Integer points in knapsack polytopes and *s*-covering radius

Iskander Aliev

School of Mathematics
Cardiff University
Cardiff, Wales, UK

alievi@cf.ac.uk

Martin Henk and Eva Linke[*]

Fakultät für Mathematik
OvG-Universität Magdeburg
39106 Magdeburg, Germany

{martin.henk, eva.linke}@ovgu.de

Abstract

Given a matrix $A \in \mathbb{Z}^{m \times n}$ satisfying certain regularity assumptions, we consider for a positive integer s the set $\mathcal{F}_s(A) \subset \mathbb{Z}^m$ of all vectors $\boldsymbol{b} \in \mathbb{Z}^m$ such that the associated *knapsack polytope*

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

contains at least s integer points. We present lower and upper bounds on the so called diagonal s-Frobenius number associated to the set $\mathcal{F}_s(A)$. In the case $m = 1$ we prove an optimal lower bound for the s-Frobenius number, which is the largest integer b such that $P(A, b)$ contains less than s integer points.

Keywords: Knapsack polytope, s-Frobenius numbers, inhomogeneous minimum, covering radius, successive minima

1 Introduction and statement of results

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

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

and let $\boldsymbol{b} \in \mathbb{Z}^m$. The *knapsack polytope* $P(A, \boldsymbol{b})$ is defined as

$$P(A, \boldsymbol{b}) = \{\boldsymbol{x} \in \mathbb{R}^n_{\geqslant 0} : A\boldsymbol{x} = \boldsymbol{b}\}. \tag{2}$$

Note that on account of (1) ii), $P(A, \boldsymbol{b})$ is indeed a polytope (or empty).

Let s be a positive integer. Consider the set $\mathcal{F}_s(A)$ of integer vectors $\boldsymbol{b}$ such that the knapsack polytope (2) contains at least s integer points, i.e.,

$$\mathcal{F}_s(A) = \{\boldsymbol{b} \in \mathbb{Z}^m : \#(P(A, \boldsymbol{b}) \cap \mathbb{Z}^n) \geqslant s\}.$$

Integer points in knapsack polytopes are a classical topic of study in combinatorics (see e.g. [18] and [19]) and in the integer linear programming (see e.g. [3] and [21]). In this paper we will study the combinatorial structure of $\mathcal{F}_s(A)$ using results from Minkowski's geometry of numbers and discrete geometry (see e. g. [13] and [14]).

First we address the special case $m = 1$. The matrix A now has the form $A = \boldsymbol{a}^{\mathsf{T}}$, where $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)^{\mathsf{T}}$ is an integer vector and (1) i) says that $\gcd(a_1, a_2, \ldots, a_n) = 1$, i.e., $\boldsymbol{a}$ is a *primitive* integer vector. Due to the second assumption (1) ii) we may assume that all entries of $\boldsymbol{a}$ are positive. The set $\mathcal{F}_s(\boldsymbol{a}^{\mathsf{T}})$ in this case contains all consecutive integers larger than the *s-Frobenius number*

$$\mathrm{F}_s(\boldsymbol{a}) := \max\{b \in \mathbb{Z} : \#(P(\boldsymbol{a}^{\mathsf{T}}, b) \cap \mathbb{Z}^n) < s\}$$

associated with vector $\boldsymbol{a}$. The s-Frobenius numbers have been introduced and studied by Beck and Robins in [8]. For more recent results please see [1], [7], [11] and [22]. Thus when $m = 1$ we have

$$\mathrm{int}\,(\mathrm{F}_s(\boldsymbol{a}) + \mathbb{R}_{\geqslant 0}) \cap \mathbb{Z} = \mathrm{F}_s(\boldsymbol{a}) + \mathbb{Z}_{>0} \subset \mathcal{F}_s(\boldsymbol{a}^{\mathsf{T}}), \tag{3}$$

where $\mathrm{int}\,(\cdot)$ denotes the interior of the set.

Note that $\mathrm{F}_1(\boldsymbol{a})$ is the classical *Frobenius number* associated with $a_1, \ldots, a_n$. The general problem of finding $\mathrm{F}_1(\boldsymbol{a})$, the *Frobenius problem*, is well known to be NP-hard (Ramírez Alfonsín [18, 19]). Kannan [15] proved that for fixed n the Frobenius problem can be solved in polynomial time. The proof is based on results from the algorithmic geometry of numbers and the integer programming.

In practice, computing Frobenius numbers remains a difficult computational problem even when dimension n is fixed. Thus the upper and lower bounds for $\mathrm{F}_1(\boldsymbol{a})$ are of special interest. In terms of the input vector $\boldsymbol{a}$, all known upper bounds for $\mathrm{F}_1(\boldsymbol{a})$ (see, e.g., Erdős and Graham [9] and Fukshansky and Robins [10]) can be represented in the form

$$\mathrm{F}_1(\boldsymbol{a}) \leqslant \mathrm{c}_n\, \boldsymbol{a}^{\mathsf{T}}\boldsymbol{a}, \tag{4}$$

for a certain constant c_n depending on the dimension. The quadratic order of (4) with respect to $\boldsymbol{a}$ is in general best possible (see, e.g., [3] and [5]).

On the other hand, Aliev and Gruber [2] proved that Frobenius numbers possess an optimal lower bound. Indeed

$$\mathrm{F}_1(\boldsymbol{a}) \geqslant \vartheta_1(S_{n-1}) \left(\prod_{i=1}^{n} a_i\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i, \tag{5}$$

where $\vartheta_1(S_{n-1})$ is the *absolute inhomogeneous minimum* of an $(n-1)$-dimensional simplex S_{n-1}.

Interestingly, the s-Frobenius number can be bounded from above by $\mathrm{F}_1(\boldsymbol{a})$ plus a term of the same order in $\boldsymbol{a}$ as the main term in the lower bound (5). The following upper bound on the s-Frobenius number was recently obtained in [1]

$$\mathrm{F}_s(\boldsymbol{a}) \leqslant \mathrm{F}_1(\boldsymbol{a}) + (s-1)^{\frac{1}{n-1}} \left((n-1)! \prod_{i=1}^n a_i \right)^{\frac{1}{n-1}} .$$

The first goal of the present paper is to obtain an optimal lower bound for $\mathrm{F}_s(\boldsymbol{a})$ that applies for all s. To this end, we will need a generalization of the quantity $\vartheta_1(S_{n-1})$ for a slightly more general setting.

By a *lattice* $L \subset \mathbb{R}^n$ we will understand a discrete submodule of the Euclidean space $\mathbb{R}^n$. Given an d-dimensional lattice L, its *determinant* $\det(L)$ is the d-dimensional volume (i.e. d-dimensional Lebesgue measure) of the parallelepiped spanned by the vectors of a basis of L. By a *convex body* $K \subset \mathrm{span}_{\mathbb{R}}(L)$ we will understand a compact convex set with nonempty interior in the Euclidean space $\mathrm{span}_{\mathbb{R}}(L) \subset \mathbb{R}^n$ spanned by the lattice L.

