SIAM J. OPTIM.
Vol. 20, No. 6, pp. 2978–2993

FEASIBILITY OF INTEGER KNAPSACKS[*]

ISKANDER ALIEV[†] AND MARTIN HENK[‡]

Abstract. Given a matrix $A \in \mathbb{Z}^{m\times n}$ satisfying certain regularity assumptions, we consider the set $\mathcal{F}(A)$ of all vectors $\boldsymbol{b} \in \mathbb{Z}^m$ such that the associated *knapsack polytope* $P(A,\boldsymbol{b}) = \{\boldsymbol{x} \in \mathbb{R}^n_{\geq 0} : A\boldsymbol{x} = \boldsymbol{b}\}$ contains an integer point. When $m = 1$ the set $\mathcal{F}(A)$ is known to contain all consecutive integers greater than the Frobenius number associated with A. In this paper we introduce the *diagonal Frobenius number* $\mathrm{g}(A)$ which reflects in an analogous way feasibility properties of the problem and the structure of $\mathcal{F}(A)$ in the general case. We give an optimal upper bound for $\mathrm{g}(A)$ and also estimate the asymptotic growth of the diagonal Frobenius number on average.

Key words. knapsack problem, Frobenius numbers, successive minima, inhomogeneous minimum, distribution of lattices

AMS subject classifications. Primary, 90C10, 90C27, 11D07; Secondary, 11H06

DOI. 10.1137/090778043

1. Introduction and statement of results.

Let $A \in \mathbb{Z}^{m\times n}$, $1 \leq m < n$, be an integral $m \times n$ matrix satisfying

$$(1.1)\qquad \begin{aligned} &\text{i) } \gcd\left(\det(A_{I_m}) : A_{I_m} \text{ is an } m\times m \text{ minor of } A\right) = 1,\\ &\text{ii) } \{\boldsymbol{x} \in \mathbb{R}^n_{\geq 0} : A\,\boldsymbol{x} = \boldsymbol{0}\} = \{\boldsymbol{0}\}. \end{aligned}$$

For such a matrix A and a vector $\boldsymbol{b} \in \mathbb{Z}^m$ the so called *knapsack polytope* $P(A,\boldsymbol{b})$ is defined as

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

Observe that on account of (1.1) ii), $P(A,\boldsymbol{b})$ is indeed a polytope (or empty).

This paper is concerned with the following integer programming feasibility problem:

$$(1.2)\qquad \text{Does the polytope } P(A,\boldsymbol{b}) \text{ contain an integer vector?}$$

The problem is often called the *integer knapsack problem* and is well known to be NP-complete (Karp [18]). Let $\mathcal{F}(A)$ be the set of integer vectors $\boldsymbol{b}$ such that the instance of (1.2) is feasible; i.e.,

$$\mathcal{F}(A) = \{\boldsymbol{b} \in \mathbb{Z}^m : P(A,\boldsymbol{b}) \cap \mathbb{Z}^n \neq \emptyset\}.$$

A description of the set $\mathcal{F}(A)$ in terms of polynomials that can be regarded as a discrete analog of the celebrated *Farkas Lemma* is obtained in Lasserre [21]. The test Gomory and Chvátal functions for $\mathcal{F}(A)$ are also given in Blair and Jeroslow [9] (see also Schrijver [30, Corollary 23.4b]). In this paper we investigate the geometric

[*] Received by the editors November 23, 2009; accepted for publication (in revised form) August 28, 2010; published electronically October 12, 2010.
http://www.siam.org/journals/siopt/20-6/77804.html

[†] School of Mathematics and Wales Institute of Mathematical and Computational Sciences, Cardiff University, Senghennydd Road, Cardiff, Wales, UK (alievi@cf.ac.uk).

[‡] Fakultät für Mathematik, Otto-von-Guericke Universität Magdeburg, Universitätsplatz 2, D-39106 Magdeburg, Germany (martin.henk@ovgu.de).

structure of the set $\mathcal{F}(A)$ which, apart from a few special cases, remains unexplored. Results of Knight [20], Simpson and Tijdeman [32] and Pleasants, Ray and Simpson [25] suggest that the set $\mathcal{F}(A)$ may be decomposed into the set of all integer points in the interior of a certain translated *feasible* cone and a complementary set with complex combinatorial structure. We give an optimal, up to a constant multiplier, estimate for the position of such a feasible cone and also prove that a much stronger asymptotic estimate holds on average.

Before formally stating our main results, we will briefly address the special case $m = 1$ which is also our guiding case. In this case the matrix A is just an input vector $\boldsymbol{a} = (a_1, a_2, \dots, a_n)^T \in \mathbb{Z}^n$ and (1.1) i) says that $\gcd(\boldsymbol{a}) := \gcd(a_1, a_2, \dots, a_n) = 1$. Due to the second assumption (1.1) ii) we may assume that all entries of $\boldsymbol{a}$ are positive, and the largest integral value b such that the instance of (1.2) with $A = \boldsymbol{a}^T$ and $\boldsymbol{b} = b$ is infeasible is called the *Frobenius number* of $\boldsymbol{a}$, denoted by $\mathrm{F}(\boldsymbol{a})$. Thus

$$\operatorname{int}\{\mathrm{F}(\boldsymbol{a}) + \mathbb{R}_{\geq 0}\} \cap \mathbb{Z} \subset \mathcal{F}(\boldsymbol{a}), \tag{1.3}$$

where $\operatorname{int}\{\cdot\}$ denotes the interior of the set.

Frobenius numbers naturally appear in the analysis of integer programming algorithms (see, e.g., Aardal and Lenstra [2], Hansen and Ryan [15], and Lee, Onn and Weismantel [22]). The general problem of finding $\mathrm{F}(\boldsymbol{a})$ has been traditionally referred to as the *Frobenius problem*. This problem is NP-hard (Ramírez Alfonsín [26, 27]) and integer programming techniques are known to be an effective tool for computing Frobenius numbers (see Beihoffer et al. [8]).

Since computing $\mathrm{F}(\boldsymbol{a})$ is NP-hard, good upper bounds for the Frobenius number itself and for its average value are of particular interest. In terms of the Euclidean norm $||\cdot||$ of the input vector $\boldsymbol{a}$, all known upper bounds for $\mathrm{F}(\boldsymbol{a})$ can be represented in the form

$$\mathrm{F}(\boldsymbol{a}) \ll_n ||\boldsymbol{a}||^2 , \tag{1.4}$$

where $\ll_n$ denotes the Vinogradov symbol with the constant depending on n only. It is also known that the exponent 2 on the right hand side of (1.4) cannot be lowered (see, e.g., Arnold [6], Erdős and Graham [11], and Schlage-Puchta [28]).

The limiting distribution of $\mathrm{F}(\boldsymbol{a})$ in the 3-dimensional case was derived in Shur, Sinai, and Ustinov [31], and for the general case, see Marklof [23]. Upper bounds for the average value of $\mathrm{F}(\boldsymbol{a})$ have been obtained in Aliev and Henk [4] and Aliev, Henk, and Hinrichs [5]. In terms of $||\boldsymbol{a}||$ the bounds have the form

$$\sim ||\boldsymbol{a}||^{1+1/(n-1)} , \tag{1.5}$$

where the exponent $1 + 1/(n-1)$ cannot be lowered [5].

The main goal of the present paper is to obtain results of the types (1.4) and (1.5) for the general integer knapsack problem. Our interest was also motivated by the papers of Aardal, Hurkens, and Lenstra [1] and Aardal, Weismantel, and Wolsey [3] on algorithmic aspects of the problem.

