1-1-2007

Frobenius Problem and the Covering Radius of a Lattice

Lenny Fukshansky
Claremont McKenna College

Sinai Robins
Nanyang Technological University

FROBENIUS PROBLEM AND THE COVERING RADIUS OF A LATTICE

LENNY FUKSHANSKY AND SINAI ROBINS

Abstract. Let $N \geq 2$ and let $1 < a_1 < \cdots < a_N$ be relatively prime integers. Frobenius number of this N-tuple is defined to be the largest positive integer that cannot be expressed as $\sum_{i=1}^{N} a_i x_i$ where $x_1, ..., x_N$ are non-negative integers. The condition that $gcd(a_1, ..., a_N) = 1$ implies that such number exists. The general problem of determining the Frobenius number given N and $a_1, ..., a_N$ is NP-hard, but there has been a number of different bounds on the Frobenius number produced by various authors. We use techniques from the geometry of numbers to produce a new bound, relating Frobenius number to the covering radius of the null-lattice of this N-tuple. Our bound is particularly interesting in the case when this lattice has equal successive minima, which, as we prove, happens infinitely often.

1. Introduction

Let $N \geq 2$ be an integer and let $a_1, ..., a_N$ be positive relatively prime integers. Define the *Frobenius number* $\mathcal{F} = \mathcal{F}(a_1, ..., a_N)$ of this N-tuple to be the largest positive integer that cannot be expressed as $\sum_{i=1}^{N} a_i x_i$ where $x_1, ..., x_N$ are non-negative integers. The condition that $gcd(a_1, ..., a_N) = 1$ implies that such $\mathcal{F}$ exists. The general problem of determining the Frobenius number given N and $a_1, ..., a_N$ is NP-hard. For each fixed N, however, it is possible to give a polynomial time algorithm for finding the Frobenius number of a given N-tuple (see [13]). Since there can be no explicit formula for the Frobenius number, it is interesting to produce upper bounds for it. A large amount of work has been done on this problem. The case of $N = 2$ is the only one where an explicit formula, known most likely to Sylvester [15], is available:

$$\mathcal{F}(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1. \tag{1}$$

In a more general case $N \geq 3$, the bounds on the Frobenius number in the literature are vast. Among many others, they include results by Beck, Diaz, and Robins [4] produced with the use of bounds on Fourier-Dedekind sums:

$$\mathcal{F} \leq \frac{1}{2}\left(\sqrt{a_1 a_2 a_3 (a_1 + a_2 + a_3)} - a_1 - a_2 - a_3\right), \tag{2}$$

as well as earlier results by Erdös and Graham [7]

$$\mathcal{F} \leq 2a_N \left[\frac{a_1}{N}\right] - a_1, \tag{3}$$

1991 *Mathematics Subject Classification.* 11D04, 11H06, 52C07.

Key words and phrases. linear Diophantine problem of Frobenius, geometry of numbers, lattices.

by Selmer [14]

$$\mathcal{F} \leq 2a_{N-1}\left[\frac{a_N}{N}\right] - a_N, \tag{4}$$

and by Vitek [16]

$$\mathcal{F} \leq \left[\frac{(a_2-1)(a_N-2)}{2}\right] - 1, \tag{5}$$

where [ ] denotes integer part function. See [4] for further bibliography. For comparison, here is a lower bound on $\mathcal{F}$ by Aliev and Gruber [1]:

$$\mathcal{F} > ((N-1)!\, a_1 \dots a_N)^{\frac{1}{N-1}} - \sum_{i=1}^{N} a_i. \tag{6}$$

See [1] for more information on lower bounds. The objective of this paper is to produce new upper bounds for the Frobenius number when $N \geq 3$.

In [13], Kannan relates the Frobenius number $\mathcal{F}$ to the covering radius of a certain convex body with respect to a certain lattice. More precisely, let

$$\mathcal{L} = \left\{ \boldsymbol{x} \in \mathbb{Z}^{N-1} : \sum_{i=1}^{N-1} a_i x_i \equiv 0 \pmod{a_N} \right\},$$

and define

$$\mathcal{S} = \left\{ \boldsymbol{x} \in \mathbb{R}^{N-1}_{\geq 0} : \sum_{i=1}^{N-1} a_i x_i \leq 1 \right\}.$$

Then Theorem 2.5 of [13] states that

$$\mathcal{F} = \mu(\mathcal{S}, \mathcal{L}) - \sum_{i=1}^{N} a_i. \tag{7}$$

where $\mu(\mathcal{S}, \mathcal{L})$ is the *covering radius* (also known as the *inhomogeneous minimum*) of $\mathcal{S}$ with respect to $\mathcal{L}$, namely

$$\mu(\mathcal{S}, \mathcal{L}) = \inf\left\{ t \in \mathbb{R}_{>0} : t\mathcal{S} + \mathcal{L} = \mathbb{R}^{N-1} \right\}. \tag{8}$$

Identity (7) then suggests that one could produce bounds on $\mathcal{F}$ by bounding $\mu(\mathcal{S}, \mathcal{L})$. This, however, appears difficult, since the standard techniques for bounding a covering radius only work in the case when the convex body is symmetric with respect to the origin, which is clearly not the case here.