For a lattice $L \subset \mathbb{R}^n$ and a convex body $K \subset \mathrm{span}_{\mathbb{R}}(L)$ let

$$\mu_s(K, L) = \min\{\mu > 0 : \text{for all } \boldsymbol{x} \in \mathrm{span}_{\mathbb{R}}(L) \text{ there exist distinct } \boldsymbol{y}_1, \dots, \boldsymbol{y}_s \in L \qquad (6)$$
$$\text{such that } \boldsymbol{x} \in \boldsymbol{y}_i + \mu K \ \forall \ 1 \leqslant i \leqslant s\}$$

be the smallest positive number such that any $\boldsymbol{x} \in \mathrm{span}_{\mathbb{R}}(L)$ is covered by at least s lattice translates of $\mu_s K$. $\mu_s(K, L)$ is called the *s-covering radius* of K with respect to L. For $s = 1$ we get the well-known covering radius for which we refer to [13] and [14].

Following Gruber [12], given a convex body $K \subset \mathbb{R}^n$ we define

$$\vartheta_s(K) = \inf \frac{\mu_s(K, L)}{\det(L)^{1/n}} ,$$

where the infimum is taken over all n-dimensional lattices L in $\mathbb{R}^n$. We call the quantity $\vartheta_s(K)$ the *absolute s-inhomogeneous minimum*. For $s = 1$ we get the classical absolute inhomogeneous minimum used in (5).

Our first theorem shows that (5) can be generalized to an optimal lower bound on the s-Frobenius number.

Theorem 1.

i) Let $n \geqslant 3$, $s \geqslant 1$. Then

$$\mathrm{F}_s(\boldsymbol{a}) \geqslant \vartheta_s(S_{n-1}) \left(\prod_{i=1}^n a_i \right)^{\frac{1}{n-1}} - \sum_{i=1}^n a_i . \qquad (7)$$

ii) For any $\epsilon > 0$ and $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{R}^{n-1}$ with $0 < \alpha_1 \leqslant \cdots \leqslant \alpha_{n-1}$, there exists a vector $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ such that

$$\left| \alpha_i - \frac{a_i}{a_n} \right| < \epsilon, \quad i = 1, 2, \ldots, n-1 \tag{8}$$

and

$$\frac{\mathrm{F}_s(\boldsymbol{a}) + \sum_{i=1}^{n} a_i}{(a_1 \cdots a_n)^{1/(n-1)}} < \vartheta_s(S_{n-1}) + \epsilon. \tag{9}$$

Note that the part ii) shows that integer vectors with relatively small Frobenius numbers approximate any given "direction" $\boldsymbol{\alpha} \in \mathbb{R}^{n-1}$.

In the general case, the structure of the set $\mathcal{F}_s(A)$, apart from a few special cases, is not well understood. It is well known that the set $\mathcal{F}_1(A)$ can be decomposed into the set of all integer points in the interior of a certain translated cone and a complex complementary set. More recent results (see [3]) attempt to estimate the "location" of such a cone in terms of $\det(AA^{\intercal})$. Following the approach of [3], we will define a suitable generalization of the Frobenius number.

Let C be the cone generated by the columns of A and let $\boldsymbol{v} = A\mathbf{1}$, where $\mathbf{1}$ is the all-1-vector. By the *diagonal s-Frobenius number* $\mathrm{g}_s(A)$ *of* A we understand the minimal $t \geqslant 0$, such that for all integer vectors $\boldsymbol{b}$ in the interior of the translated cone $t\boldsymbol{v} + C$ the knapsack polytope $P(A, \boldsymbol{b})$ contains at least s integer points, i.e.,

$$\mathrm{g}_s(A) = \min \left\{ t \in \mathbb{R}_{\geqslant 0} : \mathrm{int}(t\boldsymbol{v} + C) \cap \mathbb{Z}^m \subseteq \mathcal{F}_s(A) \right\}.$$

Note that the elements of set $\mathcal{F}_s(A)$ are exactly the vectors $\boldsymbol{b}$ such that the integer programming feasibility problem:

$$\text{Does } P(A, \boldsymbol{b}) \text{ contain at least } s \text{ integer vectors?} \tag{10}$$

is solved in affirmative. When $s = m = 1$, the problem is often called *integer knapsack problem* and is well-known to be NP-complete (see e.g. Section 15.6 in Papadimitriou and Steiglitz [16]). Therefore, given any upper bound $\mathrm{g}_s(A) \leqslant f(A)$ that can be computed in polynomial time, the complimentary set $\mathcal{F}_s(A) \setminus (\mathrm{int}(f(A)\boldsymbol{v} + C) \cap \mathbb{Z}^m)$ is likely to have a complex combinatorial structure. Roughly speaking, from the integer programming point of view, the upper bounds attempt to determine as small as possible set that contains all "computationally hard" instances $A, \boldsymbol{b}$.

The next result of this paper gives an upper bound on $\mathrm{g}_s(A)$ in terms of s and $\det(AA^{\intercal})$.

Theorem 2. *Let $n > m \geqslant 1$, $s \geqslant 1$. Then*

$$\mathrm{g}_s(A) \leqslant \frac{n-m}{2}\sqrt{\det(AA^{\intercal})} + \frac{(s-1)^{\frac{1}{n-m}}}{2} \left(\sqrt{\det(AA^{\intercal})} \right)^{\frac{1}{n-m}}. \tag{11}$$

When $s = 1$, (11) improves Theorem 1.1 in Aliev and Henk [3] by the factor $\frac{1}{2}n^{-\frac{1}{2}}$. The proof of the theorem is based on estimating $g_s(A)$ using the s-covering radius (6).

The problem of estimating the quantity $g_s(A)$ from below appears to be harder. The natural normalization $(\prod_{i=1}^{n} a_i)^{\frac{1}{n-1}}$ in (7) reflects the fact that in the case $m = 1$ the knapsack polytope $P(\boldsymbol{a}^\intercal, b)$ is always a simplex. In the general case, $P(A, \boldsymbol{b})$ may have a complex combinatorial structure even in the special choice $\boldsymbol{b} = \boldsymbol{v}$. Thus $g_s(A)$ does not seem to possess a lower bound with *simple* natural normalization that applies for all s and matrices A of any size. In this paper we tackle this problem by using lower estimates for the s-covering radius. The following theorem gives the first ever lower bound for $g_s(A)$ in the general case.

Theorem 3. *Let $n > m \geqslant 1$ and $s \geqslant 1$. Then*

$$g_s(A) \geqslant \frac{1}{n - m + 1} \left(s^{\frac{1}{n-m}} \det(AA^\intercal)^{\frac{1}{n-m}} \left(\frac{m(A)}{M(A)} \right)^2 \sqrt{\frac{n - m}{n}} \right.$$
$$\left. - (n - m) - 2 \frac{m(A)}{M(A)} \right),$$

where $m(A)$ and $M(A)$ denote the minimal and maximal absolute m-minors of A.

Pleasants et al. [17] extensively studied the special case $s = 1$ and $m = n - 1$ and proved, in particular, that the set $\mathcal{F}_1(A)$ has the following remarkable property. It is shown in Theorem 6.1 of [17] that there exists a unique maximal (w.r.t. inclusion) translated cone $\boldsymbol{h} + C$ such that all integral points in its interior belong to $\mathcal{F}_1(A)$, but there are (infinitely many) integral points on its boundary which are not in $\mathcal{F}_1(A)$. In general, i.e., for $1 < m < n - 1$, such a cone is not uniquely determined, see, for instance, [4] and Section 5. Theorem 6.1 of [17] also describes the location of the unique maximal cone $\boldsymbol{h} + C$. We show that this result implies an explicit formula for the diagonal Frobenius number $g_1(A)$.

