

POSITIVE SEMIGROUPS IN LATTICES AND TOTALLY REAL NUMBER FIELDS

LENNY FUKSHANSKY AND SIKI WANG

ABSTRACT. Let L be a full-rank lattice in \mathbb{R}^d and write L^+ for the semigroup of all vectors with nonnegative coordinates in L . We call a basis X for L positive if it is contained in L^+ . There are infinitely many such bases, and each of them spans a conical semigroup $S(X)$ consisting of all nonnegative integer linear combinations of the vectors of X . Such $S(X)$ is a sub-semigroup of L^+ , and we investigate the distribution of the gaps of $S(X)$ in L^+ , i.e. the points in $L^+ \setminus S(X)$. We describe some basic properties and counting estimates for these gaps. Our main focus is on the restrictive successive minima of L^+ and of $L^+ \setminus S(X)$, for which we produce bounds in the spirit of Minkowski's successive minima theorem and its recent generalizations. We apply these results to obtain analogous bounds for the successive minima with respect to Weil height of totally positive sub-semigroups of ideals in totally real number fields.

1. INTRODUCTION

Let $d \geq 2$ and $L \subset \mathbb{R}^d$ be a lattice of full rank, and let us write

$$\mathbb{R}_{\geq 0}^d = \{\mathbf{x} \in \mathbb{R}^d : x_i \geq 0 \forall 1 \leq i \leq d\}$$

for the positive orthant of the Euclidean space \mathbb{R}^d and $\mathbb{R}_{> 0}^d$ for its interior. Define

$$L^+ = L \cap \mathbb{R}_{\geq 0}^d,$$

then L^+ is an additive monoid in L . If $X = \{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ is a basis for L contained in L^+ , which we refer to as a *positive basis* for L , we can write

$$(1) \quad \mathcal{X} = (\mathbf{x}_1 \ \dots \ \mathbf{x}_d)$$

for the corresponding $d \times d$ positive basis matrix, so $L = \mathcal{X}\mathbb{Z}^d$. A choice of such X is always possible, since every lattice contains infinitely many positive bases (Lemma 2.1). Define a submonoid of L^+

$$S(X) = \left\{ \sum_{i=1}^n a_i \mathbf{x}_i : a_1, \dots, a_n \in \mathbb{Z}_{\geq 0} \right\} = \mathcal{X}\mathbb{Z}_{\geq 0}^d,$$

as well as the positive cone spanned by X

$$\mathcal{C}(X) = \left\{ \sum_{i=1}^n a_i \mathbf{x}_i : a_1, \dots, a_n \in \mathbb{R}_{\geq 0} \right\} = \mathcal{X}\mathbb{R}_{\geq 0}^d.$$

2010 *Mathematics Subject Classification.* 11H06, 52C07, 11G50, 11R80.

Key words and phrases. lattices, successive minima, affine semigroups, totally real number fields, heights.

Fukshansky was partially supported by the Simons Foundation grant #519058.

Define the set of *gaps* of $S(X)$ in L^+ to be $G(X) = L^+ \setminus S(X)$. We provide a basic characterization of gaps in Section 2, in particular showing that $S(X) = L \cap \mathcal{C}(X)$, meaning that no gaps can be contained in the positive cone $\mathcal{C}(X)$. Hence $G(X)$ can be described as $L^+ \setminus \mathcal{C}(X)$, which is an infinite set unless the basis X is orthogonal: in the orthogonal case, $L^+ = S(X)$. Furthermore, if X is not orthogonal, then L^+ is not contained in any set of the form

$$\left\{ \sum_{i=1}^d a_i \mathbf{x}_i : a_1, \dots, a_d \in \mathcal{Z} \right\},$$

where $\mathcal{Z} \subset \mathbb{Z}$ is a proper subset (Lemma 2.5). In other words, the gaps cannot all be “filled” by partially expanding the set of coefficients to include some (but not all) negative integers. These observations motivate further investigation of the distribution of the gaps. First, we can obtain an asymptotic estimate for the number of gaps of bounded norm of the positive semigroup $S(X)$ in L^+ as the bound tends to infinity. For a positive real number t and a set $S \subseteq \mathbb{R}^d$, define the counting function

$$\mathcal{N}(S, t) = |\{\mathbf{y} \in S : \|\mathbf{y}\| \leq t\}|,$$

where $\|\cdot\|$ stands for the usual Euclidean norm on \mathbb{R}^d .

Proposition 1.1. *Let $L \subset \mathbb{R}^d$ be a lattice of full rank and X a positive basis for L . Let $\nu(X)$ stand for the measure of the solid angle of the cone $\mathcal{C}(X)$ and write ω_d for the volume of a unit ball in \mathbb{R}^d . As $t \rightarrow \infty$,*

$$(2) \quad \mathcal{N}(G(X), t) = \left(\frac{\omega_d(1 - \nu(X)2^d)}{2^d \det L} \right) t^d + O(t^{d-1}).$$

The measure $\nu(X)$ of the solid angle of the cone $\mathcal{C}(X)$ present in the bound of (2) above is defined as the proportion of the volume of the unit ball centered at the origin which is cut-out by this cone, i.e.

$$\nu(X) = \frac{\text{Vol}_d(\mathcal{C}(X) \cap B_d(1))}{\omega_d},$$

where

$$B_d(t) = \{\mathbf{x} \in \mathbb{R}^d : \|\mathbf{x}\| \leq t\}$$

is a ball of radius $t > 0$ centered at the origin in \mathbb{R}^d . Since $\mathcal{C}(X) \subseteq \mathbb{R}_{\geq 0}^d$, the solid angle $\nu(X)$ is no bigger than $1/2^d$, meaning that the constant in the main term of (2) is nonnegative, and in fact positive whenever the basis X is not orthogonal. While there are known computational formulas for solid angles of cones (see, for instance, Theorem 2.2 of [8]) they are complicated and technical, which is why we choose not to include them here. We prove Proposition 1.1 at the end of Section 2.

