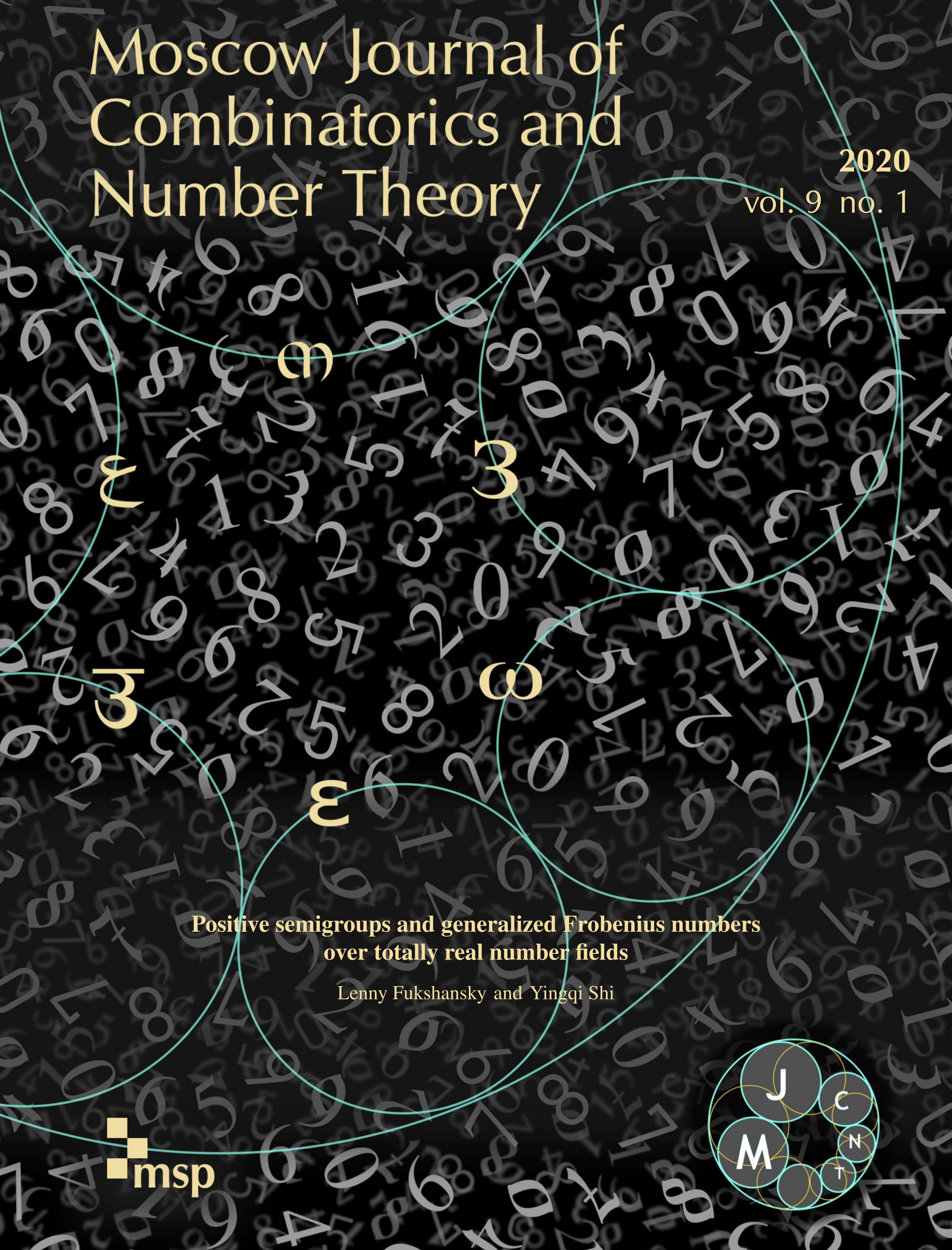

Moscow Journal of
Combinatorics and
Number Theory

2020
vol. 9 no. 1

Positive semigroups and generalized Frobenius numbers over totally real number fields

Lenny Fukshansky and Yingqi Shi

msp

Moscow Journal of Combinatorics and Number Theory
Vol. 9, No. 1, 2020
dx.doi.org/10.2140/moscow.2020.9.29

Positive semigroups and generalized Frobenius numbers over totally real number fields

Lenny Fukshansky and Yingqi Shi

The Frobenius problem and its many generalizations have been extensively studied in several areas of mathematics. We study semigroups of totally positive algebraic integers in totally real number fields, defining analogues of the Frobenius numbers in this context. We use a geometric framework recently introduced by Aliev, De Loera and Louveaux to produce upper bounds on these Frobenius numbers in terms of a certain height function. We discuss some properties of this function, relating it to absolute Weil height and obtaining a lower bound in the spirit of Lehmer's conjecture for algebraic vectors satisfying some special conditions. We also use a result of Borosh and Treybig to obtain bounds on the size of representations and number of elements of bounded height in such positive semigroups of totally real algebraic integers.

1. Introduction

Let $n \geq 2$ be an integer and let

$$1 < a_1 < \cdots < a_n \tag{1}$$

be relatively prime integers. We say that a positive integer t is *representable* by the n-tuple $\boldsymbol{a} := (a_1, \ldots, a_n)$ if

$$t = a_1 x_1 + \cdots + a_n x_n \tag{2}$$

for some nonnegative integers $x_1, \ldots, x_n$, and we call each such a solution $\boldsymbol{x} := (x_1, \ldots, x_n)$ of (2) a *representation for t in terms of $\boldsymbol{a}$*. Let $s \geq 0$ be an integer; then the *s-Frobenius number* of this n-tuple, $g_s(\boldsymbol{a})$, as defined in [Beck and Robins 2004], is the largest positive integer that has at most s distinct representations in terms of $\boldsymbol{a}$. This is a generalization of the classical Frobenius number $g_0(\boldsymbol{a})$, i.e., the largest positive integer that has no such representations. The Frobenius number has been studied extensively by a variety of authors, starting as early as late 19th century; see [Ramírez Alfonsín 2005] for a detailed account and bibliography. The condition

$$\gcd(a_1, \ldots, a_n) = 1 \tag{3}$$

implies that $g_s(\boldsymbol{a})$ exists for every s. The algorithmic *Frobenius problem*, known to be NP-hard, is to determine g_0 (or more generally g_s for $s \geq 1$) given n and the relatively prime n-tuple $a_1, \ldots, a_n$ on the

---

Fukshansky was partially supported by the Simons Foundation grant #519058.
MSC2010: 11D07, 11H06, 52C07, 11D45, 11G50.
Keywords: linear Diophantine problem of Frobenius, lattice points in polyhedra, affine semigroups, totally real number fields, heights.

input. The hardness of this problem in particular implies that no general closed form formulas for the Frobenius numbers exist, sparking interest in upper and lower bounds.

A geometric approach to the classical Frobenius problem was pioneered in the influential paper of R. Kannan [1992], leading to a polynomial-time algorithm to find the Frobenius number for each fixed n. Bounds on the classical Frobenius number stemming from further geometry-of-numbers applications were obtained in [Fukshansky and Robins 2007; Aliev and Gruber 2007]. These ideas were also extended to the more general s-Frobenius problem in [Fukshansky and Schürmann 2011; Aliev et al. 2012]. A higher-dimensional analogue of the Frobenius problem was also considered in recent years by several authors, notably in [Aliev and Henk 2010; Aliev et al. 2013; 2016].

