

Reprint from

ISSN 2220-5438

Moscow Journal

Moscow Journal

of Combinatorics and Number Theory

of Combinatorics and Number Theory

Volume 6 • Issue 2-3

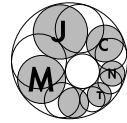
2016



URSS

Volume 6 • Issue 2-3

2016



A sharp upper bound for the lattice programming gap

Iskander Aliev (Cardiff)

Abstract: Given a full-dimensional lattice $\Lambda \subset \mathbb{Z}^d$ and a vector $\mathbf{l} \in \mathbb{Q}_{>0}^d$, we consider the family of the lattice problems

$$\text{Minimize } \{\mathbf{l} \cdot \mathbf{x} : \mathbf{x} \equiv \mathbf{r} \pmod{\Lambda}, \mathbf{x} \in \mathbb{Z}_{\geq 0}^d\}, \quad \mathbf{r} \in \mathbb{Z}^d.$$

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

Keywords: group relaxations; integer programming gap; lattices; covering radius; Frobenius numbers

AMS Subject Classification: 90C10; 11H31; 11D07

Received: 20.05.2016; **revised:** 02.08.2016

1. Introduction and statement of results

For linearly independent $\mathbf{b}_1, \dots, \mathbf{b}_k$ in \mathbb{R}^d , the set $\Lambda = \left\{ \sum_{i=1}^k x_i \mathbf{b}_i, x_i \in \mathbb{Z} \right\}$ is a k -dimensional *lattice* with *basis* $\mathbf{b}_1, \dots, \mathbf{b}_k$ and *determinant* $\det(\Lambda) = (\det[\mathbf{b}_i \cdot \mathbf{b}_j]_{1 \leq i, j \leq k})^{1/2}$, where $\mathbf{b}_i \cdot \mathbf{b}_j$ is the standard inner product of the basis vectors \mathbf{b}_i and \mathbf{b}_j . The points $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$ are *equivalent modulo* Λ , denoted as $\mathbf{x} \equiv \mathbf{y} \pmod{\Lambda}$, if the difference $\mathbf{x} - \mathbf{y}$ is a point of Λ .

For a positive rational vector $\mathbf{l} \in \mathbb{Q}_{>0}^d$, a d -dimensional integer lattice $\Lambda \subset \mathbb{Z}^d$ and an integer vector $\mathbf{r} \in \mathbb{Z}^d$ we consider the lattice problem

$$\text{Minimize } \{\mathbf{l} \cdot \mathbf{x} : \mathbf{x} \equiv \mathbf{r} \pmod{\Lambda}, \mathbf{x} \in \mathbb{Z}_{\geq 0}^d\}. \quad (1.1)$$

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

$$\text{gap}(\Lambda, \mathbf{l}) = \max_{\mathbf{r} \in \mathbb{Z}^d} m(\Lambda, \mathbf{l}, \mathbf{r}). \quad (1.2)$$

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

The lower and upper bounds for $\text{gap}(\Lambda, \mathbf{l})$ in terms of the parameters Λ, \mathbf{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 Λ, \mathbf{l} that satisfy certain arithmetic properties.

Let $|\cdot|$ denote the Euclidean norm and let γ_d be the d -dimensional Hermite constant (see e. g. Section IX.7 in [7]). In [1] it was shown that for any $\mathbf{l} \in \mathbb{Q}_{>0}^d$, $d \geq 2$, and any d -dimensional lattice $\Lambda \subset \mathbb{Z}^d$

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

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]) $\gamma_d \leq 2 \left(\frac{d+2}{\sigma_d}\right)^{2/d}$, where σ_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 $\mathbf{l} \in \mathbb{Q}_{>0}^d$, $d \geq 2$, and any d -dimensional lattice $\Lambda \subset \mathbb{Z}^d$

$$\text{gap}(\Lambda, \mathbf{l}) \leq (\det(\Lambda) - 1) \|\mathbf{l}\|_\infty. \quad (1.4)$$

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 $\mathbf{l} \in \mathbb{Z}_{>0}^d$ and a lattice $\Lambda \subset \mathbb{Z}^d$ of determinant $\det(\Lambda) = D$ such that

$$\text{gap}(\Lambda, \mathbf{l}) = (D-1) \|\mathbf{l}\|_\infty. \quad (1.5)$$

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

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

$$\begin{aligned} \widehat{\mathbf{b}}_1 &= \mathbf{b}_1, \\ \widehat{\mathbf{b}}_i &= \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \widehat{\mathbf{b}}_j, \quad j = 2, \dots, d, \end{aligned}$$

