Moscow Journal of Combinatorics and Number Theory

2019
vol. 8 no. 4

On polynomial-time solvable linear Diophantine problems

Iskander Aliev

msp

Moscow Journal of Combinatorics and Number Theory
Vol. 8, No. 4, 2019
dx.doi.org/10.2140/moscow.2019.8.357

On polynomial-time solvable linear Diophantine problems

Iskander Aliev

We obtain a polynomial-time algorithm that, given input $(A, \boldsymbol{b})$, where $A = (B \mid N) \in \mathbb{Z}^{m\times n}$, $m < n$, 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:

$$\begin{gathered}\text{Given } (A, \boldsymbol{b}), \text{ where } A \in \mathbb{Z}^{m\times n},\ m < n,\ \operatorname{rank}(A) = m \text{ and } \boldsymbol{b} \in \mathbb{Z}^m,\\ \text{find a nonnegative integer solution to the system } A\boldsymbol{x} = \boldsymbol{b}\\ \text{or determine that no such solution exists.}\end{gathered} \tag{1-1}$$

The problem (1-1) is referred to as the *multidimensional knapsack problem* and is NP-hard already for $m = 1$; see [Papadimitriou and Steiglitz 1982, Section 15.7].

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

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

be the cone generated by $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$. 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 1969], which 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

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

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.

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 $\ge t$ 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.

MSC2010: primary 11D04, 90C10; secondary 11H06.
Keywords: multidimensional knapsack problem, polynomial-time algorithms, asymptotic integer programming, lattice points, Frobenius numbers.

Theorem 1.1. *There exists a polynomial-time algorithm which, given input* $(A, \boldsymbol{b})$, *where* $A = (B \mid N) \in \mathbb{Z}^{m\times n}$, *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 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 1986, Corollary 4.1(c)]. The condition (ii) in (1-3) 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 [Ramírez Alfonsín 2005]. By condition (i) in (1-3), we have $\gcd(a_{11}, \dots, a_{1n}) = 1$ 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

$$b > F(A);$$

see Conjecture 1.1 in [Aliev and Henk 2012].

The best known result in this direction is due to [Brimkov 1989]; see also [Aliev and Henk 2012; Brimkov 1988; Brimkov and Barneva 2001]. Specifically, set

$$f_1 = a_{11}, \qquad f_i = \gcd(a_{11}, \dots, a_{1i}), \quad i \in \{2, \dots, n\}. \tag{1-4}$$

A classical upper bound of [Brauer 1942] 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 [1942] and, subsequently, Brauer and Seelbinder [1954] proved that the bound (1-5) is sharp and obtained a necessary and sufficient condition for the equality $F(A) = G(A)$. Brimkov [1989] 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 1.2. *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 [2012] 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 [Aliev and Henk 2012] 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 [Aliev and Henk 2012] 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 [Martinet 2003, 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 $A = (B \mid N)$ 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 1.3. *There exists a polynomial-time algorithm which, given input* $(A, \boldsymbol{b})$, *where* $A = (B \mid N) \in \mathbb{Z}^{2\times n}$, $B \in \mathbb{Z}^{2\times 2}$ *is nonsingular with* $\mathcal{C}_B = \mathcal{C}_A$, A *satisfies* (1-3) *and*

$$\boldsymbol{b} \in \mathbb{Z}^2 \cap \left(\frac{l_B l_N}{|\det(B)|} \Big(|\det(B)| - 1 \Big) \boldsymbol{v} + \mathcal{C}_A \right), \tag{1-9}$$

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

Noticing that $|\det(B)| \leq (\det(AA^T))^{1/2}$, condition (1-9) improves on (1-7) provided that $l_B l_N / |\det(B)| \leq 2^{(n-m)/2-1} p(m,n)$. For matrices A satisfying (1-8) an improvement occurs when $l_B l_N / |\det(B)| \leq p(m,n)$.