Theorem 4. *Let $m = n - 1$, $s = 1$, and let $\boldsymbol{z} = (z_1, z_2, \ldots, z_n)^\intercal$ be a primitive integral generator of the kernel of A, i.e., $\boldsymbol{z} \in \mathbb{Z}^n$, $A\boldsymbol{z} = 0$ and $\gcd(z_1, z_2, \ldots, z_n) = 1$. Then we have*

$$g_1(A) = \frac{z^+ z^-}{z^+ + z^-} - 1,$$

where $z^+ = \max\{z_i : z_i > 0\}$ and $z^- = \max\{|z_i| : z_i < 0\}$.

The structure of the paper is as follows. Section 2 contains results from the geometry of numbers and new estimates for $g_s(A)$ in terms of the s-covering radius needed in the proofs. In Section 3, we prove Theorem 1. The proofs of Theorems 2 and 3 are given in Section 4. Finally, the proof of Theorem 4 and a new example showing not uniqueness of the maximal cone for $1 < m < n - 1$ are presented in Section 5.

2 Bounds on $\mathrm{g}_s(A)$ in terms of the s-covering radius

First we will state results from Minkowski's geometry of numbers (see [13, 14]) needed in this paper.

For an d-dimensional lattice $L \subset \mathbb{R}^n$ and an origin-symmetric convex body $K \subset \mathrm{span}_{\mathbb{R}}(L)$ the *successive minima* $\lambda_i = \lambda_i(K, L)$ are defined by

$$\lambda_i(K, L) = \min \left\{ \lambda > 0 : \dim \left(\lambda K \cap L \right) \geqslant i \right\}, 1 \leqslant i \leqslant d.$$

Minkowski's celebrated theorem on successive minima states (cf. [13, Theorem 23.1])

$$\frac{2^d}{d!} \det(L) \leqslant \lambda_1 \lambda_2 \cdot \ldots \cdot \lambda_d \mathrm{vol}\,(K) \leqslant 2^d \det(L), \tag{12}$$

where $\mathrm{vol}\,(K)$ is the d-dimensional volume of K.

Both inequalities in (12) can be slightly improved in the special case of a ball, but since we are mainly not interested in constants depending on the dimension we do not state these improvements. There is a classical relation between the successive minima and the covering radius due to Jarnik, which we will apply in the following form [14, Chap.2, Sect.13; Theorem 1, Theorem 6]

$$\frac{1}{2}\lambda_d(K, L) \leqslant \mu(K, L) \leqslant \frac{d}{2}\lambda_d(K, L). \tag{13}$$

Next we remark, that the s-covering radius $\mu_s(K, L)$ (see (6)) may also be described equivalently as the smallest positive number μ such that any translate of K contains at least s lattice points, i.e.,

$$\mu_s(K, L) = \min\{\mu > 0 : \#\{(\boldsymbol{x} + \mu K) \cap L\} \geqslant s \text{ for all } \boldsymbol{x} \in \mathrm{span}_{\mathbb{R}}(L)\}. \tag{14}$$

In [1] the s-covering radius was bounded by

$$s^{\frac{1}{d}} \left(\frac{\det(L)}{\mathrm{vol}\,K} \right)^{\frac{1}{d}} \leqslant \mu_s(K, L) \leqslant \mu_1(K, L) + (s - 1)^{\frac{1}{d}} \left(\frac{\det(L)}{\mathrm{vol}\,(K)} \right)^{\frac{1}{d}}. \tag{15}$$

For $m = 1$ there is a nice identity, due to Kannan [15], between the Frobenius number $\mathrm{g}_1(\boldsymbol{a})$ and the covering radius of a simplex. Please see Section 3 for more details. When $m > 1$ no exact formula for $\mathrm{g}_s(A)$ in terms of the s-covering radius is known. Here we will prove upper and lower bounds needed for the proofs.

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) and let

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

Then, in particular, we have

$$\det L_A^{\perp} = \det L_A = \sqrt{\det A \, A^{\intercal}}. \tag{16}$$

Our first lemma gives an upper bound on $\mathrm{g}_s(A)$.

Lemma 5. *Let $1 \leqslant m < n$. Then*

$$\mathrm{g}_s(A) \leqslant \mu_s(P(A, \boldsymbol{v}) - \mathbf{1}, L_A^\perp).$$

Proof. Let $t \geqslant \mu_s(P(A, \boldsymbol{v}) - \mathbf{1}, L_A^\perp)$, and let $\boldsymbol{b} \in (t\,\boldsymbol{v} + C) \cap \mathbb{Z}^m$, i.e., there exists a non-negative vector $\boldsymbol{\alpha} \in \mathbb{R}^n_{\geqslant 0}$ such that $\boldsymbol{b} = A\,(t\,\mathbf{1} + \boldsymbol{\alpha})$. By (1) i) we know that the columns of A form a generating system of the lattice $\mathbb{Z}^m$ (cf. [21, Corollary 4.1c]). Thus there exists a $\boldsymbol{z} \in \mathbb{Z}^n$ such that

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

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

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

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

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

$\square$

Next, we will obtain a lower bound on $\mathrm{g}_s(A)$ in terms of the s-covering radius. The proof is based on Kannan's approach [15], but in order to apply it we have to adjust the setting. First we extend the definition of $\mathrm{g}_s(A)$ to all $\boldsymbol{w} \in \mathrm{int}\,C \cap \mathbb{Z}^m$ by defining

$$\mathrm{g}_s(A, \boldsymbol{w}) = \min\{t \geqslant 0 : \mathrm{int}(t\boldsymbol{w} + C) \cap \mathbb{Z}^n \subseteq \mathcal{F}_s(A)\}.$$

Hence, $\mathrm{g}_s(A) = \mathrm{g}_s(A, \boldsymbol{v})$ and it is easy to see that $\mathrm{g}_s(A, \boldsymbol{w})$ is well defined. For instance, since $\boldsymbol{w}$ belongs to the interior of the cone, there exists a positive vector $\boldsymbol{\rho} \in \mathbb{R}^n_{>0}$ such that $\boldsymbol{w} = A\boldsymbol{\rho}$. Denoting by $\rho_{\max}$ and $\rho_{\min}$ the maximum and the minimum of the entries of $\boldsymbol{\rho}$, respectively, we have

$$\boldsymbol{w} + C \subseteq \rho_{\min}\,\boldsymbol{v} + C \text{ and } \boldsymbol{v} + C \subseteq \frac{1}{\rho_{\max}}\,\boldsymbol{w} + C,$$

and thus

$$\frac{1}{\rho_{\max}}\mathrm{g}_s(A) \leqslant \mathrm{g}_s(A, \boldsymbol{w}) \leqslant \frac{1}{\rho_{\min}}\mathrm{g}_s(A). \tag{17}$$

In the following, let $A = (A_1, A_2)$ with $A_1 \in \mathbb{Z}^{m \times m}$ with $\det A_1 \neq 0$. Furthermore, let

$$\mathrm{c}(A_1, A) = \max_{j=1,\ldots,m} \sum_{i=1}^{n-m} \max(\alpha_{i,j}, 0),$$

where $\alpha_{i,j}$ are the entries of the matrix $A_1^{-1} A_2$. With this notation we have