First we will need a generalization of the Frobenius number which will reflect feasibility properties of problem (1.2). Let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n \in \mathbb{Z}^m$ be the columns of the matrix A and let

$$C = \{\lambda_1 \boldsymbol{v}_1 + \cdots + \lambda_n \boldsymbol{v}_n : \lambda_1, \dots, \lambda_n \geq 0\}$$

be the cone generated by $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$. Note that due to our assumption (1.1) ii), C is a pointed cone. Let also $\boldsymbol{v} := \boldsymbol{v}_1 + \ldots + \boldsymbol{v}_n$. By the *diagonal Frobenius number* $\mathrm{g}(A)$ *of*

A we understand the minimal $t \geq 0$ such that for all $\boldsymbol{b} \in \{t\boldsymbol{v} + C\} \cap \mathbb{Z}^m$ the problem (1.2) is feasible. Then, in particular, (cf.(1.3))

$$\{\mathrm{g}(A)\boldsymbol{v} + C\} \cap \mathbb{Z}^m \subset \mathcal{F}(A)\,. \tag{1.6}$$

In section 2 we show that the diagonal Frobenius number is well defined. In particular, we see that $\mathrm{g}(A) = 0$ if and only if the column vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ form a so-called Hilbert basis for the cone C (cf. [30, sec. 16.4]). From this viewpoint, roughly speaking, the smaller $\mathrm{g}(A)$ the closer the collection of vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ to being a Hilbert basis of C.

The diagonal Frobenius number $\mathrm{g}(A)$ appears in work of Khovanskii ([19, Proposition 3]), and the vector $\mathrm{g}(A)\boldsymbol{v}$ is also a special choice of a so-called *pseudo–conductor* as introduced in Vizvári [34] (cf. [27, sec. 6.5]). Moreover, $\mathrm{g}(A)$ can be easily used in order to get an inclusion as in (1.6) for an arbitrary $\boldsymbol{w} \in \operatorname{int} C \cap \mathbb{Z}^m$ instead of $\boldsymbol{v}$.

LEMMA 1.1. *Let $\boldsymbol{w} \in \operatorname{int} C \cap \mathbb{Z}^m$. Then*

$$\{t\,\boldsymbol{w} + C\} \cap \mathbb{Z}^m \subset \mathcal{F}(A)$$

for all $t \geq \sqrt{\frac{\det(AA^T)}{n-m+1}}\,\mathrm{g}(A)$.

To the best of our knowledge this generalized Frobenius problem had been investigated in the literature only in the case $n = m+1$ (see, e.g., Knight [20], Simpson and Tijdeman [32], and Pleasants, Ray, and Simpson [25]). However, even in this special case the results of the types (1.4) and (1.5) were not known.

Here we prove with respect to the diagonal Frobenius number.

THEOREM 1.1. *There exists a constant $c_{m,n}$ depending only on n and m such that*

$$\mathrm{g}(A) \leq \; c_{m,n}\sqrt{\det(AA^T)}. \tag{1.7}$$

For $c_{m,n}$ one can take

$$c_{m,n} = \frac{(n-m)\,\sqrt{n}}{2}.$$

In the special case $m = 1$, Theorem 1.1 together with Lemma 1.1 gives the best possible upper bound (1.4) on the Frobenius number $\mathrm{F}(\boldsymbol{a})$.

The next result shows optimality of the upper bound (1.7) up to a constant factor in general.

THEOREM 1.2. *Let $1 \leq m < n$. There exists an infinite sequence of matrices $A_t \in \mathbb{Z}^{m\times n}$ and a constant $c'_{m,n} > 0$ such that*

$$\mathrm{g}(A_t) > \; c'_{m,n}\sqrt{\det(A_tA_t^T)}.$$

In fact, we show that the sequence A_t can be chosen in a somewhat generic way. In the special case $m = 1$, Theorem 6.1 shows that, roughly speaking, cutting off special families of input vectors cannot make the order of upper bounds for the Frobenius number F smaller than $||\boldsymbol{a}||^2$. We discuss this result in detail in section 6.

The next natural question is to derive upper bounds for the diagonal Frobenius number of a “typical” integer knapsack problem. Our approach to this problem is based on Geometry of Numbers for which we refer to the books [10, 13, 14].

By a *lattice* we will understand a discrete submodule L of a finite-dimensional Euclidean space. Here we are mainly interested in primitive lattices $L \subset \mathbb{Z}^n$, where $L \subset \mathbb{Z}^n$ is called *primitive* if $L = \operatorname{span}_{\mathbb{R}}(L) \cap \mathbb{Z}^n$. In other words, the lattice $L \subset \mathbb{Z}^n$ is primitive if it contains all of the integer points in the real subspace $\operatorname{span}_{\mathbb{R}}(L)$.

Recall that the Frobenius number $\mathrm{F}(\boldsymbol{a})$ is defined only for integer vectors $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ with $\gcd(\boldsymbol{a}) = 1$. This is equivalent to the statement that the 1-dimensional lattice $L = \mathbb{Z}\,\boldsymbol{a}$, generated by $\boldsymbol{a}$ is primitive. This generalizes easily to an m-dimensional lattice $L \subset \mathbb{Z}^n$ generated by $a_1, \cdots, a_m \in \mathbb{Z}^n$. Here the criterion is that L is primitive if and only if the greatest common divisor of all $m \times m$-minors is 1. This is an immediate consequence of Cassels [10, Chapter 1, Lemma 2] or see Schrijver [30, Corollary 4.1c].

Hence, by our assumption (1.1) i), the rows of the matrix A generate a primitive lattice L_A. The determinant of an m-dimensional lattice is the m-dimensional volume of the parallelepiped spanned by the vectors of a basis. Thus, in our setting we have

$$\det L_A = \sqrt{\det A\, A^T}.$$

In section 2 we will see that $\mathrm{g}(A)$ depends only on the lattice L_A and not on the particular basis given by the rows of A. Hence we may also write $\mathrm{g}(L_A)$ instead of $\mathrm{g}(A)$. Now for $T \in \mathbb{R}_{>0}$ and $1 \le m \le n-1$ let

$$G(m,n,T) = \{L \subset \mathbb{Z}^n : L \text{ is an } m\text{-dimensional primitive lattice with } \det(L) \le T\},$$

and let $\operatorname{Prob}_{m,n,T}(\cdot)$ be the uniform probability distribution on $G(m,n,T)$.

THEOREM 1.3. *Let $1 \le m \le n-1$. Then*

$$\operatorname{Prob}_{m,n,T}\left(\frac{\mathrm{g}(L)}{(\det(L))^{1/(n-m)}} > t\right) \ll_{m,n} t^{-2}.$$

The next theorem gives an upper bound for the average value of the diagonal Frobenius number.

THEOREM 1.4. *Let $1 \le m \le n-1$. Then*

$$\sup_T \frac{\sum_{L \in G(m,n,T)} \frac{\mathrm{g}(L)}{(\det(L))^{1/(n-m)}}}{\# G(m,n,T)} \ll_{m,n} 1.$$

Thus, the asymptotic growth of the diagonal Frobenius number on average has order

$$\sim (\det(L))^{1/(n-m)},$$

which is significantly slower than the growth of the maximum diagonal Frobenius number as $T \to \infty$.

The paper is organized as follows. In the next section we will study basic properties of $\mathrm{g}(A)$ and its relation to Geometry of Numbers, and we will prove Theorem 1.1 and Lemma 1.1. Section 3 contains the proof of Theorem 1.2 showing that our bound on $\mathrm{g}(A)$ is best possible. For the study of the average behavior of $\mathrm{g}(L_A)$ and, in particular, for the proofs of Theorems 1.3 and 1.4 in section 5, we will need some facts on the distribution of sublattices of $\mathbb{Z}^n$ which will be collected in section 4. Finally, in the last section we will give a refinement of Theorem 1.2 for the special case $m = 1$.