Our approach relates the Frobenius number to a covering radius of a Euclidean ball with respect to a different lattice, which is much easier to estimate. Let $\boldsymbol{a} = (a_1, ..., a_N) \in \mathbb{Z}^N_{\geq 0}$, with $2 \leq a_1 < a_2 < \cdots < a_N$ relatively prime, as above. Let

$$L_{\boldsymbol{a}}(\boldsymbol{X}) = \sum_{i=1}^{N} a_i X_i,$$

be the linear form in N variables with coefficients $a_1, ..., a_N$, and define the lattice

$$\Lambda_{\boldsymbol{a}} = \left\{ \boldsymbol{x} \in \mathbb{Z}^N : L_{\boldsymbol{a}}(\boldsymbol{x}) = 0 \right\}.$$

Let $V_{\boldsymbol{a}} = \operatorname{span}_{\mathbb{R}} \Lambda_{\boldsymbol{a}}$, then $V_{\boldsymbol{a}}$ is an $(N-1)$-dimensional subspace of $\mathbb{R}^N$ and $\Lambda_{\boldsymbol{a}} = V_{\boldsymbol{a}} \cap \mathbb{Z}^N$ is a lattice of full rank in $V_{\boldsymbol{a}}$. Let $B(R)$ be the $(N-1)$-dimensional

closed ball of radius $R > 0$ centered at the origin in $V_{\boldsymbol{a}}$. Then $\mathrm{Vol}_{N-1}(B(R)) = \omega_{N-1}R^{N-1}$, where

$$\omega_{N-1} = \mathrm{Vol}_{N-1}(B(1)) = \frac{\pi^{\frac{N-1}{2}}}{\Gamma\left(\frac{N+1}{2}\right)}. \tag{9}$$

Define the covering radius of the lattice $\Lambda_{\boldsymbol{a}}$ to be

$$R_{\boldsymbol{a}} = \inf\left\{R \in \mathbb{R}_{>0} : B(R) + \Lambda_{\boldsymbol{a}} = V_{\boldsymbol{a}}\right\}. \tag{10}$$

It is not difficult to see that $R_{\boldsymbol{a}}$ is the radius of the smallest ball that can be circumscribed around the *Voronoi cell* of $\Lambda_{\boldsymbol{a}}$, which is defined by

$$\mathcal{V}(\Lambda_{\boldsymbol{a}}) = \{\boldsymbol{y} \in V_{\boldsymbol{a}} : \|\boldsymbol{y}\| \leq \|\boldsymbol{y} - \boldsymbol{x}\| \ \forall\ \boldsymbol{x} \in \Lambda_{\boldsymbol{a}}\},$$

where $\|\ \|$ stands for the usual Euclidean norm on vectors. Notice that unlike $\mu(\mathcal{S}, \mathcal{L})$ of (8), $R_{\boldsymbol{a}}$ is a well understood invariant of the lattice. We will discuss it in further details in section 3. The main result of this paper is the following theorem.

Theorem 1.1. *Let $N \geq 3$ and let $2 \leq a_1 < a_2 < \cdots < a_N$ be relatively prime integers. Write $\boldsymbol{a} = (a_1, ..., a_N)$, and let $\mathcal{F} = \mathcal{F}(\boldsymbol{a})$ be the Frobenius number of this N-tuple. Then*

$$\mathcal{F} \leq \left[\frac{(N-1)R_{\boldsymbol{a}}}{\|\boldsymbol{a}\|}\sum_{i=1}^{N} a_i\sqrt{\|\boldsymbol{a}\|^2 - a_i^2} + 1\right], \tag{11}$$

where $R_{\boldsymbol{a}}$ is as in (10).

Our approach uses some classical results from the geometry of numbers. Here is a brief outline of our argument. Let t be a positive integer, and consider the hyperplane in $\mathbb{R}^N$ defined by the equation

$$\sum_{i=1}^{N} a_i X_i = t. \tag{12}$$

The intersection of this hyperplane with the positive orthant $\mathbb{R}^N_{\geq 0}$ is an $(N-1)$-dimensonal simplex, call it $S(t)$. An integral point in this simplex corresponds to a solution of (12) in non-negative integers, hence for every $t > \mathcal{F}$ such a point must always exist. Moreover, $\mathcal{F}$ is precisely the smallest positive integer such that for each integer $t > \mathcal{F}$ the simplex $S(t)$ contains a point of $\mathbb{Z}^N$. By definition of $R_{\boldsymbol{a}}$, a ball of radius $\geq R_{\boldsymbol{a}}$ must contain an integer lattice point. On the other hand, it is possible to bound the inradius of the simplex $S(t)$ from below using a standard isoperimetric inequality. Combining these two estimates produces a value t_* large enough so that for every $t \geq t_*$ the simplex $S(t)$ is guaranteed to contain an integral point.

A particularly nice explicit bound for $\mathcal{F}$ can be derived from Theorem 1.1 for a special class of latices $\Lambda_{\boldsymbol{a}}$. For each $1 \leq i \leq N-1$, the i-th *successive minimum* λ_i of $\Lambda_{\boldsymbol{a}}$ is defined to be the infimum of all $\lambda > 0$ such that $B(\lambda) \cap \Lambda_{\boldsymbol{a}}$ contains i non-zero linearly independent vectors in $V_{\boldsymbol{a}}$. Hence $1 \leq \lambda_1 \leq ... \leq \lambda_{N-1}$. If $\lambda_1 = \cdots = \lambda_{N-1}$, we say that $\Lambda_{\boldsymbol{a}}$ is an *ESM lattice* (equal successive minima). This is a very important class of lattices, which are widely used for instance in coding theory (see [2]).

