2020

Frobenius Problem, Geometry and Number Fields

Yingqi Shi

Claremont McKenna College

Department of Mathematical Science

Frobenius Problem, Geometry and Number Fields

an interplay between arithmetics and geometry

Thesis BA Mathematics

Author:
Yingqi Shi

Supervisor:
Dr. Lenny Fukshansky

April 2020

Thank you to my Father Jianguang Shi and my Mother Xuejuan Lu for bringing me to this fantastic world and granting me the very best part of it;

Thank you to Khenpo Sodargye for always being a role model and a leader in my life;

Thank you to Lenny Fukshansky for always hearing me nagging about graduate school application and little useless thoughts related to mathematics very patiently.

Thank you to Shiyi Liao for sharing those laughters that no one else in the universe will get except for us;

Thank you to Zhian Chen for not being a dick to me and teaching me how to be a compassionate person during my relatively chaotic youth;

Thank you to Professor Jim Kreines for encouraging me to switch gears from Philosophy and take on learning mathematics.

Acknowledgement

This project would not have been possible without the support of some of the fantastic Mathematicians in Claremont. Most importantly, many thanks to my advisor, co-author and research director Lenny Fukshansky, who taught me how to truly engage in mathematical problems (with or without vodka) through countless meetings, emails, discussions and mini-teaching lessons in his office.

Also thanks to my co-author and research director Sam Nelson, who brings me into the world of mathematics through his fashion taste, for showing me how to actively engage in research-level problems. Thanks to Professor Aksoy, whom I have the luck to be friend with, for teaching me how to search for different literatures and how to break down a large problem into smaller pieces. Thanks to Winston Ou for teaching me how to reason about given problems qualitatively and logically from scratch through those challenging problems in Fourier Analysis. Lastly thanks to Professor Henry Schellhorn, Professor Qidi Peng and Adam Olive who helped me indirectly in this project by allowing me to engage in graduate-level work and gain muscles in my reasoning.

Overview

The classical Frobenius Problem, named after a 19th century German mathematician Ferdinand Georg Frobenius, asks for the largest integer that cannot be written as a nonnegative integral combination of $\{a_1, \ldots, a_n\} \in \mathbb{Z}_{>0}$ such that $\gcd(a_1, \ldots, a_n) = 1$. This integer is called the Frobenius number of the given n-tuple. Despite having closed form solutions when $n \leq 2$, it is known to be NP-hard for general n-tuples $\{a_1, \ldots, a_n\}$ when n is not fixed. As an object of both theoretical and computational interest, the problem has been studied extensively using a variety of different techniques.

Recent work by a number of authors suggests that there exists a nice interplay between the Frobenius Problem and the field of Geometric Number Theory. In particular, R. Kannan [10] showed that the Frobenius number can be interpreted geometrically as the covering radius of an appropriate simplex with respect to a certain lattice in the Euclidean space and constructs a polynomial-time algorithm for the problem with fixed n based on his result. More recently, Beck and Robins [4] introduced a generalized s-Frobenius number, which yield a similar geometric interpretation to Kannan's, as shown in [1]. Further geometric insights into the Frobenius problem are given in [7], [8] and [2], among other works.

In this thesis, we introduce the classical Frobenius Problem, discuss some geometric aspects of it, and then extend the classical setting to the case of totally real number fields via techniques from geometric number theory. The thesis is organized in two chapter.

In the first chapter, the classical problem is formulated in Section 1.1. Then techniques from geometric number theory are introduced in Section 1.2. Finally Kannan's Lemma 1.6 which ties the problem with a geometric one is stated and re-constructed in Section 1.3. We emphasize that Kannan used Lemma 1.6 as one of his main tools to explicitly construct a polynomial-time algorithm to compute the Frobenius number for fixed n.

In the second chapter, we extend the Frobenius Problem to the higher arithmetic setting of totally real number fields. We first provide a detailed introduction to the basic theory of number fields and their rings of integers in Section 2.1; Then we move to Section 2.2 in which we discuss the geometry of number fields by studying the Minkowski embedding. After that, we outline the work done by Aliev et. al [3] in Section 2.3 which relates the generalized higher-dimensional s-Frobenius numbers with the translation of convex cones into polyhedral semi-groups in Euclidean spaces. Finally, we use the setup of [3] along with techniques from geometric number theory to define the s-Frobenius numbers in the totally real number field setting and provide a bound on it. The results on the Frobenius numbers of totally real number fields, presented in Chapter 2 of this thesis appear in [9].

Contents

1 The Classical Problem and its Geometry

1.1 The Classical Frobenius Problem

We begin our discussion by defining the classical *Frobenius Number*.

Definition 1.1. Let $a_1 < a_2 < \cdots < a_n$ be positive integers such that $\gcd(a_1, \ldots, a_n) = 1$, where $n \geq 2$. Their **Frobenius Number** $g(a_1, \ldots, a_n)$ is defined as the largest positive integer that *cannot* be expressed as $\sum_{i=1}^{n} a_i x_i$ where $x_1, \ldots, x_n$ are nonnegative integers. It is not difficult to see that the fact that $\gcd(a_1, \ldots, a_n) = 1$ guarantees that $g(a_1, \ldots, a_n)$ exists.

An explicit formula for the Frobenius number is only known when $n = 2$:

$$g(a_1, a_2) = a_1 a_2 - a_1 - a_2.$$

This formula is often attributed to J. J. Sylvester (1882). More generally, one can formulate the following algorithmic problem, know as the **Frobenius Problem**.

Problem.

Given an n-tuple $(a_1, \ldots, a_n)$ on the input, where n is arbitrary, determine $g(a_1, \ldots, a_n)$.

An excellent source of information on the Frobenius problem is Ramirez-Alfonsin's book [11]. In particular, a theorem of Ramirez-Alfonsin asserts that this problem is NP-hard. This suggests that a general simple closed-form formula for the Frobenius number is unlikely to exist, which motivates the investigation of upper and lower bounds. Some such bounds can be obtained using geometric techniques that we introduce in the next section.