Our main results on lattices target the so-called restricted successive minima with respect to our semigroup $S(X)$, naturally complementing previous work on points of a lattice outside of a finite union of sublattices and hypersurfaces [3], [6]. We write $|\cdot|$ for the sup-norm on \mathbb{R}^d , and for a real number $t > 0$, let

$$C_d(t) = \{\mathbf{x} \in \mathbb{R}^d : |\mathbf{x}| \leq t\}$$

be a cube of radius t centered at the origin in \mathbb{R}^d . Let

$$\mu(L) = \min \{t \in \mathbb{R}_{>0} : B_d(t) + L = \mathbb{R}^d\}$$

be the inhomogeneous minimum (also called the covering radius) of L . We will define three different sets of successive minima with respect to the cube $C_d(1)$. First, we write $0 < \lambda_1 \leq \dots \leq \lambda_d$ for the usual successive minima of L with respect to $C_d(1)$, i.e.

$$\lambda_i = \min \{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \text{span}_{\mathbb{R}}(L \cap C_d(t)) \geq i\}.$$

We also define the successive minima of L^+ with respect to $C_d(1)$ to be

$$\lambda_i(L^+) := \min \{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \text{span}_{\mathbb{R}}(L^+ \cap C_d(t)) \geq i\}.$$

Finally, for a positive basis X of L we define the restricted successive minima of $L^+ \setminus S(X)$ with respect to $C_d(1)$ in the spirit of Henk and Thiel's definition in [6]: for each $1 \leq i \leq d$, let

$$\lambda_i(L^+, X) := \min \{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \text{span}_{\mathbb{R}}(G(X) \cap C_d(t)) \geq i\}.$$

In other words, $\lambda_i(L^+)$ (respectively, $\lambda_i(L^+, X)$) is the minimal t such that there exist i linearly independent vectors in L^+ (respectively, gaps of $S(X)$ in L^+) with sup-norm no bigger than t , so

$$0 < \lambda_1(L^+) \leq \dots \leq \lambda_d(L^+), \quad 0 < \lambda_1(L^+, X) \leq \dots \leq \lambda_d(L^+, X).$$

We obtain the following bounds on these successive minima.

Theorem 1.2. *Let $L \subset \mathbb{R}^d$ be a lattice of full rank. Then*

$$(3) \quad \lambda_1(L^+) \leq 2\mu(L) + 1, \quad \lambda_i(L^+) \leq 2\lambda_i(\mu(L) + 1) \quad \forall 2 \leq i \leq d.$$

On the other hand, for each non-orthogonal positive basis $X = \{\mathbf{x}_1, \dots, \mathbf{x}_d\}$ of L so that no $d - 1$ elements of X lie in a coordinate hyperplane, we have

$$\lambda_d(L^+, X) \leq \max_{1 \leq i \leq d} \max_{1 \leq m \leq d} \left\{ \left(\max_{1 \leq k \leq d} \left[\frac{x_{ik}}{\sum_{j=1, j \neq i}^d x_{jk}} \right] + 1 \right) \sum_{j=1, j \neq i}^d x_{jm} - x_{im} \right\},$$

where $[\]$ stands for the integer part function.

Notice that this result can be viewed as a version of Minkowski's Successive Minima Theorem with restrictions; in particular, explicit bounds for the successive minima $\lambda_i(L^+)$ can be deduced from (3) with the help of Minkowski's theorem (see, for instance [5], Section 9.1, Theorem 1) and Jarnik's inequality on inhomogeneous minimum (see, for instance [5], Section 13.2, Theorem 1). Indeed, it is known that

$$(4) \quad \prod_{i=1}^d \lambda_i \leq \det L, \quad \mu(L) \leq \frac{\sqrt{d}}{2} \sum_{i=1}^d \lambda_i.$$

The dimensional constant \sqrt{d} appears in our upper bound on $\mu(L)$ here because we are comparing the inhomogeneous minimum with respect to the Euclidean ball $B_d(1)$ to the successive minima with respect to the cube $C_d(1)$. We prove Theorem 1.2 in Section 3.

In fact, one can generalize the discussion above by considering, instead of L^+ , the intersection of L with a general convex cone spanned by a basis in \mathbb{R}^d , not just with $\mathbb{R}_{\geq 0}^d$. Such generalizations are not difficult to obtain from our results. Say, $Y = \{\mathbf{y}_1, \dots, \mathbf{y}_d\}$ is a collection of linear independent vectors in \mathbb{R}^d , and $L(Y) = L \cap \mathcal{C}(Y)$. If we write \mathcal{Y} for the $d \times d$ matrix $(\mathbf{y}_1 \dots \mathbf{y}_d)$ and let $M = \mathcal{Y}^{-1}L$, then $L(Y) = \mathcal{Y}M^+$. Thus analogues of the above observations, including Proposition 1.1 and Theorem 1.2 can be obtained for M^+ and then "transferred"

to $L(Y)$ by applying the linear transformation \mathcal{Y} ; we present these generalizations in Corollary 2.8 and Corollary 3.4, respectively. We chose to focus specifically on the positive cone $\mathbb{R}_{\geq 0}^d$, and hence on the positive semigroups L^+ because of the natural connection to totally real algebraic number fields, which we discuss next.

Let K be a totally real number field of degree d over \mathbb{Q} , and $\sigma_1, \dots, \sigma_d : K \rightarrow \mathbb{R}$ be the embeddings of K . We write \mathbb{N}_K for the field norm on K and Δ_K for the discriminant of K . Let \mathcal{O}_K be the ring of integers of K , then \mathcal{O}_K , as well as any ideal in \mathcal{O}_K , can be viewed as a Euclidean lattice of rank d with respect to the symmetric bilinear form

$$(5) \quad \langle \alpha, \beta \rangle = \text{Tr}_K(\alpha\beta) = \sum_{i=1}^d \sigma_i(\alpha)\sigma_i(\beta),$$

where Tr_K is the usual trace on K . For an ideal $I \subset \mathcal{O}_K$, let I^+ be the additive semigroup of totally positive elements in I , i.e.

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

and let us also write $\mathbb{Z}^+ = \mathbb{Z} \cap \mathcal{O}_K^+$. Then I has a \mathbb{Z} -basis contained in I^+ . Let $\beta = \{\beta_1, \dots, \beta_d\} \subset I^+$ be such a \mathbb{Z} -basis for I , which we call a positive basis. Let

$$S(\beta) = \left\{ \sum_{i=1}^d c_i \beta_i : c_1, \dots, c_d \in \mathbb{Z}^+ \right\} \subseteq I^+$$

be the corresponding sub-semigroup, and define the set of gaps of $S(\beta)$ in I^+ to be $G(\beta) = I^+ \setminus S(\beta)$. The basis β cannot be orthogonal, as we explain in Section 4, where we discuss this setup in further details. Hence the set $G(\beta)$ is infinite. With this notation, we can state a version of Theorem 1.2 for ideals, where we use Weil height h on K to measure size of points; we recall the definition and standard properties of h in Section 4.