2. Diagonal frobenius number and geometry of numbers.

Following the geometric approach developed in Kannan [16] and Kannan and Lovász [17], we will make use of tools from the Geometry of Numbers. To this end we need the following notion: For a lattice $L \subset \mathbb{R}^n$ and a compact set $S \subset \mathrm{span}_{\mathbb{R}} L$ the *inhomogeneous minimum* $\mu(S, L)$ of S with respect to L is defined as the smallest non-negative number σ such that all lattice translates of $\sigma\, S$ with respect to L; i.e., $L + \sigma\, S$ cover the whole space $\mathrm{span}_{\mathbb{R}} L$. Or equivalently, we can describe it as

$$\mu(S, L) = \min\{\sigma > 0 : (\boldsymbol{x} + \sigma\, S) \cap L \neq \emptyset \text{ for all } \boldsymbol{x} \in \mathrm{span}_{\mathbb{R}} L\}.$$

Now let $L_A \subset \mathbb{Z}^n$ be the m-dimensional lattice generated by the rows of the given matrix $A \in \mathbb{Z}^{m\times n}$ satisfying the assumptions (1.1). Furthermore let

$$L_A^{\perp} = \{\boldsymbol{z} \in \mathbb{Z}^n : A\,\boldsymbol{z} = \boldsymbol{0}\}$$

be the $(n - m)$-dimensional lattice contained in the orthogonal complement of $\mathrm{span}_{\mathbb{R}}(L)$. Observe that (cf. [24, Proposition 1.2.9])

$$\det L_A^{\perp} = \det L_A = \sqrt{\det A\, A^T}. \tag{2.1}$$

By our assumption (1.1) ii) we know that for any right hand side $\boldsymbol{b} \in \mathbb{R}^m$ the set $P(A, \boldsymbol{b})$ is bounded (or empty); hence $P(A, \boldsymbol{v})$ is a polytope.

Lemma 2.1. *Let $1 \leq m \leq n - 1$. Then*

$$\mathrm{g}(A) \leq \mu(P(A, \boldsymbol{v}) - \boldsymbol{1}, L_A^{\perp}),$$

where $\boldsymbol{1} \in \mathbb{R}^n$ denotes the all 1-vector; i.e., $\boldsymbol{1} = (1, 1, \ldots, 1)^T \in \mathbb{R}^n$.

Proof. Let $t \geq \mu(P(A, \boldsymbol{v}) - \boldsymbol{1}, L_A^{\perp})$, and let $\boldsymbol{b} \in (t\,\boldsymbol{v} + C) \cap \mathbb{Z}^m$; i.e., there exists a non-negative vector $\boldsymbol{\alpha} \in \mathbb{R}^n_{\geq 0}$ such that $\boldsymbol{b} = A\,(t\,\boldsymbol{1} + \boldsymbol{\alpha})$. On the other hand, by (1.1) i) we know that the columns of A form a generating system of the lattice $\mathbb{Z}^m$ (cf. [30, Corollary 4.1c]). Thus, there exists a $\boldsymbol{z} \in \mathbb{Z}^n$ such that

$$\boldsymbol{b} = A\,(t\,\boldsymbol{1} + \boldsymbol{\alpha}) = A\,\boldsymbol{z}.$$

So we have that $P(A, \boldsymbol{b}) - \boldsymbol{z} \subset \mathrm{span}_{\mathbb{R}}(L_A^{\perp})$, and it suffices to prove that $P(A, \boldsymbol{b}) - \boldsymbol{z}$ contains an integral point of $L_A^{\perp}$, for which it is enough to verify

$$\mu(P(A, \boldsymbol{b}) - \boldsymbol{z}, L_A^{\perp}) \leq 1.$$

Since the inhomogeneous minimum is invariant with respect to translations and since $P(A, t\boldsymbol{v}) + \boldsymbol{\alpha} \subseteq P(A, \boldsymbol{b})$, we get

$$\begin{aligned}\mu(P(A, \boldsymbol{b}) - \boldsymbol{z}, L_A^{\perp}) &= \mu(P(A, \boldsymbol{b}) - (t\,\boldsymbol{1} + \boldsymbol{\alpha}), L_A^{\perp})\\ &\leq \mu(P(A, t\boldsymbol{v}) - t\,\boldsymbol{1}, L_A^{\perp}) = \mu(t\,(P(A, \boldsymbol{v}) - \boldsymbol{1}), L_A^{\perp})\\ &\leq \frac{1}{t}\mu(P(A, \boldsymbol{v}) - \boldsymbol{1}, L_A^{\perp}) \leq 1. \qquad \square\end{aligned}$$

Thus the diagonal Frobenius number is well defined. Next we want to point out that $\mathrm{g}(A)$ depends only on the lattice L_A and not on the specific basis of that lattice as given by the rows of A. If the rows of a matrix $\overline{A}$ also build a basis of L_A, then there exists a unimodular matrix $U \in \mathbb{Z}^{m\times m}$ such that $A = U\,\overline{A}$, which implies $\mathrm{g}(A) = \mathrm{g}(\overline{A})$. Thus, it is justified to denote the diagonal Frobenius (also) by $\mathrm{g}(L_A)$.

For the proof of Theorem 1.1, which will be based on Lemma 2.1 and an upper bound on the inhomogeneous minimum, we need one more concept from Geometry of Numbers, namely, Minkowski's successive minima. For a k-dimensional lattice L and a 0-symmetric convex body $K \subset \mathrm{span}_{\mathbb{R}} L$ the i-successive minimum of K with respect to L is defined as

$$\lambda_i(K,L) = \min\{\lambda > 0 : \dim(\lambda\, K \cap L) \geq i\}, \quad 1 \leq i \leq k;$$

i.e., it is the smallest factor such that $\lambda\, K$ contains at least i linearly independent lattice points of L. We will need here only two results on the successive minima. One is Minkowski's celebrated theorem on successive minima which states (cf. [13, Theorem 23.1])

$$\frac{2^k}{k!}\det L \leq \lambda_1(K,L)\,\lambda_2(K,L) \times \cdots \times \lambda_k(K,L)\,\mathrm{vol}\,(K) \leq 2^k \det L, \tag{2.2}$$

where $\mathrm{vol}\,(K)$ denotes the volume of K. The other result is known as Jarnik's inequalities which give bounds on the inhomogeneous minimum in terms of the successive minima, namely, (cf. [14, p. 99, p. 106])

$$\frac{1}{2}\lambda_k(K,L) \leq \mu(K,L) \leq \frac{1}{2}\left(\lambda_1(K,L) + \lambda_2(K,L) + \cdots + \lambda_k(K,L)\right). \tag{2.3}$$

We remark that both inequalities can be improved in the special case of a ball, but since we are mainly not interested in constants depending on the dimension, we do not apply these improvements.

Proof of Theorem 1.1. Let B_{n-m} be the $(n-m)$-dimensional ball of radius 1 centered at the origin in the space $\mathrm{span}_{\mathbb{R}} L_A^{\perp}$. By definition of $\boldsymbol{v}$ we have $\mathbf{1} + B_{n-m} \subset P(A,\boldsymbol{v})$ and so with Lemma 2.1

$$\begin{aligned} \mathrm{g}(A) &\leq \mu(P(A,\boldsymbol{v}) - \mathbf{1}, L_A^{\perp}) \leq \mu(B_{n-m}, L_A^{\perp}) \\ &\leq \frac{n-m}{2}\lambda_{n-m}(B_{n-m}, L_A^{\perp}), \end{aligned} \tag{2.4}$$

where the last inequality follows from (2.3), and the fact that the successive minima are an increasing sequence of real numbers.