Before we move on, let us also mention a natural generalization of the Frobenius number of the n-tuple $(a_1, \ldots, a_n)$. For an integer $s \geq 0$, the **s-Frobenius number** $g_s((a_1, \ldots, a_n))$ is defined to be largest positive integer that has at most s distinct representation as nonnegative integer linear combination $\sum_{i=1}^{n} a_i x_i$. Hence $g((a_1, \ldots, a_n)) = g_0((a_1, \ldots, a_n))$. The s-Frobeinus numbers were defined in [4], where an analogue of Sylvester's formula was also proved:

$$g_s(a_1, a_2) = (s+1)a_1 a_2 - a_1 - a_2.$$

Notice that in the case $s = 0$, Sylvester's formula is recovered.

1.2 Geometry of Numbers

The field of Geometry of Numbers was pioneered by Hermann Minkowski. One important problem investigated by Minkowski involved the necessary and sufficient conditions for a **compact**, **convex**, **0-symmetric** set $M \subset \mathbb{R}^n$ to contain a non-trivial integer point. Minkowski's results motivated the use of geometric techniques in number theory and have a profound influence on other areas of modern mathematics, such as cryptography, discrete and convex geometry and functional analysis.

Let $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r\}$ be a collection of linearly independent vectors in $\mathbb{R}^n$. A lattice $\mathcal{L}$ of rank r is the set of all possible integer linear combinations of this collection, called its basis, i.e.

$$\mathcal{L} = \text{span}_{\mathbb{Z}}\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r\} := \left\{ \sum_{i=1}^{r} x_i \boldsymbol{a}_i : x_i \in \mathbb{Z}, \forall 1 \leq i \leq r \right\}.$$

If we let $A = (\boldsymbol{a}_1 \ldots \boldsymbol{a}_r) \in \mathbb{R}^{m \times r}$ be the corresponding basis matrix, we can write $\mathcal{L} = A\mathbb{Z}^r$.

Example 1. Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & \sqrt{3} \end{pmatrix}$$

The planar lattice $A\mathbb{Z}^2$ is called the **hexagonal lattice**: it is pictured in Figure 1 below.

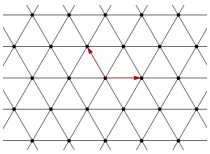

Figure 1: Hexagonal Lattice in $\mathbb{R}^2$.

A lattice has infinitely many different bases, but all of them share an important invariant.

Fact 1.2. *If A and B are two basis matrices for the same lattice $\mathcal{L}$, then:*

$$|\det(A)| = |\det(B)|.$$

We call this common value the determinant of $\mathcal{L}$, denoted $\det(\mathcal{L})$.

Now, let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice of full rank and let $M \in \mathbb{R}^n$ be a compact convex $\mathbf{0}$-symmetric set. Define the first successive minimum λ_1 of M with respect to $\mathcal{L}$ by

$$\lambda_1(M, \mathcal{L}) = min\left\{t \in \mathbb{R}_{>0} : |tM \cap \mathcal{L}| > 1\right\},$$

where $tM = \{t\boldsymbol{x} : \boldsymbol{x} \in M\}$. In other words, $\lambda_1(M, \mathcal{L})$ is the smallest real number such that the homogeneous expansion of M by a factor of λ_1 contains a nonzero point of the lattice $\mathcal{L}$. With this notation, we can state Minkowski Convex Body Theorem.

Theorem 1.3. *If* $\mathrm{Vol}(M) \geq 2^n \det(\mathcal{L})$*, then there exists* $\mathbf{0} \neq \boldsymbol{x} \in M \cap \mathcal{L}$*. Equivalently,*

$$\lambda_1(M, \mathcal{L}) \geq 2\left(\frac{\det(\mathcal{L})}{\mathrm{Vol}(M)}\right)^{1/n}.$$

Another important invariant associated with the pair M, $\mathcal{L}$ as above is the *inhomogeneous minimum* (also called *covering radius*) of M with respect to $\mathcal{L}$. It is defined as

$$\mu(M, \mathcal{L}) = min\left\{t \in \mathbb{R}_{>0} : tM + \mathcal{L} = \mathbb{R}^n\right\}.$$

In other words, $\mu(M, \mathcal{L})$ is the smallest real number such that the union of all translates by points of $\mathcal{L}$ of the homogeneous expansion of M by the factor of $\mu(M, \mathcal{L})$ covers the entire space $\mathbb{R}^n$: hence the name covering radius. Explicit bounds on the covering radius similar in flavor to the Minkowski's bound on the first successive minimum also exist, although they are somewhat harder to state, so we will not do it here.

1.3 Geometry of the Frobenius Problem

Now that we introduced some basic notation of the geometry of numbers, we can apply it to the discussion of the classical Frobenius Problem. Here we present a result of Kannan, which related the Frobenius Number to a certain covering radius. To start with, we prove an auxiliary lemma, following [10].

Lemma 1.4. *Let* $\{a_1, \ldots, a_n\}$ *be a collection of positive integers with* $\gcd(a_1, \ldots, a_n) = 1$. *Let* $g(a_1, \ldots, a_n)$ *be the Frobenius number introduced in Section 1.1. Then:*

$$g(a_1, \ldots, a_n) = max_{i \in \{1, \ldots, a_n - 1\}}\{t_i\} - a_n,$$

where t_i *is the smallest positive integer congruent to* $i \pmod{a_n}$ *that is expressible as a nonnegative integer combination of* $a_1, \ldots, a_{n-1}$.

Proof. First we note that $g = g(a_1, \ldots, a_n)$ cannot be a multiple of a_n: otherwise it would be representable by $(a_1, \ldots, a_n)$. Hence we see that $g \equiv j \pmod{a_n}$ where $1 \leq j \leq a_n - 1$. Since that t_j is the smallest positive integer congruent to j that is representable, this implies that $g + a_n \leq t_j \leq max_i\{t_i\}$;

On the other hand, note that $\forall\ 1 \leq q \leq a_{n-1}$, $t_q \leq g + a_n$, and so $max_q\{t_q\} \leq g + a_n$. Since g is the largest non-representable integer, all integers $> g$ are representable. Hence $g + k \equiv q \pmod{a_n}$ where $1 \leq k \leq a_n$. And thus we see that $t_q = g + k$. This completes the proof. □

Definition 1.5. Let

$$S = \left\{ (x_1, \ldots, x_{n-1}) \in \mathbb{R}^{n-1}_{\geq 0} : \sum_{i=1}^{n-1} a_x x_i \leq 1 \right\},$$

$$L = \left\{ (x_1, \ldots, x_{n-1}) \in \mathbb{Z}^{n-1} : \sum_{i=1}^{n-1} a_i x_i \equiv 0 \pmod{a_n} \right\}.$$

Hence S is a simplex and L is a lattice in $\mathbb{R}^{n-1}$.

