ON POLYNOMIAL-TIME SOLVABLE LINEAR DIOPHANTINE PROBLEMS

ISKANDER ALIEV

Abstract. We obtain a polynomial-time algorithm that, given input $(A, \boldsymbol{b})$, where $A = (B|N) \in \mathbb{Z}^{m\times n}$, $m < n$, with nonsingular $B \in \mathbb{Z}^{m\times m}$ and $\boldsymbol{b} \in \mathbb{Z}^m$, finds a nonnegative integer solution to the system $A\boldsymbol{x} = \boldsymbol{b}$ or determines that no such solution exists, provided that $\boldsymbol{b}$ is located sufficiently "deep" in the cone generated by the columns of B. This result improves on some of the previously known conditions that guarantee polynomial-time solvability of linear Diophantine problems.

1. Introduction and Statement of Results

Consider the linear Diophantine problem

$$\begin{array}{ll} & \text{Given } (A, \boldsymbol{b})\,, \text{ where } A \in \mathbb{Z}^{m\times n}, m < n, \operatorname{rank}(A) = m \text{ and} \\ (1.1) & \boldsymbol{b} \in \mathbb{Z}^m, \text{ find a nonnegative integer solution to the system} \\ & A\boldsymbol{x} = \boldsymbol{b} \text{ or determine that no such solution exists}\,. \end{array}$$

The problem (1.1) is referred to as the *multidimensional knapsack problem* and is NP-hard already for $m = 1$ (see Papadimitriou and Steiglitz [13, Section 15.7]).

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

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

be the cone generated by $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$. In this paper, we are interested in the problem of determining subsets $\mathcal{S} \subset \mathcal{C}_A$ such that (1.1) is solvable in polynomial time provided $\boldsymbol{b} \in \mathcal{S}$. We will use the general approach of Gomory [9], that was originally applied to study asymptotic integer programs, and combine it with results from discrete geometry.

We may assume, without loss of generality, that the matrix A is partitioned as

$$A = (B|N)\,,$$

where $B \in \mathbb{Z}^{m\times m}$ is nonsingular and $N \in \mathbb{Z}^{m\times(n-m)}$. In what follows, we will denote by l_B and l_N the Euclidean lengths of the longest columns in the matrices B and N, respectively.

2000 *Mathematics Subject Classification.* Primary: 11D04, 90C10; Secondary: 11H06.

Key words and phrases. Multidimensional knapsack problem; polynomial-time algorithms; asymptotic integer programming; lattice points; Frobenius numbers.

Let $\mathcal{C}_B \subset \mathcal{C}_A$ be the cone generated by the columns of the matrix B. The main result of this paper shows that (1.1) is solvable in polynomial time when the right-hand-side vector $\boldsymbol{b}$ is located deep enough in the cone $\mathcal{C}_B$.

Let $\mathcal{C}_B(t) \subset \mathcal{C}_B$ denote the affine cone of points in $\mathcal{C}_B$ at Euclidean distance $\geq t$ from the boundary of $\mathcal{C}_B$. We will denote by $\gcd(A)$ the greatest common divisor of all $m \times m$ subdeterminants of A.

Theorem 1.1. *There exists a polynomial-time algorithm which, given input* $(A, \boldsymbol{b})$, *where* $A = (B|N) \in \mathbb{Z}^{m\times n}$, *with nonsingular* $B \in \mathbb{Z}^{m\times m}$, *and*

$$\boldsymbol{b} \in \mathbb{Z}^m \cap \mathcal{C}_B\left(l_N\left(\frac{|\det(B)|}{\gcd(A)} - 1\right)\right), \tag{1.2}$$

finds a nonnegative integer solution to the system $A\boldsymbol{x} = \boldsymbol{b}$ *or determines that no such solution exists.*

We will now consider a special case where the matrix A satisfies the following conditions:

$$\begin{aligned} &\text{(i)}\ \gcd(A) = 1,\\ &\text{(ii)}\ \{\boldsymbol{x} \in \mathbb{R}^n_{\geq 0} : A\,\boldsymbol{x} = \boldsymbol{0}\} = \{\boldsymbol{0}\}. \end{aligned} \tag{1.3}$$

Notice that the condition (i) in (1.3) guarantees that the system $A\boldsymbol{x} = \boldsymbol{b}$ has an integer solution for each $\boldsymbol{b} \in \mathbb{Z}^m$ (see Schrijver [16, Corollary 4.1 c]). The condition (ii) in (1.3), in its turn, guarantees that the polyhedron $\{\boldsymbol{x} \in \mathbb{R}^n_{\geq 0} : A\boldsymbol{x} = \boldsymbol{b}\}$ is bounded.

