A SHARP UPPER BOUND FOR THE LATTICE PROGRAMMING GAP

ISKANDER ALIEV

Abstract. Given a full-dimensional lattice \( \Lambda \subset \mathbb{Z}^d \) and a vector \( l \in \mathbb{Q}^d \not> 0 \), we consider the family of the lattice problems

\[
\text{Minimize } \{ l \cdot x : x \equiv r \pmod{\Lambda}, x \in \mathbb{Z}^d_\geq \} , \quad r \in \mathbb{Z}^d .
\]

(0.1)

The lattice programming gap \( \text{gap}(\Lambda, l) \) is the largest value of the minima in (0.1) as \( r \) varies over \( \mathbb{Z}^d \). We obtain a sharp upper bound for \( \text{gap}(\Lambda, l) \).

1. Introduction and statement of results

For linearly independent \( b_1, \ldots, b_k \) in \( \mathbb{R}^d \), the set \( \Lambda = \{ \sum_{i=1}^k x_i b_i, x_i \in \mathbb{Z} \} \) is a \( k \)-dimensional lattice with basis \( b_1, \ldots, b_k \) and determinant \( \det(\Lambda) = (\det[b_i \cdot b_j]_{1 \leq i,j \leq k})^{1/2} \), where \( b_i \cdot b_j \) is the standard inner product of the basis vectors \( b_i \) and \( b_j \). The points \( x, y \in \mathbb{R}^d \) are equivalent modulo \( \Lambda \), denoted as \( x \equiv y \pmod{\Lambda} \), if the difference \( x - y \) is a point of \( \Lambda \).

For a positive rational vector \( l \in \mathbb{Q}^d_\not> 0 \), a \( d \)-dimensional integer lattice \( \Lambda \subset \mathbb{Z}^d \) and an integer vector \( r \in \mathbb{Z}^d \) we consider the lattice problem

\[
\text{Minimize } \{ l \cdot x : x \equiv r \pmod{\Lambda}, x \in \mathbb{Z}^d_\geq \} .
\]

(1.1)

Let \( m(\Lambda, l, r) \) denote the value of the minimum in (1.1). We are interested in the lattice programming gap \( \text{gap}(\Lambda, l) \) of (1.1) defined as

\[
\text{gap}(\Lambda, l) = \max_{r \in \mathbb{Z}^d} m(\Lambda, l, r) .
\]

(1.2)

The lattice programming gaps were introduced and studied for sublattices of all dimensions in \( \mathbb{Z}^d \) by Hošten and Sturmfels [14]. Computing \( \text{gap}(\Lambda, l) \) is known to be NP-hard when \( d \) is a part of input (see [1]). For fixed \( d \) the value of \( \text{gap}(\Lambda, l) \) can be computed in polynomial time (see Section 3 in [14], [10] and [9]).

The lower and upper bounds for \( \text{gap}(\Lambda, l) \) in terms of the parameters \( \Lambda, l \) were given in [1]. The lower bound is known to be sharp. In this paper we improve on the upper bound and show that the obtained bound is attained for parameters \( \Lambda, l \) that satisfy certain arithmetic properties.

Date: January 21, 2017.
Let $|\cdot|$ denote the Euclidean norm and let $\gamma_d$ be the $d$-dimensional Hermite constant (see e.g. Section IX.7 in [7]). In [1] it was shown that for any $\mathbf{l} \in \mathbb{Q}_d^d$, $d \geq 2$, and any $d$-dimensional lattice $\Lambda \subset \mathbb{Z}^d$

\begin{equation}
\text{gap}(\Lambda, \mathbf{l}) \leq \frac{d\gamma_d^{d/2}}{2} \det(\Lambda) \left(\sum_{i=1}^{d} l_i + |\mathbf{l}|\right) - \sum_{i=1}^{d} l_i. \tag{1.3}
\end{equation}

The bound (1.3) was obtained using a geometric argument based on estimating the covering radius of a simplex, associated with the vector $\mathbf{l}$, via the covering radius of the unit $d$-dimensional ball. Note that by a result of Blichfeldt (see e.g. §38 in Chapter 6 of [13]) $\gamma_d \leq 2^d (\frac{d+2}{\sigma_d})^{2/d}$, where $\sigma_d$ is the volume of the unit $d$-ball; thus $\gamma_d = O(d)$. It follows from results in [2, Section 6] that the order $\text{gap}(\Lambda, \mathbf{l}) = O_d, \mathbf{l}(\det(\Lambda))$, where the constant depends on $d$ and $\mathbf{l}$, cannot be improved.

