lambda_i]=D_i$ for each $1\le i\le s$, and $\Lambda=\bigcap_{i=1}^s\Lambda_i$ be a sublattice of Ω of index $D\le D_1\cdots D_s$. Assume that $\Omega\not\subseteq\bigcup_{i=1}^s\Lambda_i$. Let $P(x_1,\dots,x_d)\in\mathbb{R}[x_1,\dots,x_d]$ be a polynomial of degree m. Then there exists a point $\boldsymbol{z}\in\Omega\setminus\bigcup_{i=1}^s\Lambda_i$ so that*

$$P(\boldsymbol{z})\neq 0,\ z_i\ge 0\ \forall\ 1\le i\le d,$$

and

$$|\boldsymbol{z}| < D(m+2)(\mu(\Lambda)+1)\left(\frac{D\Delta}{\lambda_1(\Lambda)^{d-1}}\left(\sum_{i=1}^{s}\frac{1}{D_i} - \frac{s-1}{D} + \frac{\lambda_1(\Lambda)^d}{D\Delta}\right) + \sum_{i=1}^{d}\lambda_i(\Lambda)\right),$$

where $\lambda_i(\Lambda)$ *are the successive minima of* Λ *with respect to the cube* $C_d(1)$ *as defined in* (1) *and*

$$\mu(\Lambda) = \min\left\{T \in \mathbb{R}_{>0} : B_d(T) + \Lambda = \mathbb{R}^d\right\}$$

is the covering radius of Λ *with respect to the unit ball* $B_d(1)$.

Proof. Let us write

$$\Omega^+ = \{\boldsymbol{x} \in \Omega : x_j \geq 0 \ \forall\ 1 \leq j \leq d\},$$

then $\Lambda^+ \subset \Omega^+$. The restricted successive minima of Λ^+, defined as

$$\lambda_i(\Lambda^+) := \min\left\{T \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}}\left(\Lambda^+ \cap C_d(T)\right) \geq i\right\},$$

were studied in [11]. Theorem 1.2 of [11] established that

$$\lambda_1(\Lambda^+) \leq 2\mu(\Lambda)+1,\ \lambda_i(\Lambda^+) \leq 2\lambda_i(\Lambda)(\mu(\Lambda)+1)\ \forall\ 2 \leq i \leq d. \tag{30}$$

By Lemmas 3.1 and 3.2 of [11], there exist linearly independent vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_d \in \Lambda^+$ such that

$$|\boldsymbol{v}_i| \leq \lambda_i(\Lambda^+)\ \forall\ 1 \leq i \leq d, \text{ and } v_{1j} \geq 1\ \forall\ 1 \leq j \leq d.$$

Define the vectors $\boldsymbol{u}_1 = \boldsymbol{v}_1$ and $\boldsymbol{u}_i = \boldsymbol{v}_i + \boldsymbol{v}_1$ for every $2 \leq i \leq d$, then

$$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_d \in \Lambda^+ \text{ and } u_{ij} \geq 1\ \forall\ 1 \leq i,j, \leq d.$$

Further, $|\boldsymbol{u}_1| \leq 2\mu(\Lambda)+1$ and for every $2 \leq i \leq d$,

$$|\boldsymbol{u}_i| \leq |\boldsymbol{v}_i| + |\boldsymbol{v}_1| \leq 2(\lambda_i(\Lambda)+1)(\mu(\Lambda)+1) - 1. \tag{31}$$

Let $\boldsymbol{x} \in \Omega \setminus \bigcup_{i=1}^{s}\Lambda_i$ be as in (2). As in our argument in Section 2, there must exist a subset of $d-1$ vectors among $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_d$ with which $\boldsymbol{x}$ is linearly independent, assume these are $\boldsymbol{u}_2, \ldots, \boldsymbol{u}_d$, since they have larger norm. Notice that the vector

$$\boldsymbol{y} := \boldsymbol{x} + |\boldsymbol{x}|\boldsymbol{u}_1 \in \Omega^+,$$

since its coordinates are of the form

$$y_i = x_i + |\boldsymbol{x}|v_{1i} \geq 0.$$

On the other hand, $\boldsymbol{y} \notin \bigcup_{i=1}^{s}\Lambda_i$, since $\boldsymbol{x}$ is not contained in any Λ_i while $\boldsymbol{u}_1$ is contained in each of them. Additionally,

$$|\boldsymbol{y}| \leq |\boldsymbol{x}|(1+|\boldsymbol{u}_1|) \leq 2|\boldsymbol{x}|(\mu(\Lambda)+1). \tag{32}$$