Corollary 1.2. *Let the notation be as above. Then*

$$\mathcal{F} \leq \left[\frac{\lambda_{N-1}(N-1)^2 \sum_{i=1}^N a_i \sqrt{\|\boldsymbol{a}\|^2 - a_i^2}}{\lambda_1 (\|\boldsymbol{a}\|^{N-2} \omega_{N-1})^{\frac{1}{N-1}}} + 1 \right], \tag{13}$$

where ω_{N-1} is as in (9). In case $\Lambda_{\boldsymbol{a}}$ is an ESM lattice, $\lambda_{N-1} = \lambda_1$ in (13).

One interesting feature of our bounds (11) and (13) is that they depend symmetrically on all numbers $a_1, \dots, a_N$, unlike the previously known bounds (2) - (5).

In section 2 of this paper we prove Theorem 1.1. In section 3 we discuss the ESM case, deriving Corollary 1.2, as well as some other related cases using additional tools from the classical geometry of numbers. We also show some examples and exhibit some computational data comparing our bounds to the previously known ones quoted in (2) - (5). In particular, when $\Lambda_{\boldsymbol{a}}$ is an ESM lattice, Corollary 1.2 will often produce a better bound on $\mathcal{F}$ than (2) - (5). We discuss this further in section 3. In section 4 we prove that $\Lambda_{\boldsymbol{a}}$ is an ESM lattice for infinitely many N-tuples $\boldsymbol{a}$. In fact, in Theorem 4.2 we construct an explicit infinite family of ESM lattices $\Lambda_{\boldsymbol{a}}$ parametrized by integer values of a single variable t when $N = 4$. We also explain how families like this can be constructed in higher dimensions. Finally we demonstrate that for all such infinite families of ESM lattices $\Lambda_{\boldsymbol{a}}$ our bound (13) on $\mathcal{F}(\boldsymbol{a})$ is significantly better than the previously known ones.

2. Proof of Theorem 1.1

Let the notation be as in section 1 above. For each $t \in \mathbb{Z}_{\geq 0}$ consider the hyperplane lattice

$$\Lambda_{\boldsymbol{a}}(t) = \left\{ \boldsymbol{x} \in \mathbb{Z}^N : L_{\boldsymbol{a}}(\boldsymbol{x}) = t \right\},$$

and let $V_{\boldsymbol{a}}(t) = \operatorname{span}_{\mathbb{R}} \Lambda_{\boldsymbol{a}}(t)$ be the corresponding hyperplane. Fix $\boldsymbol{u}_t \in \Lambda_{\boldsymbol{a}}(t)$, and define a translation $f_t : V_{\boldsymbol{a}} \to V_{\boldsymbol{a}}(t)$ given by $f_t(\boldsymbol{x}) = \boldsymbol{x} + \boldsymbol{u}_t$ for each $\boldsymbol{x} \in V_{\boldsymbol{a}}$. Then f_t is bijective and preserves distance; moreover, it maps $\Lambda_{\boldsymbol{a}}$ bijectively onto $\Lambda_{\boldsymbol{a}}(t)$.

Notice that $S(t) = V_{\boldsymbol{a}}(t) \cap \mathbb{R}^N_{\geq 0}$ is an $(N-1)$-dimensional simplex in $\mathbb{R}^N$ with vertices $\boldsymbol{v}_i = \frac{t}{a_i} \boldsymbol{e}_i$ for each $1 \leq i \leq N$, where $\boldsymbol{e}_1, ..., \boldsymbol{e}_N$ are the standard basis vectors. For each $2 \leq i \leq N$ define

$$\boldsymbol{w}_i = (\boldsymbol{v}_i - \boldsymbol{v}_1)^T = \left(-\frac{t}{a_1}, 0, ..., 0, \frac{t}{a_i}, 0, ..., 0 \right),$$

and let W be the $(N-1) \times N$ matrix with row vectors $\boldsymbol{w}_2, ..., \boldsymbol{w}_N$. By Gram determinant formula

$$\operatorname{Vol}_{N-1}(S(t)) = \frac{\sqrt{\det(WW^T)}}{(N-1)!} \tag{14}$$

It is easy to see that

$$WW^T = \frac{t^2}{a_1^2} \begin{pmatrix} \frac{a_1^2 + a_2^2}{a_2^2} & 1 & \dots & 1 \\ 1 & \frac{a_1^2 + a_3^2}{a_3^2} & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & \frac{a_1^2 + a_N^2}{a_N^2} \end{pmatrix},$$

is an $(N-1)\times(N-1)$ symmetric matrix. We want to compute $\det(WW^T)$. For this we will need the following lemma.

Lemma 2.1. *Let*

$$\mathcal{A}=\begin{pmatrix}\alpha_1 & 1 & \dots & 1\\ 1 & \alpha_2 & \dots & 1\\ \vdots & \vdots & \ddots & \vdots\\ 1 & 1 & \dots & \alpha_k\end{pmatrix},$$

be a $k\times k$ symmetric matrix, $k\geq 2$. Then

$$\det(\mathcal{A})=\prod_{i=1}^{k}(\alpha_i-1)+\sum_{i=1}^{k}\left\{\prod_{j=1,\ j\neq i}^{k}(\alpha_j-1)\right\}. \tag{15}$$

Proof. It is easy to notice that $\det(\mathcal{A})=\det(\mathcal{B})$, where

$$\mathcal{B}=\det\begin{pmatrix}\alpha_1-1 & 0 & \dots & 0 & 1-\alpha_k\\ 0 & \alpha_2-1 & \dots & 0 & 1-\alpha_k\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \dots & \alpha_{k-1}-1 & 1-\alpha_k\\ 1 & 1 & \dots & 1 & \alpha_k\end{pmatrix}.$$