When $m = 1$ in the setting (1.3), the problem (1.1) is linked to the well-known *Frobenius problem* (see Ramirez Alfonsin [14]). By the condition (i) in (1.3), we have $\gcd(a_{11}, \ldots, a_{1n}) = 1$ and by (ii) we may assume that the entries of A are positive. For such A the largest integer b such that (1.1) is infeasible is called the *Frobenius number* associated with A, denoted by $F(A)$. It is an interesting question to determine whether there exists a polynomial-time algorithm that solves (1.1) provided that

$$b > F(A)$$

(cf. Conjecture 1.1 in [1]).

The best known result in this direction is due to Brimkov [5] (see also [1], [6] and [7]). Specifically, set

$$f_1 = a_{11}, f_i = \gcd(a_{11}, \ldots, a_{1i}),\ i \in \{2, \ldots, n\}. \tag{1.4}$$

A classical upper bound of Brauer [3] for the Frobenius numbers states that

$$F(A) \leq G(A) := a_{12}\frac{f_1}{f_2} + \cdots + a_{1n}\frac{f_{n-1}}{f_n} - \sum_{i=1}^{n} a_{1i}. \tag{1.5}$$

Brauer [3] and, subsequently, Brauer and Seelbinder [4] proved that the bound (1.5) is sharp and obtained a necessary and sufficient condition for the equality $F(A) = G(A)$. Brimkov [5] gave a polynomial-time algorithm that solves (1.1) provided that

$$b > G(A)\,. \tag{1.6}$$

We will show that an algorithm obtained in the proof of Theorem 1.1 matches the bound (1.6).

Corollary 1.1. *There exists a polynomial-time algorithm which, given input (A, b), where $A \in \mathbb{Z}^{1\times n}_{>0}$ satisfies (1.3) and $b \in \mathbb{Z}$ satisfies*

$$b > G(A)\,,$$

computes a nonnegative integer solution to the equation $A\boldsymbol{x} = b$.

Recall that the *Minkowski sum* $X + Y$ of the sets $X, Y \subset \mathbb{R}^m$ consists of all points $\boldsymbol{x} + \boldsymbol{y}$ with $\boldsymbol{x} \in X$ and $\boldsymbol{y} \in Y$. For $m \geq 2$, Aliev and Henk [1] considered the problem of estimating the minimal $t = t(A) \geq 0$ such that the problem (1.1) is solvable in polynomial time provided that A satisfies (1.3) and

$$\boldsymbol{b} \in \mathbb{Z}^m \cap (t\boldsymbol{v} + \mathcal{C}_A)\,,$$

where $\boldsymbol{v} = \boldsymbol{v}_1 + \cdots + \boldsymbol{v}_n$ is the sum of columns of A.

Theorem 1.1 in [1] gives the bound

$$t \leq 2^{(n-m)/2-1} p(m, n)(\det(AA^T))^{1/2}\,, \tag{1.7}$$

where

$$p(m, n) = 2^{-1/2}(n - m)^{1/2} n^{1/2}\,.$$

Furthermore, Theorem 1.2 in [1] shows that the exponential factor $2^{(n-m)/2-1}$ in (1.7) is redundant for matrices with

$$\det(AA^T) > \frac{(n - m)2^{2(n-m-2)}\gamma^{n-m}_{n-m}}{n^2}\,. \tag{1.8}$$

Here γ_k is the k-dimensional Hermite constant for which we refer to [12, Definition 2.2.5].

Let us now consider the case $m = 2$. Condition (1.3) (ii) implies that the cone $\mathcal{C}_A$ is pointed. Thus we may assume without loss of generality that $A = (B|N)$ with $\mathcal{C}_B = \mathcal{C}_A$. The last result of this paper gives an estimate on the function $t(A)$ that is independent on the dimension n and allows a refinement of (1.7) when the ratio $l_B l_N/|\det(B)|$ is relatively small.