Let $P(x_1, \ldots, x_d) \in \mathbb{R}[x_1, \ldots, x_d]$ be a polynomial of degree $m \geq 1$. We now argue as in Section 2. Let the sets S_1 and S_2 be as in (13), then (3) implies that there exists a vector

$$\boldsymbol{\xi} = (\xi_1, \xi_2, \ldots, \xi_d) \in S_1 \times S_2 \times \cdots \times S_2$$

so that

$$P\left(\xi_1\boldsymbol{y} + \sum_{i=2}^{d}\xi_i\boldsymbol{u}_i\right) \neq 0.$$

Let $\boldsymbol{z} = \xi_1 \boldsymbol{y} + \sum_{i=2}^{d} \xi_i \boldsymbol{u}_i \in \Omega^+ \setminus \bigcup_{i=1}^{s} \Lambda_i$ for this choice of $\boldsymbol{\xi}$, then by (31) and (32), we have

$$|\boldsymbol{z}| \leq |\boldsymbol{\xi}| \left(|\boldsymbol{y}| + \sum_{i=2}^{d} |\boldsymbol{u}_i| \right) \leq D(m+2)(\mu(\Lambda)+1) \left(|\boldsymbol{x}| + \sum_{i=1}^{d} \lambda_i(\Lambda) \right).$$

Combining this last observation with (2) and taking into account that $\mathrm{Vol}_d(C_d(1)) = 2^d$ finishes the proof of the theorem. □

We can now apply this theorem to the number field situation. Let K be a totally real number field of degree d and discriminant Δ_K with embeddings

$$\sigma_1, \ldots, \sigma_d : K \hookrightarrow \mathbb{R},$$

which define the Minkowski embedding $\Sigma_K = (\sigma_1, \ldots, \sigma_d) : K \hookrightarrow \mathbb{R}^d$. Let $I \subseteq \mathcal{O}_K$ be an ideal and write I^+ for the additive semigroup of totally positive elements in I, i.e.

$$I^+ = \{\alpha \in I : \sigma_i(\alpha) \geq 0 \ \forall \ 1 \leq i \leq d\}.$$

Same as in Section 5, let $J_1, \ldots, J_s$ be distinct ideals properly contained in I and let $J = J_1 \cdots J_s$. Let

$$\Omega = \Sigma_K(I), \ \Lambda_i = \Sigma_i(J_i) \ \forall \ 1 \leq i \leq s, \ \Lambda = \Sigma_K(J)$$

be lattices in $\mathbb{R}^d$. Let

$$P(x_1, \ldots, x_d) = \prod_{1 \leq i < j \leq d} (x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_d],$$

so an element $\alpha \in K$ is primitive if and only if $P(\Sigma_K(\alpha)) \neq 0$. Notice that $\Sigma_K(I^+) = \Sigma_K(I)^+ = \Omega^+$. Now, Lemmas 4.1 and 4.2 of [11] combined guarantee the existence of $\mathbb{Q}$-linearly independent elements $a_1, \ldots, a_d \in J$ such that

$$\sum_{i=1}^{d} \lambda_i(\Lambda) \leq \sum_{i=1}^{d} h(a_i)^d \leq d \prod_{i=1}^{d} h(a_i)^d \leq d \left(\mathbb{N}_K(J) \sqrt{|\Delta_K|} \right)^d. \tag{33}$$

Further, Lemmas 4.2 of [11] asserts that the covering radius of Λ satisfies the inequality

$$\mu(\Lambda) \leq \frac{d^{3/2}}{2} \mathbb{N}_K(J) \sqrt{|\Delta_K|}. \tag{34}$$

Putting these observations together with Theorem 6.1 and expressing indices and determinants as in Section 5, we obtain the following corollary.

