arXiv:1012.3182v1 [math.OC] 14 Dec 2010

LLL-REDUCTION FOR INTEGER KNAPSACKS

ISKANDER ALIEV AND MARTIN HENK

Abstract. Given a matrix $A \in \mathbb{Z}^{m\times n}$ satisfying certain regularity assumptions, a well-known integer programming problem asks to find an integer point in the associated *knapsack polytope*

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

or determine that no such point exists. We obtain a LLL-based polynomial time algorithm that solves the problem subject to a constraint on the location of the vector $\boldsymbol{b}$.

1. Introduction and Statement of Results

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

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

where $\gcd(a_1, \dots, a_l)$ denotes the greatest common divisor of integers a_i, $1 \leq i \leq l$. For such a matrix A and a vector $\boldsymbol{b} \in \mathbb{Z}^m$ the *knapsack polytope* $P(A, \boldsymbol{b})$ is defined as

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

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

The paper is concerned with the following integer programming problem:

$$\text{(1.2)} \qquad \begin{array}{l} \text{Given input } (A, \boldsymbol{b}) \text{, find an integer point in } P(A, \boldsymbol{b}) \\ \text{or determine that no such a point exists}\,. \end{array}$$

The problem (1.2) is well-known to be NP-hard (Karp [14]).

Let us define the set

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

Thus, the set $\mathcal{F}(A)$ will consist of all possible vectors $\boldsymbol{b}$ such that the polytope $P(A, \boldsymbol{b})$ contains an integer point.

A set $S \subset \mathbb{R}^m$ will be called a *feasible* set if $S \cap \mathbb{Z}^m \subset \mathcal{F}(A)$. Results of Aliev and Henk [2], Knight [15], Simpson and Tijdeman [25] and Pleasants, Ray and Simpson [19] show that the set $\mathcal{F}(A)$ can be decomposed into

2000 *Mathematics Subject Classification.* Primary: 90C10, 90C27, 11D07 ; Secondary: 11H06.

Key words and phrases. Knapsack problem; Frobenius numbers; successive minima; inhomogeneous minimum; distribution of lattices.

the set of all integer points in a certain feasible (translated) cone and a complementary set with complex combinatorial structure.

Note that the case $m = 1$ corresponds to the celebrated Frobenius problem and has been extensively studied in the literature. We address this problem below. When $n = m + 1$ Pleasants, Ray and Simpson [19] obtain a unique maximal cone whose interior is feasible. To the best of the authors knowledge the existence of such a maximal cone in the general case is not known.

The location of a feasible cone is given by the *diagonal Frobenius number* defined as follows. Let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n \in \mathbb{Z}^m$ be the columns of the matrix A and let

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

be the cone generated by $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$. Let also $\boldsymbol{v} := \boldsymbol{v}_1 + \ldots + \boldsymbol{v}_n$. Following Aliev and Henk [2], by the *diagonal Frobenius number* $\mathrm{g} = \mathrm{g}(A)$ *of* A we understand the minimal $s \geq 0$, such that for all $\boldsymbol{b} \in \{s\boldsymbol{v} + C\} \cap \mathbb{Z}^m$ the polytope $P(A, \boldsymbol{b})$ contains an integer point. Thus we have the inclusion

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

or, in other words, the translated cone $\{\mathrm{g}(A)\boldsymbol{v} + C\}$ is feasible.

The behavior of $\mathrm{g}(A)$ was investigated in Aliev and Henk [2]. The authors obtained an optimal up to a constant multiplier upper bound

$$\mathrm{g}(A) \leq \frac{(n-m)}{2}(n \det(AA^T))^{1/2} \tag{1.3}$$

and estimated the expected value of the diagonal Frobenius number.

It is natural to expect that the problem (1.2) is solvable in polynomial time when the right hand side vector $\boldsymbol{b}$ belongs to a feasible cone. For such vectors $\boldsymbol{b}$ we a priori know that the knapsack polytope contains at least one integer point. We conjecture that the integer knapsack problem is solvable in polynomial time for all instances $(A, \boldsymbol{b})$ with

$$\boldsymbol{b} \in \{\mathrm{g}(A)\boldsymbol{v} + C\} \cap \mathbb{Z}^m\,.$$

This question generalizes the Problem A.1.2 in Ramírez Alfonsín [21].

The first result of the paper gives an estimate for the location of the desired feasible cone and can be considered as a step towards proving our conjecture.

Theorem 1.1. *There exists a polynomial time algorithm which, given* $(A, \boldsymbol{b})$*, where* A *satisfies (1.1),* $\boldsymbol{b} \in \mathbb{Z}^m$ *with*

$$\boldsymbol{b} \in \{2^{(n-m)/2-1} p(m,n)(\det(AA^T))^{1/2}\boldsymbol{v} + C\} \tag{1.4}$$

and

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

finds an integer point in the polytope $P(A, \boldsymbol{b})$*.*

The proof of Theorem 1.1 is constructive. We obtain an LLL-based polynomial time algorithm with the desired properties. In fact, the algorithm computes in polynomial time a reasonably good approximation for the integer knapsack problem. We show that the approximation provides a solution of the problem when the input vector $\boldsymbol{b}$ belongs to a certain feasible cone.

In view of (1.3), the affirmative answer to our conjecture would imply that the factor $2^{(n-m)/2-1}p(m,n)$ in (1.4) can be replaced by $\frac{(n-m)n^{1/2}}{2}$, hence the exponent $2^{(n-m)/2-1}$ in (1.4) might be redundant.