Corollary 1.2. *There exists a polynomial-time algorithm which, given input $(A, \boldsymbol{b})$, where $A = (B|N) \in \mathbb{Z}^{2\times n}$, $B \in \mathbb{Z}^{2\times 2}$ is nonsingular with $\mathcal{C}_B = \mathcal{C}_A$, A satisfies (1.3) and*

$$\boldsymbol{b} \in \mathbb{Z}^2 \cap \left(\frac{l_B l_N}{|\det(B)|} (|\det(B)| - 1)\, \boldsymbol{v} + \mathcal{C}_A \right)\,, \tag{1.9}$$

computes a nonnegative integer solution to the system $A\boldsymbol{x} = \boldsymbol{b}$.

Noticing that $|\det(B)| \le (\det(AA^T))^{1/2}$, the condition (1.9) improves on (1.7) provided that $l_B l_N/|\det(B)| \le 2^{(n-m)/2-1}p(m,n)$. For matrices A satisfying (1.8) an improvement occurs when $l_B l_N/|\det(B)| \le p(m,n)$.

2. Tools from discrete geometry

For linearly independent $\boldsymbol{b}_1,\dots,\boldsymbol{b}_k$ in $\mathbb{R}^d$, the set $\Lambda = \{\sum_{i=1}^k \lambda_i \boldsymbol{b}_i : \lambda_i \in \mathbb{Z}\}$ is a k-dimensional *lattice* with *basis* $\boldsymbol{b}_1,\dots,\boldsymbol{b}_k$ and *determinant* $\det(\Lambda) = (\det(\boldsymbol{b}_i\cdot\boldsymbol{b}_j)_{1\le i,j\le k})^{1/2}$, where $\boldsymbol{b}_i\cdot\boldsymbol{b}_j$ is the standard inner product of the basis vectors $\boldsymbol{b}_i$ and $\boldsymbol{b}_j$. For a lattice $\Lambda\subset\mathbb{R}^d$ and $\boldsymbol{y}\in\mathbb{R}^d$, the set $\boldsymbol{y}+\Lambda$ is an *affine lattice* with determinant $\det(\Lambda)$.

Let Λ be a lattice in $\mathbb{R}^d$ with basis $\boldsymbol{b}_1,\dots,\boldsymbol{b}_d$ and let $\hat{\boldsymbol{b}}_i$ be the vectors obtained from the Gram-Schmidt orthogonalisation of $\boldsymbol{b}_1,\dots,\boldsymbol{b}_d$:

$$\begin{aligned} \hat{\boldsymbol{b}}_1 &= \boldsymbol{b}_1\,, \\ \hat{\boldsymbol{b}}_i &= \boldsymbol{b}_i - \textstyle\sum_{j=1}^{i-1}\mu_{i,j}\hat{\boldsymbol{b}}_j\,, \quad j\in\{2,\dots,d\}\,, \end{aligned} \tag{2.1}$$

where $\mu_{i,j} = (\boldsymbol{b}_i\cdot\hat{\boldsymbol{b}}_j)/|\hat{\boldsymbol{b}}_j|^2$.

We will associate with the basis $\boldsymbol{b}_1,\dots,\boldsymbol{b}_d$ of Λ the box

$$\hat{\mathcal{B}}(\boldsymbol{b}_1,\dots,\boldsymbol{b}_d) = [0,\hat{\boldsymbol{b}}_1)\times[0,\hat{\boldsymbol{b}}_2)\times\cdots\times[0,\hat{\boldsymbol{b}}_d)\,.$$

Lemma 2.1. *There exists a polynomial-time algorithm that, given a basis $\boldsymbol{b}_1,\dots,\boldsymbol{b}_d$ of a d-dimensional lattice $\Lambda\subset\mathbb{Q}^d$ and a point $\boldsymbol{x}$ in $\mathbb{Q}^d$ finds a point $\boldsymbol{y}\in\Lambda$ such that $\boldsymbol{x}\in\boldsymbol{y}+\hat{\mathcal{B}}(\boldsymbol{b}_1,\dots,\boldsymbol{b}_d)$.*

A proof of Lemma 2.1 is implicitly contained, for instance, in the description of the classical nearest plane procedure of Babai [2]. For completeness, we include a proof that follows along an argument of the proof of Theorem 5.3.26 in [10].