We will prove identity (15) for $\det(\mathcal{B})$ by induction on k. If $k=2$, then

$$\det(\mathcal{B})=\det\begin{pmatrix}\alpha_1-1 & 1-\alpha_2\\ 1 & \alpha_2\end{pmatrix}=(\alpha_1-1)\alpha_2+(\alpha_2-1),$$

which is (15). Assume $k>2$. Then, by Laplace's expansion combined with the induction hypothesis, we obtain

$$\begin{aligned}
\det(\mathcal{B}) &= (\alpha_1-1)\det\begin{pmatrix}\alpha_2-1 & 0 & \dots & 0 & 1-\alpha_k\\ 0 & \alpha_3-1 & \dots & 0 & 1-\alpha_k\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \dots & \alpha_{k-1}-1 & 1-\alpha_k\\ 1 & 1 & \dots & 1 & \alpha_k\end{pmatrix}\\
&+ (-1)^{k+1}\det\begin{pmatrix}0 & 0 & \dots & 0 & 1-\alpha_k\\ \alpha_2-1 & 0 & \dots & 0 & 1-\alpha_k\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \dots & 0 & 1-\alpha_k\\ 0 & 0 & \dots & \alpha_{k-1}-1 & 1-\alpha_k\end{pmatrix}\\
&= (\alpha_1-1)\left(\prod_{i=2}^{k}(\alpha_i-1)+\sum_{i=2}^{k}\left\{\prod_{j=2,\ j\neq i}^{k}(\alpha_j-1)\right\}\right)\\
&+ (-1)^{k+1+k}(1-\alpha_k)\det\begin{pmatrix}\alpha_2-1 & \dots & 0\\ \vdots & \ddots & \vdots\\ 0 & \dots & \alpha_{k-1}-1\end{pmatrix}\\
&= \prod_{i=1}^{k}(\alpha_i-1)+\sum_{i=2}^{k}\left\{\prod_{j=1,\ j\neq i}^{k}(\alpha_j-1)\right\}+\prod_{j=2}^{k}(\alpha_j-1).
\end{aligned}$$

This completes the proof. □

Applying Lemma 2.1 to WW^T, a direct computation shows that

$$\det(WW^T) = \frac{t^{2(N-1)}\|\boldsymbol{a}\|^2}{\prod_{i=1}^N a_i^2}, \tag{16}$$

and so combining (14) with (16) we obtain

$$\mathrm{Vol}_{N-1}(S(t)) = \frac{t^{N-1}\|\boldsymbol{a}\|}{(N-1)!\prod_{i=1}^N a_i}. \tag{17}$$

We also need to compute the surface area $A_{N-1}(S(t))$. Notice that $S(t)$ has N faces $F_1(t), ..., F_N(t)$ with each $F_i(t)$ being an $(N-2)$-dimensional simplex with vertices $\boldsymbol{v}_1, ..., \boldsymbol{v}_{i-1}, \boldsymbol{v}_{i+1}, ..., \boldsymbol{v}_N$. Then, applying (17) in one less dimension we see that for each $1 \le i \le N$.

$$\mathrm{Vol}_{N-2}(F_i(t)) = \frac{t^{N-2}\|\boldsymbol{\alpha}_i\|}{(N-2)!\prod_{j=1,\ j\neq i}^N a_j},$$

where $\boldsymbol{\alpha}_i = (a_1, ..., a_{i-1}, a_{i+1}, ..., a_N)$. Then

$$A_{N-1}(S(t)) = \sum_{i=1}^N \mathrm{Vol}_{N-2}(F_i(t)) = \frac{t^{N-2}\sum_{i=1}^N \|\boldsymbol{\alpha}_i\|a_i}{(N-2)!\prod_{i=1}^N a_i}. \tag{18}$$

Write $r(t)$ for the inradius of $S(t)$, i.e. the radius of the largest ball that can be inscribed into $S(t)$. By a standard isoperimetric inequality for the inradius of a simplex (see for instance (9) of [11])

$$r(t) \ge \frac{\mathrm{Vol}_{N-1}(S(t))}{A_{N-1}(S(t))} = \frac{t\|\boldsymbol{a}\|}{(N-1)\sum_{i=1}^N \|\boldsymbol{\alpha}_i\|a_i}, \tag{19}$$

where the last identity follows by combining (17) and (18). Let us choose a positive integer t such that $r(t) \ge R_{\boldsymbol{a}}$. By (19) we see that it suffices to take

$$t = \left\lceil \frac{(N-1)R_{\boldsymbol{a}}}{\|\boldsymbol{a}\|}\sum_{i=1}^N \|\boldsymbol{\alpha}_i\|a_i + 1 \right\rceil. \tag{20}$$

We will write t_* for the value of t as in (20). Let $t \ge t_*$, and let $B_t(r(t))$ be the $(N-1)$-dimensional ball of radius $r(t)$ contained in $S(t)$. Then $f_t^{-1}(B_t(r(t)))$ is an $(N-1)$-dimensional ball of radius $r(t) \ge R_{\boldsymbol{a}}$ in $V_{\boldsymbol{a}}$. By definition of $R_{\boldsymbol{a}}$ in (10), we see that whenever $R \ge R_{\boldsymbol{a}}$ the translated ball $B(R) + \boldsymbol{x}$ will contain at least one nonzero lattice point for every $\boldsymbol{x} \in V_{\boldsymbol{a}}$, and hence $f_t^{-1}(B_t(r(t)))$ contains a nonzero point of $\Lambda_{\boldsymbol{a}}$. Therefore $B_t(r(t))$ contains a point of $\Lambda_{\boldsymbol{a}}(t)$, that is $\Lambda_{\boldsymbol{a}}(t) \cap \mathbb{Z}^N_{\ge 0}$ is not empty for each integer $t \ge t_*$. Therefore $\mathcal{F} \le t_*$, and observing that $\|\boldsymbol{\alpha}_i\| = \sqrt{\|\boldsymbol{a}\|^2 - a_i^2}$ for each $1 \le i \le N$ finishes the proof.