This note is inspired by the work of Aliev, De Loera and Louveaux [Aliev et al. 2016]. We use the geometric setup and results of that paper (described in Section 2) to define a natural extension of the Frobenius problem to totally real number fields and to give bounds on the s-Frobenius numbers in this context. Let K be a totally real number field of degree d over $\mathbb{Q}$ with embeddings $\sigma_1, \dots, \sigma_d : K \to \mathbb{R}$. Let

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

be the Minkowski embedding of K. Let $\mathcal{O}_K$ be the ring of integers of K, and $\mathcal{O}_K^+$ the additive semigroup of totally positive elements in $\mathcal{O}_K$; i.e.,

$$\mathcal{O}_K^+ := \{\alpha \in \mathcal{O}_K : \sigma_i(\alpha) \geq 0 \text{ for all } 1 \leq i \leq d\}.$$

Let $n > d$ and let $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K^+$ be a collection of elements so that

$$\mathcal{O}_K = \operatorname{span}_{\mathbb{Z}}\{\alpha_1, \dots, \alpha_n\}. \tag{4}$$

Such a collection always exists, since there exist bases for $\mathcal{O}_K$ in $\mathcal{O}_K^+$. Indeed, let $\omega_1, \dots, \omega_d$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, where $\omega_1 = 1$, and suppose it is not in $\mathcal{O}_K^+$. Let

$$M = \Big[\max_{1 \leq i,j \leq d} |\sigma_i(\omega_j)|\Big] + 1,$$

where [ ] stands for integer part. Then $1, M + \omega_2, \dots, M + \omega_d \in \mathcal{O}_K^+$ and it is still a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Write $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$. Define the semigroup generated by $\boldsymbol{\alpha}$ to be

$$\operatorname{Sg}(\boldsymbol{\alpha}) := \left\{ \sum_{i=1}^{n} \alpha_i x_i : \boldsymbol{x} \in \mathbb{Z}_{\geq 0}^n \right\},$$

and the rational cone spanned by $\boldsymbol{\alpha}$ to be

$$\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) := \left\{ \sum_{i=1}^{n} \alpha_i x_i : \boldsymbol{x} \in \mathbb{Q}_{\geq 0}^n \right\}.$$

Then it is clear that $\operatorname{Sg}(\boldsymbol{\alpha}) \subseteq \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathcal{O}_K \subseteq \mathcal{O}_K^+$, and $\operatorname{Sg}(\boldsymbol{\alpha})$ is not necessarily equal to $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathcal{O}_K$.

Example 1. Indeed, consider for instance the real quadratic field $K = \mathbb{Q}(\sqrt{2})$ and take

$$\alpha_1 = 1, \quad \alpha_2 = 4 + \sqrt{2}, \quad \alpha_3 = 6 + 2\sqrt{2}.$$

One easily checks that these three elements are in $\mathcal{O}_K^+$ and

$$\mathcal{O}_K = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} = \{(a - 4b)\alpha_1 + b\alpha_2 : a, b \in \mathbb{Z}\}.$$

Then

$$\mathrm{Sg}(\boldsymbol{\alpha}) = \{(x_1 + 4x_2 + 6x_3) + (x_2 + 2x_3)\sqrt{2} : x_1, x_2, x_3 \in \mathbb{Z}_{\geq 0}\}.$$

On the other hand,

$$3 + \sqrt{2} = \tfrac{1}{2}\alpha_3 \in \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathcal{O}_K,$$

but it is clearly not in $\mathrm{Sg}(\boldsymbol{\alpha})$.

Further, for each $s \geq 1$ let $\mathrm{Sg}_s(\boldsymbol{\alpha})$ be the set of all points $\beta \in \mathrm{Sg}(\boldsymbol{\alpha})$ for which there are at least s distinct points $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$ such that $\sum_{i=1}^n \alpha_i x_i = \beta$; then $\mathrm{Sg}(\boldsymbol{\alpha}) = \mathrm{Sg}_1(\boldsymbol{\alpha})$.

Now, let $\beta \in \mathcal{O}_K^+$ be in the interior of the cone $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})$ and take the ray $t\beta$ as $t \in \mathbb{Z}_{\geq 0}$. Shifting the cone $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})$ along this ray and intersecting it with $\mathcal{O}_K$ we will eventually land in the semigroup $\mathrm{Sg}(\boldsymbol{\alpha})$ (this observation will follow from our results). In other words, there exists a positive integer t such that

$$\mathrm{int}(t\beta + \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})) \cap \mathcal{O}_K \subseteq \mathrm{Sg}(\boldsymbol{\alpha}).$$

More precisely, for each $s \geq 1$ we can define

$$g_s(\boldsymbol{\alpha}, \beta) := \min\{t \in \mathbb{Z}_{>0} : \mathrm{int}(t\beta + \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})) \cap \mathcal{O}_K \subseteq \mathrm{Sg}_s(\boldsymbol{\alpha})\},$$

and let

$$g_s(\boldsymbol{\alpha}) := \max\{g_s(\boldsymbol{\alpha}, \beta) : \beta \in \mathrm{int}(\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})) \cap \mathcal{O}_K^+\}.$$

We refer to $g_s(\boldsymbol{\alpha})$ as the *s-Frobenius number of $\boldsymbol{\alpha}$*.

We can see that when $K = \mathbb{Q}$ this construction reduces to the usual s-Frobenius numbers. Indeed, if $K = \mathbb{Q}$ then $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_K^+ = \mathbb{Z}_{\geq 0}$, and (4) simply means that $\alpha_1, \ldots, \alpha_n$ are positive relatively prime integers. Then $\mathrm{Sg}(\boldsymbol{a})$ is the semigroup of all positive integers representable by $\boldsymbol{\alpha}$, $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) = \mathbb{Q}_{\geq 0}$, and so $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathbb{Z}_{\geq 0} = \mathbb{Z}_{\geq 0}$. Then

$$\max_{\beta \in \mathbb{Z}_{\geq 0}} \min\{t \in \mathbb{Z}_{>0} : \mathrm{int}(t\beta + \mathbb{Q}_{\geq 0}) \cap \mathbb{Z} \subseteq \mathrm{Sg}_s(\boldsymbol{\alpha})\} \leq \min\{t \in \mathbb{Z}_{>0} : \mathrm{int}(t + \mathbb{Q}_{\geq 0}) \cap \mathbb{Z} \subseteq \mathrm{Sg}_s(\boldsymbol{\alpha})\}$$

is precisely the smallest integer t so that all integers $> t$ have at least s representations by $\boldsymbol{\alpha}$.

We present an upper bound on $g_s(\boldsymbol{\alpha})$. To state it, we need to introduce a certain measure of arithmetic complexity of $\boldsymbol{\alpha}$. Let us write $[n] := \{1, \ldots, n\}$ and define $\mathcal{J}(n, d) := \{I \subset [n] : |I| = d\}$. For each $I = \{i_1, \ldots, i_d\} \in \mathcal{J}(n, d)$, let us write $\mathrm{disc}(\boldsymbol{\alpha}_I)$ for the discriminant of the subcollection $\alpha_{i_1}, \ldots, \alpha_{i_d}$. We also write Δ_K for the discriminant of K, and define

$$\mathcal{D}(\boldsymbol{\alpha}) := \frac{1}{|\Delta_K|} \sum_{I \in \mathcal{J}(n,d)} |\mathrm{disc}(\boldsymbol{\alpha}_I)|. \tag{5}$$

Notice that absolute values in this definition are not necessary in the case of a real number field, since all the quantities are positive; we put them there so that this definition can be naturally extended to any number field. We now state our theorem.