Let $C^n = [-1,1]^n$ be the cube of edge length 2 centered at the origin and let $K = C^n \cap \mathrm{span}_{\mathbb{R}} L_A^{\perp}$. By a well-known result of Vaaler [33], any k-dimensional section of the cube C^n has k-volume at least 2^k. In particular we have

$$\mathrm{vol}_{\,n-m}(K) \geq 2^{n-m}\,.$$

All vectors of the lattice $L_A^{\perp}$ are integral vectors, thus $\lambda_i(K, L_A^{\perp}) \geq 1$, $1 \leq i \leq n-m$. Hence from (2.2) we get

$$\lambda_{n-m}(K, L_A^{\perp}) \leq \det L_A^{\perp} \tag{2.5}$$

and with (2.4) we conclude (cf. (2.1))

$$\mathrm{g}(A) \leq \frac{n-m}{2}\sqrt{n\det(AA^T)}. \qquad \square$$

Finally we come to the proof of Lemma 1.1.

Proof of Lemma 1.1. On account of Lemma 2.1 it suffices to show that for any $\boldsymbol{w} \in \operatorname{int} C \cap \mathbb{Z}^n$ the vector $\sqrt{\frac{\det A\,A^T}{n-m+1}}\,\boldsymbol{w}$ is contained in $\boldsymbol{v}+C$. For convenience we set $\gamma = \sqrt{\det(A\,A^T)/(n-m+1)}$.

Let $\boldsymbol{w} \in \operatorname{int} C \cap \mathbb{Z}^n$. Then $P(A,\boldsymbol{w})$ is an $(n-m)$-dimensional polytope, and in the following we show that there exists a point $\boldsymbol{c} \in P(A,\boldsymbol{w})$ with components

$$c_i \geq \frac{1}{\gamma},\ 1 \leq i \leq n. \tag{2.6}$$

Each vertex $\boldsymbol{y}$ of the polytope $P(A,\boldsymbol{w})$ is the unique solution of a linear system consisting of the m equations $A\,x = \boldsymbol{w}$ and $n-m$ equations of the type $x_{k_j} = 0$, $1 \leq j \leq n-m$. Hence, for each vertex $\boldsymbol{y}$ we can find a subset $I_{\boldsymbol{y}} \subset \{1,\ldots,n\}$ of cardinality m such that $A_{I_{\boldsymbol{y}}}\,(y_j : j \in I_{\boldsymbol{y}})^T = \boldsymbol{w}$ and $y_j = 0$ for $j \notin I_{\boldsymbol{y}}$. Here $A_{I_{\boldsymbol{y}}}$ denotes the $m \times m$-minor of A consisting of the columns with index in $I_{\boldsymbol{y}}$. Thus each non-zero coordinate y_i of a vertex satisfies

$$y_i \geq \frac{1}{\det A_{I_{\boldsymbol{y}}}}. \tag{2.7}$$

Taking the barycenter $\boldsymbol{c} = \frac{1}{\#V}\sum_{\boldsymbol{y}\in V}\boldsymbol{y}$, where V denotes the set of all vertices of $P(A,\boldsymbol{w})$, we get a relative interior point of $P(A,\boldsymbol{w})$; i.e., all coordinates of $\boldsymbol{c}$ are positive. By the inequality of the arithmetic and geometric mean we have for any sequence of positive numbers $a_1,\ldots,a_l$

$$\sum_{i=1}^{l}\frac{1}{a_i} \geq \frac{l^2}{\sum_{i=1}^{l} a_i},$$

and so we get by (2.7)

$$c_i \geq \frac{\#V}{\sum_{\boldsymbol{y}\in V}\det A_{I_{\boldsymbol{y}}}}.$$

Hence, together with the Cauchy-Schwarz inequality and the Cauchy-Binet formula we get

$$\begin{aligned} c_i &\geq \frac{\sqrt{\#V}}{\sqrt{\sum_{\boldsymbol{y}\in V}(\det A_{I_{\boldsymbol{y}}})^2}} \geq \frac{\sqrt{\#V}}{\sqrt{\sum_{m\times m\text{ minors }A_{I_m}}(\det A_{I_m})^2}} \\ &= \frac{\sqrt{\#V}}{\sqrt{\det A\,A^T}}. \end{aligned}$$

Since $\#V \geq n-m+1$ we obtain (2.6) which shows that the vector $\gamma\,\boldsymbol{w}$ can be written as a positive linear combination of the columns of A, where each scalar is at least 1. Thus, $\gamma\,\boldsymbol{w} \in \boldsymbol{v}+C$. $\square$

We want to point out that the assumption in Lemma 1.1 on $\boldsymbol{w}$ to be an interior point is necessary. For instance take $\boldsymbol{w} = (1,0)^T$ and

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & 0 \end{pmatrix}.$$

Then all points of the form $(2\,l+1)\,\boldsymbol{w}$, $l \in \mathbb{N}$, are not representable as non-negative integral combination of the columns.

3. Proof of Theorem 1.2.

We will construct a sequence $A_t \in \mathbb{Z}^{m\times n}$ as follows. Let us choose any $(n-m)$-dimensional subspace S such that the lattice $M = S \cap \mathbb{Z}^n$ has rank $n-m$ and the polyhedron $Q_S = \{\mathbf{1} + S\} \cap \mathbb{R}^n_{\geq 0}$ is bounded. Let B^n be the n-dimensional unit ball of radius 1 centered at the origin. Put $\lambda_i = \lambda_i(B^n \cap S, M)$, $1 \leq i \leq n-m$, and choose $n-m$ linearly independent integer vectors $\boldsymbol{b}_i$ corresponding to λ_i; i.e., $||\boldsymbol{b}_i|| = \lambda_i$, $1 \leq i \leq n-m$. Put

$$\xi = \frac{2^{n-m-1}}{(n-m)!\omega_{n-m}\mathrm{diam}\,(Q_S)\prod_{i=1}^{n-m-1}\lambda_i}\,.$$

Here $\mathrm{diam}\,(Q_S)$ denotes the diameter of Q_S; i.e., the maximum distance between two points of Q_S. Let P be the $(m+1)$-dimensional subspace orthogonal to the vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-m-1}$ so that $S^\perp \subset P$, where $S^\perp$ denotes the orthogonal complement of S.

There exists a sequence of m-dimensional subspaces $P_t \subset P$, $t = 1, 2, \ldots$, with the following properties:

(P1) the lattice $M_t = P_t \cap \mathbb{Z}^n$ has rank m and $\det(M_t) > t$;

(P2) Putting $S_t = P_t^\perp$ and $L_t = S_t \cap \mathbb{Z}^n$, the diameter of the polyhedron $Q_t = \{\xi \det(L_t)\mathbf{1} + S_t\} \cap \mathbb{R}^n_{\geq 0}$ satisfies the inequality

$$\mathrm{diam}\,(Q_t) < \frac{3}{2}\,\xi\, \det(L_t)\,\mathrm{diam}\,(Q_S)\,. \tag{3.1}$$

Remark 3.1. The sequence P_t clearly exists as it is enough to consider a sequence of approximations of a fixed basis of $S^\perp$ by m integer vectors from P and then observe that there exists only a finite number of integer sublattices of bounded determinant.