Remark. It is possible to replace (19) by stronger versions of this isoperimetric inequality, which follow from the proof of Wills conjecture and its various strengthenings (see, for instance, (4), (6), and Theorem 4 of [5]). This may lead to a slightly better although much less readable bound than (11).

3. Corollaries

In this section we discuss consequences of Theorem 1.1, in particular we derive Corollary 1.2. Let $N \geq 3$, and let all the notation be as in sections 1 and 2 above. First of all notice that if for some $1 < i \leq N$ we can express a_i in the form

$$a_i = \sum_{j=1}^{i-1} a_j x_j, \tag{21}$$

for some nonnegative integers $x_1, ..., x_{i-1}$, then

$$\mathcal{F}(a_1, ..., a_N) = \mathcal{F}(a_1, ..., a_{i-1}, a_{i+1}, ..., a_N). \tag{22}$$

We will call the relatively prime N-tuple $\boldsymbol{a}$ *reduced* if (21) is not true for any i. By (22), every relatively prime N-tuple can be reduced to a relatively prime reduced k-tuple for some $1 \leq k \leq N$ by eliminating all a_i's for which (21) is true. Moreover, if $a_1 = 2$, then there must exist $1 < i \leq N$ such that a_i is odd, since $gcd(a_1, ..., a_N) = 1$; let i be the smallest such index. It is easy to see that in this case $\mathcal{F} = a_i - 1$. In particular, if $\boldsymbol{a}$ is reduced, then $\mathcal{F} = a_2 - 1$. Hence we can conclude that either $a_1 \geq 3$, or

$$\mathcal{F} \leq a_N - 1. \tag{23}$$

From here on we will assume that $\boldsymbol{a}$ is reduced and $a_1 \geq 3$.

Fix a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_{N-1}$ for $\Lambda_{\boldsymbol{a}}$ in $\mathbb{R}^N$, and write $X = (\boldsymbol{x}_1 \ ... \ \boldsymbol{x}_{N-1})$ for the corresponding $N \times (N-1)$ basis matrix. Let $\mathcal{I}$ be the collection of all subsets I of $\{1, ..., N\}$ of cardinality $(N-1)$. For each $I \in \mathcal{I}$ let I' be its complement, i.e. $I' = \{1, ..., N\} \setminus I$. Clearly $|\mathcal{I}| = N - 1$. For each $I \in \mathcal{I}$, write X_I for the $(N-1)\times(N-1)$ submatrix of X consisting of all those rows of X which are indexed by I, and $a_{I'}$ for the coordinate of $\boldsymbol{a}$ indexed by I'. By the duality principle of Brill-Gordan [9] (also see Theorem 1 on p. 294 of [12])

$$\det(X_I) = (-1)^{N+1-I'} a_{I'}. \tag{24}$$

Therefore coordinates of $\boldsymbol{a}$ can be thought of as *Grassmann coordinates* of $\Lambda_{\boldsymbol{a}}$ up to $\pm$ signs (some sources also call them *Plucker coordinates*). They are well defined in the sense that they do not depend on the choice of the basis (see [12] for details). Then, by the Cauchy-Binet formula (see for instance [8])

$$\det(\Lambda_{\boldsymbol{a}}) = \sqrt{\det(XX^t)} = \|\boldsymbol{a}\|. \tag{25}$$

Let $\lambda_1, ..., \lambda_{N-1}$ be the successive minima for $\Lambda_{\boldsymbol{a}}$ as defined in section 1. An immediate observation is that since $\boldsymbol{a}$ is reduced,

$$2 \leq \lambda_1 \leq \cdots \leq \lambda_{N-1}. \tag{26}$$

Indeed, if $\lambda_1 < 2$, then there must exist $\boldsymbol{0} \neq \boldsymbol{x} \in \Lambda_{\boldsymbol{a}}$ with $\|\boldsymbol{x}\| < 2$, hence at most three of its coordinates are non-zero, call them x_i, x_j, x_k, $1 \leq i < j < k \leq N$. Assume $x_i \geq 0$ (take $-\boldsymbol{x}$ otherwise). Then either $x_i, x_j = 1$ and $x_k = -1$, or one of them is 0 and the other two are ± 1 and ∓ 2 respectively. In the first case it must therefore be that $a_k = a_i + a_j$ while the second case implies that one of the coordinates of $\boldsymbol{a}$ is a multiple of another. Both of these conclusions contradict the assumption that $\boldsymbol{a}$ is reduced.