Theorem 1.1. *With notation as above,*

$$g_s(\boldsymbol{\alpha}) \leq \frac{1}{2\sqrt{n-d+1}}\big((n-d)\mathcal{D}(\boldsymbol{\alpha}) + (s-1)^{1/(n-d)}\mathcal{D}(\boldsymbol{\alpha})^{(n-d+1)/(2(n-d))}\big).$$

We prove Theorem 1.1 in Section 2. Now suppose that $\beta \in \mathrm{Sg}(\boldsymbol{\alpha})$; hence there exists $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$ such that $\sum_{i=1}^n \alpha_i x_i = \beta$. It is natural to ask for the smallest such representation for β. In other words, given $\beta \in \mathrm{Sg}(\boldsymbol{\alpha})$ we want to find $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$ such that $\sum_{i=1}^n \alpha_i x_i = \beta$ with $|\boldsymbol{x}| := \max\{|x_i| : 1 \leq i \leq n\}$ as small as possible. This is our next result. To state it, let $\boldsymbol{\alpha}(\beta) := (\alpha_1, \ldots, \alpha_n, \beta) \in K^{n+1}$ and define

$$\mathcal{M}(\boldsymbol{\alpha}, \beta) := \frac{1}{|\Delta_K|^{1/2}} \max_{I \in \mathcal{J}(n+1,d)} |\operatorname{disc}(\boldsymbol{\alpha}(\beta)_I)|^{1/2}. \tag{6}$$

We also briefly recall the definition of a standard Weil-type height on K. Let us write $M(K)$ for the set of places of K, and for each $v \in M(K)$ let $d_v := [K_v : \mathbb{Q}_v]$ be the local degree of K at v; in particular, $\sum_{v|u} d_v = d$ for each $u \in M(\mathbb{Q})$. Let us normalize absolute values so that the product formula reads

$$\prod_{v \in M(K)} |a|_v = 1$$

for all nonzero $a \in K$. Then the usual *inhomogeneous height function* $H_K : K^n \to \mathbb{R}$, which extends Weil height on K, is defined as

$$H_K(\boldsymbol{\alpha}) = \prod_{v \in M(K)} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}. \tag{7}$$

We can now state our next result.

Theorem 1.2. *With notation as above, let* $\beta \in \mathrm{Sg}(\boldsymbol{\alpha})$. *Then there exists* $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$ *such that* $\sum_{i=1}^n \alpha_i x_i = \beta$, *and for any such* $\boldsymbol{x}$ *we have*

$$\frac{1}{n}\left(\frac{H_K(\beta)}{H_K(\boldsymbol{\alpha})}\right)^{1/d} \leq |\boldsymbol{x}| \leq \mathcal{M}(\boldsymbol{\alpha}, \beta).$$

We discuss some properties of $\mathcal{D}(\boldsymbol{\alpha})$ and $\mathcal{M}(\boldsymbol{\alpha}, \beta)$ in Section 3, viewing them as kinds of height functions. We use these properties along with Theorem 1.1 to obtain a lower bound on absolute Weil height of $\boldsymbol{\alpha}$ in the spirit of Lehmer's conjecture on heights of algebraic numbers.

We use a result of [Borosh and Treybig 1976] to prove Theorem 1.2 in Section 4. This theorem also allows us to obtain a counting estimate on the number of points of bounded height in the positive semigroup $\mathrm{Sg}(\boldsymbol{\alpha})$.

Theorem 1.3. *With notation as above, let* $T_1, T_2 \in \mathbb{R}_{\geq 0}$ *with* $T_1 < T_2$, *and define*

$$\mathrm{Sg}_s(\boldsymbol{\alpha}, T_1, T_2) = \{\beta \in \mathrm{Sg}_s(\boldsymbol{\alpha}) : T_1 \leq H_K(\beta) \leq T_2\}.$$

Additionally, for each $\beta \in \mathrm{Sg}(\boldsymbol{\alpha})$ *define* $r(\beta) = \max\{s : \beta \in \mathrm{Sg}_s(\boldsymbol{\alpha})\}$. *Then*

$$\sum_{\beta \in \mathrm{Sg}_1(\boldsymbol{\alpha}, T_1, T_2)} r(\beta) \leq \left(\frac{d!\, H_K(\boldsymbol{\alpha})}{|\Delta_K|^{1/2}} T_2 + 1\right)^n - \left[\frac{T_1^{1/d}}{n H_K(\boldsymbol{\alpha})^{1/d}}\right]^n.$$

In particular,

$$|\mathrm{Sg}_s(\boldsymbol{\alpha}, T_1, T_2)| \leq \frac{1}{s}\left\{\left(\frac{d!\, H_K(\boldsymbol{\alpha})}{|\Delta_K|^{1/2}} T_2 + 1\right)^n - \left[\frac{T_1^{1/d}}{n H_K(\boldsymbol{\alpha})^{1/d}}\right]^n\right\}. \tag{8}$$

On the other hand, *for* $T \geq 1$,

$$\sum_{\beta \in \mathrm{Sg}_1(\boldsymbol{\alpha}, 1, T)} r(\beta) \geq \left[\frac{T_1^{1/d}}{n H_K(\boldsymbol{\alpha})^{1/d}}\right]^n.$$

Theorem 1.3 is also proved in Section 4. It is instructive to compare the bounds of Theorem 1.3 to the known estimates on the number of algebraic integers of bounded height in a fixed number field. A result attributed to S. Lang (see [Widmer 2016] for details) asserts that in our case of a totally real number field K,

$$|\{\beta \in \mathcal{O}_K : H_K(\beta) \leq T\}| = O(T^{d^2} (\log T)^{d-1}).$$

This implies that our bound (8) is nontrivial when $n \leq d^2$. We are now ready to proceed.

2. Polyhedral semigroups and proof of Theorem 1.1

We start by briefly describing the setup and some results of [Aliev et al. 2016]. Let A be a $d \times n$ integer matrix, and for each set $I \in \mathcal{J}(n, d)$ let A_I be the $d \times d$ submatrix of A whose columns are indexed by I. Assume that

(1) $\gcd(\det(A_I) : I \in \mathcal{J}(n, d)) = 1$,
(2) $\{\boldsymbol{x} \in \mathbb{R}^n_{\geq 0} : A\boldsymbol{x} = \boldsymbol{0}\} = \{\boldsymbol{0}\}$.