Let $\lambda_i(t) = \lambda_i(B^n \cap S_t, L_t)$ and let $\boldsymbol{b}_i(t)$, $1 \leq i \leq n-m$, be linearly independent integer vectors corresponding to the successive minima $\lambda_i(t)$. We will now show that for sufficiently large t

$$\lambda_i(t) = \lambda_i\,, \quad 1 \leq i \leq n-m-1\,. \tag{3.2}$$

Since $P_t \subset P$, the lattice L_t contains the vectors $\boldsymbol{b}_i$, $1 \leq i \leq n-m-1$. Noting that $\det(L_t) = \det(M_t) \to \infty$ as $t \to \infty$, the lower bound in Minkowski's second theorem (2.2) implies that $\lambda_{n-m}(t) \to \infty$ as $t \to \infty$. This, in turn, implies that for sufficiently large t the first $n-m-1$ successive minima $\lambda_i(t)$ are attained on vectors $\boldsymbol{b}_i$, $1 \leq i \leq n-m-1$ so that (3.2) holds. Hence by (2.2) and (3.2) we may write for sufficiently large t

$$\frac{2^{n-m}\det(L_t)}{(n-m)!\omega_{n-m}} \leq \lambda_1(t)\lambda_2(t)\cdots\lambda_{n-m}(t) = \lambda_{n-m}(t)\prod_{i=1}^{n-m-1}\lambda_i.$$

Thus, when t is large enough we have

$$\lambda_{n-m}(t) \geq \frac{2^{n-m}\det(L_t)}{(n-m)!\omega_{n-m}\prod_{i=1}^{n-m-1}\lambda_i}. \tag{3.3}$$

Now choose any basis $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in \mathbb{Z}^n$ of the lattice M_t and let A_t be the matrix with rows $\boldsymbol{a}_1^T, \ldots, \boldsymbol{a}_m^T$. Noting that the subspace $P^\perp$ has codimension 1 in S, take a vertex $\boldsymbol{p}_t$ of Q_t such that $\boldsymbol{p}_t + P^\perp$ does not intersect the interior of Q_t. Choose a supporting hyperplane H of the convex cone $\mathbb{R}^n_{\geq 0}$ at the point $\boldsymbol{p}_t$ such that $\{\boldsymbol{p}_t + P^\perp\} \subset H$. Next we take a point $\boldsymbol{z}_t \in \mathbb{Z}^n$ with the following properties:

(Z1) H separates $\boldsymbol{z}_t$ and $\mathbb{R}^n_{\geq 0}$;

(Z2) with respect to the maximum norm $||\cdot||_\infty$, $\boldsymbol{z}_t$ is the closest point to $\boldsymbol{p}_t$ that satisfies (Z1).

Then we clearly have

$$||\boldsymbol{z}_t - \boldsymbol{p}_t||_\infty \leq 1. \tag{3.4}$$

Consider the polytope $Q_{\boldsymbol{z}_t} = \{S_t + \boldsymbol{z}_t\} \cap \mathbb{R}^n_{\geq 0}$. By (3.4), the diameter of $Q_{\boldsymbol{z}_t}$ satisfies

$$\operatorname{diam}(Q_{\boldsymbol{z}_t}) \leq \operatorname{diam}(Q_t) + 2\sqrt{n}\,.$$

Thus, together with (3.1), (3.3) and by the choice of the number ξ, for all sufficiently large t

$$\operatorname{diam}(Q_{\boldsymbol{z}_t}) < \lambda_{n-m}(t)\,. \tag{3.5}$$

Note that, by the choice of the point $\boldsymbol{z}_t$, the affine subspace $\boldsymbol{z}_t + P^\perp$ does not intersect the cone $\mathbb{R}^n_{\geq 0}$ and, on the other hand, for all sufficiently large t the first $n-m-1$ successive minima of the lattice L_t are attained on the vectors $\boldsymbol{b}_i$, $1 \leq i \leq n-m-1$, that belong to the subspace $P^\perp$. The inequality (3.5) now implies that $Q_{\boldsymbol{z}_t}$ does not contain integer points when t is large enough.

By (3.4), $\boldsymbol{z}_t \in \{(\xi \det(L_t) - 1)\boldsymbol{1} + \mathbb{R}^n_{\geq 0}\}$, so that $A_t\,\boldsymbol{z}_t \in \{(\xi \det(L_t) - 1)\boldsymbol{v} + C\}$. Thus, for all sufficiently large t we have

$$g(A_t) \geq \xi \det(L_t) - 1\,.$$

The theorem is proved.

4. Distribution of sublattices of $\mathbb{Z}^n$.

This section which will collect several results due to Schmidt [29] on the distribution of integer lattices essentially coincides with section 3 of Aliev and Henk [4]. However, we include it for completeness. Two lattices L, L' are similar if there is a linear bijection $\phi : L \to L'$ such that for some fixed $c > 0$ we have $||\phi(\boldsymbol{x})|| = c||\boldsymbol{x}||$. Let $\tilde{O}_m$ be the group of matrices $K = (\boldsymbol{k}_1, \ldots, \boldsymbol{k}_m) \in GL_m(\mathbb{R})$ whose columns $\boldsymbol{k}_1, \ldots, \boldsymbol{k}_m$ have $||\boldsymbol{k}_1|| = \cdots = ||\boldsymbol{k}_m|| \neq 0$ and inner products $\langle \boldsymbol{k}_i, \boldsymbol{k}_j \rangle = 0$ for $i \neq j$. It is the product of the orthogonal group O_m and the group of nonzero multiples of the identity matrix. When $X = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) \in GL_m(\mathbb{R})$, we may uniquely write the matrix X in the form

$$X = KZ\,, \tag{4.1}$$

where $K \in \tilde{O}_m$ and

$$Z = \begin{pmatrix} 1 & x_{12} & \cdots & x_{1m} \\ 0 & y_2 & \cdots & x_{2m} \\ \vdots & & & \\ 0 & 0 & \cdots & y_m \end{pmatrix} \tag{4.2}$$

with $y_2, \ldots, y_m > 0$. The matrices Z as in (4.2) form the generalized upper half–plane $\mathcal{H} = \mathcal{H}_m$. For $Z \in \mathcal{H}$ and $M \in GL_m(\mathbb{R})$, we may write ZM in the form (4.1); that is, we uniquely have $ZM = KZ_M$ with $K \in \tilde{O}_m$ and $Z_M \in \mathcal{H}$. Thus, $GL_m(\mathbb{R})$ acts on $\mathcal{H}$; to M corresponds the map $Z \mapsto Z_M$. In particular, $GL_m(\mathbb{Z})$, as a subgroup of $GL_m(\mathbb{R})$, acts on $\mathcal{H}$. We will denote by $\mathcal{F}$ a fundamental domain for the action of

$GL_m(\mathbb{Z})$ on $\mathcal{H}$. We will also write μ for the $GL_m(\mathbb{R})$ invariant measure on $\mathcal{H}$ with $\mu(\mathcal{F}) = 1$.

Suppose now that $1 < m \le n$. There is a map (see p. 38 of Schmidt [29] for details) from lattices of rank m in $\mathbb{R}^n$ onto the set $\mathcal{H}/GL_m(\mathbb{Z})$ of orbits of $GL_m(\mathbb{Z})$ in $\mathcal{H}$. The lattices L, L' are similar precisely if they have the same image in $\mathcal{H}/GL_m(\mathbb{Z})$; hence the same image in $\mathcal{F}$. Similarity classes of lattices are parametrized by the elements of a fundamental domain $\mathcal{F}$.

A subset $\mathcal{D} \subset \mathcal{H}$ is called *lean* if $\mathcal{D}$ is contained in some fundamental domain $\mathcal{F}$. For $a > 0$, $b > 0$, let $\mathcal{H}(a, b)$ consist of $Z \in \mathcal{H}$ (in the form (4.2)) with

$$y_{i+1} \ge a y_i\,, \quad 1 \le i < m, \quad |x_{ij}| \le b y_i\,, \quad 1 \le i < j \le m.$$

Here we assume $y_1 = 1$.

Clearly, there is one-to-one correspondence between primitive vectors $\boldsymbol{b} \in \mathbb{Z}^n$ and the primitive $(n-1)$-dimensional sublattices of $\mathbb{Z}^n$. This correspondence was used in [4] to investigate the average behavior of $\mathrm{F}(\boldsymbol{a})$.

Let now $P(\mathcal{D}, T)$, where $\mathcal{D}$ is lean, be the number of primitive lattices $L \subset \mathbb{Z}^n$ with similarity class in $\mathcal{D}$ and determinant $\le T$.