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

Define the box $B = B(\mathbf{b}_1, \dots, \mathbf{b}_d)$ as

$$B = [0, \widehat{\mathbf{b}}_1) \times \dots \times [0, \widehat{\mathbf{b}}_d).$$

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, \mathcal{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 $K \in \mathcal{K}^d$ and $\Lambda \in \mathcal{L}^d$ the *covering radius* of K with respect to Λ is the smallest positive number ρ such that any point $\mathbf{x} \in \mathbb{R}^d$ 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 $\mathbf{l} \in \mathbb{Q}_{>0}^d$, consider the simplex $\Delta_{\mathbf{l}} = \{\mathbf{x} \in \mathbb{R}_{\geq 0}^d : \mathbf{l} \cdot \mathbf{x} \leq 1\}$. As it was shown in [1], the lattice programming gap can be expressed via the covering radius of $\Delta_{\mathbf{l}}$ with respect to Λ :

$$\text{gap}(\Lambda, \mathbf{l}) = \rho(\Delta_{\mathbf{l}}, \Lambda) - \sum_{i=1}^d l_i. \quad (2.1)$$

3. Proof of Theorem 1.1

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

By Theorem I (A) and Corollary 1 in Chapter I of Cassels [7], there exists a basis $\mathbf{b}_1, \dots, \mathbf{b}_d$ of the lattice Λ of the form

$$\begin{aligned} \mathbf{b}_1 &= v_{11}\mathbf{e}_1, \\ \mathbf{b}_2 &= v_{21}\mathbf{e}_1 + v_{22}\mathbf{e}_2, \\ &\vdots \\ \mathbf{b}_d &= v_{d1}\mathbf{e}_1 + \dots + v_{dd}\mathbf{e}_d, \end{aligned} \quad (3.1)$$

where \mathbf{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*

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

PROOF. Note that the Gram—Schmidt orthogonalisation of $\mathbf{b}_1, \dots, \mathbf{b}_d$ has the form

$$\widehat{\mathbf{b}}_1 = v_{11} \mathbf{e}_1, \widehat{\mathbf{b}}_2 = v_{22} \mathbf{e}_2, \dots, \widehat{\mathbf{b}}_d = v_{dd} \mathbf{e}_d. \quad (3.3)$$

Hence, the box $B = B(\mathbf{b}_1, \dots, \mathbf{b}_d)$ 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 $B \subset (l_1 v_{11} + \cdots + l_d v_{dd}) \Delta_{\mathbf{l}}$, we have

$$\rho(\Delta_{\mathbf{l}}, \Lambda) \leq l_1 v_{11} + \cdots + l_d v_{dd}.$$

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

Consider the simplex $\Delta = \text{conv} \{\mathbf{1}, \mathbf{p}_1, \dots, \mathbf{p}_d\}$, where $\text{conv} \{\cdot\}$ denotes the convex hull, $\mathbf{1}$ is the all-one vector and

$$\begin{aligned} \mathbf{p}_1 &= (\det(\Lambda), 1, \dots, 1)^t, \\ \mathbf{p}_2 &= (1, \det(\Lambda), \dots, 1)^t, \\ &\vdots \\ \mathbf{p}_d &= (1, 1, \dots, \det(\Lambda))^t. \end{aligned}$$

It is easy to see that

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

Since Δ is a convex bounded polyhedron, the maximum of the linear function $\mathbf{l} \cdot \mathbf{x}$ over Δ is attained at one of its vertices $\mathbf{1}, \mathbf{p}_1, \dots, \mathbf{p}_d$. Therefore

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

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

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

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 $\mathbf{a} = (a_1, \dots, a_{d+1})^t \in \mathbb{Z}_{>0}^{d+1}$ be a positive integer vector with coprime entries, that is $\gcd(a_1, \dots, a_{d+1}) = 1$. 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

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

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

LEMMA 4.1. *The box $B = B(\mathbf{b}_1, \dots, \mathbf{b}_d)$ 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

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

Recall that Λ_i denotes the sublattice of Λ generated by the first i basis vectors $\mathbf{b}_1, \dots, \mathbf{b}_i$. We can write Λ_i in the form

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

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

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

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 $\text{gap}(\Lambda(\mathbf{a}), \mathbf{l}(\mathbf{a}))$ given by Lemma 3.1 can be obtained by replacing $F(\mathbf{a})$ on the right hand side of (4.2) by the estimate

$$F(\mathbf{a}) \leq C(\mathbf{a}) := a_2 \frac{f_1}{f_2} + \dots + a_{d+1} \frac{f_d}{f_{d+1}} - \sum_{i=1}^{d+1} a_i \quad (4.3)$$