We now state and prove Kannan's theorem, following [10].

Theorem 1.6.

$$\mu(S, L) = g(a_1, \ldots, a_n) + a_1 + a_2 + \cdots + a_n, \tag{1}$$

where $\mu(S, L)$ *is the covering radius of* S *with respect to* L.

Proof. Let us write $g = g(a_1, \ldots, a_n)$ and $\mu = \mu(S, L)$. We will prove (1) by establishing inequalities in both directions. First we work on the inequality

$$\mu \leq g + \sum_{i}^{n} a_n. \tag{2}$$

Let us begin by making a simple observation:

$$\forall\ t > 0, \quad tS = \left\{ (x_1, \ldots, x_{n-1}) \in \mathbb{R}^{n-1}_{\geq 0} : \sum_{i=1}^{n-1} a_i x_i \leq t \right\}.$$

To prove (2), it suffices to show that

$$\mathbb{R}^{n-1} \subseteq (g + a_1 + \cdots + a_{n-1})S + L$$

We achieve this set inclusion by claiming the following:

$$\mathbb{R}^{n-1} \subseteq \mathbb{Z}^{n-1} + (a_1 + \cdots + a_{n-1})S,$$

$$\mathbb{Z}^{n-1} \subseteq (g + a_n)S + L.$$

To prove the first of these claims, take an arbitrary $\boldsymbol{z} \in \mathbb{R}^{n-1}$ and write

$$[\boldsymbol{z}] := ([z_1], \ldots, [z_{n-1}]) \in \mathbb{Z}^{n-1},\ \{\boldsymbol{z}\} := \boldsymbol{z} - [\boldsymbol{z}] = (\{z_1\}, \ldots, \{z_{n-1}\}).$$

Then

$$\sum_{i=1}^{n-1} a_i\{z_i\} \leq \sum_{1=1}^{n-1},$$

and hence $\{\boldsymbol{z}\} \in (a_1 + \cdots + a_{n-1})S$. This means that

$$\boldsymbol{z} = [\boldsymbol{z}] + \{\boldsymbol{z}\} \in \mathbb{Z}^{n-1} + (a_1 + \cdots + a_{n-1})S.$$

To prove the second statement, fix $\boldsymbol{y} \in \mathbb{Z}^{n-1}$ and suppose that $\sum_{i=1}^{n-1} a_i y_i \equiv l \pmod{a_n}$. Find the corresponding t_l as in Lemma 1.4, then there exist $x_1, \ldots, x_{n-1} \geq 0$ such that

$$\sum_{i=1}^{n-1} a_i x_i = t_l = l + a_n x_n.$$

Let $\boldsymbol{x}' = (x_1, \ldots, x_{n-1})$ and note that for all $1 \leq i \leq n-1$, $y_i - x_i \geq 0$. Further, $\boldsymbol{y} - \boldsymbol{x}' \in L$, and

$$\boldsymbol{x}' = t_l \left(\frac{x_1}{t_l}, \ldots, \frac{x_{n-1}}{t_l} \right) \in t_l S.$$

Hence $\boldsymbol{y} = (\boldsymbol{y} - \boldsymbol{x}') + \boldsymbol{x}' \in L + t_l S$. Since that $g + a_n \geq t_l$ for all $1 \leq l \leq a_n - 1$ and the argument above works for arbitrary $\boldsymbol{y} \in \mathbb{Z}^{n-1}$ with its corresponding t_l, we see that

$$\mathbb{Z}^{n-1} \subseteq L + (g + a_n)S.$$

This completes the proof of inequality (2).

We now prove the other direction, i.e.,

$$\mu \geq g + \sum_{i}^{n} a_n. \tag{3}$$

First observe that

$$g + a_n = min\{t \in \mathbb{R}_{>0} : \mathbb{Z}^{n-1} \subseteq tS + L\}. \tag{4}$$

Indeed, suppose on the contrary that there exists $t' < g + a_n$ such that $L + t'S$ contains $\mathbb{Z}^{n-1}$. Then for any $l \in \{1, \ldots, a_n - 1\}$, pick $\boldsymbol{y} \in \mathbb{Z}^{n-1}$ such that $\sum_1^{n-1} a_i y_i \equiv l \pmod{a_n}$. Since $t'S + L$ covers $\mathbb{Z}^{n-1}$, we can select $\boldsymbol{x} \in L$ such that $\boldsymbol{y} \in t'S + \boldsymbol{x}$, so $\boldsymbol{y} - \boldsymbol{x} \in t'S$. Notice, however, that $\sum_{i=1}^{n-1} a_i(y_i - x_i) \equiv l \pmod{a_n}$. By the choice of t_l we see that $t_l \leq t'$. Since our choice for l is arbitrary, we see that $g + a_n = max\{t_l\} \leq t' < g + a_n$ by Lemma 1.4). Hence a contradiction occurs.

Hence there exists $\boldsymbol{y} \in \mathbb{Z}^{n-1}$ such that for all $\boldsymbol{x} \in L$ with $y_i - x_i \geq 0\ \forall i$,

$$\sum_{i}^{n-1} a_i(y_i - x_i) \geq g + a_n.$$

To see this, assume otherwise that $\forall\ \boldsymbol{y} \in \mathbb{Z}^{n-1}$, $\exists\ \boldsymbol{x} \in L$ with $y_i - x_i \geq 0\ \forall i$ and $\sum_i^{n-1} a_i(y_i - x_i) < g + a_n$. This directly contradicts (4).