Combining Minkowski's second convex body theorem (see [6], p. 203) with (25), we obtain

$$\lambda_1 \dots \lambda_{N-1} \le \frac{2^{N-1}\|\boldsymbol{a}\|}{\omega_{N-1}}. \tag{27}$$

Combining Jarnik's inequality (see Theorem 1 on p. 99 of [10]) with (27), we obtain a bound on $R_{\boldsymbol{a}}$:

$$R_{\boldsymbol{a}} \le \frac{1}{2}\sum_{i=1}^{N-1}\lambda_i \le \frac{N-1}{2}\lambda_{N-1} \le \frac{2^{N-2}(N-1)\|\boldsymbol{a}\|}{\omega_{N-1}\lambda_1 \dots \lambda_{N-2}}. \tag{28}$$

Then Theorem 1.1 combined with (26) and (28) yields a general bound

$$\mathcal{F} \le \left[\frac{(N-1)^2}{\omega_{N-1}}\sum_{i=1}^{N} a_i\sqrt{\|\boldsymbol{a}\|^2 - a_i^2} + 1\right], \tag{29}$$

however we can do much better for more specialized classes of lattices $\Lambda_{\boldsymbol{a}}$. Combining (27) and (28), we obtain

$$R_{\boldsymbol{a}} \le \frac{\lambda_1}{2}\sum_{i=1}^{N-1}\frac{\lambda_i}{\lambda_1} \le \lambda_1\frac{(N-1)\lambda_{N-1}}{2\lambda_1} \le \frac{(N-1)\lambda_{N-1}}{\lambda_1}\left(\frac{\|\boldsymbol{a}\|}{\omega_{N-1}}\right)^{\frac{1}{N-1}}, \tag{30}$$

which, combined with Theorem 1.1, immediately implies Corollary 1.2. Clearly the bound of Corollary 1.2 becomes better when the ratio $\frac{\lambda_{N-1}}{\lambda_1}$ is small, and especially in case $\Lambda_{\boldsymbol{a}}$ is an ESM lattice.

We will now show a few examples of $\boldsymbol{a}$ such that $\Lambda_{\boldsymbol{a}}$ is an ESM lattice for which (13) of Corollary 1.2 produces a better bound on the Frobenius number than (2) - (5). In the following comparison tables of the bounds (2) - (5) with (13), $\lambda_{\boldsymbol{a}}$ stands for the common value of the successive minima of $\Lambda_{\boldsymbol{a}}$. First let $N = 4$.

4-tuple $\boldsymbol{a}$	$\lambda_{\boldsymbol{a}}$	*min (2) - (5)*	*(13)*
9337, 9961, 11593, 67367	$\sqrt{1802}$	91235853 (2)	10995433
33199, 38351, 47759, 152057	$\sqrt{3218}$	1346684400 (2)	55055950

Next let $N = 5$.

5-tuple $\boldsymbol{a}$	$\lambda_{\boldsymbol{a}}$	*min (2) - (5)*	*(13)*
39221, 46967, 47869, 62839, 206749	$\sqrt{524}$	1719019240 (2)	66231577
1867558, 2348176, 2918749, 5249843, 26695349	$\sqrt{5591}$	4778060891200 (2)	14595157176

Finally let $N = 6$.

6-tuple $\boldsymbol{a}$	$\lambda_{\boldsymbol{a}}$	*min (2) - (5)*	*(13)*
6595, 90709, 110483, 121833, 147472, 462217	$\sqrt{209}$	1015946371 (3)	168600688
5958323, 14864655, 19945128, 28191201, 28507523, 117697394	$\sqrt{1915}$	134180083643479 (2)	104669816535

It is of course possible to come up with numerous such examples for these and higher dimensions. In fact, in the next section we will show that $\Lambda_{\boldsymbol{a}}$ is an ESM lattice for infinitely many $\boldsymbol{a}$.

4. ESM Lattices

Let $N \geq 4$. In this section we will describe a procedure that allows to construct infinite families of sublattices of $\mathbb{Z}^N$ of rank $N-1$ which have equal successive minima and are of the form $\Lambda_{\boldsymbol{a}}$ for N-tuples $\boldsymbol{a}$ of relatively prime positive integers $1 < a_1 < \cdots < a_N$.

We start with some additional notation, following [3]. An ordered collection of linearly independent vectors $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\} \subset \mathbb{Z}^N$, $2 \leq k \leq N$, is called *nearly orthogonal* if for each $1 < i \leq k$ the angle between $\boldsymbol{x}_i$ and the subspace of $\mathbb{R}^N$ spanned by $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{i-1}$ is in the interval $\left[\frac{\pi}{3}, \frac{\pi}{2}\right]$. In other words, this condition means that for each $1 < i \leq k$

$$\frac{|<\boldsymbol{x}_i, \boldsymbol{y}>|}{\|\boldsymbol{x}_i\|\|\boldsymbol{y}\|} \leq \frac{1}{2}, \tag{31}$$

for all non-zero vectors $\boldsymbol{y} \in \operatorname{span}_{\mathbb{R}}\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{i-1}\}$, where $<\ ,\ >$ stands for the usual inner product on $\mathbb{R}^N$. The following result is Theorem 1 of [3]; it is our main tool in this section.

Theorem 4.1 ([3])**.** *Suppose that an ordered basis $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\}$ for sublattice Λ of $\mathbb{Z}^N$ of rank $1 < k \leq N$ is nearly orthogonal. Then it contains the shortest non-zero vector of Λ.*

In particular, if all vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ of Theorem 4.1 have the same norm, then Λ is an ESM lattice. We are now ready to describe our construction for infinite families of ESM lattices.