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 $\mathbf{a} = (a_1, \dots, a_{d+1})^t \in \mathbb{Z}_{>0}^{d+1}$, $d \geq 2$, with $\gcd(a_1, \dots, a_{d+1}) = 1$. Then $F(\mathbf{a}) = C(\mathbf{a})$ if and only if for $m = 3, 4, \dots, d+1$ the integer a_m/f_m is representable in the form

$$\frac{a_m}{f_m} = \sum_{i=1}^{m-1} \frac{a_i}{f_{m-1}} y_{mi} \quad (4.4)$$

with integers $y_{mi} \geq 0$.

For $s = 2, 3, \dots, d+1$, let

$$\mathbf{a}^{(s)} = \left(\frac{a_1}{f_s}, \dots, \frac{a_s}{f_s} \right)^t.$$

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

$$\frac{a_m}{f_m} > F(\mathbf{a}^{(m-1)}).$$

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) $D = a_1 \leq a_2 \leq \dots \leq a_{d+1}$,
 - (ii) $a_2 \equiv a_3 \equiv \dots \equiv a_r \pmod{a_1}$ for some index $r \geq 3$,
 - (iii) $a_{r+1} = a_{r+2} = \dots = a_{d+1}$.
- (4.5)

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 $\text{gap}(\Lambda(\mathbf{a}), \mathbf{l}(\mathbf{a})) = (a_1 - 1)a_{d+1} = (D - 1)\|\mathbf{l}\|_\infty$. The theorem is proved.

Bibliography

1. **I. Aliev**, *On the lattice programming gap of the group problems*, Oper. Res. Lett., **43** (2015), 199–202.
2. **I. Aliev, M. Henk**, *Feasibility of integer knapsacks*, SIAM J. Opt., **20** (2010), 2978–2993.

3. **L. Babai**, *On Lovász' lattice reduction and the nearest lattice point problem*, *Combinatorica*, **6** (1986), 1–13.
4. **A. Brauer**, *On a problem of partitions*, *American Journal of Mathematics*, **64** (1942), 299–312.
5. **A. Brauer, B. M. Seelbinder**, *On a problem of partitions II*, *American Journal of Mathematics*, **76** (1954), 343–346.
6. **J.-Y. Cai, A. Nerurkar**, *An improved worst-case to average-case connection for lattice problems*, *Proc. 38th IEEE Symp. on Found. of Comp. Science*, (1997), 468–477.
7. **J. W. S. Cassels**, *An introduction to the geometry of numbers*, Springer-Verlag, 1971.
8. **C. Dwork**, *Lattices and their applications to cryptography*, *Lecture Notes*, Stanford University, 1998.
9. **F. Eisenbrand, N. Hähnle, D. Pálvölgyi and G. Shmonin**, *Testing additive integrality gaps*, *Math. Program. A*, **141** (2013), 257–271.
10. **F. Eisenbrand, G. Shmonin**, *Parametric integer programming in fixed dimension*, *Math. Oper. Res.*, **33** (2008), 839–850.
11. **M. Grötschel, L. Lovász and A. Schrijver**, *Geometric algorithms and combinatorial optimization*, *Algorithms and Combinatorics vol. 2*, Springer-Verlag, Berlin, 1988.
12. **P. M. Gruber**, *Convex and discrete geometry*, Springer, Berlin, 2007.
13. **P. M. Gruber, C. G. Lekkerkerker**, *Geometry of numbers*, North-Holland, Amsterdam 1987.
14. **S. Hoşten, B. Sturmfels**, *Computing the integer programming gap*, *Combinatorica*, **27** (2007), 367–382.
15. **R. Kannan**, *Lattice translates of a polytope and the Frobenius problem*, *Combinatorica*, **12** (1992), 161–177.
16. **J. C. Lagarias, H. W. Lenstra, Jr., C. P. Schorr**, *Korkin–Zolotarev bases and successive minima of a lattice and its reciprocal lattice*, *Combinatorica*, **10** (1990), 333–348.
17. **J. Marklof, A. Strömbergsson**, *Diameters of random circulant graphs*, *Combinatorica*, **33** (2013), 429–466.
18. **J. L. Ramírez Alfonsín**, *The Diophantine Frobenius problem*, *Oxford Lecture Series in Mathematics and its Applications* 30, 2005.

ISKANDER ALIEV

Mathematics Institute,
Cardiff University
Senghennydd Road
Cardiff
CF24 4AG, UK
alievi@cardiff.ac.uk