Our next result shows that the exponent can be removed for all matrices A with sufficiently large $\det(AA^T)$. This phenomenon is related to the bounds on the efficiency of the LLL-algorithm and is a consequence of Theorem 1.4 below. In order to state the result, let γ_k be the k-dimensional Hermite constant for which we refer to [18, Definition 2.2.5]. Here we just note that by a result of Blichfeldt (see, e.g., Gruber and Lekkerkerker [11])

$$\gamma_k \leq 2\left(\frac{k+2}{\sigma_k}\right)^{2/k},$$

where σ_k is the volume of the unit k-ball; thus $\gamma_k = O(k)$.

Theorem 1.2. *There exists a polynomial time algorithm which, given* $(A, \boldsymbol{b})$, *where A satisfies (1.1),* $\boldsymbol{b} \in \mathbb{Z}^m$ *with*

$$\boldsymbol{b} \in \{p(m,n)(\det(AA^T))^{1/2}\boldsymbol{v} + C\}$$

and

$$\det(AA^T) > \frac{2^{5(n-m)-6}(n-m-1)^3\gamma_{n-m}^{n-m}}{n}, \tag{1.5}$$

solves the problem (1.2).

Thus, if the dimension n is concerned, Theorem 1.1 gives an exponential bound in n for the location of the desired feasible cone, the affirmative answer to our conjecture would imply the bound of order $n^{3/2}$ and for large determinants $\det(AA^T)$ we obtained the bound of order n^2 in Theorem 1.2. In view of the size of γ_k, the lower bound for $\det(AA^T)$ has order $n^2 2^{n\log n+5n}$.

We would also like to mention an interesting consequence of Theorems 1.1 and 1.2. The proof of Lemma 1.1 in Aliev and Henk [2] immediately implies that for any integer vector $\boldsymbol{w}$ in the interior $\operatorname{int} C$ of the cone C we have

$$\left(\frac{\det(AA^T)}{n-m+1}\right)^{1/2}\boldsymbol{w} \in \{\boldsymbol{v} + C\}.$$

It follows then from Theorem 1.1 that for every integer vector $\boldsymbol{b} \in \operatorname{int} C$ one can find in polynomial time an integer point in the polytope $P(A, \gamma\boldsymbol{b})$ for any integer vector $\gamma\boldsymbol{b}$ with

$$\gamma > \frac{2^{(n-m)/2-1}p(m,n)}{n-m+1}\det(AA^T)\,.$$

Moreover, if we assume (1.5) to hold, then by Theorem 1.2 we can remove the exponential multiplier $2^{(n-m)/2-1}$ from the latter inequality.

Let us now consider the special case $m = 1$. Then $A = \boldsymbol{a}^T$ with $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)^T \in \mathbb{Z}^n$ and (1.1) i) says that $\gcd(\boldsymbol{a}) := \gcd(a_1, a_2, \ldots, a_n) = 1$. Due to the second assumption (1.1) ii) we may assume that all entries of $\boldsymbol{a}$ are positive. The largest integral value b such that for $A = \boldsymbol{a}^T$ and $\boldsymbol{b} = (b)$ the polytope $P(A, \boldsymbol{b})$ contains no integer point is called the *Frobenius number* of $\boldsymbol{a}$, denoted by $\mathrm{F}(\boldsymbol{a})$. Thus, when $m = 1$ the answer for the feasibility problem

(1.6) Given input $(A, \boldsymbol{b})$, does the polytope $P(A, \boldsymbol{b})$ contain an integer point?

is affirmative for all instances $(\boldsymbol{a}^T, b)$ with $b > \mathrm{F}(\boldsymbol{a})$. Therefore, it is natural to expect that the problem (1.6) can be solved in polynomial time when $b > c$, for some function $c = c(\boldsymbol{a})$. Problem A.1.2 in Ramírez Alfonsín ([21], page 185) asks whether or not it is true for $c = \mathrm{F}(\boldsymbol{a})$.

Frobenius numbers naturally appear in the analysis of integer programming algorithms (see, e.g., Aardal and Lenstra [1], Hansen and Ryan [12], and Lee, Onn and Weismantel [17]). The general problem of finding $\mathrm{F}(\boldsymbol{a})$ has been traditionally referred to as the *Frobenius problem*. This problem is NP-hard (Ramírez Alfonsín [20, 21]) and integer programming techniques are known to be an effective tool for investigating behavior of the Frobenius numbers, see e.g. Kannan [13], Eisenbrand and Shmonin [7] and Beihoffer et al [5].

For $m = 1$, we obtain the following refinement of the previous result.

Theorem 1.3. *For any $\delta > 0$ the function $p(1, n)$ in the statements of Theorems 1.1 and 1.2 can be replaced by*

$$q(n) = \frac{(1+\delta)}{n}\,p(1,n) = (1+\delta)\,2^{-1/2}\,(n-1)\,n^{1/2}. \tag{1.7}$$

Note that if Problem A.1.2 of Ramírez Alfonsín ([21], page 185) can be solved in affirmative, then the factor $2^{(n-1)/2-1}p(1,n)$ in (1.4) can be replaced by an absolute constant.