Proof. Let $\boldsymbol{x}$ be any point of $\mathbb{Q}^d$. We need to find a point $\boldsymbol{y}\in\Lambda$ such that

$$\boldsymbol{x}-\boldsymbol{y} = \sum_{i=1}^d \lambda_i\hat{\boldsymbol{b}}_i\,,\quad \lambda_i\in[0,1)\,,\quad i\in\{1,\dots,d\}\,. \tag{2.2}$$

This can be achieved using the following procedure. First, we find the rational numbers λ_i^0, $i\in\{1,\dots,d\}$ such that

$$\boldsymbol{x} = \sum_{i=1}^d \lambda_i^0\hat{\boldsymbol{b}}_i\,.$$

This can be done in polynomial time by Theorem 3.3 in [16]. Then we subtract $\lfloor\lambda_d^0\rfloor\boldsymbol{b}_d$ to get a representation

$$\boldsymbol{x} - \lfloor\lambda_d^0\rfloor\boldsymbol{b}_d = \sum_{i=1}^d \lambda_i^1\hat{\boldsymbol{b}}_i\,,$$

where $\lambda_d^1\in[0,1)$. Next subtract $\lfloor\lambda_{d-1}^1\rfloor\boldsymbol{b}_{d-1}$ and so on until we obtain the representation (2.2). $\square$

Let now Λ be a d-dimensional sublattice of $\mathbb{Z}^d$. By Theorem I (A) and Corollary 1 in Chapter I of Cassels [8], there exists a unique basis $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_d$ of the sublattice Λ of the form

$$\begin{aligned} \boldsymbol{g}_1 &= v_{11}\boldsymbol{e}_1\,, \\ \boldsymbol{g}_2 &= v_{21}\boldsymbol{e}_1 + v_{22}\boldsymbol{e}_2\,, \\ &\vdots \\ \boldsymbol{g}_d &= v_{d1}\boldsymbol{e}_1 + \cdots + v_{dd}\boldsymbol{e}_d\,, \end{aligned} \tag{2.3}$$

where $\boldsymbol{e}_i$ are the standard basis vectors of $\mathbb{Z}^d$ and the coefficients v_{ij} satisfy the conditions $v_{ij} \in \mathbb{Z}, v_{ii} > 0$ for $i \in \{1, \ldots, d\}$ and $0 \le v_{ij} < v_{jj}$ for $i, j \in \{1, \ldots, d\}, i > j$.

Lemma 2.2. *There exists a polynomial-time algorithm that, given a basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d$ of a lattice $\Lambda \subset \mathbb{Z}^d$ finds the basis of Λ of the form (2.3).*

Proof. Let $V = (v_{ij}) \in \mathbb{Z}^{d \times d}$ be the matrix formed by the coefficients v_{ij} in (2.3) with $v_{ij} = 0$ for $j > i$. Observe that after a straightforward renumbering of the rows and columns of V we obtain a matrix in the row-style Hermite Normal Form. Now it is sufficient to notice that the Hermite Normal Form can be computed in polynomial time using an algorithm of Kannan and Bachem [11]. □

The Gram-Schmidt orthogonalisation (2.1) of the basis (2.3) of Λ has the form $\hat{\boldsymbol{g}}_1 = v_{11}\boldsymbol{e}_1, \ldots, \hat{\boldsymbol{g}}_d = v_{dd}\boldsymbol{e}_d$. Therefore, noticing that the basis (2.3) is unique, we can associate with Λ the box

$$\mathcal{B}(\Lambda) = \hat{\mathcal{B}}(\boldsymbol{g}_1, \ldots, \boldsymbol{g}_d) = [0, v_{11}) \times [0, v_{22}) \times \cdots \times [0, v_{dd})\,.$$

Lemma 2.3. *For any $\boldsymbol{w} = (w_1, \ldots, w_d)^T \in \mathcal{B}(\Lambda) \cap \mathbb{Z}^d$ we have*

$$\prod_{i=1}^{d} (1 + w_i) \le \det(\Lambda)\,.$$

Proof. It is sufficient to notice that by (2.3) $\det(\Lambda) = v_{11} \cdots v_{dd}$. □

3. Proof of Theorem 1.1

Given $A \in \mathbb{Z}^{m \times n}$ and $\boldsymbol{b} \in \mathbb{Z}^m$, we will denote by $\Gamma(A, \boldsymbol{b})$ the set of integer points in the affine subspace

$$\mathcal{S}(A, \boldsymbol{b}) = \{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} = \boldsymbol{b}\}\,,$$

that is

$$\Gamma(A, \boldsymbol{b}) = \mathcal{S}(A, \boldsymbol{b}) \cap \mathbb{Z}^n\,.$$