Define the additive semigroup

$$\mathrm{Sg}(A) := \{\boldsymbol{b} \in \mathbb{Z}^d : \boldsymbol{b} = A\boldsymbol{x} \text{ for some } \boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}\},$$

and for each $s \geq 1$ let $\mathrm{Sg}_s(A)$ be the set of all points $\boldsymbol{b} \in \mathrm{Sg}(A)$ for which there are at least s distinct points $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$ such that $A\boldsymbol{x} = \boldsymbol{b}$. Thus $\mathrm{Sg}(A) = \mathrm{Sg}_1(A)$. Let

$$\mathcal{C}_{\mathbb{R}}(A) = \{A\boldsymbol{x} : \boldsymbol{x} \in \mathbb{R}^n_{\geq 0}\}$$

be the convex polyhedral cone spanned by the column vectors of A. Then it is clear that

$$\mathrm{Sg}(A) \subseteq \mathcal{C}_{\mathbb{R}}(A) \cap \mathbb{Z}^d,$$

and this containment is often proper; i.e., in general $\mathrm{Sg}(A) \neq \mathcal{C}_{\mathbb{R}}(A) \cap \mathbb{Z}^d$. For each $\boldsymbol{b} \in \mathrm{int}(\mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d$, define

$$g_s(A, \boldsymbol{b}) = \min\{t \in \mathbb{Z}_{>0} : \mathrm{int}(t\boldsymbol{b} + \mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d \subseteq \mathrm{Sg}_s(A)\},$$

and let

$$g_s(A) := \max\{g_s(\boldsymbol{\alpha}, \beta) : \beta \in \mathrm{int}(\mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d\}.$$

This is the s-Frobenius number of A as defined in [Aliev et al. 2016]. The upper bound on $g_s(A)$ proved in that paper (Theorem 2) is

$$g_s(A) \leq \frac{1}{2\sqrt{n-d+1}}((n-d)\det(AA^{\top}) + (s-1)^{1/(n-d)} \det(AA^{\top})^{(n-d+1)/(2(n-d))}). \tag{9}$$

We can now use this result to prove our Theorem 1.1. Our strategy is straightforward: we use the Minkowski embedding to convert our setup into that of a lattice in a Euclidean space, prove that our resulting ingredients satisfy the hypotheses of Theorem 2 of [Aliev et al. 2016], apply their bound (9), and then reinterpret it in terms of the original setup in the number field.

Proof of Theorem 1.1. Let the setup be as in Section 1. Let $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K^+$ be a collection of elements satisfying (4), and let us fix $\omega_1, \dots, \omega_d$, a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Then there exist integers a_{ij}, where $1 \leq i \leq n$, $1 \leq j \leq d$ so that

$$\alpha_i = \sum_{j=1}^{d} a_{ij} \omega_j.$$

Let us write $A = (a_{ij})^\top$ for the $d \times n$ matrix of these integer coefficients. Let

$$B = (\Sigma(\omega_1) \ \cdots \ \Sigma(\omega_d)).$$

Then $\Delta_K = \det(B)^2$ and

$$C := (\Sigma(\alpha_1) \ \cdots \ \Sigma(\alpha_n)) = BA.$$

Since $\alpha_1, \dots, \alpha_n$ satisfy (4), we must have $\Sigma(\mathcal{O}_K) = C\mathbb{Z}^n$. On the other hand, certainly $\Sigma(\mathcal{O}_K) = B\mathbb{Z}^d$; hence $B\mathbb{Z}^d = B(A\mathbb{Z}^n)$, which means that $A\mathbb{Z}^n = \mathbb{Z}^d$. This implies that row vectors of A are extendable to a basis for $\mathbb{Z}^n$. By Lemma 2 on p. 15 of [Cassels 1959], this is equivalent to the condition that

$$\gcd(\det(A_I) : I \in \mathcal{J}(n, d)) = 1.$$

Now suppose $\boldsymbol{x} \in \mathbb{R}^n_{\geq 0}$ and assume $A\boldsymbol{x} = \boldsymbol{0}$. Then

$$C\boldsymbol{x} = B(A\boldsymbol{x}) = \boldsymbol{0},$$

but entries of C are of the form $\sigma_i(\alpha_j)$, which are all positive real numbers, since $\alpha_j \in \mathcal{O}_K^+$. Therefore $\boldsymbol{x}$ must be equal to $\boldsymbol{0}$, and so

$$\{\boldsymbol{x} \in \mathbb{R}^n_{\geq 0} : A\boldsymbol{x} = \boldsymbol{0}\} = \{\boldsymbol{0}\}.$$

Thus matrix A satisfies conditions (1) and (2) above, and so we can apply (9) to get a bound on $g_s(A)$.

Now notice that $\Sigma(\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})) = B\mathcal{C}_{\mathbb{Q}}(A)$, where

$$\mathcal{C}_{\mathbb{Q}}(A) := \{A\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Q}^n_{\geq 0}\},$$

and $\operatorname{int}(\mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d = \operatorname{int}(\mathcal{C}_{\mathbb{Q}}(A)) \cap \mathbb{Z}^d$. Indeed, it is clear that

$$\operatorname{int}(\mathcal{C}_{\mathbb{Q}}(A)) \cap \mathbb{Z}^d \subseteq \operatorname{int}(\mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d,$$

so let us show containment in the opposite direction. Suppose $\boldsymbol{z} \in \operatorname{int}(\mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d$. Then there exists $\boldsymbol{x} \in \mathbb{R}^n_{\geq 0}$ such that

$$A\boldsymbol{x} = \boldsymbol{z}.$$

In fact, this equation defines a hyperplane in $\mathbb{R}^n$, which is defined over $\mathbb{Q}$ (since A and $\boldsymbol{z}$ have integer coordinates), and hence points with rational coordinates are dense in it. Thus taking a sufficiently small open ball in this hyperplane centered at $\boldsymbol{x}$, we can find a rational point with positive coordinates satisfying the same equation. This means that $\boldsymbol{z} \in \operatorname{int}(\mathcal{C}_{\mathbb{Q}}(A)) \cap \mathbb{Z}^d$.

With this setup in mind, let $\beta \in \operatorname{int}(\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})) \cap \mathcal{O}_K^+$ and let $\boldsymbol{b} \in \mathbb{Z}^d$ be such that $\Sigma(\beta) = B\boldsymbol{b}$. Then for $t \in \mathbb{Z}_{>0}$ we have

$$\begin{aligned} \operatorname{int}(t\beta + \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})) \cap \mathcal{O}_K \subseteq \operatorname{Sg}_s(\boldsymbol{\alpha}) \quad &\Longleftrightarrow \quad \operatorname{int}(tB\boldsymbol{b} + B\mathcal{C}_{\mathbb{Q}}(A)) \cap B\mathbb{Z}^d \subseteq B\operatorname{Sg}_s(A) \\ &\Longleftrightarrow \quad \operatorname{int}(t\boldsymbol{b} + \mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d \subseteq \operatorname{Sg}_s(A). \end{aligned}$$

This implies that $g_s(\boldsymbol{\alpha}) = g_s(A)$, and so we only need to express $\det(AA^\top)$ in terms of $\boldsymbol{\alpha}$. Notice that

$$\det(AA^\top) = \det((B^{-1}C)(B^{-1}C)^\top) = \frac{1}{\det(B)^2}\det(CC^\top).$$

Now, $\det(B)^2 = \Delta_K$, and by the Cauchy–Binet formula

$$\det(CC^\top) = \sum_{I \in \mathcal{J}(n,d)} \det(C_I)^2,$$

where for each $I = \{i_1, \dots, i_d\}$,

$$\det(C_I)^2 = \det(\Sigma(\alpha_{i_1}) \ \cdots \ \Sigma(\alpha_{i_d}))^2 = \operatorname{disc}(\boldsymbol{\alpha}_I).$$

Combining these observations with (9) completes the proof. □

3. Height functions

In this section we study some basic properties of the functions $\mathcal{D}(\boldsymbol{\alpha})$ and $\mathcal{M}(\boldsymbol{\alpha}, \beta)$ that we introduced in (5) and (6), respectively. Since we view these functions as certain measures of arithmetic complexity, it makes sense to compare them to a traditional height function on number fields.