Theorem 1.3. *Let $I \subseteq \mathcal{O}_K$ be an ideal. Then there exist \mathbb{Q} -linearly independent elements $s_1, \dots, s_d \in I$ such that*

$$\prod_{i=1}^d h(s_i) \leq \mathbb{N}_K(I) \sqrt{|\Delta_K|}.$$

Further, there exist \mathbb{Q} -linearly independent elements $\alpha_1, \dots, \alpha_d \in I^+$ such that

$$\prod_{i=1}^d h(\alpha_i) \leq (3d\sqrt{d})^d \left(\mathbb{N}_K(I) \sqrt{|\Delta_K|} \right)^{d+1}.$$

Additionally, let $\beta = \{\beta_1, \dots, \beta_d\} \subset I^+$ be a positive basis for I and $G(\beta)$ the corresponding set of gaps. For each $1 \leq i \leq d$, let $\beta'_i = \sum_{j=1, j \neq i}^d \beta_j$. Then there exist \mathbb{Q} -linearly independent gaps $\alpha_1, \dots, \alpha_d \in G(\beta)$ such that

$$h(\alpha_i) \leq (h(\beta_i/\beta'_i)^d + 1) h(\beta'_i)^d,$$

for each $1 \leq i \leq d$.

We prove this theorem in Section 4 by embedding our ideal into Euclidean space, applying Theorem 1.2, and then “lifting” the results back up to the number field. We are now ready to proceed.

2. POSITIVE SEMIGROUPS IN LATTICES

In this section, we develop the necessary basic observations for positive semigroups in general Euclidean lattices in a series of lemmas.

Lemma 2.1. *There exists a basis $\mathbf{x}_1, \dots, \mathbf{x}_d$ for L contained in $\mathbb{R}_{>0}^d$. Therefore there exist infinitely many such bases.*

Proof. Let $\mathbf{y}_1, \dots, \mathbf{y}_d \in L$ be a basis for L , and write $Y = (\mathbf{y}_1 \dots \mathbf{y}_d)$ for the corresponding $d \times d$ basis matrix, so $L = Y\mathbb{Z}^d$. Let \mathbf{x}_1 be any point in $L \cap \mathbb{R}_{>0}^d$. Then

$$\mathbf{x}_1 = \sum_{i=1}^d a_i \mathbf{y}_i$$

for some integer coefficients a_1, \dots, a_d . In fact, we can assume that $\gcd(a_1, \dots, a_d) = 1$: if not, divide these coefficients by their gcd and replace \mathbf{x}_1 with the resulting vector, which is still in $L \cap \mathbb{R}_{>0}^d$. Let $\mathbf{a} = (a_1 \dots a_d)$ be the row vector of these relatively prime coefficients, then \mathbf{a} is extendable to a matrix $A \in \text{GL}_n(\mathbb{Z})$ (Lemma 2, p. 15, [2]). Then YA is another basis matrix for L , the first column vector of which is \mathbf{x}_1 , hence \mathbf{x}_1 is extendable to a basis $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_d$ for L . Since all coordinates of \mathbf{x}_1 are positive, we can now replace each \mathbf{x}_i , $2 \leq i \leq d$ with $\mathbf{x}_i + M_i \mathbf{x}_1$ for an appropriately large integer M_i to ensure that $\mathbf{x}_i + M_i \mathbf{x}_1$ also has all positive coordinates. The resulting collection

$$\mathbf{x}_1, \mathbf{x}_2 + M_2 \mathbf{x}_1, \dots, \mathbf{x}_d + M_d \mathbf{x}_1$$

is again a basis for L , contained in $\mathbb{R}_{>0}^d$. Once we have one such basis, we can obtain infinitely many simply by adding positive integer multiples of one of the vectors to the others. Further, there are infinitely many choices for the vector \mathbf{x}_1 , which is the starting point of our construction. \square

Remark 2.1. Since every matrix in $\text{GL}_d(\mathbb{R})$ is a basis matrix for some lattice, and change of basis is performed by right multiplication by a matrix from $\text{GL}_d(\mathbb{Z})$, we can rephrase Lemma 2.1 as follows: every orbit of $\text{GL}_d(\mathbb{R})$ under the action of $\text{GL}_d(\mathbb{Z})$ by right multiplication contains a matrix with all positive entries.

Lemma 2.2. *Let $X = \{\mathbf{x}_1, \dots, \mathbf{x}_d\}$ be a positive basis for L , then $L^+ \cap \mathcal{C}(X) = S(X)$.*

Proof. Clearly $S(X) \subseteq L^+ \cap \mathcal{C}(X)$, so we only need to prove that $L^+ \cap \mathcal{C}(X) \subseteq S(X)$. Suppose not, then there exists some $\mathbf{y} \in L^+ \cap \mathcal{C}(X)$ which is not in $S(X)$. Since $\mathbf{y} \in L^+ \setminus S(X)$, we must have

$$\mathbf{y} = \sum_{i=1}^d a_i \mathbf{x}_i,$$

where the coefficients $a_1, \dots, a_d \in \mathbb{Z}$ are not all nonnegative. On the other hand, since $\mathbf{y} \in \mathcal{C}(X)$, we must have

$$\mathbf{y} = \sum_{i=1}^d c_i \mathbf{x}_i$$

for some nonnegative real coefficients c_1, \dots, c_d . Thus $\sum_{i=1}^d a_i \mathbf{x}_i = \sum_{i=1}^d c_i \mathbf{x}_i$, meaning that

$$\sum_{i=1}^d (a_i - c_i) \mathbf{x}_i = \mathbf{0},$$

where not all of the coefficients $a_i - c_i$ can be equal to 0. This contradicts the fact that the vectors $\mathbf{x}_1, \dots, \mathbf{x}_d$ are linearly independent in \mathbb{R}^d . Hence we have $L^+ \cap \mathcal{C}(X) = S(X)$. \square

Therefore Lemma 2.2 implies that all the gaps of $S(X)$ in L^+ are outside of the cone $\mathcal{C}(X)$. On the other hand, there are infinitely many such gaps. Define the set of *primitive gaps* to be

$$G_{\text{pr}}(X) = \{\mathbf{y} \in G(X) : \mathbf{y} \neq m\mathbf{y}' \text{ for any } \mathbf{y}' \in L \text{ and integer } m > 1\},$$

i.e. $G_{\text{pr}}(X)$ is the set of gaps that are primitive points of the lattice L .

Lemma 2.3. *The set $G_{\text{pr}}(X)$ is infinite, unless the positive basis X is orthogonal.*

Proof. Suppose X is not an orthogonal basis, then $\mathcal{C}(X)$ is an acute cone, and so the set $\mathbb{R}_{\geq 0}^d \setminus \mathcal{C}(X)$ is unbounded. Thus its interior contains Euclidean balls of arbitrarily large radius, hence the union of all such balls must contain infinitely many primitive points of the lattice L . \square

In fact, all gaps are multiples of primitive gaps.