The set $\Gamma(A, \boldsymbol{b})$ is either empty or is an affine lattice of the form $\Gamma(A, \boldsymbol{b}) = \boldsymbol{r} + \Gamma(A)$, where $\boldsymbol{r}$ is any integer vector with $A\boldsymbol{r} = \boldsymbol{b}$ and $\Gamma(A) = \Gamma(A, \boldsymbol{0})$ is the lattice formed by all integer points in the kernel of the matrix A. We will call the system $A\boldsymbol{x} = \boldsymbol{b}$ *integer feasible* if it has integer solutions or, equivalently, $\Gamma(A, \boldsymbol{b}) \ne \emptyset$. Otherwise the system is called *integer infeasible.*

Let π denote the projection map from $\mathbb{R}^n$ to $\mathbb{R}^{n-m}$ that forgets the first m coordinates. Recall that Theorem 1.1 applies to $A = (B|N)$, where B is nonsingular. It follows that the restricted map $\pi|_{\mathcal{S}(A,\boldsymbol{b})} : \mathcal{S}(A, \boldsymbol{b}) \to \mathbb{R}^{n-m}$ is bijective. Specifically, for any $\boldsymbol{w} \in \mathbb{R}^{n-m}$ we have

$$\pi|^{-1}_{\mathcal{S}(A,\boldsymbol{b})}(\boldsymbol{w}) = \begin{pmatrix} \boldsymbol{u} \\ \boldsymbol{w} \end{pmatrix} \text{ with } \boldsymbol{u} = B^{-1}(\boldsymbol{b} - N\boldsymbol{w})\,.$$

For technical reasons, it is convenient to consider the projected set $\Lambda(A, \boldsymbol{b}) = \pi(\Gamma(A, \boldsymbol{b}))$ and the projected lattice $\Lambda(A) = \pi(\Gamma(A))$. Since the map $\pi|_{\mathcal{S}(A,\boldsymbol{0})}$ is bijective, we obtain the following lemma.

Lemma 3.1. *Let $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_{n-m}$ be a basis of $\Gamma(A)$. The vectors $\boldsymbol{b}_1 = \pi(\boldsymbol{g}_1), \ldots, \boldsymbol{b}_{n-m} = \pi(\boldsymbol{g}_{n-m})$ form a basis of the lattice $\Lambda(A)$.*

Using notation of Lemma 3.1, let $G \in \mathbb{Z}^{n\times(n-m)}$ be the matrix with columns $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_{n-m}$. We will denote by F the $(n-m)\times(n-m)$-submatrix of G consisting of the last $n-m$ rows; hence, the columns of F are $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-m}$. Then $\det(\Lambda(A)) = |\det(F)|$. The rows of the matrix A span the m-dimensional rational subspace of $\mathbb{R}^n$ orthogonal to the $(n-m)$-dimensional rational subspace spanned by the columns of G. Therefore, by Lemma 5G and Corollary 5I in [15], we have $|\det(F)| = |\det(B)|/\gcd(A)$ and, consequently,

$$\det(\Lambda(A)) = \frac{|\det(B)|}{\gcd(A)}\,. \tag{3.1}$$

Consider the following algorithm.

Algorithm 1

Input: $(A, \boldsymbol{b})$, where $A = (B|N) \in \mathbb{Z}^{m\times n}$, $m < n$, with nonsingular $B \in \mathbb{Z}^{m\times m}$ and $\boldsymbol{b} \in \mathbb{Z}^m$.
Output: Solution $\boldsymbol{x} \in \mathbb{Z}^n$ to an integer feasible system $A\boldsymbol{x} = \boldsymbol{b}$.

Step 0: If $\Gamma(A, \boldsymbol{b}) = \emptyset$ then the system $A\boldsymbol{x} = \boldsymbol{b}$ is integer infeasible. Stop.
Step 1: Compute a point $\boldsymbol{z}$ of the affine lattice $\Lambda(A, \boldsymbol{b})$.
Step 2: Find a point $\boldsymbol{y} \in \Lambda(A)$ such that $\boldsymbol{z} \in \boldsymbol{y} + \mathcal{B}(\Lambda(A))$.
Step 3: Set $\boldsymbol{w} = \boldsymbol{z} - \boldsymbol{y}$ and output the vector

$$\boldsymbol{x} = \begin{pmatrix} \boldsymbol{u} \\ \boldsymbol{w} \end{pmatrix} \text{ with } \boldsymbol{u} = B^{-1}(\boldsymbol{b} - N\boldsymbol{w})\,. \tag{3.2}$$

Note that Algorithm 1 will be also used in the proof of Corollary 1.1, where the condition (1.2) is replaced by its refinement (1.6). For this reason, we do not require that the input of the algorithm satisfies (1.2) and, as a consequence, the algorithm outputs a certain integer, but not necessarily nonnegative solution to an integer feasible system $A\boldsymbol{x} = \boldsymbol{b}$ or detects integer infeasibility.