Corollary 6.2. *There exists a primitive totally positive element $\alpha \in I \setminus \bigcup_{i=1}^{s} J_i$ so that*

$$\begin{aligned} h(\alpha) \ &\leq \ \left(\binom{d}{2} + 2 \right) \left(\frac{d^{3/2}}{2} \mathbb{N}_K(J) \sqrt{|\Delta_K|} + 1 \right) \frac{\mathbb{N}_K(J)^2 \sqrt{|\Delta_K|}}{\mathbb{N}_K(I)} \times \\ &\times \ \left(\sum_{i=1}^{s} \frac{\mathbb{N}_K(I)}{\mathbb{N}_K(J_i)} - \frac{(s-1)\mathbb{N}_K(I)}{\mathbb{N}_K(J)} + \frac{\mathbb{N}_K(J)^{d-1}}{\sqrt{|\Delta_K|}} + d \left(\mathbb{N}_K(J) \sqrt{|\Delta_K|} \right)^{d-1} \right). \end{aligned}$$

7. Non-sparse polynomials with bounded Mahler measure

Let K be a number field of degree d, then (6) guarantees that there exists a primitive element $\alpha \in \mathcal{O}_K$ with $h(\alpha) \leq |\Delta_K|^{\frac{1}{d}}$. Let

$$f_\alpha(x) = x^d + \sum_{k=0}^{d-1} a_k x^k \in \mathbb{Z}[x]$$

be the minimal polynomial of α. Then $f_\alpha(x)$ is a monic irreducible polynomial with integer coefficients and $K \cong \mathbb{Q}[x]/\langle f_\alpha(x)\rangle$. Let $\sigma_1, \dots, \sigma_d$ be the embeddings of K, as usual, ordered in such a way that $\sigma_1(\alpha) = \alpha$. Then

$$\alpha_k = \sigma_k(\alpha_1), \ \forall \ 1 \leq k \leq d$$

are all the roots of $f_\alpha(x)$ with $\alpha_1 = \alpha$. Since $f_\alpha(x)$ is monic, all of these roots are algebraic integers. The Mahler measure of $f_\alpha(x)$ is given by

$$\mathcal{M}(f_\alpha) = \prod_{k=1}^{d} \max\{1, |\alpha_k|\} = h(\alpha)^d \leq |\Delta_K|.$$

Hence, the result of Pazuki and Widmer [19, Lemma 7.1] (see equation (5) above) can be reformulated to say that there exists a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ such that $K \cong \mathbb{Q}[x]/\langle f(x)\rangle$ and $\mathcal{M}(f) \leq |\Delta_K|$. We can use our Diophantine avoidance method to obtain a similar result with additional non-vanishing conditions.

Theorem 7.1. *Given a number field K of degree d, there exists a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ with all nonzero coefficients such that $K \cong \mathbb{Q}[x]/\langle f(x)\rangle$ and*

$$\mathcal{M}(f) \leq \left\{ \left(\frac{4}{\pi}\right)^{r_2} \left(\frac{d(d^2-d+2)}{2}\right) |\Delta_K|^{1/2} \right\}^d.$$

Proof. Our argument here is similar to the proof of Theorem 1.3. Let the lattice $\Omega = \Sigma_K(\mathcal{O}_K)$ in $\mathbb{E}^d = K_{\mathbb{R}}$ be the image of $\mathcal{O}_K$ under the Minkowski embedding. For $1 \leq k \leq d$, let $e_k(x_1, \dots, x_d)$ be the elementary symmetric polynomial of degree k. Let $\alpha \in \mathcal{O}_K$ and $\boldsymbol{\alpha} := \Sigma_K(\alpha) = (\alpha_1, \dots, \alpha_d) \in \Omega$. Then α is a primitive element in K if and only if its minimal polynomial is of the form