Theorem 4.1 (Schmidt [29, Theorem 2]). *Suppose* $1 < m < n$ *and let* $\mathcal{D} \subset \mathcal{H}(a, b)$ *be lean and Jordan-measurable. Then, as* $T \to \infty$*,*

$$P(\mathcal{D}, T) \sim c_2(m, n)\mu(\mathcal{D})T^n \tag{4.3}$$

with

$$c_2(m, n) = \frac{1}{n}\binom{n}{m}\frac{\omega_{n-m+1}\cdots\omega_n}{\omega_1\omega_2\cdots\omega_m}\cdot\frac{\zeta(2)\cdots\zeta(m)}{\zeta(n-m+1)\cdots\zeta(n)}\,.$$

Here ω_l *is the volume of the unit ball in* $\mathbb{R}^l$ *and* $\zeta(\cdot)$ *is the Riemann zeta–function.*

Thus, roughly speaking, the proportion of primitive lattices with similarity class in $\mathcal{D}$ is $\mu(\mathcal{D})$.

As before we denote by $B^n \subset \mathbb{R}^m$ the n-dimensional ball of radius 1. Given a vector $\boldsymbol{u} = (u_1, u_2, \ldots, u_{m-1})^T \in \mathbb{R}^{m-1}$ with $u_i \ge 1$ $(1 \le i < m)$, the m-dimensional sublattices $L \subset \mathbb{Z}^n$ with

$$\frac{\lambda_{i+1}(B^n \cap \mathrm{span}_{\mathbb{R}}(L), L)}{\lambda_i(B^n \cap \mathrm{span}_{\mathbb{R}}(L), L)} \ge u_i$$

form a set of similarity classes, which will be denoted by $\mathcal{D}(\boldsymbol{u})$.

Theorem 4.2 (Schmidt [29, Theorem 5 (i)]). *The set* $\mathcal{D}(\boldsymbol{u})$ *may be realized as a lean, Jordan–measurable subset of* $\mathcal{H}$*. We have*

$$\mu(\mathcal{D}(\boldsymbol{u})) \ll_{m,n} \prod_{i=1}^{m-1} u_i^{-i(m-i)}\,. \tag{4.4}$$

Here $\ll_{m,n}$ *denotes the Vinogradov symbol with the constant depending on* m *and* n *only.*

5. The average behavior.

We recall that by (2.4) we have

$$\mathrm{g}(A) \le \frac{n-m}{2}\lambda_{n-m}(B^n \cap \mathrm{span}_{\mathbb{R}}(L_A^{\perp}), L_A^{\perp}),$$

where B^n is the n-dimensional ball of radius 1 centered at the origin. Thus, with $L = L_A$, $\Gamma = (\det(L))^{-\frac{1}{n-m}} L^{\perp}$ we may write

$$\mathrm{g}(L) \leq \frac{(n-m)(\det(L))^{\frac{1}{n-m}}}{2} \lambda_{n-m}(B^n \cap \mathrm{span}_{\mathbb{R}}(\Gamma), \Gamma). \tag{5.1}$$

Observe that $\det(L) = \det(L^{\perp})$ (cf. (2.1)) and that the determinant of Γ is 1. We consider the sequence of discrete random variables $X_T : G(m, n, T) \to \mathbb{R}_{\geq 0}$ defined as

$$X_T(L) = \frac{\mathrm{g}(L)}{(\det(L))^{\frac{1}{n-m}}}\,.$$

Recall that the *cumulative distribution function* (CDF) F_T of X_T is defined for $t \in \mathbb{R}_{\geq 0}$ as

$$F_T(t) = \mathrm{Prob}_{\,m,n,T}(X_T \leq t\,)\,.$$

In order to apply Schmidt's result stated in the previous section, let a real number $u \geq 1$, $\boldsymbol{\delta}_i(u) = (u_1, u_2, \ldots, u_{n-m-1})$ be the vector with $u_i = u$ and $u_j = 1$ for all $j \neq i$. Define the set $\mathcal{D}(u)$ of similarity classes as (cf. section 3)

$$\mathcal{D}(u) = \bigcup_{i=1}^{n-m-1} \mathcal{D}(\boldsymbol{\delta}_i(u))\,.$$

By (4.4) the measure of this set satisfies

$$\mu(\mathcal{D}(u)) \ll_{m,n} \frac{1}{u^{n-m-1}}\,. \tag{5.2}$$

Let $Y_T : G(m, n, T) \to \mathbb{R}_{>0}$ be the sequence of random variables defined as

$$Y_T(L) = \sup\{v \in \mathbb{R}_{>0} : L \in \mathcal{D}(c_1 v^{2/(n-m-1)})\}\,,$$

where the constant $c_1 = c_1(m, n)$ is given by

$$c_1 = \frac{\omega_{n-m}^{\frac{2}{(n-m)(n-m-1)}}}{(n-m)^{2/(n-m-1)}}.$$

Since the set $\mathcal{D}(1)$ contains all similarity classes we have for all $L \in G(m, n, T)$

$$Y_T(L) \geq c_1^{-(n-m-1)/2}. \tag{5.3}$$

Next we need the following observation.

Lemma 5.1. *Let $\lambda_i := \lambda_i(B^n \cap \mathrm{span}_{\mathbb{R}}(\Gamma), \Gamma)$, $1 \leq i \leq n-m$, and let $\lambda_{n-m} > \lambda > 0$. Then there exists an index $i \in \{1, \ldots, n-m-1\}$ with*

$$\frac{\lambda_{i+1}}{\lambda_i} > c_2(m, n)\lambda^{2/(n-m-1)}\,,$$

where $c_2(m, n) = 2^{-\frac{2}{n-m-1}} \omega_{n-m}^{\frac{2}{(n-m)(n-m-1)}}$.

Proof. Suppose the opposite; i.e.,

$$\frac{\lambda_{i+1}}{\lambda_i} \leq c_2(m, n)\lambda^{2/(n-m-1)}$$

for all $1 \le i \le n-m-1$. Then, $\lambda_{n-m} \le (c_2(n,m)\lambda^{2/(n-m-1)})^{n-m-i}\lambda_i$, and by Minkowski's second fundamental theorem (2.2)

$$\lambda_1\lambda_2\cdots\lambda_{n-m} \le \frac{2^{n-m}}{\omega_{n-m}}\,. \tag{5.4}$$

Thus we obtain the contradiction

$$\lambda_{n-m} \le (c_2(m,n)\lambda^{2/(n-m-1)})^{\frac{(n-m-1)}{2}}\frac{2}{\omega_{n-m}^{1/(n-m)}} = \lambda\,. \qquad \square$$

Let now $\tilde{F}_T$ be the CDF of the random variable Y_T.

LEMMA 5.2. *For any $T \ge 1$ and $t \ge 0$ we have*

$$\tilde{F}_T(t) \le F_T(t).$$

Proof. Let $\lambda_i := \lambda_i(B^n \cap \operatorname{span}_{\mathbb{R}}(\Gamma), \Gamma)$, $1 \le i \le n-m$. By (5.1), we have

$$\frac{\mathrm{g}(L)}{(\det(L))^{\frac{1}{n-m}}} \le \frac{(n-m)}{2}\lambda_{n-m}\,.$$

Hence, if for some t

$$X_T(L) = \frac{\mathrm{g}(L)}{(\det(L))^{\frac{1}{n-m}}} > t,$$

then clearly $\lambda_{n-m} > \frac{2t}{(n-m)}$. By Lemma 5.1, applied with $\lambda = \frac{2t}{(n-m)}$, we get

$$\frac{\lambda_{i+1}}{\lambda_i} > c_1(m,n)t^{2/(n-m-1)}\,.$$

Consequently, the lattice Γ belongs to a similarity class in $\mathcal{D}(c_1 t^{2/(n-m-1)})$ so that $Y_T(L) > t$. Therefore,

$$\begin{aligned}\mathrm{Prob}_{\,m,n,T}(X_T \le t\,) &= 1 - \frac{\#\{L \in G(m,n,T) : \mathrm{g}(L)/(\det(L))^{\frac{1}{n-m}} > t\}}{\#G(m,n,T)}\\ &\ge 1 - \frac{\#\{L \in G(m,n,T) : Y_T(L) > t\}}{\#G(m,n,T)}\\ &= \mathrm{Prob}_{\,m,n,T}(Y_T \le t\,). \qquad \square\end{aligned}$$

The proofs of Theorems 1.3 and 1.4 are now an easy consequence of Lemma 5.2 and Schmidt's results on the distribution of sublattices.