2. Tools from discrete geometry

For linearly independent $\boldsymbol{b}_1, \dots, \boldsymbol{b}_k$ in $\mathbb{R}^d$, the set $\Lambda = \left\{ \sum_{i=1}^k \lambda_i \boldsymbol{b}_i : \lambda_i \in \mathbb{Z} \right\}$ is a k-dimensional *lattice* with *basis* $\boldsymbol{b}_1, \dots, \boldsymbol{b}_k$ and *determinant* $\det(\Lambda) = (\det(\boldsymbol{b}_i \cdot \boldsymbol{b}_j)_{1 \leq i,j \leq k})^{1/2}$, 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 $\boldsymbol{b}_1, \dots, \boldsymbol{b}_d$:

$$\hat{\boldsymbol{b}}_1 = \boldsymbol{b}_1, \qquad \hat{\boldsymbol{b}}_i = \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \hat{\boldsymbol{b}}_j, \qquad j \in \{2, \dots, d\}, \tag{2-1}$$

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

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

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 $\boldsymbol{x} \in \boldsymbol{y} + \widehat{\mathcal{B}}(\boldsymbol{b}_1, \dots, \boldsymbol{b}_d)$.*

A proof of Lemma 2.1 is implicitly contained, for instance, in the description of the classical nearest-plane procedure of [Babai 1986]. For completeness, we include a proof that follows along an argument of the proof of Theorem 5.3.26 in [Grötschel et al. 1988].

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

$$\boldsymbol{x} - \boldsymbol{y} = \sum_{i=1}^{d} \lambda_i \hat{\boldsymbol{b}}_i, \quad \lambda_i \in [0, 1), \ i \in \{1, \dots, d\}. \tag{2-2}$$

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 [Schrijver 1986]. 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). □

Let now Λ be a d-dimensional sublattice of $\mathbb{Z}^d$. By Theorem I(A) and Corollary 1 in Chapter I of [Cassels 1959], there exists a unique basis $\boldsymbol{g}_1, \dots, \boldsymbol{g}_d$ 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 $i \in \{1, \dots, d\}$ and $0 \le v_{ij} < v_{jj}$ for $i, j \in \{1, \dots, d\}$, $i > j$.

Lemma 2.2. *There exists a polynomial-time algorithm that, given a basis $\boldsymbol{b}_1, \dots, \boldsymbol{b}_d$ 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 1979]. □

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

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

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, $\Gamma(A, \boldsymbol{b}) \neq \varnothing$. 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 $A = (B \mid N)$, 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

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

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 [Schmidt 1991], 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 $A = (B \mid N) \in \mathbb{Z}^{m\times n}$, $m < n$, 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 $\Gamma(A, \boldsymbol{b}) = \varnothing$ 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

$$\boldsymbol{x} = \begin{pmatrix} \boldsymbol{u} \\ \boldsymbol{w} \end{pmatrix}, \quad \text{with } \boldsymbol{u} = B^{-1}(\boldsymbol{b} - N\boldsymbol{w}). \tag{3-2}$$

Note that Algorithm 1 will be also used in the proof of Corollary 1.2, 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 Algorithm 1 can be computed in polynomial time. By Corollaries 5.3(b,c) in [Schrijver 1986] we can compute in polynomial time integer vectors $\boldsymbol{r}, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{n-m}$ such that

$$\Gamma(A, \boldsymbol{b}) = \boldsymbol{r} + \sum_{i=1}^{n-m} \lambda_i \boldsymbol{g}_i, \quad \lambda_i \in \mathbb{Z},\ i \in \{1, \ldots, n-m\}, \tag{3-3}$$

or determine that $\Gamma(A, \boldsymbol{b})$ is empty. This settles Steps 0 and 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 $\Gamma(A, \boldsymbol{b}) \neq \varnothing$ 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 $\boldsymbol{x} = \pi|_{\mathcal{S}(A,\boldsymbol{b})}^{-1}(\boldsymbol{w})$ is integer. Summarising, we have

$$\boldsymbol{x} = \begin{pmatrix} \boldsymbol{u} \\ \boldsymbol{w} \end{pmatrix} \in \mathcal{S}(A, \boldsymbol{b}) \cap \mathbb{Z}^n \quad \text{and} \quad \pi(\boldsymbol{x}) = \boldsymbol{w} \geq \boldsymbol{0}. \tag{3-4}$$

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

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

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

$$\|N\boldsymbol{w}\|_2 \le l_N \sum_{i=1}^{n-m} w_i \le l_N(\det(\Lambda(A)) - 1). \tag{3-6}$$

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

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

and therefore

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

□

4. Proof of Corollary 1.2

Let $A = (a_{11}, \dots, a_{1n}) \in \mathbb{Z}^{1\times n}$ satisfy (1-3). Then the lattice $\Lambda(A)$ can be written in the form

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

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

$$v_{11} = \frac{f_1}{f_2}, \quad v_{22} = \frac{f_2}{f_3}, \quad \dots, \quad v_{n-1\,n-1} = \frac{f_{n-1}}{f_n}. \tag{4-1}$$

Let $\boldsymbol{g}_1, \dots, \boldsymbol{g}_{n-1}$ 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 $\boldsymbol{g}_1, \dots, \boldsymbol{g}_i$. We can write $\Lambda_i(A)$ in the form