$$f_\alpha(x) = x^d + \sum_{k=1}^{d} e_k(\alpha_1, \dots, \alpha_d) x^{d-k},$$

which is equivalent to the condition that $K \cong \mathbb{Q}[x]/\langle f_\alpha(x)\rangle$. Let

$$Q(x_1, \dots, x_d) = P(x_1, \dots, x_d) \prod_{k=1}^{d-1} e_k(x_1, \dots, x_d),$$

where $P(x_1, \dots, x_d)$ is as in (29), then

$$\deg Q = \deg P + \sum_{k=1}^{d-1} k = d(d-1).$$

Notice then that α is primitive and $f_\alpha(x)$ has all nonzero coefficients if and only if $Q(\boldsymbol{\alpha}) \neq 0$. Hence, we want to find $\boldsymbol{\alpha} \in \Omega$ such that $Q(\boldsymbol{\alpha}) \neq 0$ and $|\boldsymbol{\alpha}|$ bounded. Let

$$\boldsymbol{v}_1, \dots, \boldsymbol{v}_d \in \Omega$$

be vectors corresponding to the successive minima of Ω with respect to the cube $C_d(1) \subset K_{\mathbb{R}}$. Then $\mathrm{Vol}_d(C_d(1)) = 2^{r_1}\pi^{r_2}$ and $\det \Omega = |\Delta_K|^{1/2}$, and so Minkowski's successive minima theorem implies that

$$\lambda_d(\Omega) \leq \frac{2^d |\Delta_K|^{1/2}}{\lambda_1(\Lambda)^{d-1} \mathrm{Vol}_d(C_d(1))} \leq \left(\frac{4}{\pi}\right)^{r_2} |\Delta_K|^{1/2}, \tag{35}$$

since

$$\lambda_1(\Omega) = \min\left\{ \max_{1\leq k\leq d} |\sigma_k(\alpha)| : \alpha \in \mathcal{O}_K \right\} = 1.$$

Let $S = \left\{ -\left[\frac{d(d-1)}{2}\right] - 1, \ldots, \left[\frac{d(d-1)}{2}\right] + 1 \right\}$, and for each vector $\boldsymbol{\xi} \in S^d$ define

$$\boldsymbol{\alpha}(\boldsymbol{\xi}) = \sum_{k=1}^{d} \xi_k \boldsymbol{v}_k.$$

Then Theorem 4.2 of [10] implies that there exists $\boldsymbol{\xi} \in S^d$ such that

$$P(\boldsymbol{\alpha}(\boldsymbol{\xi})) \neq 0.$$

Let $\alpha \in \mathcal{O}_K$ be such that $\boldsymbol{\alpha}(\boldsymbol{\xi}) = \Sigma_K(\alpha)$ for this choice of $\boldsymbol{\xi}$. Then Lemma 3.2 together with (35) implies that

$$h(\alpha) \leq |\boldsymbol{\alpha}(\boldsymbol{\xi})| \leq d\left(\frac{d(d-1)}{2} + 1\right)\lambda_d(\Omega) \leq \left(\frac{4}{\pi}\right)^{r_2}\left(\frac{d(d^2-d+2)}{2}\right)|\Delta_K|^{1/2}.$$

If $f(x)$ is the minimal polynomial of this α, then $\mathcal{M}(f) \leq h(\alpha)^d$, and the result follows. □

It is interesting to remark that some previous literature featured lower bounds on the Mahler measure of *fewnomials*, i.e., polynomials with few nonzero coefficients; see, for instance, [6] and references within, such as a classical paper of Mahler [18]. Our Theorem 7.1 goes in the opposite direction, providing an upper bound on the Mahler measure of polynomials with all nonzero coefficients generating a given number field. For comparison, inequality (7) of [18] gives an upper bound on $\mathcal{M}(f)$, however it is in terms of height (maximum of absolute values of coefficients) of the polynomial f, whereas we prove the existence of a non-sparse generating polynomial f for K with Mahler measure bounded in terms of the invariants of K.