Let $0 < \epsilon < 1$, and for the choice of $\boldsymbol{y}$ as above, define $p_i = y_i + (1 - \epsilon)$ for all $i = 1, \ldots, n-1$. Then for any $\boldsymbol{q} \in L$ such that $q_i \leq p_i\ \forall i$, we have:

$$q_i \leq p_i = y_i + (1 - \epsilon),$$

and so $q_i \leq y_i$ since all q_i are integers. Hence we see that:

$$\sum_{i=1}^{n-1} a_i(p_i - q_i) = \sum_{i=1}^{n-1} a_i(1-\epsilon) + \sum_{i=1}^{n-1} a_i(y_i - q_i) \geq (1-\epsilon)\sum_{i=1}^{n-1} a_i + (g + a_n).$$

But notice that $\mathbb{Z}^{n-1} \subseteq \mu S + L$, hence there exists $\boldsymbol{x} \in L$ such that $\sum_{i=1}^{n-1} a_i(y_i - x_i) \leq \mu$. Since $x_i \leq y_i \ \forall i$, we see that

$$\mu \geq \sum_{i=1}^{n-1} a_i(p_i - q_i) \geq (1-\epsilon)\sum_{1}^{n-1} a_i + (g + a_n).$$

Since the choice of ϵ is arbitrary, we see that

$$\mu \geq \lim_{\epsilon \to 0}(1-\epsilon)g + \sum_{i=1}^{n} a_n,$$

which proves (3). This completes the proof of the theorem. □

Kannan [10] constructed a polynomial-time algorithm to find $\mu(S, L)$ in fixed dimension n. Combining this algorithm with his Theorem 1.6 yields a polynomial time algorithm that computes $g(a_1, \ldots, a_n)$ for fixed n.

2 Frobenius Problem over Number Fields

2.1 Number Fields and Rings of Integers

In this section, we introduce the concepts of a number field K and its ring of integers $\mathcal{O}_K \subset K$. These algebraic structures are natural extensions of $\mathbb{Q}$ and $\mathbb{Z}$, respectively. We briefly review the necessary background in algebraic number theory (much of it without proof), assuming no prior knowledge of this subject. A more detailed account can be found, for instance in [6].

Definition 2.1. A complex number a is called algebraic if it is a root of some polynomial with integer coefficients. The set of all algebraic numbers is

$$\mathbb{A} = \{a \in \mathbb{C} : \exists\ f(x) \in \mathbb{Z}[x], f(a) = 0\}\,.$$

Lemma 2.2. *Let $a \in \mathbb{A}$. There exists a unique monic polynomial $f(x) \in \mathbb{Q}[x]$ of smallest degree with a as a root. This polynomial $f(x)$ is irreducible. Further, for any $h(x) \in \mathbb{Q}[x]$ such that $h(a) = 0$, $f(x) \mid h(x)$.*

Proof. Since $a \in \mathbb{A}$, there must exist some $g(x) \in \mathbb{Z}[x]$ such that $g(a) = 0$. We can select a nonzero $g(x)$ like this of smallest degree, say

$$g(x) = a_n x^n + \cdots + a_1 x + a_0$$

with $a_n \neq 0$. The take $f(x) = \frac{1}{a_n} g(x) \in \mathbb{Q}[x]$, and so $f(a) = 0$. Suppose that $f_1(x), f_2(x) \in \mathbb{Q}[x]$ are both monic polynomials of minimal possible degree n such that $f_1(a) = f_2(a) = 0$. Let $h(x) = f_1(x) - f_2(x)$, then degree of $h(x)$ is $\leq n - 1$, and $h(a) = 0$. This implies that $h(x)$ must be identically 0, and so $f_1(x) = f_2(x)$.

Suppose $f(x)$ is reducible, say $f(x) = g_1(x)g_2(x)$ for some two non-constant polynomials $g_1(x), g_2(x) \in \mathbb{Q}[x]$. The degrees of $g_1(x)$ and $g_2(x)$ are $< n = \deg(f)$. Since $f(a) = 0$, it must be true $g_1(a) = 0$ or $g_2(a) = 0$, but this contradicts minimality of $f(x)$.

Finally, suppose $h(a) = 0$ for some $h(x) \in \mathbb{Q}[x]$. By Euclidean division lemma in $\mathbb{Q}[x]$, there exist $q(x), r(x) \in \mathbb{Q}[X]$ with $\deg(r) < n$ such that

$$h(x) = q(x)f(x) + r(x).$$

Then $r(a) = h(a) - q(a)f(a) = 0$, and so $r(x)$ must be identically 0 by minimality of $f(x)$. Therefore $f(x) \mid h(x)$. □

Definition 2.3. Give $a \in \mathbb{A}$, the polynomial $f(x)$ as in Lemma 2.2 is called its minimal polynomial (over $\mathbb{Q}$), denoted $m_a(x)$. The degree n of $m_a(x)$ is called the degree of the algebraic number a.

Fact 2.4. *The set $\mathbb{A}$ is a countable subset of $\mathbb{C}$. It is a field under the addition and multiplication operations on $\mathbb{C}$.*

Definition 2.5. Let $a \in \mathbb{A}$. We write $\mathbb{Q}(a)$ for the smallest subfield of $\mathbb{A}$ (with respect to inclusion) containing both $\mathbb{Q}$ and a. In particular, $\mathbb{Q}(a)$ consists of all quotients $\frac{p(a)}{q(a)}$ where $p(x), q(x) \in \mathbb{Q}[x]$, such that $q(a) \neq 0$.

Fact 2.6. *Let $a \in \mathbb{A}$ have degree n. Define*

$$\mathbb{Q}[a] := \left\{ \sum_{k=0}^{n-1} c_k a^k : c_0, \ldots, c_{n-1} \in \mathbb{Q} \right\}.$$

Then $\mathbb{Q}[a]$ is an n-dimensional $\mathbb{Q}$-vector space with $1, a, \ldots, a^{n-1}$ for its basis.

While we do not give a formal proof of this fact here, it is not difficult to see: the algebraic numbers $1, a, \ldots, a^{n-1}$ must be linearly independent over $\mathbb{Q}$, since otherwise a would be a root of a rational polynomial of degree less than n.