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

Hence, $\det(\Lambda_i(A)) = a_{11}/f_{i+1}$, $i \in \{1, \dots, n-1\}$. On the other hand, (2-3) implies

$$\det(\Lambda_i(A)) = v_{11}v_{22}\cdots v_{ii}, \quad i \in \{1, \dots, n-1\}.$$

Since $a_{11} = \det(\Lambda(A)) = v_{11}v_{22}\cdots v_{n-1\,n-1}$, we have

$$f_{i+1} = v_{i+1\,i+1}\cdots v_{n-1\,n-1} \quad \text{for } i \in \{1, \dots, n-2\}.$$

Noticing that $f_1 = a_{11}$ and $f_n = 1$, we obtain (4-1). □

Suppose that $b > G(A)$. 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 $\boldsymbol{x} = (u, w_1, \dots, w_{n-1})^T$ with

$$u = \frac{b - a_{12}w_1 - \cdots - a_{1n}w_{n-1}}{a_{11}}. \tag{4-2}$$

Further, (3-4) implies that $\boldsymbol{w} = (w_1, \dots, w_{n-1})^T \in \Lambda(A, b)$ 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 layers of the form

$$a_{12}x_1 + \cdots + a_{1n}x_{n-1} = b + ka_{11}, \quad k \in \mathbb{Z}. \tag{4-3}$$

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 1.3

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 $\mathcal{C}_B$.

Acknowledgement

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

References

[Aliev and Henk 2012] I. Aliev and M. Henk, "LLL-reduction for integer knapsacks", *J. Comb. Optim.* **24**:4 (2012), 613–626. MR Zbl

[Babai 1986] L. Babai, "On Lovász' lattice reduction and the nearest lattice point problem", *Combinatorica* **6**:1 (1986), 1–13. MR Zbl

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

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

[Brimkov 1988] V. E. Brimkov, "A polynomial algorithm for solving a large subclass of linear Diophantine equations in nonnegative integers", *C. R. Acad. Bulgare Sci.* **41**:11 (1988), 33–35. MR Zbl

[Brimkov 1989] V. E. Brimkov, "Effective algorithms for solving a broad class of linear Diophantine equations in nonnegative integers", pp. 241–246 in *Mathematics and education in mathematics* (Albena, Bulgaria, 1989), edited by G. Gerov, Bulgar. Akad. Nauk, Sofia, 1989. In Bulgarian. MR

[Brimkov and Barneva 2001] V. E. Brimkov and R. P. Barneva, "Gradient elements of the knapsack polytope", *Calcolo* **38**:1 (2001), 49–66. MR Zbl

[Cassels 1959] J. W. S. Cassels, *An introduction to the geometry of numbers*, Grundlehren der Math. Wissenschaften **99**, Springer, 1959. MR Zbl

[Gomory 1969] R. E. Gomory, "Some polyhedra related to combinatorial problems", *Linear Algebra and Appl.* **2** (1969), 451–558. MR Zbl

[Grötschel et al. 1988] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric algorithms and combinatorial optimization*, Algorithms Combinator. Study Res. Texts **2**, Springer, 1988. MR Zbl

[Kannan and Bachem 1979] R. Kannan and A. Bachem, "Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix", *SIAM J. Comput.* **8**:4 (1979), 499–507. MR Zbl

[Martinet 2003] J. Martinet, *Perfect lattices in Euclidean spaces*, Grundlehren der Math. Wissenschaften **327**, Springer, 2003. MR Zbl

[Papadimitriou and Steiglitz 1982] C. H. Papadimitriou and K. Steiglitz, *Combinatorial optimization: algorithms and complexity*, Prentice-Hall, Englewood Cliffs, NJ, 1982. MR Zbl

[Ramírez Alfonsín 2005] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lect. Series Math. Appl. **30**, Oxford Univ. Press, 2005. MR Zbl

[Schmidt 1991] W. M. Schmidt, *Diophantine approximations and Diophantine equations*, Lecture Notes in Math. **1467**, Springer, 1991. MR Zbl

[Schrijver 1986] A. Schrijver, *Theory of linear and integer programming*, Wiley, Chichester, 1986. MR Zbl

Received 15 Mar 2019. Revised 1 Jul 2019.

ISKANDER ALIEV:

alievi@cardiff.ac.uk
Mathematics Institute, Cardiff University, Cardiff, United Kingdom

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

Moscow Journal of Combinatorics and Number Theory

vol. 8 no. 4 2019