The proof of Theorem 1.1 is based on an algorithm of Schnorr [23], which extends and improves the classical Babai's nearest point algorithm [4]. The algorithm is searching for a nearby lattice point and is built on the LLL lattice basis reduction (see Section 3). In the course of the proof we need to estimate the quality of the LLL-reduced lattice basis in terms of the determinant of the lattice. The key ingredient of the proof is the following result.

For $1 \le k \le n$ let

$$\rho_k = \left(\frac{2^{5k-7}(k-1)^3 \gamma_k^k}{n} \right)^{1/2},$$

and let $||\cdot||$ denote the Euclidean norm.

Theorem 1.4. *Let $L \subset \mathbb{Z}^n$ be a k-dimensional lattice with $\det(L) > \rho_k$ and let $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ be an LLL–reduced basis of L. Then for $1 \le i \le k$*

$$||\boldsymbol{b}_i|| \le \left(\left(1 + \frac{\rho_k^2}{(\det(L))^2} \right) n \right)^{1/2} \det(L)\,. \tag{1.8}$$

Note that the classical bounds for the lengths of the vectors in an LLL-reduced basis imply for all $1 \le i \le k$ the estimates

$$||\boldsymbol{b}_i|| \le 2^{\frac{k-1}{2}} n^{1/2} \det(L)\,,$$

see Lemma 4.1 below. In (1.8) we manage to remove the exponential multiplier $2^{(k-1)/2}$ for integer lattices with sufficiently large determinant.

2. Integer Knapsacks and Geometry of Numbers

Our approach to the problem is based on Geometry of Numbers for which we refer to the books [6, 10, 11].

By a *lattice* we will understand a discrete submodule L of a finite-dimensional Euclidean space. Here we are mainly interested in primitive lattices $L \subset \mathbb{Z}^n$, where such a lattice is called *primitive* if $L = \operatorname{span}_{\mathbb{R}}(L) \cap \mathbb{Z}^n$.

Recall that the Frobenius number $\mathrm{F}(\boldsymbol{a})$ is defined only for integer vectors $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ with $\gcd(\boldsymbol{a}) = 1$. This is equivalent to the statement that the 1-dimensional lattice $L = \mathbb{Z}\,\boldsymbol{a}$, generated by $\boldsymbol{a}$ is primitive. This generalizes easily to an m-dimensional lattice $L \subset \mathbb{Z}^n$ generated by $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in \mathbb{Z}^n$. Here the criterion is that L is primitive if and only if the greatest common divisor of all $m \times m$-minors is 1. This is an immediate consequence of Cassels [6, Lemma 2, Chapter1] or see Schrijver [24, Corollary 4.1c].

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

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

Now let $A \in \mathbb{Z}^{m \times n}$ be a matrix satisfying the assumptions (1.1). By V_A we will denote the m-dimensional subspace of $\mathbb{R}^n$ spanned by the rows of A. The orthogonal complement of V_A in $\mathbb{R}^n$ will be denoted as $V_A^\perp$, so that

$$V_A^\perp = \{\boldsymbol{x} \in \mathbb{R}^n : A\,\boldsymbol{x} = \boldsymbol{0}\}\,.$$

Furthermore, we will use the notation

$$L_A^{\perp} = V_A^{\perp} \cap \mathbb{Z}^n$$

for the integer sublattice contained in $V_A^{\perp}$. Observe that (cf. [18, Proposition 1.2.9])

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

For a k-dimensional lattice L and an 0-symmetric convex body $K \subset \mathrm{span}_{\mathbb{R}} L$ the ith-successive minimum of K with respect to L is defined as

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

i.e., it is the smallest factor such that $\lambda\, K$ contains at least i linearly independent lattice points of L.

The Minkowski's celebrated theorem on successive minima states (cf. [10, Theorem 23.1])

$$\frac{2^k}{k!} \det(L) \leq \mathrm{vol}\,(K) \prod_{i=1}^{k} \lambda_i(K, L) \leq 2^k \det(L), \tag{2.2}$$

where $\mathrm{vol}\,(K)$ denotes the volume of K.

Let $\Delta_k = \gamma_k^{-k/2}$ denote the critical determinant of the unit k–ball. Let also B be the unit ball in $\mathrm{span}_{\mathbb{R}} L$. In the important special case $K = B$ the Minkowski's theorem on successive minima can be improved (cf. [11, §18.4, Theorem 3]) to

$$\det(L) \leq \prod_{i=1}^{k} \lambda_i(B, L) \leq \Delta_k^{-1} \det(L)\,. \tag{2.3}$$

3. LLL-reduction and successive minima

For a basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ of a lattice L in $\mathbb{R}^n$ we denote by $\hat{\boldsymbol{b}}_1, \hat{\boldsymbol{b}}_2, \ldots, \hat{\boldsymbol{b}}_k$ its Gram-Schmidt orthogonalization and by $\mu_{i,j}$ the corresponding Gram-Schmidt coefficients, that is

$$\hat{\boldsymbol{b}}_1 = \boldsymbol{b}_1\,, \quad \hat{\boldsymbol{b}}_i = \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \hat{\boldsymbol{b}}_i\,, \quad 2 \leq i \leq k\,,$$

and

$$\mu_{ij} = \frac{\langle \boldsymbol{b}_i, \hat{\boldsymbol{b}}_j \rangle}{||\hat{\boldsymbol{b}}_j||^2}\,.$$

Put $\lambda_i = \lambda(B, L)$, where B is the unit ball in $\mathrm{span}_{\mathbb{R}} L$. We first recall the following technical observation.