Lemma 2.7. *Let $a \in \mathbb{A}$, then $\mathbb{Q}(a) = \mathbb{Q}[a]$.*

Proof. It is clear that $\mathbb{Q}[a] \subseteq \mathbb{Q}(a)$. Hence we only need to show that $\mathbb{Q}(a) \subseteq \mathbb{Q}[a]$. Clearly, $\mathbb{Q}[a]$ contains $\mathbb{Q}$ and a. We will show that it is a field: this will imply that $\mathbb{Q}(a)$ must be contained in $\mathbb{Q}[a]$ by minimality of $\mathbb{Q}(a)$.

Notice that $\mathbb{Q}[a]$ is closed under addition, since it is a vector space. Let

$$m_a(x) = x^n + \sum_{k=0}^{n-1} u_k x^k \in \mathbb{Q}[x]$$

be the minimal polynomial of a, then $m_a(a) = 0$, i.e.

$$a^n = -\sum_{k=0}^{n-1} u_k x^k. \tag{5}$$

Let

$$p(a) = \sum_{k=0}^{n-1} b_k a^k,\ q(a) = \sum_{k=0}^{n-1} c_k a^k \in \mathbb{Q}[a],$$

then $p(a)q(a)$ can also be expressed as a linear combination of $1, \ldots, a^{n-1}$ with rational coefficients, using (5). Hence $\mathbb{Q}[a]$ is closed under multiplications. Further for any $0 \neq p(a) \in \mathbb{Q}[a]$ as above, $\frac{1}{p(a)}$ can be written as a polynomial expression of a with coefficients in $\mathbb{Q}$. Indeed, let $p(x) \in \mathbb{Q}[x]$ be the polynomial corresponding to $p(a)$. Since $p(a) \neq 0$, $m_a(x) \nmid p(x)$. Since $m_a(x)$ is irreducible, the polynomial $\gcd(p(x), m_a(x))$ must be equal to 1. Euclidean algorithm in $\mathbb{Q}[x]$ then guarantees the existence of $s(x), t(x) \in \mathbb{Q}[x]$ such that:

$$s(x)p(x) + t(x)m_a(x) = 1.$$

In particular, $s(a)p(a) = 1$, which implies that $s(a) = \frac{1}{p(a)}$. This proves that every nonzero element in $\mathbb{Q}[a]$ has a multiplicative inverse, and so $\mathbb{Q}[a]$ is a field. □

Definition 2.8. If K is a subfield of $\mathbb{C}$ containing $\mathbb{Q}$, then K is called an extension field of $\mathbb{Q}$. Since every such extension field can be viewed as a $\mathbb{Q}$-vector space, we define the degree of K over $\mathbb{Q}$, denoted $[K : \mathbb{Q}]$ to be the dimension of K as a $\mathbb{Q}$-vector space. Extensions of $\mathbb{Q}$ of finite degree are called number fields.

Lemma 2.9. *Let $a \in \mathbb{C}$. Then $a \in \mathbb{A}$ if and only if $[\mathbb{Q}(a) : \mathbb{Q}] < \infty$.*

Proof. ($\rightarrow$) Suppose that $a \in \mathbb{A}$, then $\mathbb{Q}(a) = \mathbb{Q}[a]$, which is an n-dimensional $\mathbb{Q}$-vector space, where $n = \deg(a)$.

($\leftarrow$) Suppose that $[\mathbb{Q}(a) : \mathbb{Q}] = n$ is finite. Then the collection $\{1, a, a^2, a^3, \ldots, a^n\}$ must be linearly dependent, since it has cardinality larger than a basis. This implies that:

$$0 = \sum_{j=0}^{n} q_j a^j,$$

where $q_0, \ldots, q_n \in \mathbb{Q}$, not all 0. Let d be the common denominator of these coefficients, then a is a zero of the polynomial $\sum_{j=0}^{n} dq_j x^j$ with integer coefficients, and so $a \in \mathbb{A}$. □

Corollary 2.9.1. *Let K be a number field, then $K \subset \mathbb{A}$.*

Proof. Pick an arbitrary $a \in K$, then $\mathbb{Q}(a) \subseteq K$. Hence

$$[\mathbb{Q}(a) : \mathbb{Q}] \leq [K : \mathbb{Q}] < \infty.$$

Hence $a \in \mathbb{A}$ by Lemma 2.9. □

In fact, every number field K has a generating element. The proof of this observation is nontrivial and readers can refer to [6] for a more complete discussion.

Theorem 2.10 (Primitive Element Theorem). *Let K be a number field, then there exists $a \in K$ such that $K = \mathbb{Q}(a)$.*

Now that we have a basic understanding of K, we are going to study a special ring that lives inside K, often known as its *ring of algebraic integers*. Again we begin by some basic definitions.

Definition 2.11. An algebraic number $a \in \mathbb{A}$ is called an algebraic integer if its minimal polynomial $m_a(x)$ has integer coefficients. Write

$$\mathbb{I} := \{a \in \mathbb{A} : m_a(x) \in \mathbb{Z}[x]\}$$

for the set of all algebraic integers.

A nontrivial fact that we will not prove here is that $\mathbb{I}$ is a ring under the usual addition and multiplication of complex numbers, hence it is a subring of $\mathbb{A}$. Given a number field K, we can then define

$$\mathcal{O}_K := K \cap \mathbb{I},$$

i.e. the set of all algebraic integers in K. Since $\mathcal{O}_K$ is an intersection of two subrings of $\mathbb{A}$, it is also a ring: it is called the ring of algebraic integers of K.

Lemma 2.12. *The ring of algebraic integers of $\mathbb{Q}$ is $\mathbb{Z}$, i.e.*

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Q} \cap \mathbb{I} = \mathbb{Z}.$$

Proof. Notice that $a \in \mathbb{Z}$ is a zero of the polynomial $x - a \in \mathbb{Z}[x]$, hence $\mathbb{Z} \subseteq \mathcal{O}_{\mathbb{Q}}$. On the other hand, let $a \in \mathcal{O}_{\mathbb{Q}}$, then $a = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$ with $\gcd(p, q) = 1$ such that

$$c_0 + c_1 \frac{p}{q} + \ldots.. + \frac{p^n}{q^n} = 0,$$

where n is the degree of a. Then

$$q^n z_0 + q^{n-1} p + \cdots + p^n = 0,$$

and so $p^n \equiv 0 \pmod{q}$. Since $\gcd(p, q) = 1$, we must have $q = 1$, and hence $a \in \mathbb{Z}$. □

We therefore refer to elements of $\mathbb{Z}$ as rational integers. It is easy to see that in fact $\mathbb{Z}$ is contained in $\mathcal{O}_K$ for any number field K.