Lemma 2.4. *For any $\mathbf{y} \in G(X)$ and $m \in \mathbb{Z}^+$, $m\mathbf{y} \in G(X)$. Further, for any $\mathbf{y} \in G(X)$ there exists $\mathbf{z} \in G_{\text{pr}}(X)$ and $m \in \mathbb{Z}^+$ such that $\mathbf{y} = m\mathbf{z}$, i.e.*

$$G(X) = \{m\mathbf{z} : \mathbf{z} \in G_{\text{pr}}(X), m \in \mathbb{Z}^+\}.$$

Proof. Suppose that \mathbf{y} and \mathbf{z} are two vectors in L^+ such that $\mathbf{y} = m\mathbf{z}$ for some $m \in \mathbb{Z}^+$. We just need to show that either both \mathbf{y}, \mathbf{z} are in $S(X)$, or they are both not. Indeed, suppose one of them, say, \mathbf{y} is in $S(X)$ and \mathbf{z} is not. Then

$$\mathbf{y} = \sum_{i=1}^d a_i \mathbf{x}_i, \quad \mathbf{z} = \sum_{i=1}^d c_i \mathbf{x}_i,$$

where the coefficients $a_1, \dots, a_d \in \mathbb{Z}^+$ and some of the coefficients $c_1, \dots, c_d \in \mathbb{Z}$ are negative. Therefore

$$m \sum_{i=1}^d c_i \mathbf{x}_i = \sum_{i=1}^d a_i \mathbf{x}_i,$$

i.e. $\sum_{i=1}^d (mc_i - a_i) \mathbf{x}_i = \mathbf{0}$ with not all of the coefficients $mc_i - a_i = 0$. This contradicts linear independence of $\mathbf{x}_1, \dots, \mathbf{x}_d$, and thus completes the proof. \square

Remark 2.2. Notice that the above lemma is in fact equivalent to the observation that a ray emanating from the origin either does not intersect the cone $\mathcal{C}(X)$ or is contained in it.

Lemma 2.5. *Suppose that $X = \{\mathbf{x}_1, \dots, \mathbf{x}_d\}$ is a positive non-orthogonal basis for L . Then L^+ is not contained in any set of the form*

$$S(X, \mathcal{Z}) := \left\{ \sum_{i=1}^d a_i \mathbf{x}_i : a_1, \dots, a_d \in \mathcal{Z} \right\},$$

where $\mathcal{Z} \subset \mathbb{Z}$ is a proper subset.

Proof. Suppose that there exists some proper subset $\mathcal{Z} \subset \mathbb{Z}$ such that $L^+ \subseteq S(X, \mathcal{Z})$, and let $b \in \mathbb{Z} \setminus \mathcal{Z}$. If $b \geq 0$, then by uniqueness of representation of vectors in L with respect to X , the vector $b\mathbf{x}_1 \in L^+ \setminus S(X, \mathcal{Z})$. Hence we can assume that $b < 0$.

For a vector $\mathbf{x} \in \mathbb{R}^d$, let us define its support as

$$\text{supp}(\mathbf{x}) := \{1 \leq i \leq d : x_i \neq 0\}.$$

Since X is a basis for \mathbb{R}^d ,

$$\bigcup_{i=1}^d \text{supp}(\mathbf{x}_i) = \{1, \dots, d\}.$$

Assume that for every $1 \leq j \leq d$,

$$\text{supp}(\mathbf{x}_j) \not\subseteq \bigcup_{i=1, i \neq j}^d \text{supp}(\mathbf{x}_i),$$

then for each $1 \leq j \leq d$ there exists some $1 \leq k \leq d$ such that $x_{jk} \neq 0$ while $x_{ik} = 0$ for every $i \neq j$. Since there are d vectors and d coordinates, this is only possible if every vector has a unique nonzero coordinate, which implies that the vectors $\mathbf{x}_1, \dots, \mathbf{x}_d$ are simply multiples of the standard basis vectors. This, however, contradicts the assumption that X is not an orthogonal basis.

Therefore there exists some vector in X , say \mathbf{x}_1 , such that

$$\text{supp}(\mathbf{x}_1) \subseteq \bigcup_{i=2}^d \text{supp}(\mathbf{x}_i).$$

Since all the nonzero coordinates of $b\mathbf{x}_1$ are negative and all the nonzero coordinates of \mathbf{x}_i 's are positive, we can always pick positive integers a_2, \dots, a_d large enough so that

$$\mathbf{z} := b\mathbf{x}_1 + \sum_{i=2}^d a_i \mathbf{x}_i \in L^+,$$

however, again by uniqueness of representation of vectors with respect to the basis X , $\mathbf{z} \notin S(X, \mathcal{Z})$, since $b \notin \mathcal{Z}$. This finishes the proof. \square

Finally, we prove the counting estimate of Proposition 1.1. Let X be a positive basis for L and \mathcal{X} the corresponding basis matrix as in (1). We obtain counting estimates for the number of points of bounded norm in L^+ and in the semigroup $S(X)$. Since $G(X) = L^+ \setminus S(X)$, we can then easily compute

$$(6) \quad |\{\mathbf{y} \in G(X) : \|\mathbf{y}\| \leq t\}| = |\{\mathbf{y} \in L^+ : \|\mathbf{y}\| \leq t\}| - |\{\mathbf{y} \in S(X) : \|\mathbf{y}\| \leq t\}|.$$

Lemma 2.6. *As $t \rightarrow \infty$,*

$$\mathcal{N}(L^+, t) = \left(\frac{\omega_d}{2^d \det L} \right) t^d + O(t^{d-1}).$$

Proof. It is a well-known fact (see, for instance, Theorem 2 on p.128 of [7]) that for a lattice L and a compact convex body E in \mathbb{R}^d ,

$$(7) \quad |tE \cap L| = \left(\frac{\text{Vol}_d(E)}{\det L} \right) t^d + O(t^{d-1}),$$

as $t \rightarrow \infty$. Let $E = B_d(1) \cap \mathbb{R}_{\geq 0}^d$, then $tE = B_d(t) \cap \mathbb{R}_{\geq 0}^d$ and $\text{Vol}_d(E) = \omega_d/2^d$. Since $\mathcal{N}(L^+, t) = |(B_d(t) \cap \mathbb{R}_{\geq 0}^d) \cap L|$, the result follows from (7). \square

Lemma 2.7. *Let $\nu(X)$ be the measure of the solid angle of the cone $\mathcal{C}(X)$. Then*

$$\mathcal{N}(S(X), t) = \left(\frac{\omega_d \nu(X)}{\det L} \right) t^d + O(t^{d-1}),$$

as $t \rightarrow \infty$.