Lemma 3.1. *We have*

$$\lambda_i \geq \min_{j=i,i+1,\ldots,k} ||\hat{\boldsymbol{b}}_j||\,, \quad i = 1, 2, \ldots, k\,.$$

Proof. The proof can be easily derived from the proof of Proposition 1.12 in [16]. □

Recall that a lattice basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ is *LLL–reduced* if

(a) $|\mu_{ij}| \le \frac{1}{2}$, for $1 \le j < i \le k$;

(b) $\frac{3}{4}||\hat{\boldsymbol{b}}_{i-1}||^2 \le ||\hat{\boldsymbol{b}}_i||^2 + \mu_{i\,i-1}^2||\hat{\boldsymbol{b}}_{i-1}||^2$, for $2 \le i \le k$.

The next lemma shows that the ith successive minimum λ_i is essentially equal to both the ith vector of the LLL-reduced basis and the ith vector of its Gram–Schmidt orthogonalization. The involved constants are exponential in k.

Lemma 3.2. *Suppose that the basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_k$ is LLL–reduced. Then for $1 \le i \le k$ the inequalities*

$$2^{1-i}\lambda_i^2 \le ||\boldsymbol{b}_i||^2 \le 2^{k-1}\lambda_i^2\,, \tag{3.1}$$

$$2^{2-2i}\lambda_i^2 \le ||\hat{\boldsymbol{b}}_i||^2 \le 2^{k-i}\lambda_i^2 \tag{3.2}$$

hold.

Proof. The inequalities (3.1) are given in a remark in the original paper of Lenstra, Lenstra and Lovasz [16, after Proposition 1.12]. Next, since the basis is LLL–reduced, the inequalities

$$||\boldsymbol{b}_i||^2 \le 2^{i-1}||\hat{\boldsymbol{b}}_i||^2\,, \quad 1 \le i \le k\,, \tag{3.3}$$

and

$$||\hat{\boldsymbol{b}}_j||^2 \ge 2^{i-j}||\hat{\boldsymbol{b}}_i||^2\,, \quad 1 \le i \le j \le k\,, \tag{3.4}$$

hold (see the proof of Proposition 1.6 in [16] for more details). Clearly, (3.1) and (3.3) imply the left hand side inequality in (3.2). Furthermore, by Lemma 3.1, there is some $j \ge i$ such that $\lambda_i^2 \ge ||\hat{\boldsymbol{b}}_j||^2 \ge 2^{i-k}||\hat{\boldsymbol{b}}_i||^2$. This justifies the right-hand side inequality in (3.2). □

Consequently, the ratios of the lengths of the vectors $\boldsymbol{b}_i$ can be controlled by the ratios of successive minima. In particular, the following result holds.

Corollary 3.1. *If*

$$\frac{\lambda_{k-1}}{\lambda_k} \le 2^{1-k}\,,$$

then

$$\max_{i=1,\ldots,k} ||\boldsymbol{b}_i|| = ||\boldsymbol{b}_k||\,.$$

For technical reasons we will need an upper bound for the ratios

$$\eta_i = ||\hat{\boldsymbol{b}}_i||/||\hat{\boldsymbol{b}}_k||\,, \quad i = 1, \ldots, k-1\,.$$

The following corollary gives a slightly more general result.

Corollary 3.2. *We have*

$$\frac{||\hat{\boldsymbol{b}}_i||^2}{||\hat{\boldsymbol{b}}_j||^2} \le 2^{k+2j-i-2}\frac{\lambda_i^2}{\lambda_j^2},$$

and, in particular,

$$\eta_i^2 \le 2^{3\,k-3}\frac{\lambda_i^2}{\lambda_k^2}.$$

Thus if the last successive minimum λ_k is large enough with respect to $\lambda_1, \dots, \lambda_{k-1}$ then all the numbers η_i are bounded by a small constant. The next result implies that in this case λ_k is a very good approximation of $||\boldsymbol{b}_k||$.

Lemma 3.3. *We have*

$$||\boldsymbol{b}_k|| \le \left(\frac{k-1}{4}\max_{i=1,\dots,k-1}\eta_i^2+1\right)^{1/2}\lambda_k\,.$$

Proof. By (3.2) we have

$$||\hat{\boldsymbol{b}}_k|| \le \lambda_k\,.$$

Observe that

$$\begin{aligned}||\boldsymbol{b}_k|| &= (\mu_{k,1}^2||\hat{\boldsymbol{b}}_1||^2+\dots+\mu_{k,k-1}^2||\hat{\boldsymbol{b}}_{k-1}||^2+||\hat{\boldsymbol{b}}_k||^2)^{1/2}\\ &= ||\hat{\boldsymbol{b}}_k||(\mu_{k,1}^2\eta_1^2+\dots+\mu_{k,k-1}^2\eta_{k-1}^2+1)^{1/2}\,.\end{aligned}$$

Thus

$$||\boldsymbol{b}_k|| \le \left(\frac{k-1}{4}\max_{i=1,\dots,k-1}\eta_i^2+1\right)^{1/2}\lambda_k\,.$$

□

4. LLL-reduction and determinant of the lattice

In this section we give an upper bound for the lengths of the vectors in an LLL-reduced basis in terms of the determinant of the lattice. The bound is based on the classical estimates from Lenstra, Lenstra and Lovasz [16] and, consequently, involves the exponential multiplier $2^{(k-1)/2}$.