Definition 2.13 (embedding). Let K be a number field. An embedding of K is an injective homomorphism $\sigma : K \hookrightarrow \mathbb{C}$.

If $a \in K$ is its primitive element, i.e. $K = \mathbb{Q}(a)$, then the degree $[K : \mathbb{Q}]$ is equal to the degree of a, i.e. the degree of its minimal polynomial $m_a(x)$, let this degree be d. Let

$$a = a_1, \ldots, a_d \in \mathbb{C}$$

be all the roots of $m_a(x)$ – they are called the algebraic conjugates of a. Then any homomorphism must take a to one of its algebraic conjugates, and so there are d embeddings of K into $\mathbb{C}$, given by $\sigma_k(a) = a_k$. Since every element of K is a $\mathbb{Q}$-linear combination of powers of a, these maps uniquely extend to homomorphisms.

Definition 2.14 (Discriminant Δ). Let $\alpha_1, \ldots, \alpha_d \in K$ be a $\mathbb{Q}$-basis of K, then define

$$\Delta(\alpha_1, \ldots, \alpha_d) := \det\{(\sigma_n(a_k))_{1 \le n,k \le d}\}^2.$$

Fact 2.15. *Let $\alpha_1, \ldots, \alpha_d \in K$ be a $\mathbb{Q}$-basis, then:*

$$\Delta(\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}$$

Further if $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$, then

$$\Delta(\alpha_1, \ldots, \alpha_d) \in \mathbb{Z}$$

One essential property of $\mathcal{O}_K$ is that it is a lattice.

Theorem 2.16. *Let K be a number field of degree d over $\mathbb{Q}$. Then $\mathcal{O}_K$ is a lattice of rank d, i.e. there exists a collection of $\mathbb{Q}$-linearly independent elements $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$ such that*

$$\mathcal{O}_K = \left\{ \sum_{k=1}^{d} c_k \alpha_k : c_1, \ldots, c_d \in \mathbb{Z} \right\}.$$

Further, if $\{\alpha_1, \ldots, \alpha_d\} \in \mathcal{O}_K$ and $\{\beta_1, \ldots, \beta_d\} \in \mathcal{O}_K$ are two $\mathbb{Z}$-bases for $\mathcal{O}_K$, then

$$\Delta(\alpha_1, \ldots, \alpha_d) = \Delta(\beta_1, \ldots, \beta_d).$$

This common value is called the discriminant of K, denoted Δ_K: it is an important invariant of the number field.

2.2 Geometry of Number Fields

In this section, we outline a canonical way to embed the lattice $\mathcal{O}_K$ into a finite-dimensional Euclidean space, making it into a Euclidean lattice. This method is called *Minkowski embedding*, and is given by the field embeddings discussed in the previous section. Let K be a number field of degree d over $\mathbb{Q}$, and let $\sigma_1, \ldots, \alpha_d$ be the embeddings of K into $\mathbb{C}$. We distinguish between *real* and *complex* embeddings: σ_i is said to be real if $\sigma_i(K) \subset \mathbb{R}$, and complex otherwise. Note that complex embeddings come in conjugate pairs: if σ_i is complex, then there is $\bar{\sigma}_i(x) := \overline{\sigma_i(x)}$. We order the embeddings as

$$\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \bar{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+s},$$

where the first r are real and the remaining s pairs are complex conjugates, so $r+2s = d$.

Definition 2.17. With the notations as above, define a map

$$\Sigma := (\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots, \sigma_{r+s}) : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$$

where $\Sigma(x) = (\sigma_1(x), \ldots, \sigma_r(x), \ldots, \sigma_{r+s}(x))$ for all $x \in K$.

Under this Minkowski embedding Σ, the ring $\mathcal{O}_K$ becomes a lattices of full rank in the Euclidean space $\mathbb{R}^r \times \mathbb{C}^s$. The determinant of this lattice is then

$$\det\left(\Sigma(\mathcal{O}_K)\right) = 2^{-s} |\Delta_K|^{1/2}.$$

Minkowski embedding often allows to restate arithmetic questions geometrically, and vice versa. This general principle will be important to us.

2.3 Polyhedral Semigroups

Let A be a $d \times n$ integer matrix, where $n \geq d \geq 1$. Define $\mathcal{J}(n,d)$ to be the set of all cardinality d subsets of the indexing set $\{1,\ldots,n\}$. For each $I \in \mathcal{J}(n,d)$, let A_I be the $d \times d$ submatrix of A consisting of columns indexed by I. Further, assume that:

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

Define the additive semigroup:

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

More generally, for each $s \geq 1$, let

$$Sg_s(A) = \{\boldsymbol{b} \in Sg(A) : \exists\ \boldsymbol{x}_1,\ldots,\boldsymbol{x}_s \in \mathbb{Z}^n_{\geq 0} \text{ such that } \boldsymbol{b} = A\boldsymbol{x}_i\},$$

so $Sg(A) = Sg_1(A)$. Define the convex polyhedral cone spanned by the column vectors of A:

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

It is clear that

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

and this containment is often proper, i.e. in general $Sg(A) \neq \mathcal{C}_{\mathbb{R}}(A) \cap \mathbb{Z}^d$. Now write $\text{int}(\mathcal{C}_{\mathbb{R}}(A))$ for the interior of this cone. Then $\forall \boldsymbol{b} \in \text{int}(\mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d$, define

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

With this notation, we define

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

We refer to $g_s(A)$ as the s-Frobenius number of A.