To complete the proof of Theorem 1.1, it is sufficient to show that Algorithm 1 is polynomial-time and that this algorithm computes a nonnegative integer solution to any integer feasible system $A\boldsymbol{x} = \boldsymbol{b}$ that satisfies its input conditions together with (1.2).

Let us show that all steps of the Algorithm 1 can be computed in polynomial time. By Corollaries 5.3 b,c in [16] we can compute in polynomial time integer vectors $\boldsymbol{r}, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{n-m}$ such that

$$\Gamma(A, \boldsymbol{b}) = \boldsymbol{r} + \sum_{i=1}^{n-m} \lambda_i \boldsymbol{g}_i \,, \lambda_i \in \mathbb{Z} \,, i \in \{1, \ldots, n-m\} \tag{3.3}$$

or determine that $\Gamma(A, \boldsymbol{b})$ is empty. This settles Step 0 and Step 1. Further, the vectors $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_{n-m}$ in (3.3) form a basis of the lattice $\Gamma(A)$. In Step 2 we first find the projected vectors $\boldsymbol{b}_1 = \pi(\boldsymbol{g}_1), \ldots, \boldsymbol{b}_{n-m} = \pi(\boldsymbol{g}_{n-m})$ that form a basis of the lattice $\Lambda(A)$ by Lemma 3.1. Then the point $\boldsymbol{y}$ can be computed in polynomial time using Lemmas 2.2 and 2.1. Finally, the lifted point $\boldsymbol{x}$ in Step 3 is computed in polynomial time by a straightforward calculation (3.2).

We will now show that Algorithm 1 computes a nonnegative integer solution to any integer feasible system $A\boldsymbol{x} = \boldsymbol{b}$ with $(A, \boldsymbol{b})$ satisfying its input conditions together with (1.2). By Step 0, we may assume that $\Gamma(A, \boldsymbol{b}) \neq \emptyset$ and hence at Step 1 we can find a point $\boldsymbol{z} \in \Lambda(A, \boldsymbol{b})$. At Step 2 we can find a point $\boldsymbol{y} \in \Lambda(A)$ with $\boldsymbol{z} \in \boldsymbol{y} + \mathcal{B}(\Lambda(A))$ by Lemma 2.1. Hence, the point $\boldsymbol{w} = \boldsymbol{z} - \boldsymbol{y}$ at Step 3 is a nonnegative point of the affine lattice $\Lambda(A, \boldsymbol{b})$. Further, since $\boldsymbol{w} \in \Lambda(A, \boldsymbol{b})$ and $\pi|_{\mathcal{S}(A,\boldsymbol{b})}$ is bijective, the point $\boldsymbol{x} = \pi|^{-1}_{\mathcal{S}(A,\boldsymbol{b})}(\boldsymbol{w})$ is integer. Summarising, we have

$$\boldsymbol{x} = \begin{pmatrix} \boldsymbol{u} \\ \boldsymbol{w} \end{pmatrix} \in \mathcal{S}(A, \boldsymbol{b}) \cap \mathbb{Z}^n \text{ and } \pi(\boldsymbol{x}) = \boldsymbol{w} \geq \boldsymbol{0} \,. \tag{3.4}$$

It is now sufficient to show that $\boldsymbol{u} \geq \boldsymbol{0}$.

Observe that, by construction, $\boldsymbol{w} \in \mathcal{B}(\Lambda(A))$. Hence, Lemma 2.3, applied to $\boldsymbol{w}$ and $\Lambda = \Lambda(A)$, implies

$$\prod_{i=1}^{n-m} (1 + w_i) \leq \det(\Lambda(A)) \,. \tag{3.5}$$

Expanding the product in (3.5) gives

$$\sum_{i=1}^{n-m} w_i \leq \det(\Lambda(A)) - 1 \,.$$

Hence, denoting by $\| \cdot \|_2$ the Euclidean norm, we obtain the inequality

$$\|N\boldsymbol{w}\|_2 \leq l_N \sum_{i=1}^{n-m} w_i \leq l_N(\det(\Lambda(A)) - 1) \,. \tag{3.6}$$