Let $\|\cdot\|_\infty$ denote the maximum norm. In this paper we use coverings that are based on the arithmetic properties of the integer lattices and improve the bound (1.3) as follows.

**Theorem 1.1.** For any $\mathbf{l} \in \mathbb{Q}_d^d$, $d \geq 2$, and any $d$-dimensional lattice $\Lambda \subset \mathbb{Z}^d$

\begin{equation}
\text{gap}(\Lambda, \mathbf{l}) \leq (\det(\Lambda) - 1)\|\mathbf{l}\|_\infty. \tag{1.4}
\end{equation}

Using a link between the lattice programming gaps and the Frobenius numbers we also show that the bound (1.4) is sharp.

**Theorem 1.2.** For $d \geq 2$ and any positive integer $D$ there exist $\mathbf{l} \in \mathbb{Z}_d^d$ and a lattice $\Lambda \subset \mathbb{Z}^d$ of determinant $\det(\Lambda) = D$ such that

\begin{equation}
\text{gap}(\Lambda, \mathbf{l}) = (D - 1)\|\mathbf{l}\|_\infty. \tag{1.5}
\end{equation}

2. Coverings of $\mathbb{R}^d$ and lattice programming gaps

Recall that the Minkowski sum $X + Y$ of the sets $X, Y \subset \mathbb{R}^d$ consists of all points $\mathbf{x} + \mathbf{y}$ with $\mathbf{x} \in X$ and $\mathbf{y} \in Y$. For a set $K \subset \mathbb{R}^d$ and a lattice $\Lambda \subset \mathbb{R}^d$, the Minkowski sum $K + \Lambda$ is a packing if the translates of $K$ are mutually disjoint, a covering if $\mathbb{R}^d = K + \Lambda$ and a tiling if it is both packing and covering, simultaneously.

Let $\Lambda$ be a lattice in $\mathbb{R}^d$ with basis $\mathbf{b}_1, \ldots, \mathbf{b}_d$. Let $\Lambda_i$ denote the lattice generated by the first $i$ basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_i$ and let $\pi_i : \mathbb{R}^d \to \text{span}_\mathbb{R}(\Lambda_{i-1})^\perp$ be the orthogonal projection onto the subspace $\text{span}_\mathbb{R}(\Lambda_{i-1})^\perp$ orthogonal to $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$.

The vectors $\hat{\mathbf{b}}_i = \pi_i(\mathbf{b}_i)$ can be obtained using the Gram-Schmidt orthogonalisation of $\mathbf{b}_1, \ldots, \mathbf{b}_d$:

\begin{align*}
\hat{\mathbf{b}}_1 &= \mathbf{b}_1, \\
\hat{\mathbf{b}}_i &= \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \hat{\mathbf{b}}_j, \quad j = 2, \ldots, d,
\end{align*}
where \( \mu_{i,j} = (b_i \cdot \hat{b}_j) / |\hat{b}_j|^2 \).

Define the box \( B = B(b_1, \ldots, b_d) \) as

\[
B = [0, \hat{b}_1) \times \cdots \times [0, \hat{b}_d).
\]

We will need the following well-known and useful observation.

**Lemma 2.1.** \( B + \Lambda \) is a tiling of \( \mathbb{R}^d \).

Tilings of \( \mathbb{R}^d \) with lattice translates of \( B \) were implicitly used already in the classical Babai's nearest lattice point algorithm (see [3] and Theorem 5.3.26 in [11]) and in the work of Lagarias, Lenstra and Schorr on Korkin-Zolotarev bases (see the proof of Theorem 2.6 in [16]). Lemma 2.1 was also explicitly stated (with translated \( B \)) by Cai and Nerurkar (see [6], Lemma 2). A proof of this result can be obtained by modifying the proof of Theorem 5.3.26 in [11]. We also remark that for the purposes of this paper we only need the coverings of \( \mathbb{R}^d \) by the lattice translates of the closure of \( B \).