To understand the generalization $g_s(A)$ properly, let us see how the case $d = s = 1$ recovers the classical Frobenius number outlined in Section 1.1. In this case

$$\text{int}(\mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d = \mathbb{Z}_{>0},$$

where $A = [a_1,\ldots,a_n]^T = \{a_1,\ldots,a_n\} \in \mathbb{Z}^n_{>0}$. Then for every $b \in \mathbb{Z}_{>0}$, $g_s(A,b)$ computes the minimum multiple of b for which the translated set $tb + \mathbb{Z}_{>0} \subseteq Sg(A)$. This is precisely the minimum integral multiple of b such that every integer greater than it is representable by the set $\{a_1,\ldots,a_n\}$. Then

$$g(A) = max\{g(A,b) : \beta \in \text{int}(\mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}\} = g(A,1),$$

which is precisely the smallest positive integer after which every integer is representable as a nonnegative integral combination of $\{a_1,\ldots,a_n\}$. The two conditions

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

then translate as

$$\gcd(a_1,\ldots,a_d) = 1,\ \{a_1,\ldots,a_n\} \in \mathbb{Z}^n_{>0}.$$

And thereby the classical Frobenius number is indeed recovered.

This higher-dimensional generalization of the Frobenius problem was introduced in [3], where the following bound was obtained.

Theorem 2.18. *With notation as above,*

$$g_s(A) \leq \frac{1}{2\sqrt{n-d+1}} \left((n-d)\det(AA^T) + (s-1)^{\frac{1}{n-d}} \det(AA^T)^{\frac{n-d+1}{2(n-d)}}\right).$$

2.4 Frobenius Number Over Totally Real Number Fields

We can now apply the geometric setup of Section 2.3 to formulate a Frobenius-type problem in a certain number field setting. The essential conditions for the Frobenius Problem for the n-tuple $a_1, \ldots, a_n \in \mathbb{Z}$ are:

1. $\gcd(a_1, \ldots., a_n) = 1$,
2. $\forall i, a_i \geq 0$.

We need to generalize these in $\mathcal{O}_K$, where the notion of gcd do not necessarily exist. To retain the ability of using the ordering $\geq$, we restrict to totally real number fields.

Definition 2.19. A number field K of degree d is called *totally real* if $\sigma_i(K) \subset \mathbb{R}$ for all of its embeddings $\sigma_1, \ldots, \sigma_d$. If this is the case, define the semigroup of *totally positive* algebraic integers in K as

$$\mathcal{O}_K^+ := \{a \in \mathcal{O}_k : \sigma_i(a) \geq 0 \ \forall \ 1 \leq i \leq d\}.$$

From here on, we always assume that K is totally real and use the above notation.

Lemma 2.20. *There exists a basis $a_1, \ldots, a_d$ for $\mathcal{O}_K$ contained in $\mathcal{O}_K^+$.*

Proof. Let $w_1, \ldots w_d \in \mathcal{O}_K$ be a basis for $\mathcal{O}_K$ with $w_1 = 1$. Define

$$M := max_{1 \leq i,j \leq d} |\sigma_i(w_j)| + 1.$$

Let $a_1 = 1$ and for every $2 \leq i \leq d$, let $a_i = w_i + M$. Then $a_1, \ldots, a_d \in \mathcal{O}_K^+$ is still a basis for $\mathcal{O}_K$. □

From here on, we always assume that $n \geq d \geq 1$ and $\boldsymbol{\alpha} = (a_1, \ldots, a_n) \in (\mathcal{O}_K^+)^n$ is such that $\mathcal{O}_K = \text{span}_{\mathbb{Z}}\{a_1, \ldots, a_n\}$. Define the semi-group generated by $\boldsymbol{\alpha}$ as

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

and the rational cone generated by $\boldsymbol{\alpha}$ as

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

It is clear that $Sg(\boldsymbol{\alpha}) \subseteq \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathcal{O}_K^+ \subseteq \mathcal{O}_K^+$. However, it is not always the case that $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathcal{O}_K^+ \subseteq Sg(\boldsymbol{\alpha})$. Let us provide a concrete example. Take the real quadratic number field $K = \mathcal{O}(\sqrt{2})$ and let

$$a_1 = 1, a_2 = 4 + \sqrt{2}, a_3 = 6 + 2\sqrt{2}.$$

Then $\boldsymbol{\alpha} := (a_1, a_2, a_3) \in (\mathcal{O}_K^+)^3$,

$$\mathcal{O}_K = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} = \{(a - 4b)a_1 + ba_2 : a, b \in \mathbb{Z}\},$$

and

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

On the other hand, $3 + \sqrt{2} = \frac{1}{2}a_3 \in \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathcal{O}_K$, but it is clearly not in $Sg(\boldsymbol{\alpha})$. See Figure 2.4 for a more visual introduction. In this example, the set of red dots represent O_K, green dots represent $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})$, and blue dots represent $Sg(\boldsymbol{\alpha})$. We can see that in the

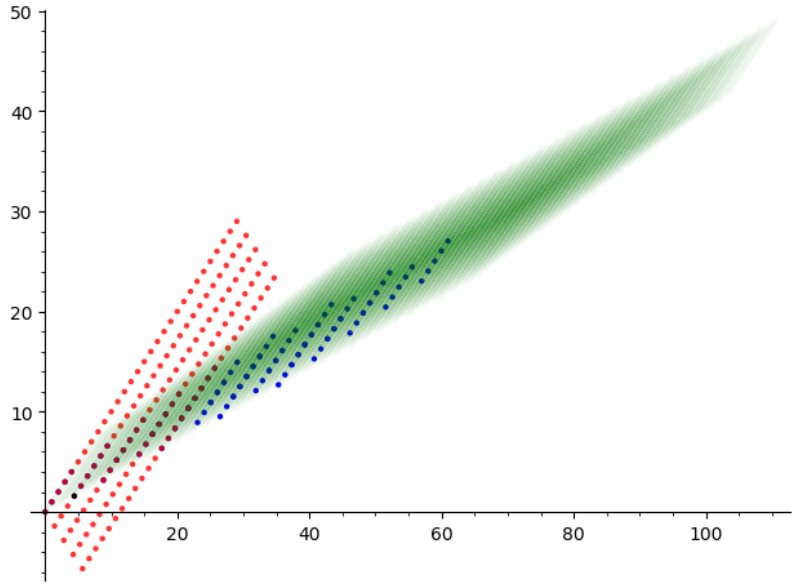

Figure 2: Visual Example of Cone-Translation

diagram, the intersection of the red and green dots (purple dots) represent $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})\cap\mathcal{O}_K$. Notice that a majority of purple dots overlap with the blue ones, yet in the bottom left corner there is a black dot corresponding to $3+\sqrt{2}$ that overlaps with the purple set, but is not included in the blue set. Now that we have described the geometric setup, we can introduce the Frobenius number in this setting.