Lemma 6. *Let $\overline{\boldsymbol{v}} = A_1 \overline{\mathbf{1}}$ be the sum of the first m columns of A. Let $\widehat{\mathbf{1}} = (\overline{\mathbf{1}}, \mathbf{0})^{\mathsf{T}} \in \mathbb{Z}^n$ be the vector consisting of m ones and $n - m$ zeros. Then*

$$\lceil g_s(A, \overline{\boldsymbol{v}}) \rceil \geqslant \mu_s(P(A, \overline{\boldsymbol{v}}) - \widehat{\mathbf{1}}, L_A^\perp) - 1 - c(A_1, A).$$

Proof. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \in \mathbb{Z}^m$ be the columns of A, and let

$$Q_A = \{A\boldsymbol{\zeta} : 0 < \zeta_i \leqslant 1\}$$

be the half-open zonotope generated by the columns of A. Since every lattice point $\boldsymbol{b} \in \operatorname{int} C$, $\boldsymbol{b} = \sum_{i=1}^n \rho_i \boldsymbol{a}_i$, $\rho_i > 0$, can be written as

$$\boldsymbol{b} = \sum_{i=1}^n (\rho_i + 1 - \lceil \rho_i \rceil) \boldsymbol{a}_i + \sum_{i=1}^n (\lceil \rho_i \rceil - 1) \boldsymbol{a}_i,$$

i.e., as a point in Q_A plus a non-negative integral combination of the generators of C we have

$$g_s(A, \overline{\boldsymbol{v}}) = \min \left\{ t \in \mathbb{R}_{\geqslant 0} : (t\,\overline{\boldsymbol{v}} + Q_A) \cap \mathbb{Z}^m \subset \mathcal{F}_s(A) \right\}.$$

Now for $\boldsymbol{l} \in Q_A \cap \mathbb{Z}^m$ let

$$t(\boldsymbol{l}) = \min \left\{ t \in \mathbb{Z}_{\geqslant 0} : t\,\overline{\boldsymbol{v}} + \boldsymbol{l} \in \mathcal{F}_s(A) \right\}.$$

Then we have

$$\begin{aligned}
\lceil g_s(A, \overline{\boldsymbol{v}}) \rceil &= \min \{ t \in \mathbb{Z}_{\geqslant 0} : t\,\overline{\boldsymbol{v}} + (Q_A \cap \mathbb{Z}^m) \subset \mathcal{F}_s(A) \} \\
&= \max \{ t(\boldsymbol{l}) : \boldsymbol{l} \in Q_A \cap \mathbb{Z}^m \}.
\end{aligned} \tag{18}$$

In analogy to [15] we consider $L = L_A^\perp | \mathbb{R}^{n-m}$ and $P = P(A, \overline{\boldsymbol{v}}) | \mathbb{R}^{n-m}$, where $\cdot | \mathbb{R}^{n-m}$ denotes the orthogonal projection which forgets the first m coordinates. Hence

$$L = \{ \boldsymbol{z} \in \mathbb{Z}^{n-m} : A_1^{-1} A_2 \, \boldsymbol{z} \in \mathbb{Z}^m \} \text{ and } P = \{ \boldsymbol{x} \in \mathbb{R}_{\geqslant 0}^{n-m} : A_1^{-1} A_2 \, \boldsymbol{x} \leqslant \overline{\mathbf{1}} \}.$$

Since the projections $L_A^\perp$ to L and $P(A, \overline{\boldsymbol{v}})$ to P are bijections we have

$$\mu_s(P(A, \overline{\boldsymbol{v}}) - \widehat{\mathbf{1}}, L_A^\perp) = \mu_s(P, L)$$

and we have to prove

$$\mu_s(P, L) \leqslant \lceil g_s(A, \overline{\boldsymbol{v}}) \rceil + 1 + c(A_1, A). \tag{19}$$

Claim. For $\boldsymbol{y} \in \mathbb{Z}^{n-m}$ there exist distinct $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_s \in L$ such that $\boldsymbol{y} \in \boldsymbol{z}_i + (\lceil g_s(A, \overline{\boldsymbol{v}}) \rceil + 1)P$, $1 \leqslant i \leqslant s$.

For the proof of the claim, let $\boldsymbol{l} \in Q_A \cap \mathbb{Z}^m$ such that $A_1^{-1}(A_2 \boldsymbol{y} - \boldsymbol{l}) \in \mathbb{Z}^m$, which can be found as follows: write $A_1 \boldsymbol{\rho} = A_2 \boldsymbol{y}$ for some $\boldsymbol{\rho} \in \mathbb{R}^m$ and set $\boldsymbol{l} = \sum_{i=1}^m (\rho_i - \lfloor \rho_i \rfloor) \boldsymbol{a}_i$.

By definition of $t(\boldsymbol{l})$, there are s distinct $\boldsymbol{x}_i \in \mathbb{Z}_{\geqslant 0}^n$, $1 \leqslant i \leqslant s$, with $A\boldsymbol{x}_i = t(\boldsymbol{l})\overline{\boldsymbol{v}} + \boldsymbol{l}$. We denote by $\overline{\boldsymbol{x}}_i$ and $\widetilde{\boldsymbol{x}}_i$ the vectors consisting of the first m and the last $n - m$ coordinates of $\boldsymbol{x}_i$, respectively. Then

$$
\begin{aligned}
A_1^{-1} A_2(\boldsymbol{y} - \widetilde{\boldsymbol{x}}_i) &= A_1^{-1}(A_2\boldsymbol{y} - \boldsymbol{l}) - A_1^{-1}(A_2\widetilde{\boldsymbol{x}}_i - \boldsymbol{l}) \\
&= A_1^{-1}(A_2\boldsymbol{y} - \boldsymbol{l}) - t(\boldsymbol{l})\overline{\mathbf{1}} + \overline{\boldsymbol{x}}_i \in \mathbb{Z}^m.
\end{aligned}
$$

Hence $\boldsymbol{y} - \widetilde{\boldsymbol{x}}_i \in L$, $1 \leqslant i \leqslant s$, and observe, that they are also distinct. Since

$$
A_1^{-1} A_2 \widetilde{\boldsymbol{x}}_i = A_1^{-1}(t(\boldsymbol{l})\overline{\boldsymbol{v}} + \boldsymbol{l} - A_1\overline{\boldsymbol{x}}_i) = t(\boldsymbol{l})\overline{\mathbf{1}} + A_1^{-1}\boldsymbol{l} - \overline{\boldsymbol{x}}_i \leqslant (t(\boldsymbol{l}) + 1)\overline{\mathbf{1}}
$$

by the choice of $\boldsymbol{l}$, we also have $\widetilde{\boldsymbol{x}}_i \in (t(\boldsymbol{l}) + 1)P$ and with $\boldsymbol{z}_i = \boldsymbol{y} - \widetilde{\boldsymbol{x}}_i$, $1 \leqslant i \leqslant s$, the claim is proven.

Finally, we extend this covering property to all points in $\mathbb{R}^{n-m}$. So let $\boldsymbol{y} \in \mathbb{R}^{n-m}$, and we write $\boldsymbol{y} = \boldsymbol{z} + \boldsymbol{x}$ with $\boldsymbol{z} \in \mathbb{Z}^{n-m}$ and $\boldsymbol{x} \in [0, 1]^{n-m}$. According to the claim there exist s distinct $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_s \in L$ such that $\boldsymbol{z} \in \boldsymbol{z}_i + (\lceil \mathrm{g}_s(A, \overline{\boldsymbol{v}}) \rceil + 1)P$, $1 \leqslant i \leqslant s$. By the definition of $c(A_1, A)$ we have $A_1^{-1}A_2\boldsymbol{x} \leqslant c(A_1, A)\mathbf{1}$ and so $\boldsymbol{x} \in c(A_1, A)\,P$. Hence

$$
\boldsymbol{y} \in \boldsymbol{z}_i + (\lceil \mathrm{g}_s(A, \overline{\boldsymbol{v}}) \rceil + 1 + c(A_1, A))P, \quad 1 \leqslant i \leqslant s,
$$

and (19) is shown. $\qquad\square$

Now, based on this lemma, we can easily derive the desired lower bound for $\mathrm{g}_s(A)$.