In what follows, \( K^d \) will denote the space of all \( d \)-dimensional convex bodies, i.e., closed bounded convex sets with non-empty interior in the \( d \)-dimensional Euclidean space \( \mathbb{R}^d \). Let also \( \mathcal{L}^d \) denote the set of all \( d \)-dimensional lattices in \( \mathbb{R}^d \). For \( K \in K^d \) and \( \Lambda \in \mathcal{L}^d \) the covering radius of \( K \) with respect to \( \Lambda \) is the smallest positive number \( \rho \) such that any point \( x \in \mathbb{R}^d \) is covered by \( \rho K + \Lambda \), that is

\[
\rho(K, \Lambda) = \min \{ \rho > 0 : \mathbb{R}^d = \rho K + \Lambda \}.
\]

For further information on covering radii in the context of the geometry of numbers see e.g. Gruber [12] and Gruber and Lekkerkerker [13].

Given \( l \in \mathbb{Q}^d_{>0} \), consider the simplex \( \Delta_l = \{ x \in \mathbb{R}^d_{>0} : l \cdot x \leq 1 \} \). As it was shown in [1], the lattice programming gap can be expressed via the covering radius of \( \Delta_l \) with respect to \( \Lambda \):

\[
\text{gap}(\Lambda, l) = \rho(\Delta_l, \Lambda) - \sum_{i=1}^{d} l_i.
\]

**3. Proof of Theorem 1.1**

We will obtain an upper bound for \( \text{gap}(\Lambda, l) \) in terms of \( l \) and certain parameters of the lattice \( \Lambda \) that will imply (1.4).

By Theorem I (A) and Corollary 1 in Chapter I of Cassels [7], there exists a basis \( b_1, \ldots, b_d \) of the lattice \( \Lambda \) of the form

\[
b_1 = v_{11} e_1, \quad b_2 = v_{21} e_1 + v_{22} e_2, \quad \vdots \quad b_d = v_{d1} e_1 + \cdots + v_{dd} e_d,
\]

(3.1)
where $e_i$ are the standard basis vectors of $\mathbb{Z}^d$, the coefficients $v_{ij}$ are integers, $v_{ii} > 0$ and $0 \leq v_{ij} < v_{jj}$.

**Lemma 3.1.** We have

$$\text{gap}(\Lambda, l) \leq l_1 v_{11} + \cdots + l_d v_{dd} - \sum_{i=1}^d l_i. \quad (3.2)$$

**Proof.** Note that the Gram-Schmidt orthogonalisation of $b_1, \ldots, b_d$ has the form

$$\tilde{b}_1 = v_{11} e_1, \tilde{b}_2 = v_{22} e_2, \ldots, \tilde{b}_d = v_{dd} e_d. \quad (3.3)$$

Hence, the box $B = B(b_1, \ldots, b_d)$ can be written as

$$B = [0, v_{11}) \times \cdots \times [0, v_{dd}).$$

By Lemma 2.1, $B + \Lambda$ is a tiling of $\mathbb{R}^d$. In particular, $B + \Lambda$ covers $\mathbb{R}^d$.

Since $B \subset (l_1 v_{11} + \cdots + l_d v_{dd}) \Delta_l$, we have

$$\rho(\Delta_l, \Lambda) \leq l_1 v_{11} + \cdots + l_d v_{dd}. \quad (3.2)$$

By (2.1), the bound (3.2) holds. \[\square\]

Consider the simplex $\Delta = \text{conv} \{1, p_1, \ldots, p_d\}$, where $\text{conv} \{\cdot\}$ denotes the convex hull, $1$ is the all-one vector and

$$p_1 = (\det(\Lambda), 1, \ldots, 1)^t, \quad p_2 = (1, \det(\Lambda), \ldots, 1)^t, \quad \vdots \quad p_d = (1, 1, \ldots, \det(\Lambda))^t.$$  

It is easy to see that

$$\{x \in \mathbb{R}_{\geq 1}^d : x_1 \cdots x_d = \det(\Lambda)\} \subset \Delta. \quad (3.4)$$