Lemma 4.1. *Let $L \subset \mathbb{Z}^n$ be given by an LLL–reduced basis $\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_k$. Then*

$$\max_{i=1,\dots,k}||\boldsymbol{b}_i|| \le 2^{\frac{k-1}{2}}n^{1/2}\det(L)\,. \tag{4.1}$$

Proof. By Proposition 1.12 of Lenstra, Lenstra and Lovasz [16] for any choice of linearly independent vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \in L$ the inequality

$$||\boldsymbol{b}_i|| \leq 2^{\frac{k-1}{2}} \max\{||\boldsymbol{x}_1||, \ldots, ||\boldsymbol{x}_k||\} \tag{4.2}$$

holds.

Put $C^n = [-1,1]^n$, i.e., C^n is the n-dimensional cube of edge length 2 centered at the origin. By a well-known result of Vaaler [26], any k-dimensional section of the cube C^n has k-volume at least 2^k. In particular we have

$$\mathrm{vol}_k(C^n \cap \mathrm{span}_{\mathbb{R}}(L)) \geq 2^k .$$

Thus, by the Minkowski theorem on successive minima, applied to the section $C^n \cap \mathrm{span}_{\mathbb{R}}(L)$ and L, there exist linearly independent vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \in L$ such that

$$||\boldsymbol{x}_1||_\infty \cdots ||\boldsymbol{x}_k||_\infty \leq \det(L) ,$$

where $|| \cdot ||_\infty$ denotes the maximum norm.

Since $\boldsymbol{x}_i$ are nontrivial integral vectors we have

$$\max\{||\boldsymbol{x}_1||_\infty, \ldots, ||\boldsymbol{x}_k||_\infty\} \leq \det(L) .$$

Combining the latter inequality with (4.2) we obtain the inequality (4.1). □

5. Proof of Theorem 1.4

For $k = 1$ we have $||\boldsymbol{b}_1|| = \det(L)$, so that the result holds. In the rest of the proof we assume $k \geq 2$.

Suppose that

$$\max_{i=1,\ldots,k} ||\boldsymbol{b}_i|| = ||\boldsymbol{b}_l|| > ((1 + \rho_k^2/(\det(L))^2)n)^{1/2} \det(L) . \tag{5.1}$$

Then, by (3.1), we obtain

$$\lambda_k > ((1 + \rho_k^2/(\det(L))^2)n)^{1/2} \frac{\det(L)}{2^{\frac{k-1}{2}}} . \tag{5.2}$$

Thus, if (5.1) holds, then $\lambda_k \gg_n \det(L)$.

By the Minkowski theorem on successive minima for balls (2.3)

$$\lambda_1 \cdots \lambda_{k-1}\lambda_k \leq \Delta_k^{-1} \det(L) . \tag{5.3}$$

Since $L \subset \mathbb{Z}^k$, we clearly have $\lambda_i \geq 1$, $i = 1, \ldots, n-1$. The inequality (5.2) then implies

$$\lambda_{k-1} \leq \lambda_1 \cdots \lambda_{k-1} \leq 2^{\frac{k-1}{2}} \Delta_k^{-1} , \tag{5.4}$$

In other words, if $\lambda_k \gg_n \det(L)$ then $\lambda_{k-1} \ll_k 1$. Consequently, if (5.1) holds then the ratio λ_{k-1}/λ_k can be sufficiently small for large determinants.

Indeed, from (5.4) and (5.2) we get,

$$\frac{\lambda_{k-1}}{\lambda_k} \le \frac{2^{k-1}\Delta_k^{-1}}{((1+\rho_k^2/(\det(L))^2)n)^{1/2}\det(L)} \le 2^{1-k}\,.$$

Therefore, by Corollary 3.1, we have

$$\max_{i=1,\dots,k} ||\boldsymbol{b}_i|| = ||\boldsymbol{b}_k||\,. \tag{5.5}$$

This is an important observation as from now on we can restrict our attention to the behavior of the last vector of the LLL-reduced basis only.

By Lemma 3.3, the inequality (5.1) then implies that

$$\lambda_k > \frac{((1+\rho_k^2/(\det(L))^2)n)^{1/2}\det(L)}{\left(\frac{k-1}{4}\max_{i=1,\dots,k-1}\eta_i^2+1\right)^{1/2}}\,. \tag{5.6}$$

This estimate allows us to improve the bound (5.2). We will now use (5.6) to obtain an upper bound for $\max_{i=1,\dots,k-1}\eta_i^2$.

By (5.3), we get

$$\lambda_{k-1} \le \lambda_1\cdots\lambda_{k-1} \le \Delta_k^{-1}\left(\frac{k-1}{4}\max_{i=1,\dots,k-1}\eta_i^2+1\right)^{1/2},$$

so that, by Corollary 3.2 and (5.6), we have

$$\max_{i=1,\dots,k-1}\eta_i^2 \le 2^{3k-3}\Delta_k^{-2}\frac{\left(\frac{k-1}{4}\max_{i=1,\dots,k-1}\eta_i^2+1\right)^2}{n(\det(L))^2}\,.$$

Since, by Corollary 3.2, $\max_{i=1,\dots,k-1}\eta_i^2 \le 2^{k-1}$, we obtain the inequality

$$\max_{i=1,\dots,k-1}\eta_i^2 \le 2^{3k-3}\Delta_k^{-2}\frac{\left(\frac{k-1}{4}2^{k-1}+1\right)^2}{n(\det(L))^2}\,. \tag{5.7}$$

Consequently, if (5.1) holds then all numbers η_i approach zero as $\det(L)$ tends to infinity.