Let $\boldsymbol{x}_1 = (t_1, \ldots, t_N)$ be a variable vector, and write S_N for the symmetric group on N letters where id stands for the identity permutaion. Assume that there exist $id = \sigma_1, \sigma_2, \ldots, \sigma_{N-1} \in S_N$ and $N(N-1)$ integers $m_{11}, \ldots, m_{(N-1)N} \in \{0, 1\}$ such that

$$\boldsymbol{x}_i = \left((-1)^{m_{i1}} t_{\sigma_i(1)}, \ldots, (-1)^{m_{iN}} t_{\sigma_i(N)}\right),\ 1 \leq i \leq N-1,$$

satisfy the following conditions for infinitely many positive integer values of the variables $t_1, \ldots, t_N$:

(1) $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{N-1}$ are linearly independent,
(2) For each $1 \leq i \leq N$ the corresponding Grassmann coordinate $\det(X_{I_i})$ of the matrix $X = (\boldsymbol{x}_1 \ldots \boldsymbol{x}_{N-1})^t$ satisfies the condition
$$(-1)^{N+1-i} \det(X_{I_i}) > 0,$$
where $I_i = \{1, \ldots, N\} \setminus \{i\}$,
(3) Absolute values of Grassmann coordinates of X are relatively prime,
(4) $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{N-1}\}$ is a nearly orthogonal collection of vectors.

Then, by construction and by Theorem 4.1, for each such N-tuple $t_1, \ldots, t_N$ the lattice

$$\operatorname{span}_{\mathbb{Z}}\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{N-1}\}$$

is ESM and of the form $\Lambda_{\boldsymbol{a}}$ where $\boldsymbol{a}$ is the vector with coordinates

$$a_i = (-1)^{N+1-i} \det(X_{I_i}),$$

for each $1 \leq i \leq N$; the last statement follows by (24). This would mean that there exist infinite families of ESM lattices of the form $\Lambda_{\boldsymbol{a}}$. It appears to be possible to find such permutations for each N. As an example, we exhibit such a family for $N = 4$.

Theorem 4.2. *Let $t \in \mathbb{Z}_{>0}$, and define*

$$a_1(t) = 6t^2 - 13t - 216, \ a_2(t) = 6t^2 - 125,$$
$$a_3(t) = 7t^2 - 174, \ a_4(t) = t^3 - 36t - 78. \tag{32}$$

Then for each $t \in \mathbb{Z}_{>0}$, $\boldsymbol{a}(t) = (a_1(t), a_2(t), a_3(t), a_4(t)) \in \mathbb{Z}^4$, and there exist infinitely many positive integer values of t such that

$$0 < a_1(t) < a_2(t) < a_3(t) < a_4(t), \tag{33}$$

$$gcd\,(a_1(t), a_2(t), a_3(t), a_4(t)) = 1, \tag{34}$$

and the lattice

$$\Lambda_{\boldsymbol{a}(t)} = \left\{ \boldsymbol{x} \in \mathbb{Z}^4 : \sum_{i=1}^{4} a_i(t) x_i = 0 \right\}$$

is ESM. Moreover, for each such $\boldsymbol{a}(t)$ the minimum of bounds (2) - (5) on the Frobenius number $\mathcal{F}(\boldsymbol{a}(t))$ is $O(t^4)$ while our bound (13) is $O(t^3)$. For instance, $\boldsymbol{a}(t)$ has these properties for all $t = 13s + 2$, where $s \geq 2$ is an integer.

Proof. Let $t \in \mathbb{Z}_{>0}$ and define

$$\boldsymbol{x}_1(t) = (-7, t, 6, -6), \ \boldsymbol{x}_2(t) = (-6, 7, t, -6), \ \boldsymbol{x}_3(t) = (-6, -6, 7, t). \tag{35}$$

A direct computation shows that

$$\Lambda_{\boldsymbol{a}(t)} = \left\{ \boldsymbol{x} \in \mathbb{Z}^4 : \sum_{i=1}^{4} a_i(t) x_i = 0 \right\} = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{x}_1(t), \boldsymbol{x}_2(t), \boldsymbol{x}_3(t)\},$$

where $\boldsymbol{a}(t)$ is as in (32), and its coordinates can be seen to have no common roots. In particular, $\Lambda_{\boldsymbol{a}(t)}$ has rank 3 and basis vectors $\boldsymbol{x}_1(t), \boldsymbol{x}_2(t), \boldsymbol{x}_3(t)$ are linearly independent for all real values of t. Also notice that for each $t \geq 10$, (33) is satisfied.

To demonstrate that (34) holds infinitely often, notice that

$$gcd(a_1(t), a_2(t), a_3(t), a_4(t)) \leq gcd(a_2(t), a_3(t)),$$

and define $d(t) = gcd(a_2(t), a_3(t)) = gcd(7t^2 - 174, 6t^2 - 125)$. Then $d(t)$ must divide both

$$a_2(t) - a_3(t) = t^2 - 49, \ 7a_2(t) - 6a_3(t) = 13^2.$$

Notice that if, for instance, $t = 13s + 2$ for any $s \in \mathbb{Z}_{>0}$, then

$$t^2 - 49 = 169s^2 + 52s - 45 \equiv 7 \pmod{13},$$

hence $gcd(t^2 - 49, 13^2) = 1$, and so $d(t) = 1$ for all such t. This proves that (34) holds for infinitely many $t \in \mathbb{Z}_{>0}$.