Since $\Delta$ is a convex bounded polyhedron, the maximum of the linear function $l \cdot x$ over $\Delta$ is attained at one of its vertices $1, p_1, \ldots, p_d$. Therefore

$$\max\{l \cdot x : x \in \Delta\} = (\det(\Lambda) - 1)\|l\|_\infty + \sum_{i=1}^d l_i. \quad (3.5)$$

Since $v_{11} \cdots v_{dd} = \det(\Lambda)$, we obtain by (3.4) and (3.5)

$$l_1 v_{11} + \cdots + l_d v_{dd} \leq (\det(\Lambda) - 1)\|l\|_\infty + \sum_{i=1}^d l_i. \quad (3.6)$$

By (3.2) and (3.6) we obtain (1.4).
4. Proof of Theorem 1.2

In this section we will use classical results of Brauer [4] and Brauer and Seelbinder [5] to prove Theorem 1.2. In the course of the proof we also show that the bound (3.2) in Lemma 3.1 is sharp.

Let \( \mathbf{a} = (a_1, \ldots, a_{d+1})^t \in \mathbb{Z}_{>0}^{d+1} \) be a positive integer vector with coprime entries, that is \( \gcd(a_1, \ldots, a_{d+1}) = 1 \). Consider the lattice \( \Lambda = \Lambda(\mathbf{a}) \) defined as

\[
\Lambda = \{ \mathbf{x} \in \mathbb{Z}^d : a_2 x_1 + \cdots + a_{d+1} x_d \equiv 0 \pmod{a_1} \}.
\]

Note that \( \det(\Lambda) = a_1 \) (see e.g. Corollary 3.2.20 in [8]).

Let \( f_1 = a_1, f_2 = \gcd(a_1, a_2), \ldots, f_{d+1} = \gcd(a_1, a_2, \ldots, a_{d+1}) = 1 \).

Consider the basis \( \mathbf{b}_1, \ldots, \mathbf{b}_d \) of the lattice \( \Lambda \) given by (3.1). The next lemma shows that the Gram-Schmidt box \( B(\mathbf{b}_1, \ldots, \mathbf{b}_d) \) is entirely determined by the parameters \( f_i \).

**Lemma 4.1.** The box \( B = B(\mathbf{b}_1, \ldots, \mathbf{b}_d) \) has the form

\[
B = \left[ 0, \frac{f_1}{f_2} \right] \times \left[ 0, \frac{f_2}{f_3} \right] \times \cdots \times \left[ 0, \frac{f_d}{f_{d+1}} \right].
\]

**Proof.** By the definition of the box \( B \) and (3.3), it is enough to show that

\[
(4.1) \quad v_{11} = \frac{f_1}{f_2}, v_{22} = \frac{f_2}{f_3}, \ldots, v_{dd} = \frac{f_d}{f_{d+1}}.
\]

Recall that \( \Lambda_i \) denotes the sublattice of \( \Lambda \) generated by the first \( i \) basis vectors \( \mathbf{b}_1, \ldots, \mathbf{b}_i \). We can write \( \Lambda_i \) in the form

\[
\Lambda_i = \left\{ (x_1, \ldots, x_i, 0, \ldots, 0) \in \mathbb{Z}^d : \frac{a_2}{f_{i+1}} x_1 + \cdots + \frac{a_{i+1}}{f_{i+1}} x_i \equiv 0 \pmod{\frac{a_1}{f_{i+1}}} \right\}.
\]

Hence, \( \det(\Lambda_i) = a_1/f_{i+1} \). On the other hand, (3.1) implies that \( \det(\Lambda_i) = v_{11} v_{22} \cdots v_{ii} \). Since \( \det(\Lambda) = v_{11} v_{22} \cdots v_{dd} = a_1 \), we have \( f_{i+1} = v_{i+1} v_{i+2} \cdots v_{dd} \) for \( i \leq d-1 \), which immediately implies (4.1).

\[\square\]

The **Frobenius number** \( F(\mathbf{a}) \) associated with the integer vector \( \mathbf{a} \) is the largest integer number which cannot be represented as a nonnegative integer combination of the \( a_i \)'s. The problem of finding \( F(\mathbf{a}) \) has a long history and is traditionally referred to as the **Frobenius problem**, see e. g. [18].