Lemma 7. *With the notation of Lemma 6 we have*

$$
\mathrm{g}_s(A) \geqslant \frac{1}{(n - m + 1)} \frac{m(A)}{M(A)} \left(\mu_s(P(A, \overline{\boldsymbol{v}}) - \mathbf{1}, L_A^{\perp}) - 2 - c(A_1, A) \right).
$$

Proof. On account of Lemma 6 we know that

$$
\mathrm{g}_s(A, \overline{\boldsymbol{v}}) \geqslant \mu_s(P(A, \overline{\boldsymbol{v}}) - \mathbf{1}, L_A^{\perp}) - 2 - c(A_1, A),
$$

and with the notation in (17) we get

$$
\mathrm{g}_s(A) \geqslant \rho_{\min} \left(\mu_s(P(A, \overline{\boldsymbol{v}}) - \mathbf{1}, L_A^{\perp}) - 2 - c(A_1, A) \right),
$$

where $\rho_{\min}$ is the minimal positive entry in a representation of $\overline{\boldsymbol{v}} = A\boldsymbol{\rho}$ with $\boldsymbol{\rho} \in \mathbb{R}_{>0}^n$. Now $\{\boldsymbol{x} \in \mathbb{R}_{\geqslant 0}^n : A\boldsymbol{x} = \overline{\boldsymbol{v}}\}$ is an $(n - m)$-dimensional polytope in $\mathbb{R}^n$, and its vertices $\boldsymbol{u}$ are determined by $A\boldsymbol{u} = \overline{\boldsymbol{v}}$ and $u_i = 0$ for some $n - m$ coordinates. Hence, according to Cramer's rule the non-zero coordinates are the ratio of two $(m \times m)$-minors of A, and a suitable convex combination of $n - m + 1$ affinely independent vertices gives us a representation of $A\overline{\boldsymbol{v}}$ as an interior point. Thus $\rho_{\min} \geqslant \frac{1}{(n-m+1)} \frac{m(A)}{M(A)}$. $\qquad\square$

3 Proof of Theorem 1

In [1], a fundamental formula of Kannan [15] relating the Frobenius number $F_1(\boldsymbol{a})$ with the covering radius was extended to the s-Frobenius number $F_s(\boldsymbol{a})$ and the s-covering radius. In order to describe it, let for a given primitive positive vector $\boldsymbol{a} = (a_1, \ldots, a_n)^\mathsf{T} \in \mathbb{Z}_{>0}^n$

$$S_{\boldsymbol{a}} = \left\{ \boldsymbol{x} \in \mathbb{R}_{\geqslant 0}^{n-1} : a_1 x_1 + \cdots + a_{n-1} x_{n-1} \leqslant 1 \right\}$$

be the $(n-1)$-dimensional simplex with vertices $\boldsymbol{0}, \frac{1}{a_i}\boldsymbol{e}_i$ where $\boldsymbol{e}_i$ is the i-th unit vector in $\mathbb{R}^{n-1}$, $1 \leqslant i \leqslant n-1$. Furthermore, we consider the following sublattice of $\mathbb{Z}^{n-1}$

$$L_{\boldsymbol{a}} = \left\{ \boldsymbol{z} \in \mathbb{Z}^{n-1} : a_1 z_1 + \cdots + a_{n-1} z_{n-1} \equiv 0 \bmod a_n \right\}.$$

Then

$$\mu_s(S_{\boldsymbol{a}}, L_{\boldsymbol{a}}) = F_s(\boldsymbol{a}) + a_1 + \cdots + a_n, \tag{20}$$

which for $s = 1$ is the above mentioned formula of Kannan. So the problem to bound $F_s(\boldsymbol{a})$ is equivalent to the study of $\mu_s(S_{\boldsymbol{a}}, L_{\boldsymbol{a}})$.

Set

$$\alpha_1 = \frac{a_1}{a_n}, \ldots, \alpha_{n-1} = \frac{a_{n-1}}{a_n}.$$

For

$$S_{\boldsymbol{\alpha}} = a_n S_{\boldsymbol{a}} = \left\{ \boldsymbol{x} \in \mathbb{R}_{\geqslant 0}^{n-1} : \sum_{i=1}^{n-1} \alpha_i x_i \leqslant 1 \right\} \quad \text{and} \quad L_u = a_n^{-1/(n-1)} L_{\boldsymbol{a}}$$

we have

$$\mu_s(S_{\boldsymbol{a}}, L_{\boldsymbol{a}}) = a_n^{1+1/(n-1)} \mu_s(S_{\boldsymbol{\alpha}}, L_u). \tag{21}$$

Observe that $\det L_{\boldsymbol{a}} = a_n$ and hence $\det(L_u) = 1$. Consequently,

$$\vartheta_s(S_{\boldsymbol{\alpha}}) \leqslant \mu_s(S_{\boldsymbol{\alpha}}, L_u). \tag{22}$$

The simplex $(\alpha_1 \cdots \alpha_{n-1})^{1/(n-1)} S_{\boldsymbol{\alpha}}$ and the standard simplex $S_{n-1} = \{ \boldsymbol{x} \in \mathbb{R}_{\geqslant 0}^{n-1} : x_1 + \cdots + x_{n-1} \leqslant 1 \}$ are equivalent up to a linear transformation of determinant 1. Therefore

$$\vartheta_s(S_{n-1}) = \frac{\vartheta_s(S_{\boldsymbol{\alpha}})}{(\alpha_1 \cdots \alpha_{n-1})^{1/(n-1)}}, \tag{23}$$

and by (22), (21) and (20) we have

$$\vartheta_s(S_{n-1}) \leqslant \frac{\mu_s(S_{\boldsymbol{\alpha}}, L_u)}{(\alpha_1 \cdots \alpha_{n-1})^{1/(n-1)}} = \frac{\mu_s(S_{\boldsymbol{a}}, L_{\boldsymbol{a}})}{a_n^{1+1/(n-1)}(\alpha_1 \cdots \alpha_{n-1})^{1/(n-1)}}$$

$$= \frac{F_s(a) + a_1 + \cdots + a_n}{(a_1 \cdots a_n)^{1/(n-1)}},$$

which shows Theorem 1 i).

One of the main ingredients of the proof of Theorem 1 ii) is Theorem 1.2 in Aliev and Gruber [2] which is also implicit in Schinzel [20]. For completeness we give below the statement of this result.