Proof. Let $E = B_d(1) \cap \mathcal{C}(X)$, then $tE = B_d(t) \cap \mathcal{C}(X)$ and $\text{Vol}_d(E) = \omega_d \nu(X)$. Since $\mathcal{N}(S(X), t) = |(B_d(t) \cap \mathcal{C}(X)) \cap L|$, the result follows from (7). \square

Proposition 1.1 now follows by combining (6) with Lemmas 2.6 and 2.7. We can also extend it to more general cones. Let $Y = \{\mathbf{y}_1, \dots, \mathbf{y}_d\}$ be a collection of linearly independent vectors in \mathbb{R}^d and write $\mathcal{Y} = (\mathbf{y}_1 \ \dots \ \mathbf{y}_d) \in \text{GL}_d(\mathbb{R})$ for the corresponding matrix. Let $\mathcal{C}(Y) = \mathcal{Y}\mathbb{R}_{\geq 0}^d$ be the positive cone spanned by Y and let $L(Y) = L \cap \mathcal{C}(Y)$.

Corollary 2.8. *There exist infinitely many bases for L contained in $L(Y)$. If X is such a basis, then $\mathcal{C}(X) \subseteq \mathcal{C}(Y)$ and $S(X) = L \cap \mathcal{C}(X)$. The set of gaps $G_Y(X) := L(Y) \setminus S(X)$ is infinite unless $\mathcal{C}(X) = \mathcal{C}(Y)$ and*

$$\mathcal{N}(G_Y(X), t) = \left(\frac{\omega_d(\nu(Y) - \nu(X))}{\det L} \right) t^d + O(t^{d-1})$$

as $t \rightarrow \infty$, where $\nu(Y)$ and $\nu(X)$ are the measures of the solid angles of the cones $\mathcal{C}(Y)$ and $\mathcal{C}(X)$, respectively.

Proof. Let $M = \mathcal{Y}^{-1}L$, then $M \subset \mathbb{R}^d$ is also a full-rank lattice and $\det M = \frac{\det L}{|\det \mathcal{Y}|}$. Further, $\mathcal{Y}^{-1}\mathcal{C}(Y) = \mathbb{R}_{\geq 0}^d$ and $\mathcal{Y}^{-1}L(Y) = M^+$. Hence existence of infinitely many bases for L contained in $L(Y)$ follows from the existence of infinitely many positive bases for M . If $X \subset L(Y)$ is such a basis for L , then $\mathcal{Y}^{-1}X$ is a positive basis for M , $S(X) = \mathcal{Y}S(\mathcal{Y}^{-1}X)$ and the set of gaps $G_Y(X) = \mathcal{Y}G(\mathcal{Y}^{-1}X)$ is infinite, unless $\mathcal{Y}^{-1}X$ is orthogonal, which is equivalent to the assertion that $\mathcal{C}(X) = \mathcal{C}(Y)$.

To obtain the counting estimate on the number of gaps of bounded Euclidean norm, observe that

$$\mathcal{N}(G_Y(X), t) = \mathcal{N}(L(Y), t) - \mathcal{N}(S(X), t),$$

where $\mathcal{N}(S(X), t)$ is given by Lemma 2.7. To obtain an estimate $\mathcal{N}(L(Y), t)$, we use (7) with the choice of $E = B_d(1) \cap \mathcal{C}(Y)$, noting that $\text{Vol}_d(E) = \omega_d \nu(Y)$. \square

3. RESTRICTED SUCCESSIVE MINIMA

In this section we prove Theorem 1.2. Throughout this section we use notation as in Sections 1 and 2 above, and let X be a positive basis for a full-rank lattice $L \subset \mathbb{R}^d$.

Lemma 3.1. *There exists a point $\mathbf{y} \in L$ such that*

$$1 \leq y_i \leq 2\mu(L) + 1,$$

for each $1 \leq i \leq d$. Hence

$$\lambda_1(L^+) \leq 2\mu(L) + 1.$$

Proof. For $r = \mu(L)$, let

$$\mathbf{z}_r = (r+1)(1, \dots, 1)^\top \in \mathbb{R}^d,$$

and consider the cube

$$C_d(r) + \mathbf{z}_r = \{\mathbf{x} \in \mathbb{R}^d : 1 \leq x_i \leq 2r+1\}$$

in the positive orthant of \mathbb{R}^d . Then $B_d(r) + \mathbf{z}_r$ is the ball of radius r inscribed in $C_d(r) + \mathbf{z}_r$. Since

$$\mathbb{R}^d = \bigcup_{\mathbf{x} \in L} (B_d(r) + \mathbf{x}),$$

the ball $B_d(r) + \mathbf{z}_r$ must be covered by some translates of $B_d(r)$ by points of the lattice L . On the other hand, the ball $B_d(r) + \mathbf{z}_r$ of radius r cannot be covered by other balls of the same radius unless at least one of them has its center in $B_d(r) + \mathbf{z}_r$. This means that there must exist

$$\mathbf{y} \in L \cap (B_d(r) + \mathbf{z}_r) \subset C_d(r) + \mathbf{z}_r,$$

and so $1 \leq y_i \leq 2r+1 = 2\mu(L)+1$. \square

Lemma 3.2. For each $2 \leq i \leq d$,

$$\lambda_i(L^+) \leq 2\lambda_i(\mu(L)+1).$$

Proof. Let \mathbf{y} be the vector constructed in Lemma 3.1 above, and let $\mathbf{x}_1, \dots, \mathbf{x}_d$ be vectors corresponding to successive minima $\lambda_1, \dots, \lambda_d$. Then for at least one $1 \leq j \leq d$,

$$\mathbf{y} \notin \text{span}_{\mathbb{R}}\{\mathbf{x}_i : i \neq j\},$$

so for this j let $I_j = \{1 \leq i \leq d : i \neq j\}$. Then the collection of d vectors

$$\{\mathbf{y}\} \cup \{\lambda_i \mathbf{y} + \mathbf{x}_i : i \in I_j\}$$

is linearly independent, and for each $i \in I_j$,

$$|\lambda_i \mathbf{y} + \mathbf{x}_i| \leq \lambda_i |\mathbf{y}| + |\mathbf{x}_i| \leq 2\lambda_i(\mu(L)+1).$$