By the Minkowski theorem on successive minima, applied to the set $C^n \cap \mathrm{span}_{\mathbb{R}}(L)$ and the lattice L, and by the already mentioned result of Vaaler [26], we have

$$\prod_{i=1}^{k}\lambda_i(C^n\cap\mathrm{span}_{\mathbb{R}}(L),L) \le \det(L)\,.$$

Since $L\subset\mathbb{Z}^n$, the interior of $C^n\cap\mathrm{span}_{\mathbb{R}}(L)$ does not contain any nonzero point of L. This implies

$$\lambda_k(C^n\cap V_A^{\perp},L)\le\det(L)\,,$$

so that

$$\lambda_k \le n^{1/2}\det(L)\,.$$

Consequently, by Lemma 3.3, the inequality (5.7) and condition $\det(L) > \rho_k$, we have

$$||\boldsymbol{b}_k|| \leq \left(\left(\frac{k-1}{4} \max_{i=1,\ldots,k-1} \eta_i^2 + 1\right) n\right)^{1/2} \det(L)$$

$$\leq ((1 + \rho_k^2/(\det(L))^2)n)^{1/2} \det(L)\,.$$

That is the condition $\det(L) > \rho_k$ guarantees that $\max_{i=1,\ldots,k-1} \eta_i^2$ is sufficiently small and so $||\boldsymbol{b}_k||$ is small. On account of (5.5) we obtain a contradiction with (5.1). The theorem is proved.

6. The Algorithm. Proofs of Theorems 1.1 and 1.2

6.1. **Proof of Theorem 1.1.** Let $\boldsymbol{c} \in \mathbb{R}^n$ be any point that does not lie in the subspace $V_A^\perp$. The projection of a point $\boldsymbol{x} \in \{\boldsymbol{c} + V_A^\perp\}$ along the vector $\boldsymbol{c}$ onto the subspace $V_A^\perp$ will be denoted as $\pi_{\boldsymbol{c}}(\boldsymbol{x})$. That is for some $t \in \mathbb{R}^n$ we can write $\pi_{\boldsymbol{c}}(\boldsymbol{x}) = \boldsymbol{x} + t\boldsymbol{c} \in V_A^\perp$.

Suppose that

$$\boldsymbol{b} \in \{\mu(m,n)(\det(AA^T))^{1/2}\boldsymbol{v} + C\} \cap \mathbb{Z}^m \tag{6.1}$$

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

To prove Theorem 1.1 it is enough to construct a polynomial time algorithm that finds an integer point in $P(A,\boldsymbol{b})$. The algorithm is described below:

Input : $(A,\boldsymbol{b})$ with A and $\boldsymbol{b}$ satisfying (1.1) and (6.1) respectively;

Output : $\boldsymbol{z} \in P(A,\boldsymbol{b}) \cap \mathbb{Z}^n$;

Step 1 : Find a basis $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-m}$ of $L_A^\perp$ and an integer solution $\boldsymbol{u}$ of the equation $A\boldsymbol{x} = \boldsymbol{b}$. This step can be performed in polynomial time by Corollary 5.3c of Schrijver [24];

Step 2 : Find a point $\boldsymbol{c}$ such that $P(A,\boldsymbol{b})$ contains an $(n-m)$-dimensional ball centered at $\boldsymbol{c}$ and of radius

$$r \geq \frac{\mu(m,n)(\det(AA^T))^{1/2}}{n-m+1}\,. \tag{6.2}$$

As we show below the point $\boldsymbol{c}$ can be found in polynomial time.

Step 3 : Apply the algorithm for finding a nearby lattice point, described in Section 4 of Schnorr [23] (putting in this algorithm the parameter $\beta = 2$), to the basis $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-m}$ and the point $\pi_{\boldsymbol{c}}(\boldsymbol{u})$. The algorithm is polynomial in time and returns a lattice point $\boldsymbol{v} \in L_A^\perp$ satisfying

$$||\pi_{\boldsymbol{c}}(\boldsymbol{u}) - \boldsymbol{v}||^2 \leq (||\boldsymbol{b}_1||^2 + \cdots + ||\boldsymbol{b}_{n-m}||^2)/4\,, \tag{6.3}$$

where $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-m}$ is a LLL–reduced basis of $L_A^\perp$.

Step 4 : The output vector $\boldsymbol{z} = \boldsymbol{u} - \boldsymbol{v}$.

First, we justify Step 3. We show that the polytope $P(A, \boldsymbol{b})$ contains an $(n-m)$-dimensional ball $B(\boldsymbol{c}, r)$ of radius satisfying (6.2) and that the center $\boldsymbol{c}$ of the ball can be found in polynomial time. We will need the following observation.