Theorem 8. *For any lattice L with basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}$, $\boldsymbol{b}_i \in \mathbb{Q}^{n-1}$, $i = 1, \ldots, n-1$ and for all rationals $\alpha_1, \ldots, \alpha_{n-1}$ with $0 < \alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_{n-1} \leqslant 1$, there exists a sequence*

$$\boldsymbol{a}(t) = (a_1(t), \ldots, a_{n-1}(t), a_n(t)) \in \mathbb{Z}^n, t = 1, 2, \ldots,$$

such that $\gcd(a_1(t), \ldots, a_{n-1}(t), a_n(t)) = 1$ and the lattice $L_{\boldsymbol{a}(t)}$ has a basis

$$\boldsymbol{b}_1(t), \ldots, \boldsymbol{b}_{n-1}(t)$$

with

$$\frac{b_{ij}(t)}{k\,t} = b_{ij} + O\left(\frac{1}{t}\right), \quad i, j = 1, \ldots, n-1, \tag{24}$$

where $k \in \mathbb{N}$ is such that $k\,b_{ij}, k\,\alpha_j\,b_{ij} \in \mathbb{Z}$ for all $i, j = 1, \ldots, n-1$. Moreover,

$$a_n(t) = \det(L)k^{n-1}t^{n-1} + O(t^{n-2}) \tag{25}$$

and

$$\alpha_i(t) := \frac{a_i(t)}{a_n(t)} = \alpha_i + O\left(\frac{1}{t}\right). \tag{26}$$

Following Gruber [12], we say that a sequence S_t of convex bodies in $\mathbb{R}^{n-1}$ converges to a convex body S if the sequence of *distance functions* of S_t converges uniformly on the unit ball in $\mathbb{R}^{n-1}$ to the distance function of S. For the notion of convergence of a sequence of lattices to a given lattice we refer the reader to p. 178 of [14].

Lemma 9 (see Satz 1 in [12]). *Let S_t be a sequence of convex bodies in $\mathbb{R}^{n-1}$ which converges to a convex body S and let L_t be a sequence of lattices in $\mathbb{R}^{n-1}$ convergent to a lattice L. Then*

$$\lim_{t \to \infty} \mu_s(S_t, L_t) = \mu_s(S, L).$$

Without loss of generality, we may assume that $\boldsymbol{\alpha} \in \mathbb{Q}^{n-1}$ and

$$0 < \alpha_1 < \alpha_2 < \ldots < \alpha_{n-1} < 1. \tag{27}$$

For $\epsilon > 0$ we can choose a lattice L_ϵ of determinant 1 with

$$\mu_s(S_{\boldsymbol{\alpha}}, L_\epsilon) < \vartheta_s(S_{\boldsymbol{\alpha}}) + \frac{\epsilon(\alpha_1 \cdots \alpha_{n-1})^{1/(n-1)}}{2}. \tag{28}$$

The inhomogeneous minimum is independent of translation and rational lattices are dense in the space of all lattices. Thus, by Lemma 9, we may assume that $L_\epsilon \subset \mathbb{Q}^{n-1}$. Applying Theorem 8 to the lattice L_ϵ and the numbers $\alpha_1, \ldots, \alpha_{n-1}$, we get a sequence $\boldsymbol{a}(t)$, satisfying (24), (25) and (26). Note also that, by (27),

$$0 < a_1(t) < a_2(t) < \ldots < a_n(t)$$

for sufficiently large t.

Observe that the identity (26) implies (8) with $a_i = a_i(t)$, $i = 1, \ldots, n$, for t large enough. Let us show that, for sufficiently large t, the inequality (9) also holds. Define a simplex $S_{\boldsymbol{\alpha}(t)}$ and a lattice L_t by

$$S_t = a_n(t) S_{\boldsymbol{a}(t)} = \left\{ (x_1, \ldots, x_{n-1}) \in \mathbb{R}_{\geqslant 0}^{n-1} : \sum_{i=1}^{n-1} \alpha_i(t) x_i \leqslant 1 \right\},$$

$$L_t = a_n(t)^{-1/(n-1)} L_{\boldsymbol{a}(t)}.$$

By (24) and (25), the sequence L_t converges to the lattice L_ϵ. Next, the point $\boldsymbol{p} = (1/(2n), \ldots, 1/(2n))$ is an inner point of the simplex $S_{\boldsymbol{\alpha}}$ and all the simplicies S_t for sufficiently large t. By (26) and Lemma 9, the sequence $\mu_s(S_t - \boldsymbol{p}, L_t)$ converges to $\mu_s(S_{\boldsymbol{\alpha}} - \boldsymbol{p}, L_\epsilon)$. Here we consider the sequence $\mu_s(S_t - \boldsymbol{p}, L_t)$ instead of $\mu_s(S_t, L_t)$ because the distance functions of the family of convex bodies in Lemma 9 need to converge on the unit ball. Now, since the inhomogeneous minimum is independent of translation, the sequence $\mu_s(S_t, L_t)$ converges to $\mu_s(S_{\boldsymbol{\alpha}}, L_\epsilon)$. Consequently, by (26),

$$\frac{\mu_s(S_t, L_t)}{(\alpha_1(t) \cdots \alpha_{n-1}(t))^{1/(n-1)}} \to \frac{\mu_s(S_{\boldsymbol{\alpha}}, L_\epsilon)}{(\alpha_1 \cdots \alpha_{n-1})^{1/(n-1)}}, \quad \text{as } t \to \infty,$$

and, by (20), (28) and (23),

$$\frac{\mathrm{F}_s(\boldsymbol{a}(t)) + \sum_{i=1}^n a_i(t)}{(a_1(t) \cdots a_n(t))^{1/(n-1)}} = \frac{\mu_s(S_t, L_t)}{(\alpha_1(t) \cdots \alpha_{n-1}(t))^{1/(n-1)}} < \vartheta_s(S_{n-1}) + \epsilon$$

for sufficiently large t. This concludes the proof of Theorem 1 $\qquad \blacksquare$

4 Proof of Theorem 2 and Theorem 3

In Section 2 we have already proven the bounds for $\mathrm{g}_s(A)$ in terms of the s-covering radius and it remains now to bound the s-covering radius itself.

Lemma 10. *The inequality*

$$\mu_1(P(A, \boldsymbol{v}) - \mathbf{1}, L_A^\perp) \leqslant \frac{n - m}{2} \sqrt{\det(A A^\intercal)}$$

holds.

Proof. Let $C^n = [-1, 1]^n$ and $K = C^n \cap \mathrm{lin}\, L_A^\perp$. By a well-known result of Vaaler [23], any k-dimensional section of the cube C^n has k-volume at least 2^k. Since $\mathbf{1} \in P(A, \boldsymbol{v})$, the latter observation implies that the polytope $P(A, \boldsymbol{v}) - \mathbf{1}$ contains an $(n-m)$-dimensional section Q of the cube C^n and, in particular,

$$\mathrm{vol}_{n-m}(P(A, \boldsymbol{v})) \geqslant \mathrm{vol}_{n-m}(Q) \geqslant 2^{n-m}, \tag{29}$$

and by (13)

$$\mu_1(P(A, \boldsymbol{v}) - \mathbf{1}, L_A^\perp) \leqslant \mu_1(Q, L_A^\perp) \leqslant \frac{n-m}{2} \lambda_{n-m}(Q, L_A^\perp). \tag{30}$$

All vectors of the lattice $L_A^\perp$ are integral vectors, thus $\lambda_i(Q, L_A^\perp) \geqslant 1$, $1 \leqslant i \leqslant n - m$. Hence from (12) and (29) we get

$$\lambda_{n-m}(Q, L_A^\perp) \leqslant \det L_A^\perp, \tag{31}$$

and with (30) we are done. $\qquad\square$

One can also obtain a refinement of the bound above.