Further, since all coordinates of \mathbf{y} are ≥ 1 , for each $1 \leq k \leq d$, the k -th coordinate of each such vector $\lambda_i \mathbf{y} + \mathbf{x}_i$ is greater or equal than

$$\lambda_i + x_{ik} \geq 0,$$

so all of these vectors are in L^+ . Finally notice that $\lambda_i(L^+) \leq |\mathbf{z}|$ for each $\mathbf{z} \in L^+$ such that

$$\dim_{\mathbb{R}} \{\lambda_1 \mathbf{y} + \mathbf{x}_1, \dots, \lambda_{i-1} \mathbf{y} + \mathbf{x}_{i-1}, \mathbf{z}\} = i$$

if $i \leq j$ and

$$\dim_{\mathbb{R}} \{\lambda_1 \mathbf{y} + \mathbf{x}_1, \dots, \lambda_{j-1} \mathbf{y} + \mathbf{x}_{j-1}, \mathbf{y}, \lambda_{j+1} \mathbf{y} + \mathbf{x}_{j+1}, \dots, \lambda_{i-1} \mathbf{y} + \mathbf{x}_{i-1}, \mathbf{z}\} = i$$

if $i > j$. We can then take $\mathbf{z} = \lambda_i \mathbf{y} + \mathbf{x}_i$ for each $i \neq j$ and $\mathbf{z} = \mathbf{y}$ for $i = j$. The lemma follows. \square

Lemma 3.3. Let $X = \{\mathbf{x}_1, \dots, \mathbf{x}_d\}$ be a positive basis for L so that no $d-1$ elements of X lie in a coordinate hyperplane. There exist linearly independent vectors $\mathbf{z}_1, \dots, \mathbf{z}_d \in G_{\text{pr}}(X)$ with

$$(8) \quad |\mathbf{z}_i| = \max_{1 \leq m \leq d} \left\{ \left(\max_{1 \leq k \leq d} \left[\frac{x_{ik}}{\sum_{j=1, j \neq i}^d x_{jk}} \right] + 1 \right) \sum_{j=1, j \neq i}^d x_{jm} - x_{im} \right\}.$$

Proof. It is enough to prove that there exist such vectors $\mathbf{z}_i \in G(X)$ satisfying (8): if, say, some \mathbf{z}_i is not in $G_{\text{pr}}(X)$, then $\mathbf{z}_i = m\mathbf{z}'_i$ for some $m \in \mathbb{Z}^+$ and $\mathbf{z}'_i \in G_{\text{pr}}(X)$, so $|\mathbf{z}'_i| \leq |\mathbf{z}_i|$. Suppose that a vector $\mathbf{z} = \sum_{i=1}^d a_i \mathbf{x}_i \in L^+$ with at least one of the integer coefficients a_i equal to -1 . Since the representation of \mathbf{z} in terms of the basis X is unique, and at least one of the coefficients in this representation is negative, \mathbf{z} is not in $S(X)$, thus $\mathbf{z} \in G(X)$.

First, we want to select a point $\mathbf{y} \in S(X)$ that would have all positive coordinates. Let

$$\mathbf{y} = \mathbf{x}_1 + \cdots + \mathbf{x}_d.$$

Since all the coordinates of \mathbf{x}_i 's are nonnegative and these vectors form a basis for \mathbb{R}^d , the sum of their k -th coordinates has to be positive for each $1 \leq k \leq d$. Now, for each $1 \leq i \leq d$ define

$$\mathbf{z}_i = a_i \mathbf{y} - (a_i + 1) \mathbf{x}_i = a_i \sum_{j=1, j \neq i}^d \mathbf{x}_j - \mathbf{x}_i,$$

where a_i is a positive integer to be specified. In order for such \mathbf{z}_i to be in $G(X)$, we only need it to be in L^+ , meaning that for each $1 \leq k \leq d$, we must have

$$a_i \sum_{j=1, j \neq i}^d x_{jk} > x_{ik},$$

so take

$$a_i = \max_{1 \leq k \leq d} \left[\frac{x_{ik}}{\sum_{j=1, j \neq i}^d x_{jk}} \right] + 1.$$

Notice that $\sum_{j=1, j \neq i}^d x_{jk} \neq 0$ since no $d-1$ elements of X lie in a coordinate hyperplane. With this choice of a_i ,

$$|\mathbf{z}_i| = \max_{1 \leq m \leq d} \left\{ \left(\max_{1 \leq k \leq d} \left[\frac{x_{ik}}{\sum_{j=1, j \neq i}^d x_{jk}} \right] + 1 \right) \sum_{j=1, j \neq i}^d x_{jm} - x_{im} \right\},$$

which yields (8). Finally, notice that the vectors $\mathbf{z}_1, \dots, \mathbf{z}_d$ are linearly independent since the vectors $\mathbf{x}_1, \dots, \mathbf{x}_d$ are. \square

Now Theorem 1.2 follows from Lemmas 3.2 and 3.3. We can also extend it to more general cones $\mathcal{C}(Y) = \mathcal{Y}\mathbb{R}_{\geq 0}^d$ as in Corollary 2.8, where $Y = \{\mathbf{y}_1, \dots, \mathbf{y}_d\} \subset \mathbb{R}^d$ is a collection of linearly independent vectors and $\mathcal{Y} = (\mathbf{y}_1 \ \dots \ \mathbf{y}_d) \in \text{GL}_d(\mathbb{R})$ is the corresponding matrix. Write $|\mathcal{Y}|$ and $|\mathcal{Y}^{-1}|$ for the sup-norm of matrices \mathcal{Y} and \mathcal{Y}^{-1} , respectively, viewed as vectors in \mathbb{R}^{d^2} , and for each $1 \leq i \leq d$ define

$$\lambda_i(L(Y)) := \min \{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \text{span}_{\mathbb{R}}(L(Y) \cap C_d(t)) \geq i\},$$

and

$$\lambda_i(L(Y), X) := \min \{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \text{span}_{\mathbb{R}}(G_Y(X) \cap C_d(t)) \geq i\}.$$

These successive minima are easy to relate to the corresponding successive minima of the lattice $M = \mathcal{Y}^{-1}L$.