By (3.1), $\boldsymbol{b} \in \mathcal{C}_B(l_N(\det(\Lambda(A)) - 1))$ and by (3.6), $\boldsymbol{b} - N\boldsymbol{w} \in \mathcal{C}_B$. The cone $\mathcal{C}_B$ can be written as

$$\mathcal{C}_B = \{\boldsymbol{y} \in \mathbb{R}^m : B^{-1}\boldsymbol{y} \geq \boldsymbol{0}\}$$

and therefore

$$\boldsymbol{u} = B^{-1}(\boldsymbol{b} - N\boldsymbol{w}) \geq \boldsymbol{0}\,.$$

□

4. Proof of Corollary 1.1

Let $A = (a_{11}, \ldots, a_{1n}) \in \mathbb{Z}^{1\times n}$ satisfy (1.3). Then the lattice $\Lambda(A)$ can be written in the form

$$\Lambda(A) = \{\boldsymbol{x} \in \mathbb{Z}^{n-1} : a_{12}x_1 + \cdots + a_{1n}x_{n-1} \equiv 0 \,(\bmod a_{11})\}\,.$$

Note also that $\det(\Lambda(A)) = a_{11}$ by (3.1).

The next lemma shows that the box $B(\Lambda(A))$ is entirely determined by the parameters f_i defined by (1.4).

Lemma 4.1. *The box $B = B(\Lambda(A))$ has the form*

$$B = \left[0, \frac{f_1}{f_2}\right) \times \left[0, \frac{f_2}{f_3}\right) \times \cdots \times \left[0, \frac{f_{n-1}}{f_n}\right)\,.$$

Proof. By the definition of the box $B(\Lambda(A))$, it is sufficient to show that

$$v_{11} = \frac{f_1}{f_2}, v_{22} = \frac{f_2}{f_3}, \ldots, v_{n-1\,n-1} = \frac{f_{n-1}}{f_n}\,. \tag{4.1}$$

Let $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_{n-1}$ be the basis of the form (2.3) of the lattice $\Lambda(A)$. Let $\Lambda_i(A)$ denote the sublattice of $\Lambda(A)$ generated by the first i basis vectors $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_i$. We can write $\Lambda_i(A)$ in the form

$$\Lambda_i(A) = \Big\{(x_1, \ldots, x_i, 0, \ldots, 0)^T \in \mathbb{Z}^{n-1} : \frac{a_{12}}{f_{i+1}}x_1 + \cdots + \frac{a_{1i+1}}{f_{i+1}}x_i \equiv 0 \left(\bmod \frac{a_{11}}{f_{i+1}}\right)\Big\}\,.$$

Hence, $\det(\Lambda_i(A)) = a_{11}/f_{i+1}$, $i \in \{1, \ldots, n-1\}$. On the other hand, (2.3) implies $\det(\Lambda_i(A)) = v_{11}v_{22}\cdots v_{ii}$, $i \in \{1, \ldots, n-1\}$. Since $a_{11} = \det(\Lambda(A)) = v_{11}v_{22}\cdots v_{n-1\,n-1}$, we have $f_{i+1} = v_{i+1\,i+1}\cdots v_{n-1\,n-1}$ for $i \in \{1, \ldots, n-2\}$. Noticing that $f_1 = a_{11}$ and $f_n = 1$, we obtain (4.1). □

Suppose that $b > G(A)$. The condition (1.3) (i) implies that the equation $A\boldsymbol{x} = b$ has integer solutions. Therefore, it is sufficient to show that the vector $\boldsymbol{x}$ computed by Algorithm 1 is nonnegative. When $m = 1$, (3.2) sets $\boldsymbol{x} = (u, w_1, \ldots, w_{n-1})^T$ with

$$u = \frac{b - a_{12}w_1 - \cdots - a_{1n}w_{n-1}}{a_{11}}\,. \tag{4.2}$$

Further, (3.4) implies that $\boldsymbol{w} = (w_1, \ldots, w_{n-1})^T \in \Lambda(A, b)$ is nonnegative and $u \in \mathbb{Z}$.