Until further notice, let K be any number field of degree d, not necessarily totally real as above. As in (7) above, we write H_K for the inhomogeneous height on K. We can also define the absolute version of Weil height by $H(\boldsymbol{\alpha}) = H_K(\boldsymbol{\alpha})^{1/d}$: this height no longer depends on the field of definition. Let us establish some basic properties of $\mathcal{D}$ and $\mathcal{M}$ as defined in (5) and (6), respectively.

Lemma 3.1. *Let K be a number field of degree d over $\mathbb{Q}$, $n \geq d$, and let $\boldsymbol{\alpha} \in K^n$, $\beta \in K$. Then the following are true*:

(1) $\mathcal{D}(\boldsymbol{\alpha}) = 0$ *if and only if* $\operatorname{span}_{\mathbb{Q}} \boldsymbol{\alpha} \neq K$, *and* $\mathcal{M}(\boldsymbol{\alpha}, \beta) = 0$ *if and only if* $\operatorname{span}_{\mathbb{Q}} \boldsymbol{\alpha}(\beta) \neq K$.

(2) *If* $\boldsymbol{\alpha} \in \mathcal{O}_K^n$, *then either* $\mathcal{D}(\boldsymbol{\alpha}) = 0$, *or* $\mathcal{D}(\boldsymbol{\alpha}) \geq 1$; *similarly, if* $\beta \in \mathcal{O}_K$, *then either* $\mathcal{M}(\boldsymbol{\alpha}, \beta) = 0$, *or* $\mathcal{M}(\boldsymbol{\alpha}, \beta) \geq 1$. *Furthermore,* $\mathcal{D}(\boldsymbol{\alpha}), \mathcal{M}(\boldsymbol{\alpha}, \beta) \in \mathbb{Z}_{\geq 0}$.

(3) $$\mathcal{D}(\boldsymbol{\alpha}) \leq \frac{(d!)^2}{|\Delta_K|}\binom{n}{d} H_K(\boldsymbol{\alpha})^2, \quad \mathcal{M}(\boldsymbol{\alpha}, \beta) \leq \frac{d!}{|\Delta_K|^{1/2}} H_K(\boldsymbol{\alpha}) H_K(\beta).$$

Proof. To prove (1), notice that $\mathcal{D}(\boldsymbol{\alpha}) = 0$ if and only if the discriminant of every d-tuple of coordinates of $\boldsymbol{\alpha}$ is equal to 0. This happens if and only if every d-tuple of coordinates of $\boldsymbol{\alpha}$ is linearly dependent over $\mathbb{Q}$, meaning that $\operatorname{span}_{\mathbb{Q}} \boldsymbol{\alpha} \neq K$. Similarly, $\mathcal{M}(\boldsymbol{\alpha}, \beta) = 0$ if and only if the discriminant of every d-tuple of coordinates of the vector $\boldsymbol{\alpha}(\beta)$ is equal to 0, which happens if and only if $\operatorname{span}_{\mathbb{Q}} \boldsymbol{\alpha}(\beta) \neq K$.

To prove (2), assume that $\boldsymbol{\alpha} \in \mathcal{O}_K^n$ and $\mathcal{D}(\boldsymbol{\alpha}) \neq 0$. Then there exists some $I = \{i_1, \dots, i_d\} \in \mathcal{J}(n, d)$ such that $\mathrm{disc}(\boldsymbol{\alpha}_I) \neq 0$. Since coordinates of $\boldsymbol{\alpha}$ are algebraic integers, it must be true that for each $1 \leq j \leq d$

$$\alpha_{i_j} = u_{j1}\omega_1 + \cdots + u_{jd}\omega_d,$$

where $\omega_1, \dots, \omega_d$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$ and u_{jk} are integers such that the matrix $U = (u_{jk})_{1 \leq j,k \leq d}$ is nonsingular. Therefore $\mathrm{disc}(\boldsymbol{\alpha}_I) = \Delta_K \det(U)^2$, and hence

$$\mathcal{D}(\boldsymbol{\alpha}) \geq \frac{|\mathrm{disc}(\boldsymbol{\alpha}_I)|}{|\Delta_K|} = \det(U)^2 \in \mathbb{Z}_{>0}.$$

The argument for $\mathcal{M}(\boldsymbol{\alpha}, \beta)$ is analogous, replacing $\boldsymbol{\alpha}$ with $(\boldsymbol{\alpha}, \beta)$ and $\mathcal{J}(n, d)$ with $\mathcal{J}(n+1, d)$, and then observing that $\mathcal{M}(\boldsymbol{\alpha}, \beta) \geq |\mathrm{disc}(\boldsymbol{\alpha}(\beta)_I)/\Delta_K|^{1/2} \in \mathbb{Z}_{>0}$. In particular, $\mathcal{D}(\boldsymbol{\alpha}), \mathcal{M}(\boldsymbol{\alpha}, \beta) \in \mathbb{Z}_{\geq 0}$.

To prove (3), let $I = \{i_1, \dots, i_d\} \in \mathcal{J}(n, d)$ and consider the matrix

$$\Sigma(\boldsymbol{\alpha}_I) := \begin{pmatrix} \sigma_1(\alpha_{i_1}) & \cdots & \sigma_1(\alpha_{i_d}) \\ \vdots & \ddots & \vdots \\ \sigma_d(\alpha_{i_1}) & \cdots & \sigma_d(\alpha_{i_d}) \end{pmatrix}.$$

The archimedean absolute values on K are $v_1, \dots, v_d$, given by $|a|_{v_i} = |\sigma_i(a)|^{d_{v_i}}$ for each $a \in K$. Hence

$$\begin{aligned} |\mathrm{disc}(\boldsymbol{\alpha}_I)|^{1/2} = |\det(\Sigma(\boldsymbol{\alpha}_I))| &= \left| \sum_{\tau \in S_d} \mathrm{sgn}(\tau) \sigma_1(\alpha_{i_{\tau(1)}}) \cdots \sigma_d(\alpha_{i_{\tau(d)}}) \right| \\ &\leq \sum_{\tau \in S_d} |\sigma_1(\alpha_{i_{\tau(1)}})| \cdots |\sigma_d(\alpha_{i_{\tau(d)}})| \\ &\leq d! \prod_{j=1}^{d} \max\{1, |\sigma_j(\alpha_{i_1})|^{d_{v_j}}, \dots, |\sigma_j(\alpha_{i_d})|^{d_{v_j}}\} \\ &= d! \prod_{v \mid \infty} \max\{1, |\alpha_{i_1}|_v, \dots, |\alpha_{i_d}|_v\}, \end{aligned} \tag{10}$$

where $\mathrm{sgn}(\tau) = \pm 1$ is the sign of the permutation τ. Therefore

$$\begin{aligned} \mathcal{D}(\boldsymbol{\alpha}) = \frac{1}{|\Delta_K|} \sum_{I \in \mathcal{J}(n,d)} |\mathrm{disc}(\boldsymbol{\alpha}_I)| &\leq \frac{(d!)^2}{|\Delta_K|} \binom{n}{d} \left(\prod_{v \mid \infty} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\} \right)^2 \\ &\leq \frac{(d!)^2}{|\Delta_K|} \binom{n}{d} \left(\prod_{v \in M(K)} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\} \right)^2 = \frac{(d!)^2}{|\Delta_K|} \binom{n}{d} H_K(\boldsymbol{\alpha})^2. \end{aligned}$$