Lemma 11. *The inequality*

$$\mu_1(P(A, \boldsymbol{v}) - \mathbf{1}, L_A^\perp) \leqslant \frac{n-m}{2} M(A)$$

holds.

Proof. For an m-subset $J \subset \{1, \ldots, n\}$ let A_J be the submatrix of A consisting of the columns with index set J. Let $I = \{1, \ldots, m\}$ and without loss of generality let $\det A_I \neq 0$. Then, for $k = m + 1, \ldots, n$, the 1-dimensional subspace $\{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} = 0, \ x_i = 0 \text{ for } i \notin I \cup \{k\}\}$ is generated by the vector $\boldsymbol{z}_k \in \mathbb{Z}^n$ with

$$\boldsymbol{z}_{ki} = (-1)^{m-i} \det A_{\{1,\ldots,i-1,i+1,\ldots,m,k\}}, \ 1 \leqslant i \leqslant m, \quad \boldsymbol{z}_{kk} = -\det A_I,$$

and zero otherwise. Clearly, $\boldsymbol{z}_k \in L_A^\perp$ for $k = m + 1, \ldots, n$.

We have to show that

$$\left(\boldsymbol{x} + \frac{n-m}{2} M(A) \left(P(A, \boldsymbol{v}) - \mathbf{1}\right)\right) \cap L_A^\perp \neq \emptyset$$

for all $\boldsymbol{x} \in \lin L_A^\perp$.

To this end let $\boldsymbol{c} = \frac{n-m}{2} M(A)\mathbf{1}$. Due to the maximality of $M(A)$ we have $\boldsymbol{c} \pm \frac{(n-m)}{2} \boldsymbol{z}_k \in \mathbb{R}^n_{\geqslant 0}$ and so $\boldsymbol{c} \pm \frac{(n-m)}{2} \boldsymbol{z}_k \in \frac{n-m}{2} M(A)P(A, \boldsymbol{v})$ for $k = m + 1, \ldots, n$. Hence the convex hull C of these points, i.e.,

$$C = \left\{\boldsymbol{c} + \frac{(n-m)}{2} \sum_{k=m+1}^{n} \mu_k \pm \boldsymbol{z}_k : \sum_{k=m+1}^{n} \mu_k = 1, \mu_k \geqslant 0\right\}$$

is contained in $\frac{n-m}{2} M(A)P(A, \boldsymbol{v})$. Now this cross-polytope C contains the parallelepiped

$$\left\{\boldsymbol{c} \pm \rho_{m+1} \frac{1}{2} \boldsymbol{z}_{m+1} \pm \cdots \pm \rho_n \frac{1}{2} \boldsymbol{z}_n : \rho_k \in [0, 1]\right\},$$

which shows that $\frac{n-m}{2} M(A) \left(P(A, \boldsymbol{v}) - \mathbf{1}\right)$ contains a translation of the lattice (w.r.t. $L_A^\perp$) parallelepiped $U = \{\sum_{k=m+1}^{m} \rho_k \boldsymbol{z}_k : 0 \leqslant \rho_k \leqslant 1\}$. Since any translated lattice parallelepiped in $\lin L_A^\perp$ contains a lattice point of $L_A^\perp$ we know that $\boldsymbol{x} + \frac{n-m}{2} M(A) \left(P(A, \boldsymbol{v}) - \mathbf{1}\right)$ contains a point of $L_A^\perp$ for all $\boldsymbol{x} \in \lin L_A^\perp$. $\qquad\square$

Now we are ready to complete the proof of Theorem 2

Proof of Theorem 2. By Lemma 5 and (15) we have

$$\mathrm{g}_s(A) \leqslant \mu_s(P(A, \boldsymbol{v}) - \mathbf{1}, L_A^\perp)$$

$$\leqslant \mu_1(P(A, \boldsymbol{v}) - \mathbf{1}, L_A^\perp) + (s-1)^{\frac{1}{n-m}} \left(\frac{\det L_A^\perp}{\mathrm{vol}\,(P(A, \boldsymbol{v}))} \right)^{\frac{1}{n-m}}.$$

Together with Lemma 10 and the lower bound on $\mathrm{vol}\,(P(A, \boldsymbol{v}))$ given in (29) we obtain the inequality (11). □

Observe that using Lemma 11 instead of Lemma 10 results in the better but less nice bound

$$\mathrm{g}_s(A) \leqslant \frac{n-m}{2} M(A) + \frac{(s-1)^{\frac{1}{n-m}}}{2} \left(\sqrt{\det(AA^\intercal)} \right)^{\frac{1}{n-m}}.$$

Finally we give the proof of Theorem 3

Proof of Theorem 3. In view of Lemma 7 and (15) we have

$$\mathrm{g}_s(A) \geqslant \frac{1}{n-m+1} \frac{m(A)}{M(A)} \left(s^{\frac{1}{n-m}} \left(\frac{\sqrt{\det AA^\intercal}}{\mathrm{vol}\,(P(A, \overline{\boldsymbol{v}}))} \right)^{\frac{1}{n-m}} - 2 - c(A_1, A) \right).$$

Thus we need an upper bound on $c(A_1, A)$ and on $\mathrm{vol}\,(P(A, \overline{\boldsymbol{v}}))$. With Cramer's rule each entry of $A_1^{-1} A_2$ is of the form $\det A_I / \det A_1$, where A_I is a certain $m \times m$ minor. Consequently, we have

$$c(A_1, A) \leqslant (n-m) \frac{M(A)}{m(A)}. \tag{32}$$

Let $\boldsymbol{u} \in \mathbb{R}^n$ be a vertex of $P(A, \overline{\boldsymbol{v}})$. As in the proof of Lemma 7 we may argue that each of the m non-zero entries of $\boldsymbol{u}$ is bounded by $M(A)/m(A)$. So $P(A, \overline{\boldsymbol{v}})$ is contained in an n-dimensional cube of edge length $M(A)/m(A)$. By [6], the largest volume of an $(n-m)$-dimensional section of a cube of dimension n with edge length σ is $\left(\sigma \sqrt{\frac{n}{n-m}} \right)^{n-m}$ which finishes the proof. □

5 The case $m = n - 1$. Proof of Theorem 4

Recall that an integer vector $\boldsymbol{z} = (z_1, z_2, \ldots, z_n)$ is called *primitive* if $\gcd(z_1, z_2, \ldots, z_n) = 1$. In the case $m = n-1$ the lattice $L_A^\perp$ has dimension one, so it is generated by a primitive vector $\boldsymbol{z} \in \mathbb{Z}^n$. Following [17], we put

$$\mathbf{u} = \sum_{i: z_i \geqslant 0} z_i \, \mathbf{a}_i = - \sum_{i: z_i \leqslant 0} z_i \, \mathbf{a}_i.$$

It is shown in [17, Theorem 6.1] that all points in the interior of $C + \boldsymbol{u} - \boldsymbol{v}$ admit a non-negative integral representation, but that, all the lattice points in the facets, which are contained in the lattice generated by those $\boldsymbol{a}_i$'s contained in the facet, are non-reachable. Hence we have

$$\mathrm{g}_1(A) = \min\{\gamma \in \mathbb{R}_{\geqslant 0} : \gamma \, \boldsymbol{v} \in C + \boldsymbol{u} - \boldsymbol{v}\}.$$