We now want to show that $\{\boldsymbol{x}_1(t), \boldsymbol{x}_2(t), \boldsymbol{x}_3(t)\}$ is a nearly orthogonal ordered collection of vectors for infinitely many $t \in \mathbb{Z}_{>0}$. For this we refer to criterion (31) and first observe that

$$\frac{| < \boldsymbol{x}_1, \boldsymbol{x}_2 > |}{\|\boldsymbol{x}_1\| \|\boldsymbol{x}_2\|} = \frac{13t + 78}{t^2 + 121} \leq \frac{1}{2},$$

for all $t \geq 28$. Also, for each non-zero vector $\boldsymbol{y} = u\boldsymbol{x}_1 + v\boldsymbol{x}_2 \in \text{span}_{\mathbb{R}}\{\boldsymbol{x}_1, \boldsymbol{x}_2\}$ define

$$f(u,v) = \frac{t(12u-v) - 6(14u-v)}{\sqrt{(t^2+121)\left\{(u^2+v^2)(t^2+121) + 26uv(t+6)\right\}}} = \frac{< \boldsymbol{x}_3, \boldsymbol{y} >}{\|\boldsymbol{x}_3\|\|\boldsymbol{y}\|}. \tag{36}$$

A computation of the critical points of $f(u,v)$ in Maple shows that if $t \geq 17$ then $-\frac{1}{2} \leq f(u,v) \leq \frac{1}{2}$ for all $u, v \in \mathbb{R}$, not both zero. Hence by criterion (31) we conclude that $\{\boldsymbol{x}_1(t), \boldsymbol{x}_2(t), \boldsymbol{x}_3(t)\}$ is a nearly orthogonal ordered collection of vectors for all integers $t \geq 28$. Therefore, by Theorem 4.1 and remark after it the lattice $\Lambda_{\boldsymbol{a}(t)}$ is ESM for all such values of t.

Finally, a direct computation shows that for each $\boldsymbol{a}(t)$ as in (32) the minimum of bounds (2) - (5) on the Frobenius number $\mathcal{F}(\boldsymbol{a}(t))$ is $O(t^4)$ while bound (13) is $O(t^3)$.

Combining all these observations, we conclude that the statement of the theorem is true for instance for all t of the form

$$t = 13s + 2, \tag{37}$$

where $s \geq 2$ is an integer. This completes the proof. □

Notice in particular that the first example from the table in case $N = 4$ in section 3 is precisely of the form (32) where t is as in (37) with $s = 3$. A good strategy to obtain one-parameter infinite families of ESM lattices of the form $\Lambda_{\boldsymbol{a}}$ in different dimensions seems to be by a variation on a circulant basis matrix with $\pm$ signs as in (35). In fact, the rest of the examples in the table of section 3 can also be seen to come from such infinite families.

Moreover, one can see that for a general N if a lattice $\Lambda_{\boldsymbol{a}(t)}$ is ESM and is generated by an $(N-1) \times N$ circulant basis matrix with $\pm$ signs similar to (35), call this matrix $X(t)$, then t appears precisely once in every row of $X(t)$ and in all, except for one, columns of $X(t)$. This means that all, except for one, Grassmann coordinates of $X(t)$ in general will be polynomials of degree $N-2$ in t, and one will be a polynomial of degree $N-1$. It is not difficult to see that in general in this case the minimum of bounds (2) - (5) on the Frobenius number $\mathcal{F}(\boldsymbol{a}(t))$ will be $O\left(t^{2(N-2)}\right)$ while our bound (13) will be $O\left(t^{N-1}\right)$.

References

[1] I. Aliev and P. M. Gruber. An optimal lower bound for the Frobenius problem. *J. Number Theory*, 2006. to appear.

[2] A. H. Banihashemi and A. K. Khandani. On the complexity of decoding lattices using the Korkin-Zolotarev reduced basis. *IEEE Trans. Inform. Theory*, 44(1):162–171, 1998.

[3] R. Baraniuk, S. Dash, and R. Neelamani. On nearly orthogonal lattice bases. *SIAM J. Discrete Math.*, 2005. submitted.

[4] M. Beck, R. Diaz, and S. Robins. The Frobenius problem, rational polytopes, and Fourier-Dedekind sums. *J. Number Theory*, 96(1):1–21, 2002.

[5] N. S. Brannen. The Wills conjecture. *Trans. Amer. Math. Soc.*, 349:3977–3987, 1997.

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

[7] P. Erdös and R. Graham. On a linear Diophantine problem of Frobenius. *Acta Arithm.*, 21:399–408, 1972.

[8] F. R. Gantmacher. *The theory of matrices, Volume 1*. Chelsea Publishing Co., New York, 1959.

[9] P. Gordan. Uber den grossten gemeinsamen factor. *Math. Ann.*, 7:443–448, 1873.

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

[11] J. Hansen and M. Reitzner. Electromagnetic wave propagation and inequalities for moments of chord lengths. *Adv. in Appl. Probab.*, 36(4):987–995, 2004.
[12] W. V. D. Hodge and D. Pedoe. *Methods of Algebraic Geometry, Volume 1*. Cambridge Univ. Press, 1947.
[13] R. Kannan. Lattice translates of a polytope and the Frobenius problem. *Combinatorica*, 12(2):161–177, 1992.
[14] E. S. Selmer. On the linear Diophantine problem of Frobenius. *J. Reine Angew. Math.*, 293/294:1–17, 1977.
[15] J. J. Sylvester. Mathematical questions with their solutions. *Educational times*, 41:21, 1884.
[16] Y. Vitek. Bounds for a linear Diophantine problem of Frobenius. *J. London Math. Soc. (2)*, 10:390–398, 1975.

Department of Mathematics, Mailstop 3368, Texas A&M University, College Station, Texas 77843-3368
E-mail address: lenny@math.tamu.edu

Department of Mathematics, Temple University, Philadelphia, Pennsylvania, 19122
E-mail address: srobins@math.temple.edu