This gives the desired bound on $\mathcal{D}(\boldsymbol{\alpha})$ in terms of $H_K(\boldsymbol{\alpha})$. Now, in a manner completely analogous to (10), we can obtain

$$\begin{aligned} |\,\mathrm{disc}(\boldsymbol{\alpha}(\beta)_I)|^{1/2} &\leq d! \prod_{v \mid \infty} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v, |\beta|_v\} \\ &\leq d! \prod_{v \in M(K)} (\max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\} \max\{1, |\beta|_v\}) = d!\, H_K(\boldsymbol{\alpha}) H_K(\beta), \end{aligned}$$

and so

$$\mathcal{M}(\boldsymbol{\alpha}, \beta) \leq \frac{d!}{|\Delta_K|^{1/2}} H_K(\boldsymbol{\alpha}) H_K(\beta). \qquad \square$$

Part (3) of Lemma 3.1 and its proof show that $\mathcal{D}(\boldsymbol{\alpha})$ and $\mathcal{M}(\boldsymbol{\alpha}, \beta)$ measure the arithmetic complexity of $\boldsymbol{\alpha}$ and $\boldsymbol{\alpha}(\beta)$, respectively, at the archimedean places, allowing for a comparison to the more traditional height function $H_K(\boldsymbol{\alpha})$. Notice, however, that $\mathcal{D}(\boldsymbol{\alpha})$ and $\mathcal{M}(\boldsymbol{\alpha}, \beta)$ are different from traditional heights in the sense that they do not take into account information at the nonarchimedean places and do not satisfy Northcott's finiteness property, as does $H_K(\boldsymbol{\alpha})$: For each $c \in \mathbb{R}_{>0}$, the set $\{\boldsymbol{\alpha} \in K^n : H_K(\boldsymbol{\alpha}) \leq c\}$ is finite, but, say, the set $\{\boldsymbol{\alpha} \in K^n : \mathcal{D}(\boldsymbol{\alpha}) \leq c\}$ is not. Well, clearly $\mathcal{D}(\boldsymbol{\alpha}) = 0$ for any $\boldsymbol{\alpha}$ with $\operatorname{span}_{\mathbb{Q}} \boldsymbol{\alpha} \neq K$ (part (1) of Lemma 3.1 above), but even sets like

$$\{\boldsymbol{\alpha} \in (\mathcal{O}_K^+)^n : \operatorname{span}_{\mathbb{Z}} \boldsymbol{\alpha} = \mathcal{O}_K, \mathcal{D}(\boldsymbol{\alpha}) \leq c\}$$

do not have to be finite.

Example 2. Indeed, let for instance $K = \mathbb{Q}(\sqrt{2})$, $t \geq 2$ be a rational integer, and

$$\alpha_1 = 1 \in \mathcal{O}_K^+, \quad \alpha_2 = t + \sqrt{2} \in \mathcal{O}_K^+, \quad \alpha_3 = 2t + 2\sqrt{2} \in \mathcal{O}_K^+.$$

It is easy to see that $\sqrt{2} = \alpha_2 - t\alpha_1$; hence

$$\mathcal{O}_K = \operatorname{span}_{\mathbb{Z}}\{\alpha_1, \alpha_2, \alpha_3\}$$

for every t. On the other hand,

$$\mathcal{D}(\boldsymbol{\alpha}) = \tfrac{1}{8}(8 + 32 + 0) = 5,$$

also for every nonzero $t \in \mathbb{Z}$. Hence the set

$$\{\boldsymbol{\alpha} \in (\mathcal{O}_K^+)^3 : \operatorname{span}_{\mathbb{Z}} \boldsymbol{\alpha} = \mathcal{O}_K,\ \mathcal{D}(\boldsymbol{\alpha}) \leq 5\}$$

in this case is infinite.

Remark. One can think of $\mathcal{D}(\boldsymbol{\alpha})$ as Euclidean norm of the vector of Grassmann coordinates of the matrix $\Sigma(\boldsymbol{\alpha})$, normalized by the discriminant Δ_K. The transpose of such a matrix can be viewed as a basis matrix for a lattice of rank d in $\mathbb{R}^n$, and choosing any other basis for this lattice does not change the value of $\mathcal{D}(\boldsymbol{\alpha})$. Indeed, rewriting Example 2 in the notation of Section 2, we have $\Sigma(\boldsymbol{\alpha}) = C = BA$, where

$$B = (\Sigma(1)\ \ \Sigma(\sqrt{2})) = \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}, \quad A = \begin{pmatrix} 1 & t & 2t \\ 0 & 1 & 2 \end{pmatrix},$$

and so

$$A^\top = \begin{pmatrix} 1 & 0 \\ t & 1 \\ 2t & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

is a basis matrix of the lattice

$$\operatorname{span}_{\mathbb{Z}} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right\},$$

where $\left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ is just a change of basis matrix. More generally, if $\Sigma(\boldsymbol{\alpha}) = BA$ then for any matrix $U \in \mathrm{GL}_d(\mathbb{Z})$ the matrix $C = B(A^\top U)^\top = B(U^\top A)$ is equal to $\Sigma(\boldsymbol{\alpha}')$ for some $\boldsymbol{\alpha}' \in \mathcal{O}_K$ with $\mathcal{D}(\boldsymbol{\alpha}') = \mathcal{D}(\boldsymbol{\alpha})$; hence there are infinitely many such $\boldsymbol{\alpha}'$. Choosing U carefully, it is easy to construct such examples with $\boldsymbol{\alpha}' \in \mathcal{O}_K^+$. An analogous observation also applies to the function $\mathcal{M}(\boldsymbol{\alpha}, \beta)$.

The above observations in particular imply that there cannot exist a general lower bound on $\mathcal{D}(\boldsymbol{\alpha})$ in terms of $H_K(\boldsymbol{\alpha})$: if such a bound existed, we would have

$$\{\boldsymbol{\alpha} \in K^n : \mathcal{D}(\boldsymbol{\alpha}) \leq c_1\} \subseteq \{\boldsymbol{\alpha} \in K^n : H_K(\boldsymbol{\alpha}) \leq c_2\}$$

for some appropriate constants c_1, c_2. It is therefore interesting to obtain lower bounds on $\mathcal{D}(\boldsymbol{\alpha})$ besides the trivial one in part (2) of Lemma 3.1. Hence, in situations when, say, $g_1(\boldsymbol{\alpha})$ is known (with the setup of Section 1), one can conversely think of Theorem 1.1 as providing a lower bound on $\mathcal{D}(\boldsymbol{\alpha})$:

$$\mathcal{D}(\boldsymbol{\alpha}) \geq \frac{2\sqrt{n-d+1}}{n-d} g_1(\boldsymbol{\alpha}).$$

For instance, in a situation when $n = d + 1$ and $g_1(\boldsymbol{\alpha}) \geq 1$ (a rather common situation, as in Example 1, for instance), we obtain $\mathcal{D}(\boldsymbol{\alpha}) \geq 2\sqrt{2}$ (and hence $\mathcal{D}(\boldsymbol{\alpha}) \geq 4$, since it is an integer), which is already better than that of part (2) of Lemma 3.1. In fact, $g_1(\boldsymbol{\alpha}) \geq 1$ whenever $\operatorname{Sg}(\boldsymbol{\alpha}) \neq \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathcal{O}_K$, and hence we have the following immediate corollary.