Set \( \mathbf{l}(\mathbf{a}) = (a_2, \ldots, a_{d+1})^t \). It is known (see e.g. proof of Theorem 1.1 in [1] and Section 5.1 in [17]) that

\[
(4.2) \quad \text{gap}(\Lambda(\mathbf{a}), \mathbf{l}(\mathbf{a})) = F(\mathbf{a}) + a_1.
\]

Note also that, in this special case, (2.1) follows from Theorem 2.5 of Kannan [15].
By Lemma 4.1, the bound \(3.2\) for \(\text{gap}(\Lambda(\mathbf{a}), l(\mathbf{a}))\) given by Lemma 3.1 can be obtained by replacing \(F(\mathbf{a})\) on the right hand side of \(4.2\) by the estimate

\[
F(\mathbf{a}) \leq C(\mathbf{a}) := a_2 \frac{f_1}{f_2} + \cdots + a_{d+1} \frac{f_d}{f_{d+1}} - \sum_{i=1}^{d+1} a_i
\]

given in Brauer [4]. It should be remarked here that Brauer [4] rather worked with the quantity \(F^+(\mathbf{a}) = F(\mathbf{a}) + \sum_{i=1}^{d+1} a_i\), the largest number which cannot be represented as a *positive* integer combination of the \(a_i\)'s. Brauer [4] and, subsequently, Brauer and Seelbinder [5] proved that the bound \(4.3\) is sharp and obtained the following necessary and sufficient condition for the equality \(F(\mathbf{a}) = C(\mathbf{a})\).

**Lemma 4.2** (see Theorem 5 in [4] and Theorem 1 in [5]). Let \(\mathbf{a} = (a_1, \ldots, a_{d+1})^t \in \mathbb{Z}_{>0}^{d+1}, \ d \geq 2, \) with \(\gcd(a_1, \ldots, a_{d+1}) = 1\). Then \(F(\mathbf{a}) = C(\mathbf{a})\) if and only if for \(m = 3, 4, \ldots, d+1\) the integer \(a_m/f_m\) is representable in the form

\[
a_m/f_m = \sum_{i=1}^{m-1} \frac{a_i}{f_{m-1}} y_{mi}
\]

with integers \(y_{mi} \geq 0\).

For \(s = 2, 3, \ldots, d+1,\) let

\[
\mathbf{a}^{(s)} = \left(\frac{a_1}{f_s}, \ldots, \frac{a_s}{f_s}\right)^t.
\]

The condition \(4.4\) is satisfied, in particular, if

\[
a_m/f_m > F(\mathbf{a}^{(m-1)}).
\]

Hence the bound \(3.2\) in Lemma 3.1 is sharp and the vectors \(\mathbf{a}\) satisfying \(4.4\) can be easily constructed. To show that \((1.4)\) is sharp, we will use a special case of Lemma 4.2, that regards the optimality of the Schur’s upper bound for the Frobenius number (see [4]). Suppose that a vector \(\mathbf{a} \in \mathbb{Z}_{>0}^{d+1} \) with coprime entries satisfies the following conditions:

\[
(i) \quad D = a_1 \leq a_2 \leq \cdots \leq a_{d+1},
(ii) \quad a_2 \equiv a_3 \equiv \cdots \equiv a_r mod a_1 \) for some index \(r \geq 3, \)
(iii) \quad a_{r+1} = a_{r+2} = \cdots = a_{d+1}.
\]

By Theorem 3 in [4] (cf. Theorem 4 ibid.) conditions \(4.5\) imply that \(F(\mathbf{a}) = a_1 a_{d+1} - a_1 - a_{d+1}\). Hence \(\text{gap}(\Lambda(\mathbf{a}), l(\mathbf{a})) = (a_1 - 1)a_{d+1} = (D - 1)||l||_{\infty}.\) The theorem is proved.
LATTICE PROGRAMMING GAP

References


Mathematics Institute, Cardiff University, UK
E-mail address: alievi@cardiff.ac.uk