Therefore

$$\mathrm{g}_1(A) = \min\{\gamma \in \mathbb{R}_{\geqslant 0} : \exists \, \rho \in \mathbb{R} \quad \text{s.t.} \quad (\gamma + 1)\,\boldsymbol{1} - (z_i)_{z_i \geqslant 0}^{\mathsf{T}} + \rho\,\boldsymbol{z} \geqslant 0\}.$$

Here $(z_i)_{z_i \geqslant 0}^{\mathsf{T}} \in \mathbb{R}^n$ denotes the vector consisting of the nonnegative entries of $\boldsymbol{z}$ (the others are 0). So we may write $\boldsymbol{z} = (z_i)_{z_i \geqslant 0}^{\mathsf{T}} + (z_i)_{z_i \leqslant 0}^{\mathsf{T}}$ and we are interested in the minimal $\gamma \in \mathbb{R}_{\geqslant 0}$ such that there exists a ρ with

$$\gamma + 1 \geqslant (1 - \rho)\,z_i, \text{ for } z_i \geqslant 0 \quad \text{and } \gamma + 1 \geqslant -\rho\,z_i, \text{ for } z_i \leqslant 0.$$

Recall that we put $z^+ = \max\{z_i : z_i > 0\}$ and $z^- = \max\{|z_i| : z_i < 0\}$. Then

$$\gamma + 1 = \min_{\rho} \max\{(1 - \rho)\,z^+, \rho\,z^-\}.$$

The first function is decreasing in ρ whereas the second is increasing in ρ. Both coincide for $\rho = z^+/(z^+ + z^-)$ and so we have proved Theorem 4.

As mentioned in the introduction, it was also shown in [17] that the $C + \boldsymbol{u} - \boldsymbol{v}$ is the unique maximal cone with the property that all points in the interior admit a non-negative integral representation, but infinitely many on the boundary do not have such a representation. This seems to be a very particular property of the case $m = n - 1$ as it was already pointed out in [4]. We want to conclude the paper with another example showing that, in general, we have more than one maximal cone.
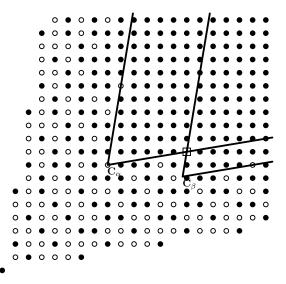

Figure 1: Non-uniqueness for $m = n - 2$.

For $k \in \mathbb{N}$ let
$$A = \begin{pmatrix} 1 & 2 & 1 & 3k \\ 2 & 1 & 3k & 1 \end{pmatrix}.$$

Then the cone C (see Figure 1 for $k = 2$) is generated by the two vectors $(1, 3k)^\intercal$ and $(3k, 1)^\intercal$. By elementary calculations, we get, that $\binom{9k-4}{6k-3} \notin \mathcal{F}_1(A)$ but all other integral points in $\binom{9k-4}{6k-3} + \text{conv}\left\{\binom{0}{0}, \binom{1}{3k}, \binom{3k}{1}, \binom{3k+1}{3k+1}\right\}$ are contained in $\mathcal{F}_1(A)$.

This implies, that all integral points but $\binom{9k-4}{6k-3}$ in

$$\binom{9k-4}{6k-3} + C = \left\{ \binom{x}{y} \in \mathbb{R}^2 : \begin{array}{l} 3kx - y \geqslant 3(3k-1)^2, \\ -x + 3ky \geqslant 2(3k-1)(3k-2) \end{array} \right\}$$

are contained in $\mathcal{F}_1(A)$. Now let

$$\alpha = \min\left\{ t \in \mathbb{Z} : \left\{ \binom{x}{y} \in \mathbb{Z}^2 : \begin{array}{l} 3kx - y > t \\ -x + 3ky > 2(3k-1)(3k-2) \end{array} \right\} \subset \mathcal{F}_1(A) \right\}$$

and

$$\beta = \min\left\{ t \in \mathbb{Z} : \left\{ \binom{x}{y} \in \mathbb{Z}^2 : \begin{array}{l} 3kx - y > 3(3k-1)^2 \\ -x + 3ky > t \end{array} \right\} \subset \mathcal{F}_1(A) \right\}.$$

Then it is clear, that $\alpha < 3(3k-1)^2$ and $\beta < 2(3k-1)(3k-2)$. This gives us two cones, namely

$$C_\alpha = \left\{ \binom{x}{y} \in \mathbb{R}^2 : \begin{array}{l} 3kx - y \geqslant \alpha, \\ -x + 3ky \geqslant 2(3k-1)(3k-2) \end{array} \right\}$$

$$C_\beta = \left\{ \binom{x}{y} \in \mathbb{R}^2 : \begin{array}{l} 3kx - y \geqslant 3(3k-1)^2, \\ -x + 3ky \geqslant \beta \end{array} \right\},$$

that are maximal w.r.t. inclusion with the property, that all integral points in their interiors are in $\mathcal{F}_1(A)$. By symmetries, the same is true for $\binom{6k-3}{9k-4}$.

For $k = 2$ the two maximal cones C_α and C_β are depicted in Figure 1. Black dots are in $\mathcal{F}_1(A)$, circles/squares with white interior are not. The square represents the point $\binom{14}{9} = \binom{9k-4}{6k-3}$ for $k = 2$.

Acknowledgements

References

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

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

[3] I. Aliev and M. Henk. Feasibility of integer knapsacks. *SIAM J. Optimization.* 20:2978–2993, 2010.

[4] J. Amos, I. Pascu, V. Ponomarenko, E. Trevino and Y. Zhang. The multidimensional Frobenius problem. *Involve.* 4(2):187–197, 2011.

[5] V.I. Arnold. Geometry and growth rate of Frobenius numbers of additive semigroups. *Math. Phys. Anal. Geom.* 9(2):95–108, 2006.

[6] K. Ball. Volumes of sections of cubes and related problems. *Geometric Aspects of Functional Analysis* (Joram Lindenstrauss and Vitali Milman, eds.). Lecture Notes in Mathematics, vol. 1376, Springer, 251–260, 1989.

[7] M. Beck and C. Kifer. An extreme family of generalized Frobenius numbers. *Integers.* 11:5, 639–645, 2011.

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

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

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

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

[12] P. M. Gruber. Zur Gitterüberdeckung des $\mathbb{R}^n$ durch Sternkörper. *Österreich. Akad. Wiss. Math.-Natur. Kl. S.-B. II.* 176:1–7, 1967.

[13] P. M. Gruber. *Convex and discrete geometry.* Springer, 2007.

[14] P. M. Gruber and C. G. Lekkerkerker. *Geometry of numbers.* North-Holland, 1987.

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

[16] C. H. Papadimitriou and K. Steiglitz. *Combinatorial optimization: algorithms and complexity.* Dover Publications, Inc., 1998.

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

[18] J. L. Ramírez Alfonsín. Complexity of the Frobenius problem. *Combinatorica.* 16(1):143–147, 1996.

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

[20] A. Schinzel. A property of polynomials with an application to Siegel's lemma. *Monatsh. Math.* 137:239–251, 2002.

[21] A. Schrijver. *Theory of linear and integer programming.* Wiley, 1986.

[22] J. Shallit and J. Stankewicz. Unbounded discrepancy in Frobenius numbers. *Integers.* 11(1):27–34, 2011.

[23] J. Vaaler. A geometric inequality with applications to linear forms. *Pacific J. Math.* 83(2):543–553, 1979.