Corollary 3.2. *Let the notation be as in Theorem 1.1 and assume that* $\operatorname{Sg}(\boldsymbol{\alpha}) \neq \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathcal{O}_K$. *Then*

$$\mathcal{D}(\boldsymbol{\alpha}) \geq \max\left\{1, \frac{2\sqrt{n-d+1}}{n-d}\right\}.$$

This lower bound is greater than 1 *as long as* $n \leq d + 4$.

Combining Corollary 3.2 with part (3) of Lemma 3.1, we also obtain the following lower bound on the absolute Weil height of $\boldsymbol{\alpha}$.

Corollary 3.3. *Let the notation be as in Theorem 1.1 and assume that* $\operatorname{Sg}(\boldsymbol{\alpha}) \neq \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathcal{O}_K$. *Then*

$$H(\boldsymbol{\alpha}) \geq \left(\frac{2|\Delta_K|\sqrt{n-d+1}\,(n-d-1)!}{d!\,n!}\right)^{1/(2d)}.$$

The lower bound of Corollary 3.3 is greater than 1 when $|\Delta_K|$ is large in comparison to n. For instance, in the case K is a quadratic number field and $n = 3$, we have

$$H(\boldsymbol{\alpha}) \geq \left(\frac{|\Delta_K|}{3\sqrt{2}}\right)^{1/4},$$

while $|\Delta_K|$ can be arbitrarily large (for a general totally real field, Minkowski's bound guarantees that $|\Delta_K| \geq (d^d/d!)^2$).

These observations should be viewed in light of Lehmer's problem on the lower bound for absolute Weil height of algebraic numbers and the great amount of work done in this direction (see [Mossinghoff 2011] for detailed information). Lehmer's conjecture dating back to 1933 states that there exists a constant $c > 1$ such that for every algebraic number α of degree d, $H(\alpha) > c^{1/d}$. While the conjecture is still open, there is a great number of partial results and generalizations in a variety of special cases. Our lower bound on $H(\boldsymbol{\alpha})$ for the special types of algebraic n-tuples $\boldsymbol{\alpha}$ is a small contribution in that general direction.

4. Proofs of Theorems 1.2 and 1.3

Let us start by reviewing what we may call a "positive" version of Siegel's lemma as established in [Borosh and Treybig 1976]. The name Siegel's lemma often refers to results about the size of solutions of systems of linear equations. The particular version we are interested in is concerned with nonnegative solutions to inhomogeneous integer linear systems. Let A be a $d \times n$ integer matrix such that the equation $A\boldsymbol{x} = \boldsymbol{0}$ has no nonzero solutions $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$. Let $\boldsymbol{b} \in \mathbb{Z}^d$ and let $(A\ \boldsymbol{b})$ be the augmented $d \times (n+1)$ matrix. Define

$$\mathcal{M}(A, \boldsymbol{b}) = \max\{|\det((A\ \boldsymbol{b})_I)| : I \in \mathcal{J}(n+1, d)\}.$$

Theorem 4 of [Borosh and Treybig 1976] asserts that every $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$ such that $A\boldsymbol{x} = \boldsymbol{b}$ satisfies

$$|\boldsymbol{x}| \leq \mathcal{M}(A, \boldsymbol{b}). \tag{11}$$

We now use this result to prove Theorem 1.2.

Proof of Theorem 1.2. Let $\beta \in \operatorname{Sg}(\boldsymbol{\alpha})$; then for some $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$ we have $\sum_{i=1}^n x_i \alpha_i = \beta$. This means that

$$\Sigma(\beta) = \sum_{i=1}^n x_i \Sigma(\alpha_i) = \Sigma(\boldsymbol{\alpha})\boldsymbol{x}.$$

Using the same notation as in Section 2 above, we write $C = \Sigma(\boldsymbol{\alpha}) = BA$, and so

$$\beta = C\boldsymbol{x} = BA\boldsymbol{x} = B\boldsymbol{b},$$

where $\boldsymbol{b} \in \mathbb{Z}^m$; hence $A\boldsymbol{x} = \boldsymbol{b}$. Suppose now that for some $\boldsymbol{y} \in \mathbb{Z}^n_{\geq 0}$ we have $A\boldsymbol{y} = \boldsymbol{0}$. Then

$$BA\boldsymbol{y} = C\boldsymbol{y} = \Sigma\left(\sum_{i=1}^n y_i \alpha_i\right) = \boldsymbol{0},$$

which implies that $\sum_{i=1}^n y_i \alpha_i = \boldsymbol{0}$. Since $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K^+$, this is only possible if $\boldsymbol{y} = \boldsymbol{0}$. Then every $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$ such that $A\boldsymbol{x} = \boldsymbol{b}$ satisfies (11), and for each such $\boldsymbol{x}$ we have $\beta = \sum_{i=1}^n \alpha_i x_i$. Observe also that for each $I \in \mathcal{J}(n+1, d)$,

$$|\det((A\ \boldsymbol{b})_I)| = |\det((B^{-1}C\ B^{-1}\Sigma(\beta))_I)| = \frac{|\det((\Sigma(\boldsymbol{\alpha})\ \Sigma(\beta))_I)|}{|\det(B)|} = \left|\frac{\operatorname{disc}(\boldsymbol{\alpha}(\beta)_I)}{\Delta_K}\right|^{1/2},$$

which implies that $\mathcal{M}(A, \boldsymbol{b}) = \mathcal{M}(\boldsymbol{\alpha}, \beta)$. This completes the proof of the upper bound of the theorem.

To establish the lower bound, let $\boldsymbol{\alpha} \in K^n$ and $\boldsymbol{x} \in \mathbb{Z}^n$, and let $\beta = \sum_{i=1}^n \alpha_i x_i$. We will prove

$$H_K(\beta) \leq n^d |\boldsymbol{x}|^d H_K(\boldsymbol{\alpha}). \tag{12}$$

Indeed, if $v \mid \infty$ in $M(K)$, then

$$|\beta|_v \leq \sum_{i=1}^n |\alpha_i|_v |x_i|_v \leq n|\boldsymbol{x}| \max\{|\alpha_1|_v, \dots, |\alpha_n|_v\}.$$

If $v \nmid \infty$ in $M(K)$, then

$$|\beta|_v \leq \max_{1 \leq i \leq n} |\alpha_i|_v |x_i|_v \leq \max\{|\alpha_1|_v, \dots, |\alpha_n|_v\},$$

since $\boldsymbol{x} \in \mathbb{Z}^n \subseteq \mathcal{O}_K^n$, and so $|x_i|_v \leq 1$ for every $v \nmid \infty$ and $1 \leq i \leq n$. Therefore

$$\begin{aligned} H_K(\beta) &= \prod_{v \in M(K)} \max\{1, |\beta|_v\} \\ &\leq \prod_{v|\infty} (n|\boldsymbol{x}| \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}) \times \prod_{v \nmid \infty} (\max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}) \\ &\leq n^d |\boldsymbol{x}|^d H_K(\boldsymbol{\alpha}). \end{aligned}$$