8. Small-height ideal generators

In this section, we prove Theorem 1.4. As in Section 4, we consider a quadratic number field $K = \mathbb{Q}(\sqrt{D})$ for squarefree integer D, and let $I \subseteq \mathcal{O}_K$ be an ideal with the canonical basis $a, b + g\delta$. Suppose $I = \langle \mu \rangle$ is a principal ideal, then $\mathbb{N}_K(\mu) = \mathbb{N}_K(I)$. Also recall that we are defining the quantity $H(I)$, the "height" of the ideal I as in (10).

Case 1. Assume $D \not\equiv 1 \pmod 4$, then $\mathbb{N}_K(\mu) = \mathbb{N}_K(I) = ag$. On the other hand,

$$\mu = ax + (b - g\sqrt{D})y = (ax + by) - yg\sqrt{D},$$

for some integers x, y such that $y \neq 0$, and thus

$$ag = \mathbb{N}_K(\mu) = (ax + by)^2 - Dgy^2 = a^2x^2 + 2abxy + (b^2 - Dg)y^2.$$

This implies that the quadratic equation with integer coefficients

$$f_I(x,y) := \frac{a}{g}x^2 + \frac{2b}{g}xy + \left(\frac{b^2 - Dg}{ag}\right)y^2 = 1 \tag{36}$$

has a solution in integers x, y. Define

$$|f_I| := \max\left\{1, \frac{|a|}{g}, \frac{|2b|}{g}, \frac{|b^2 - D|}{ag}\right\} = H(I)$$

to be the maximum of absolute values of the coefficients of f_I. Then a theorem of Kornhauser [17, Theorem 1] guarantees that (36) has an integer solution (x, y) with

$$\max\{|x|, |y|\} \leq (14|f_I|)^{5|f_I|}. \tag{37}$$

Now, using inequalities analogous to (22) and applying (37) yields the inequality

$$h(\mu) \leq |x|a + |y|b + |y|g\sqrt{|D|} \leq \left(a + b + g\sqrt{|D|}\right)(14|f_I|)^{5|f_I|}. \tag{38}$$

Case 2. Assume $D \equiv 1 \pmod 4$, then $\mathbb{N}_K(\mu) = \mathbb{N}_K(I) = \frac{ag}{2}$. On the other hand,

$$\mu = ax + \left(b + g\left(\frac{1-\sqrt{D}}{2}\right)\right)y = \left(ax + by + \frac{gy}{2}\right) - y\left(\frac{g\sqrt{D}}{2}\right)$$

for some integers x, y such that $y \neq 0$, and thus

$$\begin{aligned} \frac{ag}{2} &= \mathbb{N}_K(\mu) = \left(ax + by + \frac{yg}{2}\right)^2 - \frac{gD}{4}y^2 \\ &= a^2x^2 + a(2b+g)xy + \left(b^2 + bg - \frac{D-1}{4}g\right)y^2. \end{aligned}$$

This implies that the quadratic equation with integer coefficients

$$f_I(x,y) := \frac{2a}{g}x^2 + \frac{2(2b+g)}{g}xy + \left(\frac{4b^2 + 4b - Dg + g}{2ag}\right)y^2 = 1 \tag{39}$$

has a solution in integers x, y. Define

$$|f_I| := \max\left\{1, \frac{|2a|}{g}, \frac{2|2b+g|}{g}, \frac{|4b^2 + 4b - Dg + g|}{2ag}\right\} = H(I)$$

to be the maximum of absolute values of the coefficients of f_I. Now, using inequalities analogous to (26) and applying (37) yields the inequality

$$h(\mu) \leq |x|a + \frac{|y|(2b+g)}{2} + \frac{|y|g\sqrt{|D|}}{2} \leq \left(a + \frac{2b + g + g\sqrt{|D|}}{2}\right)(14|f_I|)^{5|f_I|}. \tag{40}$$

The theorem now follows upon combining (38) and (40). Notice that the element μ we produced here is primitive since $y \neq 0$ in both cases.