Definition 2.21 (Extension $Sg_s(\boldsymbol{\alpha})$). For $s \geq 1$, define $Sg_s(\boldsymbol{\alpha})$ to be the set of all points $\beta \in Sg(\boldsymbol{\alpha})$ for which there are at least s distinct points $\boldsymbol{x} \in \mathbb{Z}^n_{\geq 0}$ such that $\sum_{i=1}^n a_i x_i = \beta$.

Take $\beta \in \mathcal{O}_K^+$ to 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 $Sg(\boldsymbol{\alpha})$ (see Theorem 2.23 below). In other words, there exists a positive integer t such that

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

Define

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

and let

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

We call the quantity $g_s(\boldsymbol{\alpha})$ the *s-Frobenius number* of $\boldsymbol{\alpha}$. We first demonstrate that this s-Frobenius number is an intrinsic generalization of the classical one, i.e., setting $K = \mathbb{Q}$ and $s = 1$ we indeed recover the classical Frobenius number.

Lemma 2.22. *Set $K = \mathbb{Q}$, then $g_1(\boldsymbol{\alpha})$ equals the classical Frobenius number.*

Proof. Suppose that $K = \mathbb{Q}$, then $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_K^+ = \mathbb{Z}_{\geq 0}$. Let $a_1, \ldots, a_n \in \mathbb{Z}_{>0}$, then $\text{span}_{\mathbb{Z}}\{a_1, \ldots, a_n\} = \mathbb{Z}$ is equivalent to saying that $\gcd(a_1, \ldots, a_n) = 1$. Then we see that $Sg(\boldsymbol{\alpha})$ is the semigroup of all positive integers representable by $\boldsymbol{\alpha}$, $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) = \mathbb{Q}_{\geq 0}$ and so we have $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})\cap\mathbb{Z}_{\geq 0} = \mathbb{Z}_{\geq 0}$. Then we see that

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

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

is precisely the smallest integer t so that all integers $> t$ are representable by $\boldsymbol{\alpha}$. □

Our main result is an upper bound on $g_s(\boldsymbol{\alpha})$, which we present here as in [9]. Before we can state and prove it, we need to introduce a certain measure of arithmetic complexity of $\boldsymbol{\alpha}$. For each subset indexing subset $I = \{i_1, \ldots, i_d\} \in \mathcal{J}(n, d)$ let $\boldsymbol{\alpha}_I$ be the d-tuple of coordinates of $\boldsymbol{\alpha}$ indexed by I. Let

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

where $\Delta(\boldsymbol{\alpha}_I)$ is the discriminant of the d-tuple of algebraic numbers $\boldsymbol{\alpha}_I$, as defined above. Finally, recall from linear algebra that if a system of homogeneous linear equations with integer coefficients has a positive real solution, then it also has a positive integer solution. We now state and prove our bound, directly following the exposition of our paper [9].

Theorem 2.23. *With notation as above,*

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

Proof. Let $\boldsymbol{\alpha} = (a_1, \ldots, a_n) \in (\mathcal{O}_K^+)^n$ be as above, and let us fix $\omega_1, \ldots, \omega_d$, 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

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

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

$$B = \begin{pmatrix} \Sigma(\omega_1) & \ldots & \Sigma(\omega_d) \end{pmatrix},$$

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

$$C := \begin{pmatrix} \Sigma(\alpha_1) & \ldots & \Sigma(\alpha_n) \end{pmatrix} = BA.$$

Since $\alpha_1, \ldots, \alpha_n$ span $\mathcal{O}_K$, 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 [5], 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 $A\boldsymbol{x} = \mathbf{0}$. Then

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

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 $\mathbf{0}$, and so

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

Thus matrix A satisfies conditions (1) and (2) in Section 2.3, and so we can apply Theorem 2.18 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

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

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:

$$\begin{aligned} & \operatorname{int}\left(t\beta + \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})\right) \cap \mathcal{O}_K \subseteq Sg_s(\boldsymbol{\alpha}) \\ \iff & \operatorname{int}\left(tB\boldsymbol{b} + B\mathcal{C}_{\mathbb{Q}}(A)\right) \cap B\mathbb{Z}^d \subseteq BSg_s(A) \\ \iff & \operatorname{int}\left(t\boldsymbol{b} + \mathcal{C}_{\mathbb{R}}(A)\right) \cap \mathbb{Z}^d \subseteq Sg_s(A). \end{aligned}$$

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

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

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 $I = \{i_1, \ldots, i_d\}$,

$$\det(C_I)^2 = \det\begin{pmatrix}\Sigma(\alpha_{i_1}) & \ldots & \Sigma(\alpha_{i_d})\end{pmatrix}^2 = \Delta(\boldsymbol{\alpha}_I).$$

Combining these observations with Theorem 2.18 completes the proof. □

References

[1] I. Aliev, L. Fukshansky, and M. Henk. Generalized Frobenius numbers: bounds and average behavior. *Acta Arith.*, 155:53–63, 2012.

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

[3] I. Aliev, J. De Loera, and Q. Louveaux. Parametric polyhedra with at least k lattice points: their semigroup structure and the k-Frobenius problem. In *Recent trends in combinatorics, IMA Vol. Math. Appl., 159*, pages 753–778. Springer, 2016.

[4] M. Beck and S. Robins. A formula related to the Frobenius problem in two dimensions. *Number theory (New York, 2003), Springer, New York*, pages 17–23, 2004.

[5] J. W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer-Verlag, 1959.

[6] L. Fukshansky. Geometric number theory, lecture notes. `https://www1.cmc.edu/pages/faculty/lenny/classes/spring_2019/m195/GNT_lecture-notes.pdf`, 2019.

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

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

[9] 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.

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

[11] J. L. Ramírez Alfonsín. *The Diophantine Frobenius problem*. Oxford University Press, 2005.