Proof of Theorem 1.3. By Lemma 5.2 and Theorem 4.1 we have

$$\begin{aligned}\mathrm{Prob}_{\,m,n,T}(\mathrm{g}(L)/(\det(L))^{\frac{1}{n-m}} > t) &= 1 - F_T(t) \le 1 - \tilde{F}_T(t)\\ &= \frac{\#\{L \in G(m,n,T) : Y_T(L) > t\}}{\#G(m,n,T)}\\ &\ll_{m,n} \mu(\mathcal{D}(c_1 t^{\frac{2}{n-m-1}})) \ll_{m,n} t^{-2}. \qquad \square\end{aligned}$$

Proof of Theorem 1.4. Let $E(\cdot)$ denote the mathematical expectation. Since for any non-negative real-valued random variable X

$$E(X) = \int_0^\infty (1 - F_X(t))dt\,, \tag{5.5}$$

Lemma 5.2 implies that $E(X_T) \le E(Y_T)$ and, consequently,

$$\sup_T E(X_T) \le \sup_T E(Y_T)\,. \tag{5.6}$$

Next, by Theorem 4.1 we also have

$$\begin{aligned} 1 - \tilde{F}_T(t) &= \frac{\#\{L \in G(m,n,T) : Y_T(L) > t\}}{\#G(m,n,T)} \\ &\ll_{m,n} \mu(\mathcal{D}(c_1 t^{\frac{2}{n-m-1}})) \ll_{m,n} t^{-2}. \end{aligned}$$

Thus, by (5.5), (5.6), and observation (5.3), we obtain

$$\sup_T E(X_T) \ll_{m,n} \int_{c_1^{-(n-m-1)/2}}^\infty t^{-2}\,dt \ll_{m,n} 1,$$

which proves the theorem. □

6. Appendix: On upper bounds for the Frobenius number.

From the viewpoint of analysis of integer programming algorithms, upper bounds for the Frobenius number $\mathrm{F}(\boldsymbol{a})$ in terms of the input vector $\boldsymbol{a}$ are of primary interest. All known upper bounds are of order $||\boldsymbol{a}||^2$ and, as it was shown in Erdös and Graham [11], the quantity $||\boldsymbol{a}||^2$ plays a role of a limit for estimating the Frobenius number $\mathrm{F}(\boldsymbol{a})$ from above. For $n = 3$ Beck and Zacks [7] conjectured that, except for a special family of input vectors, the Frobenius number does not exceed $c(a_1a_2a_3)^\alpha$ with absolute constants c and $\alpha < 2/3$. This conjecture has been disproved by Schlage-Puchta [28]. As a special case, the latter result implies that, roughly speaking, cutting off special families of input vectors cannot make the order of upper bounds for g_3 smaller than $||\boldsymbol{a}||^2$.

In this appendix we consider the general case $n \ge 3$ and show that the order $||\boldsymbol{a}||^2$ cannot be improved along any given "direction" $\boldsymbol{\alpha} \in \mathbb{R}^n$. Although the proof of this result follows the general line of the proof of Theorem 1.2, in this special setting it can be significantly simplified.

For $\boldsymbol{a} \in \mathbb{Z}^n_{>0}$ and $t \in \mathbb{Z}$, let

$$V_{\boldsymbol{a}}(t) = \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a}^T\boldsymbol{x} = t\}$$

and $\Lambda_{\boldsymbol{a}}(t) = V_{\boldsymbol{a}}(t) \cap \mathbb{Z}^n$. Here and throughout the rest of the paper we consider $V_{\boldsymbol{a}}(t)$ as a usual $(n-1)$-dimensional Euclidean space. Denote by $S_{\boldsymbol{a}}(t)$ the $(n-1)$-dimensional simplex $V_{\boldsymbol{a}}(t) \cap \mathbb{R}^n_{\ge 0}$. For convenience we will also use the notation $V_{\boldsymbol{a}} = V_{\boldsymbol{a}}(0)$ and $\Lambda_{\boldsymbol{a}} = \Lambda_{\boldsymbol{a}}(0)$. With respect to that notation, Kannan [16] showed that

$$\mathrm{F}(\boldsymbol{a}) - ||\boldsymbol{a}||_1 = \mu(S_{\boldsymbol{a}}(1), \Lambda_{\boldsymbol{a}}(1))\,. \tag{6.1}$$

Fix a point $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_{n-1}, 1)$, $n \ge 3$, with $0 \le \alpha_1 \le \alpha_2 \le \ldots \le \alpha_{n-1} \le 1$.

THEOREM 6.1. *There exists a sequence of integer vectors $\boldsymbol{a}(t)$ and a constant $c_3 = c_3(\boldsymbol{\alpha})$ such that*

$$\mathrm{F}(\boldsymbol{a}(t)) > c_3||\boldsymbol{a}(t)||^2 + ||\boldsymbol{a}(t)||_1 \quad t = 1, 2, \ldots \tag{6.2}$$

and for any $\epsilon > 0$ we have

$$\left\| \boldsymbol{\alpha} - \frac{\boldsymbol{a}(t)}{||\boldsymbol{a}(t)||_\infty} \right\| < \epsilon \tag{6.3}$$

for all sufficiently large t.

Proof. Without loss of generality, we may assume that $\boldsymbol{\alpha} \in \mathbb{Q}^n$ and

$$0 < \alpha_1 < \alpha_2 < \cdots < \alpha_{n-1} < 1\,. \tag{6.4}$$

Let us choose an integer number q such that $\boldsymbol{a} := q\boldsymbol{\alpha}$ is a primitive integer vector in $\mathbb{Z}^n_{>0}$. Put $\lambda_i = \lambda_i(B^n \cap \mathrm{span}_{\mathbb{R}}\Lambda_{\boldsymbol{a}}, \Lambda_{\boldsymbol{a}})$, $1 \le i \le n-1$, and choose $n-1$ linearly independent integer vectors $\boldsymbol{a}_i$ corresponding to λ_i. Then we clearly have $||\boldsymbol{a}_i|| = \lambda_i$, $1 \le i \le n-1$.

Next let $P_{\boldsymbol{a}}$ be the 2-dimensional plane orthogonal to the vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-2}$. The plane $P_{\boldsymbol{a}}$ can be considered as a usual Euclidean 2-dimensional plane. Thus, one can choose a sequence $\boldsymbol{a}(t)$ of primitive vectors of the lattice $P_{\boldsymbol{a}} \cap \mathbb{Z}^n$ with the following properties:

(A1) $\boldsymbol{a}(t) \ne \boldsymbol{a}$ for $t = 1, 2, \ldots$;

(A2) For any $\epsilon > 0$ the inequality (6.3) holds for all sufficiently large t.

Let $\lambda_i(t) = \lambda_i(B^n \cap \mathrm{span}_{\mathbb{R}}\Lambda_{\boldsymbol{a}(t)}, \Lambda_{\boldsymbol{a}(t)})$, $1 \le i \le n-1$, and let $\boldsymbol{a}_i(t)$, $1 \le i \le n-1$, be linearly independent integer vectors corresponding to the successive minima $\lambda_i(t)$. Similarly to (3.2) we have

$$\lambda_i(t) = \lambda_i\,, \quad 1 \le i \le n-2 \tag{6.5}$$

for all sufficiently large t.