Acknowledgement: We wish to thank the anonymous referee for a thorough reading and multiple suggestions that improved the quality of this paper.

References

[1] S. Akhtari and J. D. Vaaler. On the height of solutions to norm form equations. *Acta Arith.*, 183 (2018), no. 4, pp.385–396.

[2] S. Akhtari and J. D. Vaaler. Independent relative units of low height. *Acta Arith.*, 202 (2022), no. 4, pp.389–401.

[3] N. Alon. Combinatorial Nullstellensatz. *Combin. Probab. Comput.*, 8 (1999), no. 1-2, pp. 7–29.

[4] E. Bayer Fluckiger. Upper bounds for Euclidean minima of algebraic number fields. *J. Number Theory*, 121 (2006), no. 2, pp. 305–323.

[5] D. A. Buell. Binary Quadratic Forms. Springer-Verlag, 1989.

[6] E. Dobrowolski and C. Smyth. Mahler measures of polynomials that are sums of a bounded number of monomials. *Int. J. Number Theory*, 121 (2017), no. 6, pp. 1603–1610.

[7] G. Faltings. Diophantine approximation on abelian varieties. *Ann. of Math.*, 133 (1991), no. 3, pp. 549–576.

[8] L. Fukshansky. Integral points of small height outside of a hypersurface. *Monatsh. Math.*, 147 (2006), no. 1, pp. 25–41.

[9] L. Fukshansky. Siegel's lemma with additional conditions. *J. Number Theory*, 120 (2006), no. 1, pp. 13–25.

[10] L. Fukshansky. Algebraic points of small height missing a union of varieties. *J. Number Theory*, 130 (2010), no. 10, pp. 2099–2118.

[11] L. Fukshansky and S. Wang. Positive semigroups in lattices and totally real number fields. *Adv. Geom.*, 22 (2022), no. 4, pp. 503–512.

[12] E. Gaudron. Géométrie des nombres adélique et lemmes de Siegel généralisés. *Manuscripta Math.*, 130 (2009), no. 2, pp. 159–182.

[13] E. Gaudron and G. Rémond. Lemmes de Siegel d'évitement. *Acta Arith.*, 154 (2012), no. 2, pp. 125–136.

[14] P. M. Gruber and C. G. Lekkerkerker. Geometry of Numbers. North-Holland Publishing Co., 1987.

[15] M. Henk and C. Thiel. Restricted successive minima. *Pacific J. Math.*, 269 (2014), no. 2, pp. 341–354.

[16] R. J. Kooman. Faltings's version of Siegel's lemma. *Lecture Notes in Math.*, 1566 (1993), Diophantine approximation and abelian varieties (Soesterberg, 1992), Springer, Berlin, pp. 93–96.

[17] D. M. Kornhauser. On the smallest solution to the general binary quadratic diophantine equation. *Acta Arith.*, 55 (1990), no. 1, pp. 83–94.

[18] K. Mahler. On some inequalities for polynomials in several variables. *J. London Math. Soc.*, 37 (1962), pp. 341–344.

[19] F. Pazuki and M. Widmer. Bertini and Northcott. *Res. Number Theory*, 7 (2021), Paper no. 12, 18 pp.

[20] W. M. Ruppert. Small generators of number fields. *Manuscripta Math.*, 96 (1998), no. 1, pp. 17–22.

[21] W. M. Schmidt. Diophantine approximations and Diophantine equations. Lecture Notes in Mathematics, 1467. Springer-Verlag, Berlin, 1991.

[22] I. Stewart and D. Tall. Algebraic number theory and Fermat's last theorem. Fourth edition. CRC Press, Boca Raton, FL, 2016.

[23] J. D. Vaaler and M. Widmer. A note on generators of number fields. Diophantine methods, lattices, and arithmetic theory of quadratic forms, *Contemp. Math.*, 587 (2013), Amer. Math. Soc., Providence, RI, pp. 201–211.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711

Email address: lenny@cmc.edu

Institute of Mathematical Sciences, Claremont Graduate University, Claremont, CA 91711

Email address: sehun.jeong@cgu.edu