Lemma 6.1. *If* $\boldsymbol{b} \in \{t\boldsymbol{v} + C\} \cap \mathbb{Z}^m$, $t > 0$, *then*

$$P(A, \boldsymbol{b}) \cap \{t\,\mathbf{1} + \mathbb{R}^n_{\geq 0}\} \neq \emptyset, \tag{6.4}$$

where $\mathbf{1}$ *denotes the all* 1*-vector.*

Proof. Consider the map $\tau : V_A \to \mathbb{R}^m$ defined as $\tau(\boldsymbol{h}) = A\boldsymbol{h}$. Clearly, $P(A, \boldsymbol{b}) = \{\tau^{-1}(\boldsymbol{b}) + V_A^{\perp}\} \cap \mathbb{R}^n_{\geq 0}$. Observe that $\tau^{-1}(\boldsymbol{v}_i) \in \{\boldsymbol{e}_i + L_A^{\perp}\}$, where $\boldsymbol{e}_i$ is the ith standard basis vector of $\mathbb{R}^n$. Thus for $\boldsymbol{b} \in \{t\boldsymbol{v} + C\}$ we obtain (6.4). □

Next, by Lemma 6.5.3 of Grötschel, Lovász and Schrijver [9] there exists a polynomial time algorithm that finds affinely independent vertices $\boldsymbol{y}_0, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_{n-m}$ of $P(A, \boldsymbol{b})$. On account of (6.4) and (1.1) ii), each nonzero coordinate y_i of a vertex of $P(A, \boldsymbol{b})$ satisfies

$$y_i \geq \mu(m, n)(\det(AA^T))^{1/2}. \tag{6.5}$$

Taking the barycenter $\boldsymbol{c} = \frac{1}{n-m+1}\sum_{i=0}^{n-m} \boldsymbol{y}_i$, we get a relative interior point of $P(A, \boldsymbol{b})$, i.e., all coordinates of $\boldsymbol{c}$ are positive. Thus

$$c_i \geq \frac{\mu(m, n)(\det(AA^T))^{1/2}}{n - m + 1}.$$

Clearly, the polytope $P(A, \boldsymbol{b})$ contains a ball centered at $\boldsymbol{c}$ whose radius is at least $\min_i c_i$. This implies (6.2).

It remains to justify Step 4. The output vector $\boldsymbol{z}$ clearly satisfies the condition $A\boldsymbol{z} = \boldsymbol{b}$. Thus, by the choice of the point $\boldsymbol{c}$, it is enough to show that

$$||\boldsymbol{z} - \boldsymbol{c}|| \leq \frac{\mu(m, n)(\det(AA^T))^{1/2}}{n - m + 1}. \tag{6.6}$$

Since $||\boldsymbol{z} - \boldsymbol{c}|| = ||\pi_{\boldsymbol{c}}(\boldsymbol{u}) - \boldsymbol{v}||$, by (6.3) we have

$$||\boldsymbol{z} - \boldsymbol{c}|| \leq \frac{(n - m)^{1/2}}{2} \max_{i=1,\ldots,n-m} ||\boldsymbol{b}_i||.$$

By Lemma 4.1 and the choice of μ we obtain the inequality (6.6).

6.2. **Proof of Theorem 1.2.** We will show that the above algorithm can be easily modified to satisfy the statement of Theorem 1.2. Indeed, we only need to replace $\mu(m, n) = 2^{(n-m)/2-1}p(m, n)$ by $\mu(m, n) = p(m, n)$. The proof of Step 3 remains the same and in the proof of Step 4 we need to apply Theorem 1.4 with $\rho_k^2/(\det(L))^2$ replaced by 1 instead of Lemma 4.1.

7. Case $m = 1$. Proof of Theorem 1.3

Put $\nu(n) = 2^{(n-1)/2-1} q(n)$ and suppose that

$$b \geq \nu(n) ||\boldsymbol{a}|| \sum_{i=1}^{n} a_i \,. \tag{7.1}$$

To prove Theorem 1.3 we will find in polynomial time an integer point in $P(\boldsymbol{a}^T, b)$.

Let $\boldsymbol{a}[i] = (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_N)$. We propose the following modification of the algorithm from Section 6 for solving this problem.

Steps 1 and 3 and 4 remain the same. Step 2 will be modified as follows

Step 2* : Find a point $\boldsymbol{c}$ such that $P(\boldsymbol{a}^T, b)$ contains an $(n-m)$-dimensional ball centered at $\boldsymbol{c}$ and of radius

$$r = \frac{b||\boldsymbol{a}||}{(1+\delta)\sum_{i=1}^{n} ||\boldsymbol{a}[i]|| a_i} \,. \tag{7.2}$$

The polytope $P(\boldsymbol{a}^T, b)$ is the simplex with vertices $\boldsymbol{v}_i = (b/a_i)\boldsymbol{e}_i$, $1 \leq i \leq n$, where $\boldsymbol{e}_i$ are the standard basis vectors. Hence the inner unit normal vectors of the facets of this simplex (in the hyperplane $\{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a}^T \boldsymbol{x} = 0\}$) are given by

$$\boldsymbol{u}_j := \frac{||\boldsymbol{a}||}{||\boldsymbol{a}[j]||} \left(\boldsymbol{e}_j - \frac{a_j}{||\boldsymbol{a}||^2} \boldsymbol{a} \right), \quad 1 \leq j \leq n.$$

Here $\boldsymbol{e}_j$ denotes j-th unit vector in $\mathbb{R}^n$, and the facet corresponding to $\boldsymbol{u}_j$ is the convex hull of all vertices except $(b/a_j)\,\boldsymbol{e}_j$.