To see that $u \geq 0$, we observe first that the points of the affine lattice $\Lambda(A, b)$ are split into the layers of the form

$$a_{12}x_1 + \cdots + a_{1n}x_{n-1} = b + ka_{11}\,, k \in \mathbb{Z}\,. \tag{4.3}$$

Suppose, to derive a contradiction, that $u < 0$. Then, by (4.2),

$$a_{12}w_1 + \cdots + a_{1n}w_{n-1} > b\,. \tag{4.4}$$

On the other hand, by construction, $\boldsymbol{w} \in B(\Lambda(A))$ and hence, using Lemma 4.1 and noticing (1.5),

$$a_{12}w_1 + \cdots + a_{1n}w_{n-1} \leq G(A) + a_{11} < b + a_{11}\,. \tag{4.5}$$

Due to (4.3), the bounds (4.4) and (4.5) imply $\boldsymbol{w} \notin \Lambda(A, b)$. The obtained contradiction shows that $u \geq 0$.

5. Proof of Corollary 1.2

We will show that a nonnegative integer solution to the system $A\boldsymbol{x} = \boldsymbol{b}$ can be computed using Algorithm 1 from the proof of Theorem 1.1. By condition (1.3) (i), the system $A\boldsymbol{x} = \boldsymbol{b}$ is integer feasible. Following the proof of Theorem 1.1, it is sufficient to show that any $\boldsymbol{b}$ that satisfies (1.9) must satisfy (1.2).

Let h denote the distance from the vector $\boldsymbol{v}$ to the boundary of $\mathcal{C}_B$. Observe that we can write $\boldsymbol{v} = \boldsymbol{v}_1 + \boldsymbol{v}_2 + \boldsymbol{p}$, where $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ are the columns of B and $\boldsymbol{p} \in \mathcal{C}_B$. Therefore, we have

$$h \geq \frac{|\det(B)|}{l_B}$$

and, consequently, the points of the affine cone

$$\frac{l_B l_N}{|\det(B)|}\,(|\det(B)| - 1)\,\boldsymbol{v} + \mathcal{C}_A$$

are at the distance $\geq l_N(|\det(B)| - 1)$ to the boundary of $\mathcal{C}_B$.

6. Acknowledgement

The author is grateful to Valentin Brimkov, Martin Henk and Timm Oertel for valuable comments and suggestions.

References

[1] I. Aliev and M. Henk, *LLL-reduction for integer knapsacks*, J. Comb. Optim. **24** (2012), 613–626.

[2] L. Babai, *On Lovász' lattice reduction and the nearest lattice point problem*, Combinatorica **6** (1986), no. 1, 1–13.

[3] A. Brauer, *On a problem of partitions*, Amer. J. Math., **64** (1942), 299–312.

[4] A. Brauer and B. M. Seelbinder, *On a problem of partitions II*, Amer. J. Math., **76** (1954), 343–346.

[5] V. Brimkov, *Effective algorithms for solving a broad class of linear Diophantine equations in nonnegative integers*, Mathematics and mathematical education (Bulgarian) (Albena, 1989), 241–246.

[6] V. Brimkov, *A polynomial algorithm for solving a large subclass of linear Diophantine equations in nonnegative integers*, C. R. Acad. Bulgare Sci. **41** (1988), no. 11, 33–35.
[7] V. Brimkov and R. Barneva, *Gradient elements of the knapsack polytope*, Calcolo **38** (2001), 49–66.
[8] J. W. S. Cassels, *An introduction to the Geometry of Numbers*, Springer-Verlag 1971.
[9] R. E. Gomory (1969), *Some polyhedra related to combinatorial problems*, Linear Algebra and Appl. **2**, 451–558.
[10] M. Grötschel, L. Lovász and A. Schrijver, *Geometric algorithms and combinatorial optimization*, Algorithms and Combinatorics: Study and Research Texts, 2. Springer-Verlag, Berlin, 1988.
[11] R. Kannan and A. Bachem, *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM J. Comput. **8** (1979), 499–507.
[12] J. Martinet, *Perfect lattices in Euclidean spaces*, Grundlehren der Mathematischen Wissenschaften, vol. **327** (2003), Springer-Verlag, Berlin.
[13] C. H. Papadimitriou and K. Steiglitz, *Combinatorial optimization: algorithms and complexity*, Dover Publications, Inc., Mineola, NY, 1998.
[14] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and Its Applications, 2005.
[15] W. M. Schmidt, *Diophantine approximations and Diophantine equations*, Lecture Notes in Mathematics, Springer-Verlag, 1991.
[16] A. Schrijver, *Theory of linear and integer programming*, Wiley, Chichester, 1986.

Mathematics Institute, Cardiff University, Cardiff, Wales, UK
Email address: alievi@cardiff.ac.uk