Corollary 3.4. *Let $M = \mathcal{Y}^{-1}L$, then for each $1 \leq i \leq d$,*

$$\frac{\lambda_i(M^+)}{d|\mathcal{Y}^{-1}|} \leq \lambda_i(L(Y)) \leq d|\mathcal{Y}|\lambda_i(M^+).$$

Additionally,

$$\lambda_d(L(Y), X) \leq d|\mathcal{Y}|\lambda_d(M^+, \mathcal{Y}^{-1}X).$$

Proof. Let $M = \mathcal{Y}^{-1}L$, then $M^+ = L(Y)$ and a vector $\mathbf{z}_i \in M^+$ corresponds to the successive minimum $\lambda_i(M^+)$ if and only if $\mathcal{Y}\mathbf{z}_i$ corresponds to the successive minimum $\lambda_i(L(Y))$. Then

$$\lambda_i(L(Y)) = |\mathcal{Y}\mathbf{z}_i| \leq d|\mathcal{Y}||\mathbf{z}_i| = d|\mathcal{Y}|\lambda_i(M^+),$$

as well as

$$\lambda_i(M^+) = |\mathcal{Y}^{-1}(\mathcal{Y}\mathbf{z}_i)| \leq d|\mathcal{Y}^{-1}||\mathcal{Y}\mathbf{z}_i| = d|\mathcal{Y}^{-1}|\lambda_i(L(Y)).$$

Further, $\mathbf{z} \in G_Y(X)$ corresponds to the successive minimum $\lambda_i(L(Y), X)$ if and only if $\mathcal{Y}^{-1}\mathbf{z}$ is a gap of $S(\mathcal{Y}^{-1}X)$ in M^+ corresponding to the successive minimum $\lambda_i(M^+, \mathcal{Y}^{-1}X)$. This observation combined with the inequalities above completes the proof. \square

4. POSITIVE SEMIGROUPS IN NUMBER FIELDS

In this section, we let K be a totally real number field and use the notation of Section 1. Investigation of totally positive semigroups in totally real number fields from the standpoint of the generalized Frobenius problem, a somewhat different perspective, has been initiated in [4]. We can view an ideal $I \subseteq \mathcal{O}_K$ as a lattice embedded into the Euclidean space \mathbb{R}^d via the Minkowski embedding

$$\Sigma = (\sigma_1, \dots, \sigma_d) : K \rightarrow \mathbb{R}^d.$$

Indeed, the image of our ideal I under Σ , $\Sigma(I)$ is a lattice of full rank in \mathbb{R}^d , call it L_I , and $L_I^+ = \Sigma(I^+)$. The Euclidean norm $\|\cdot\|$ on L_I then precisely corresponds to the trace form on K , defined in (5), i.e.

$$\|\Sigma(\alpha)\|^2 = \text{Tr}_K(\alpha^2),$$

for any $\alpha \in I$. Further,

$$(9) \quad \det L_I = \mathbb{N}_K(I)\sqrt{|\Delta_K|},$$

where \mathbb{N}_K is the norm on K and Δ_K the discriminant of K , as stated in Section 1 (see, for instance, Lemma 2 on p. 115 of [7]). Notice that a basis $\beta = \{\beta_1, \dots, \beta_d\}$ for I is contained in I^+ if and only if its image

$$X = \{\mathbf{x}_1, \dots, \mathbf{x}_d\} := \{\Sigma(\beta_1), \dots, \Sigma(\beta_d)\}$$

is a basis for L_I contained in L_I^+ , and $\Sigma(S(\beta)) = S(X)$. Then Lemma 2.1 implies that I has infinitely many bases contained in I^+ . Further, for a positive basis β of I , α is a gap of $S(\beta)$ if and only if $\Sigma(\alpha)$ is a gap of $S(\Sigma(\beta))$.

The basis β is not orthogonal. Indeed, since $X \subset L_I^+$, in order for β to be orthogonal the vectors of X must be along the coordinate axes in \mathbb{R}^d , meaning that these vectors have zero coordinates. This is not possible, since coordinates of any nonzero vector $\mathbf{y} = \Sigma(\alpha) \in L_I$ are conjugates of a nonzero element $\alpha \in I$, hence cannot be zero. Therefore the set of gaps $G(\beta) := I^+ \setminus S(\beta)$ is infinite.

To measure size of elements in our number field, we use Weil height. Let $M(K)$ be the set of all places of K , and for every $\alpha \in K$ let

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

where $d_v = [K_v : \mathbb{Q}_v]$ is the local degree of K at the place $v \in M(K)$. Notice that for each $v \nmid \infty$, $d_v = 1$ since K is totally real.

Lemma 4.1. *For every nonzero $\alpha \in \mathcal{O}_K$,*

$$1 \leq h(\alpha) \leq |\Sigma(\alpha)|,$$

and for every nonzero $\alpha \in K$,

$$|\Sigma(\alpha)| \leq h(\alpha)^d.$$

Proof. Let $\alpha \in \mathcal{O}_K$ be nonzero. For each $v \nmid \infty$, $|\alpha|_v \leq 1$, and so

$$h(\alpha) = \prod_{v|\infty} \max\{1, |\alpha|_v\}^{1/d} = \left(\prod_{i=1}^d \max\{1, |\sigma_i(\alpha)|\} \right)^{1/d}.$$

By the Artin-Whaples product formula [1] combined with the arithmetic-geometric mean inequality,

$$1 = \prod_{v \in M(K)} |\alpha|^{d_v/d} \leq \prod_{i=1}^d |\sigma_i(\alpha)|^{1/d} \leq \frac{1}{d} \sum_{i=1}^d |\sigma_i(\alpha)| \leq \max_{1 \leq i \leq d} |\sigma_i(\alpha)| = |\Sigma(\alpha)|.$$

This implies that

$$h(\alpha) \leq \left(\prod_{i=1}^d \max_{1 \leq j \leq d} \{|\sigma_j(\alpha)|\} \right)^{1/d} \leq |\Sigma(\alpha)|.$$

On the other hand, for any nonzero $\alpha \in K$,

$$|\Sigma(\alpha)| = \max_{1 \leq i \leq d} |\sigma_i(\alpha)| \leq \prod_{i=1}^d \max\{1, |\sigma_i(\alpha)|\} \leq \prod_{v \in M(K)} \max\{1, |\alpha|_v^{d_v}\} = h(\alpha)^d.$$

□

We can now state the bounds on the successive minima of the ideal I with respect to the Weil height.