Now let $\boldsymbol{c}^*$ be the center of the maximal inscribed ball in the simplex $P(\boldsymbol{a}^T, b)$, and let r^* be its radius. Since this maximal ball touches all facets of the simplex, the radius is $(n-1)$ times the ratio of volume to surface area. Standard calculations (see, e.g., Fukshansky and Robins [8, (17), (18)]) gives

$$r^* = b \, \frac{||\boldsymbol{a}||}{\sum_{i=1}^{n} ||\boldsymbol{a}[i]|| a_i} \,.$$

Furthermore, we know that for $1 \leq j \leq n$, the vector $\boldsymbol{c}^* - r^* \, \boldsymbol{u}_j$ has to lie in the facet corresponding to $\boldsymbol{u}_j$. Hence the jth coordinate of $\boldsymbol{c}^* - r^* \, \boldsymbol{u}_j$ has to be zero and so we find

$$c_j^* = r^* \frac{||\boldsymbol{a}||}{||\boldsymbol{a}[j]||} \left(1 - \frac{a_j^2}{||\boldsymbol{a}||^2} \right) = b \, \frac{||\boldsymbol{a}[j]||}{\sum_{i=1}^{n} ||\boldsymbol{a}[i]|| a_i}.$$

Note that the numbers c_j^* are in general not rational. However we can find in polynomial time a rational approximation $\boldsymbol{c}$ of the vector $\boldsymbol{c}^*$ which satisfies the condition of Step 2*.

To justify Step 4, by the choice of the point $\boldsymbol{c}$, it is enough to show that

$$||\boldsymbol{z} - \boldsymbol{c}|| \leq r \,. \tag{7.3}$$

Since $||\boldsymbol{z}-\boldsymbol{c}|| = ||\pi_{\boldsymbol{c}}(\boldsymbol{u})-\boldsymbol{v}||$, by (6.3) we have

$$||\boldsymbol{z}-\boldsymbol{c}|| \le \frac{(n-1)^{1/2}}{2} \max_{i=1,\ldots,n-1} ||\boldsymbol{b}_i||\,.$$

By Theorem 1.4, for simplicity applied with $\rho_k^2/(\det(L))^2$ replaced by 1, Lemma 4.1 and (7.1) we obtain the inequality (7.3).

References

[1] K. Aardal, A. Lenstra, *Hard equality constrained integer knapsacks*, Math. Oper. Res. **29** (2004), no. 3, 724–738.

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

[3] I. Aliev and M. Henk, *Integer knapsacks: average behavior of the Frobenius numbers*, Mathematics of Operations Research, Mathematics of Operations Research **34** (3), 2009, 698-705.

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

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

[6] J. W. S. Cassels, *An introduction to the Geometry of Numbers*, Springer-Verlag 1971.

[7] F. Eisenbrand, G. Shmonin, *Parametric integer programming in fixed dimension*, Math. Oper. Res. **33** (2008), no. 4, 839-850.

[8] L. Fukshansky, S. Robins, *Frobenius problem and the covering radius of a lattice*, Discrete Comput. Geom. **37** (2007), no. 3, 471–483.

[9] M. Grötschel, L. Lovász, A. Schrijver, *Geometric algorithms and combinatorial optimization*, Algorithms and Combinatorics: Study and Research Texts, 2. Springer-Verlag, Berlin, 1988.

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

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

[12] P. Hansen, J. Ryan, *Testing integer knapsacks for feasibility*, European Journal of Operational Research, **88**, 1996, no. 3, 578–582.

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

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

[15] M. J. Knight, *A generalization of a result of Sylvester's*, J. Number Theory **12** (1980), no. 3, 364–366.

[16] A. K. Lenstra, H. W. Lenstra Jr., L. Lovsz, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534.

[17] J. Lee, S. Onn, R. Weismantel, *Nonlinear optimization over a weighted independence system*, submitted.

[18] J. Martinet, *Perfect lattices in Euclidean spaces*, Grundlehren der Mathematischen Wissenschaften, vol. **327** (2003), Springer-Verlag, Berlin.

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

[20] J. L. Ramírez Alfonsín, *Complexity of the Frobenius problem*, Combinatorica, **16** (1996), no. 1, 143–147.

[21] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and Its Applications, 2005.

[22] W. M. Schmidt, *The distribution of sublattices of Z^m*, Monatsh. Math. **125** (1998), no. 1, 37–81.
[23] C. P. Schnorr, *Block reduced lattice bases and successive minima* Combin. Probab. Comput. **3** (1994), no. 4, 507–522.
[24] A. Schrijver, *Theory of linear and integer programming*, Wiley, Chichester, 1986.
[25] R. J. Simpson, R. Tijdeman, *Multi-dimensional versions of a theorem of Fine and Wilf and a formula of Sylvester*, Proc. Amer. Math. Soc. **131** (2003), no. 6, 1661–1671.
[26] J. Vaaler, *A geometric inequality with applications to linear forms*, Pacific J. Math. **83** (1979), no. 2, 543–553.

School of Mathematics and Wales Institute of Mathematical and Computational Sciences, Cardiff University, Senghennydd Road, Cardiff, Wales, UK
E-mail address: alievi@cf.ac.uk

Fakultät für Mathematik, Otto-von-Guericke Universität Magdeburg, Universitätsplatz 2, D-39106 Magdeburg, Germany
E-mail address: martin.henk@ovgu.de