By (6.5) and Minkowski's second fundamental theorem (2.2),

$$\frac{2^{n-1}||\boldsymbol{a}(t)||}{(n-1)!\omega_{n-1}} \le \lambda_1(t)\lambda_2(t)\cdots\lambda_{n-1}(t) = \lambda_{n-1}(t)\prod_{i=1}^{n-2}\lambda_i$$

so that

$$\lambda_{n-1}(t) \ge \frac{2^{n-1}||\boldsymbol{a}(t)||}{(n-1)!\omega_{n-1}\prod_{i=1}^{n-2}\lambda_i} \tag{6.6}$$

for all sufficiently large t.

The vectors $\boldsymbol{a}(t)$ are primitive and by (6.4) for all sufficiently large t we have $\boldsymbol{a}(t) \in \mathbb{Z}^n_{>0}$. Thus, the Frobenius numbers $\mathrm{F}(\boldsymbol{a}(t))$ are well defined when t is large enough. Observe also that by (6.1)

$$\mathrm{F}(\boldsymbol{a}(t)) - ||\boldsymbol{a}(t)||_1 = \mu(S_{\boldsymbol{a}(t)}(1), \Lambda_{\boldsymbol{a}(t)}(1))\,.$$

In view of (6.3) and (6.4) one can choose some constant $r = r(\boldsymbol{\alpha})$ such that for all sufficiently large t a translate of $S_{\boldsymbol{a}(t)}(1)$ lies in $\frac{r}{||\boldsymbol{a}(t)||}B^n_1$. Therefore,

$$\begin{aligned}\mathrm{F}(\boldsymbol{a}(t)) - ||\boldsymbol{a}(t)||_1 &> \mu\left(\frac{r}{||\boldsymbol{a}(t)||}B^n(t) \cap V_{\boldsymbol{a}(t)}, \Lambda_{\boldsymbol{a}(t)}\right)\\ &= \frac{||\boldsymbol{a}||}{r}\mu(B^n \cap V_{\boldsymbol{a}(t)}, \Lambda_{\boldsymbol{a}(t)})\,.\end{aligned}$$

By the lower bound in Jarnik's inequalities (2.3), we have

$$\mu(B_1^n \cap V_{\boldsymbol{a}(t)}, \Lambda_{\boldsymbol{a}(t)}) \geq \frac{\lambda_{n-1}(t)}{2}$$

and with (6.6) we finally get

$$\mathrm{F}(\boldsymbol{a}(t)) - ||\boldsymbol{a}(t)||_1 > \frac{2^{n-2}}{(n-1)!\omega_{n-1} r(\boldsymbol{\alpha}) \prod_{i=1}^{n-2} \lambda_i} ||\boldsymbol{a}(t)||^2$$

for all sufficiently large t. □

Acknowledgment. The authors are grateful to the referees for valuable comments.

REFERENCES

[1] K. Aardal, C. A. J. Hurkens, and A. K. Lenstra, *Solving a system of linear Diophantine equations with lower and upper bounds on the variables*, Math. Oper. Res., 25 (2000), pp. 427–442.

[2] K. Aardal and A. Lenstra, *Hard equality constrained integer knapsacks*, Math. Oper. Res., 29 (2004), pp. 724–738.

[3] K. Aardal, R. Weismantel, and L. A. Wolsey, *Non-standard approaches to integer programming*, Discrete Appl. Math., 123 (2002), pp. 5–74.

[4] I. Aliev and M. Henk, *Integer knapsacks: Average behavior of the Frobenius numbers*, Math. Oper. Res., 34 (2009), pp. 698–705.

[5] I. Aliev, M. Henk, and A. Hinrichs, *Expected Frobenius numbers*, J. Combin. Theory Ser. A, to appear.

[6] V. I. Arnold, *Geometry and growth rate of Frobenius numbers of additive semigroups*, Math. Phys. Anal. Geom., 9 (2006), pp. 95–108.

[7] M. Beck and S. Zacks, *Refined upper bounds for the linear Diophantine problem of Frobenius*, Adv. Appl. Math., 32 (2004), pp. 454–467.

[8] D. Beihoffer, J. Hendry, A. Nijenhuis, and S. Wagon, *Faster algorithms for Frobenius numbers*, Electron. J. Combin., 12 (2005), Research Paper 27, 38 pp. (electronic).

[9] C. E. Blair and R. G. Jeroslow, *The value function of an integer program*, Math. Prog., 23 (1982), pp. 237–273.

[10] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, Berlin, 1971.

[11] P. Erdős and R. Graham, *On a linear Diophantine problem of Frobenius*, Acta Arith., 21 (1972), pp. 399–408.

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

[13] P. M. Gruber, *Convex and Discrete Geometry*, Springer, Berlin, 2007.

[14] P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, North–Holland, Amsterdam, 1987.

[15] P. Hansen and J. Ryan, *Testing integer knapsacks for feasibility*, European J. Oper. Res., 88 (1996), pp. 578–582.

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

[17] R. Kannan and L. Lovász, *Covering minima and lattice-point-free convex bodies*, Ann. of Math. (2), 128 (1988), pp. 577–602.

[18] R. M. Karp, *Reducibility among combinatorial problems*, in Complexity of Computer Computations, R. E. Miller and J. W. Thatcher, eds, Plenum, New York, 1972, pp. 85–103.

[19] A. G. Khovanskii, *The Newton polytope, the Hilbert polynomial and sums of finite sets*, Funktsional. Anal. i Prilozhen., 26 (1992), pp. 57–63.

[20] M. J. Knight, *A generalization of a result of Sylvester's*, J. Number Theory, 12 (1980), pp. 364–366.

[21] J-B, Lasserre, *A discrete Farkas lemma*, Discrete Optim., 1 (2004), pp. 67–75.

[22] J. Lee, S. Onn, and R. Weismantel, *Nonlinear optimization over a weighted independence system*, in Lecture Notes in Comput. Sci. 5564, Springer, Berlin, 2009, pp. 251–264.

[23] J. Marklof, *The asymptotic distribution of Frobenius numbers*, Invent. Math., 181 (2010), pp. 179–207.

[24] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Grundlehren Math. Wiss. 327, Springer, New York, 2003.

[25] P. Pleasants, H. Ray, and J. Simpson, *The Frobenius problem on lattices*, Australas. J. Combin., 32 (2005), pp. 27–45.

[26] J. L. Ramírez Alfonsín, *Complexity of the Frobenius problem*, Combinatorica, 16 (1996), pp. 143–147.

[27] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Ser. Math. Appl., Oxford Univ. Press, New York, 2005.

[28] J.-C. Schlage-Puchta, *An estimate for Frobenius' Diophantine problem in three dimensions*, J. Integer Seq., 8 (2005), Article 05.1.7, 4 pp. (electronic).

[29] W. M. Schmidt, *The distribution of sublattices of Z^m*, Monatsh. Math., 125 (1998), pp. 37–81.

[30] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, Chichester, 1986.

[31] V. Shur, Ya. Sinai, and A. Ustinov, *Limiting distribution of Frobenius numbers for $n = 3$*, J. Number Theory, 129 (2009), pp. 2778–2789.

[32] R. J. Simpson and R. Tijdeman, *Multi-dimensional versions of a theorem of Fine and Wilf and a formula of Sylvester*, Proc. Amer. Math. Soc., 131 (2003), pp. 1661–1671.

[33] J. Vaaler, *A geometric inequality with applications to linear forms*, Pacific J. Math., 83 (1979), pp. 543–553.

[34] B. Vizvári, *Beiträge zum Frobenius Problem*, D. Sc. Nat. Dissertation, Technische Hochschule Carl Schorlemmer, Leuna-Merseburg, Germany, 1987.