The lower bound of Theorem 1.2 now follows from (12). □

Proof of Theorem 1.3. Let $1 \leq T_1 < T_2$ be real numbers. Then for each $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$ such that $\beta = \sum_{i=1}^n \alpha_i x_i \in \mathrm{Sg}_1(\boldsymbol{\alpha}, T_1, T_2)$, by Theorem 1.2 and Lemma 3.1 we have

$$\frac{1}{n}\left(\frac{T_1}{H_K(\boldsymbol{\alpha})}\right)^{1/d} \leq \frac{1}{n}\left(\frac{H_K(\beta)}{H_K(\boldsymbol{\alpha})}\right)^{1/d} \leq |\boldsymbol{x}| \leq \mathcal{M}(\boldsymbol{\alpha}, \beta) \leq \frac{d!}{|\Delta_K|^{1/2}} H_K(\boldsymbol{\alpha}) H_K(\beta) \leq \frac{d!\, H_K(\boldsymbol{\alpha})}{|\Delta_K|^{1/2}} T_2.$$

Now, let

$$\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2) = \left\{\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0} : \frac{1}{n}\left(\frac{T_1}{H_K(\boldsymbol{\alpha})}\right)^{1/d} \leq |\boldsymbol{x}| \leq \frac{d!\, H_K(\boldsymbol{\alpha})}{|\Delta_K|^{1/2}} T_2\right\},$$

and notice that

$$|\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2)| \leq \left(\frac{d!\, H_K(\boldsymbol{\alpha})}{|\Delta_K|^{1/2}} T_2 + 1\right)^n - \left[\frac{T_1^{1/d}}{n H_K(\boldsymbol{\alpha})^{1/d}}\right]^n. \tag{13}$$

To each $\beta \in \mathrm{Sg}_1(\boldsymbol{\alpha}, T_1, T_2)$ there correspond $r(\beta)$ vectors in $\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2)$. Therefore

$$|\,\mathrm{Sg}_1(\boldsymbol{\alpha}, T_1, T_2)| \leq \sum_{\beta \in \mathrm{Sg}_1(\boldsymbol{\alpha}, T_1, T_2)} r(\beta) \leq |\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2)|. \tag{14}$$

Further, for each $\beta \in \mathrm{Sg}_s(\boldsymbol{\alpha}, T_1, T_2)$ there are at least s distinct $\boldsymbol{x}$ in the set $\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2)$, and so

$$|\,\mathrm{Sg}_s(\boldsymbol{\alpha}, T_1, T_2)| \leq \frac{1}{s} |\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2)|. \tag{15}$$

On the other hand, for $T > 1$ and each $\beta \in \mathrm{Sg}_1(\boldsymbol{\alpha}, 1, T)$ there are $r(\beta)$ points in the set

$$\left\{\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0} : |\boldsymbol{x}| \leq \frac{1}{n}\left(\frac{T}{H_K(\boldsymbol{\alpha})}\right)^{1/d}\right\},$$

and so

$$\sum_{\beta \in Sg_1(\boldsymbol{\alpha}, 1, T)} r(\beta) \geq \left[\frac{T_1^{1/d}}{n H_K(\boldsymbol{\alpha})^{1/d}}\right]^n. \tag{16}$$

The theorem now follows upon combining (13) with (14), (15) and (16). □

Acknowledgement

We thank the referee for a careful reading of our paper and helpful suggestions that improved the quality of presentation.

References

[Aliev and Gruber 2007] I. M. Aliev and P. M. Gruber, “An optimal lower bound for the Frobenius problem”, *J. Number Theory* **123**:1 (2007), 71–79. MR Zbl

[Aliev and Henk 2010] I. Aliev and M. Henk, “Feasibility of integer knapsacks”, *SIAM J. Optim.* **20**:6 (2010), 2978–2993. MR Zbl

[Aliev et al. 2012] I. Aliev, L. Fukshansky, and M. Henk, “Generalized Frobenius numbers: bounds and average behavior”, *Acta Arith.* **155**:1 (2012), 53–62. MR Zbl

[Aliev et al. 2013] I. Aliev, M. Henk, and E. Linke, “Integer points in knapsack polytopes and s-covering radius”, *Electron. J. Combin.* **20**:2 (2013), art.id. P42. MR Zbl

[Aliev et al. 2016] I. Aliev, J. A. De Loera, and Q. Louveaux, “Parametric polyhedra with at least k lattice points: their semigroup structure and the k-Frobenius problem”, pp. 753–778 in *Recent trends in combinatorics*, edited by A. Beveridge et al., IMA Vol. Math. Appl. **159**, Springer, 2016. MR Zbl

[Beck and Robins 2004] M. Beck and S. Robins, “A formula related to the Frobenius problem in two dimensions”, pp. 17–23 in *Number theory* (New York, 2003), edited by D. Chudnovsky et al., Springer, 2004. MR Zbl

[Borosh and Treybig 1976] I. Borosh and L. B. Treybig, “Bounds on positive integral solutions of linear Diophantine equations”, *Proc. Amer. Math. Soc.* **55**:2 (1976), 299–304. MR Zbl

[Cassels 1959] J. W. S. Cassels, *An introduction to the geometry of numbers*, Grundlehren der Mathematischen Wissenschaften **99**, Springer, 1959. MR Zbl

[Fukshansky and Robins 2007] L. Fukshansky and S. Robins, “Frobenius problem and the covering radius of a lattice”, *Discrete Comput. Geom.* **37**:3 (2007), 471–483. MR Zbl

[Fukshansky and Schürmann 2011] L. Fukshansky and A. Schürmann, “Bounds on generalized Frobenius numbers”, *European J. Combin.* **32**:3 (2011), 361–368. MR Zbl

[Kannan 1992] R. Kannan, “Lattice translates of a polytope and the Frobenius problem”, *Combinatorica* **12**:2 (1992), 161–177. MR Zbl

[Mossinghoff 2011] M. Mossinghoff, “Lehmer’s problem”, website, 2011, available at http://www.cecm.sfu.ca/∼mjm/Lehmer/.

[Ramírez Alfonsín 2005] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and its Applications **30**, Oxford University Press, Oxford, 2005. MR Zbl

[Widmer 2016] M. Widmer, “Integral points of fixed degree and bounded height”, *Int. Math. Res. Not.* **2016**:13 (2016), 3906–3943. MR Zbl

Received 30 Jul 2019. Revised 3 Nov 2019.

LENNY FUKSHANSKY:

lenny@cmc.edu
Department of Mathematical Sciences, Claremont McKenna College, Claremont, CA, United States

YINGQI SHI:

yshi20@students.claremontmckenna.edu
Department of Mathematical Sciences, Claremont McKenna College, Claremont, CA, United States

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

Cover design: Blake Knoll, Alex Scorpan and Silvio Levy

See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2020 is US $310/year for the electronic version, and $365/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

Moscow Journal of Combinatorics and Number Theory
vol. 9 no. 1 2020