Lemma 4.2. *There exist \mathbb{Q} -linearly independent elements $s_1, \dots, s_d \in I$ such that*

$$(10) \quad \prod_{i=1}^d h(s_i) \leq \prod_{i=1}^d |\Sigma(s_i)| \leq \mathbb{N}_K(I) \sqrt{|\Delta_K|}.$$

Further, the inhomogeneous minimum of the lattice L_I satisfies the inequality

$$(11) \quad \mu(L_I) \leq \frac{d^{3/2}}{2} \mathbb{N}_K(I) \sqrt{|\Delta_K|}.$$

Proof. Notice that the successive minima λ_i of the lattice L_I , as we defined them in Section 1 are the smallest sup-norms of \mathbb{Q} -linearly independent vectors in L_I . Taking $s_1, \dots, s_d \in I$ to be a collection of elements so that $\Sigma(s_1), \dots, \Sigma(s_d) \in L_I$ are such \mathbb{Q} -linearly independent vectors corresponding to these successive minima, (10) follows immediately by combining (4) with (9) and Lemma 4.1. To obtain (11), notice that the second inequality of (4) implies that

$$\mu(L_I) \leq \frac{d^{3/2}}{2} \lambda_d.$$

On the other hand, Lemma 4.1 guarantees that $\lambda_1 \geq 1$, and so $\prod_{i=1}^d \lambda_i \geq \lambda_d$. Thus applying now the first inequality of (4), we see that

$$\mu(L_I) \leq \frac{d^{3/2}}{2} \lambda_d \leq \frac{d^{3/2}}{2} \prod_{i=1}^d \lambda_i \leq \frac{d^{3/2}}{2} \det L_I = \frac{d^{3/2}}{2} \mathbb{N}_K(I) \sqrt{|\Delta_K|},$$

where the last equality is given by (9). \square

Lemma 4.3. *There exist \mathbb{Q} -linearly independent elements $\alpha_1, \dots, \alpha_d \in I^+$ such that*

$$\prod_{i=1}^d h(\alpha_i) \leq (3d\sqrt{d})^d \left(\mathbb{N}_K(I) \sqrt{|\Delta_K|} \right)^{d+1}.$$

Proof. A collection of elements $\alpha_1, \dots, \alpha_d$ is \mathbb{Q} -linearly independent in I^+ if and only if the collection $\Sigma(\alpha_1), \dots, \Sigma(\alpha_d)$ is \mathbb{Q} -linearly independent in L_I^+ . Take a collection $s_1, \dots, s_d \in I$ as guaranteed by Lemma 4.2 above. Notice that Lemma 4.1 implies that $\mu(L_I) \geq 1/2$. Then combining (3) with Lemma 4.1, we see that there exist such \mathbb{Q} -linearly independent in I^+ so that

$$\begin{aligned} \prod_{i=1}^d h(\alpha_i) &\leq \prod_{i=1}^d |\Sigma(\alpha_i)| \leq (2\mu(L_I) + 1) \prod_{i=2}^d 2|\Sigma(s_i)|(\mu(L_I) + 1) \\ &\leq 6^d \mu(L_I)^d \prod_{i=2}^d |\Sigma(s_i)| \leq 6^d \mu(L_I)^d \prod_{i=1}^d |\Sigma(s_i)| \\ &\leq (3d^{3/2})^d \left(\mathbb{N}_K(I) \sqrt{|\Delta_K|} \right)^{d+1}, \end{aligned}$$

where the last inequality follows by Lemma 4.2. \square

Lemma 4.4. *Let $\beta = \{\beta_1, \dots, \beta_d\}$ be a positive basis for the ideal I and $G(\beta) = I^+ \setminus S(\beta)$ be the corresponding set of gaps. For each $1 \leq i \leq d$, let $\beta'_i = \sum_{j=1, j \neq i}^d \beta_j$. Then there exist \mathbb{Q} -linearly independent gaps $\alpha_1, \dots, \alpha_d \in G(\beta)$ such that*

$$h(\alpha_i) \leq (h(\beta_i/\beta'_i)^d + 1) h(\beta'_i)^d.$$

Proof. Notice that $G(\Sigma(\beta)) = \Sigma(G(\beta))$. Then Lemma 3.3 implies existence of \mathbb{Q} -linearly independent $\alpha_1, \dots, \alpha_d \in G(\beta)$ such that

$$\begin{aligned} |\Sigma(\alpha_i)| &= \max_{1 \leq m \leq d} \left\{ \left(\max_{1 \leq k \leq d} \left[\frac{\sigma_k(\beta_i)}{\sum_{j=1, j \neq i}^d \sigma_k(\beta_j)} \right] + 1 \right) \sum_{j=1, j \neq i}^d \sigma_m(\beta_j) - \sigma_m(\beta_i) \right\} \\ &\leq \max_{1 \leq m \leq d} \left\{ \left(\max_{1 \leq k \leq d} \sigma_k \left(\frac{\beta_i}{\beta'_i} \right) + 1 \right) \sigma_m(\beta'_i) - \sigma_m(\beta_i) \right\} \\ &\leq (|\Sigma(\beta_i/\beta'_i)| + 1) |\Sigma(\beta'_i)| \leq (h(\beta_i/\beta'_i)^d + 1) h(\beta'_i)^d, \end{aligned}$$

by Lemma 4.1, and $h(\alpha_i) \leq |\Sigma(\alpha_i)|$ also by Lemma 4.1. This completes the proof. \square

Now Theorem 1.3 follows by combining Lemmas 4.2, 4.3 and 4.4.

Acknowledgement: We would like to sincerely thank the anonymous referee whose excellent suggestions helped to significantly improve our paper.

REFERENCES

- [1] E. Artin and G. Whaples. Axiomatic characterization of fields by the product formula for valuations. *Bull. Amer. Math. Soc.*, 51(7):469–492, 1945.
- [2] J. W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer-Verlag, 1959.
- [3] L. Fukshansky. Integral points of small height outside of a hypersurface. *Monatsh. Math.*, 147(1):25–41, 2006.
- [4] L. Fukshansky and Y. Shi. Positive semigroups and generalized frobenius numbers over totally real number fields. *Mosc. J. Comb. Number Theory*, 9(1):29–41, 2020.
- [5] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*. North-Holland Publishing Co., 1987.
- [6] M. Henk and C. Thiel. Restricted successive minima. *Pacific J. Math.*, 269(2):341–354, 2014.
- [7] S. Lang. *Algebraic Number Theory*. Springer-Verlag, 1986.
- [8] J. M. Ribando. Measuring solid angles beyond dimension three. *Discrete Comput. Geom.*, 36(3):479–487, 2006.

DEPARTMENT OF MATHEMATICS, 850 COLUMBIA AVENUE, CLAREMONT MCKENNA COLLEGE,
CLAREMONT, CA 91711, USA
Email address: `lenny@cmc.edu`

DEPARTMENT OF MATHEMATICS, 850 COLUMBIA AVENUE, CLAREMONT MCKENNA COLLEGE,
CLAREMONT, CA 91711, USA
Email address: `swang21@students.claremontmckenna.edu`