COMBINATORICA
Akadémiai Kiadó — Springer-Verlag

COMBINATORICA 8 (1) (1988) 75—81

DUAL VECTORS AND LOWER BOUNDS FOR THE NEAREST LATTICE POINT PROBLEM

J. HASTAD*

Received November 10, 1986
Revised April 14, 1987

We prove that given a point $\vec{z}$ outside a given lattice L then there is a dual vector which gives a fairly good estimate for how far from the lattice the vector is. To be more precise, there is a set of translated hyperplanes H_i such that $L \subset \cup_i H_i$ and $d(\vec{z}, \cup_i H_i) \geq (6n^2+1)^{-1} d(\vec{z}, L)$.

1. Introduction

Let $\{\theta\}$ denote the fractional part of a real number θ defined in such a way that $|\{\theta\}|$ is the distance to the closest integer. A classical theorem by Kronecker says that if θ is an irrational number and x any real number, then for every $\varepsilon > 0$ there is an integer a such that $|\{a\theta - x\}| \leq \varepsilon$. Furthermore it is possible to estimate the size of the smallest a satisfying the inequality in terms of ε an how well θ can be approximated by rational numbers.

Khinchin [5] studied the following generalization of the problem. Given real numbers $(\theta_{ij})_{j,i=1}^{m,n}$, $(\alpha_j)_{j=1}^{m}$ and a positive number ε, when is it possible to solve $\left|\left\{\sum_{i=1}^{n} \theta_{ij} a_i - \alpha_j\right\}\right| \leq \varepsilon$, $j = 1, \ldots, m$ with integers a_i. If there is a solution for any $\varepsilon > 0$, then if c_j are integers such that $\left\{\sum_{j=1}^{m} c_j \theta_{ij}\right\} = 0$ for all i then $\sum_{j=1}^{m} c_j \alpha_j$ must necessarily be an integer. When this condition is satisfied Khinchin bounds the size of the numbers a_i in terms of ε using the two quantities $\max_i \left|\left\{\sum_{j=1}^{m} c_j \theta_{ij}\right\}\right|$ and $\left|\left\{\sum_{j=1}^{m} c_j \alpha_j\right\}\right|$. This question and related questions can be phrased very nicely using the concept of a lattice and its dual.

A lattice is defined to be a set of vectors in $\mathbf{R}^n$ defined as $\left\{\vec{y} \mid \vec{y} = \sum_{i=1}^{k} a_i \vec{b}_i,\ a_i \in \mathbf{Z}\right\}$ where the vectors $\vec{b}_i$ are linearly independent over $\mathbf{R}$. We will denote a typical lattice by L and $(\vec{b}_i)_{i=1}^{k}$ is called a basis for the lattice. The dual lattice L^* is defined to be the set of vectors in the linear span of L which have an integer inner product with

* Supported by an IBM fellowship.
AMS subject classification (1980): 11 H 60, 11 Y 65, 68 R 99.

all elements of L. L^* is also a lattice and to every basis $(\vec{b}_i)_{i=1}^k$ of L there is a dual basis $(\vec{b}_i^*)_{i=1}^k$ of L^* satisfying $(\vec{b}_i, \vec{b}_j^*)=\delta_{ij}$. Here $\delta_{ij}=1$ if $i=j$ and 0 otherwise.

The idea to use lattices is the following. Suppose we are given a lattice L and a point $\vec{x}$ which is not in L. Suppose further that $\vec{v}$ is a vector in L^* such that $(\vec{x}, \vec{v})$ is not an integer. This will give a lower bound for the distance from $\vec{x}$ to L as follows. We know that for any vector $\vec{y}\in L$, $(\vec{y}, \vec{v})$ is an integer. Hence $|(\vec{x}-\vec{y}, \vec{v})| \geqq \geqq |\{(\vec{v}, \vec{x})\}|$ for any $\vec{y}\in L$. From this it follows that $d(\vec{x}, L)\geqq |\{(\vec{x}, \vec{v})\}|/\|\vec{v}\|$. Khinchin's result follows from establishing a weaker converse of the above inequality, namely $\max_{\vec{v}\in L^*} |\{(\vec{x}, \vec{v})\}|/\|\vec{v}\| \geqq c_n d(\vec{x}, L)$. To see why this is the case consider the lattice L_t, defined by the following basis.

$$\vec{b}_1 = \left(\theta_{11}, \theta_{12}, \theta_{13}, \ldots, \theta_{1m}, \frac{1}{t}, 0, 0, \ldots, 0\right)$$

$$\vec{b}_2 = \left(\theta_{21}, \theta_{22}, \theta_{23}, \ldots, \theta_{2m}, 0, \frac{1}{t}, 0, \ldots, 0\right)$$

$$\vec{b}_3 = \left(\theta_{31}, \theta_{32}, \theta_{33}, \ldots, \theta_{3m}, 0, 0, \frac{1}{t}, \ldots, 0\right)$$

$$\vec{b}_n = \left(\theta_{n1}, \theta_{n2}, \theta_{n3}, \ldots, \theta_{nm}, 0, 0, 0, \ldots, \frac{1}{t}\right)$$

$$\vec{b}_{n+i} = \vec{e}_i, 1 \leqq i \leqq m$$

where t is a parameter which should be thought of as a large number. We can view the approximation problem as finding a vector $\vec{y}\in L_t$ which is close to $\vec{\alpha}= =(\alpha_1, \alpha_2, \ldots, \alpha_m, 0, \ldots, 0)$. The dual lattice of L_t has basis:

$$\begin{aligned}
\vec{b}_1^* &= (0, 0, 0, \ldots, 0, t, 0, 0, \ldots, 0)\\
\vec{b}_2^* &= (0, 0, 0, \ldots, 0, 0, t, 0, \ldots, 0)\\
\vec{b}_3^* &= (0, 0, 0, \ldots, 0, 0, 0, t, \ldots, 0)\\
&\vdots\\
\vec{b}_n^* &= (0, 0, 0, \ldots, 0, 0, 0, 0, \ldots, t)\\
\vec{b}_{n+1}^* &= (1, 0, 0, \ldots, 0, -t\theta_{11}, -t\theta_{21}, -t\theta_{31}, \ldots, -t\theta_{n1})\\
\vec{b}_{n+2}^* &= (0, 1, 0, \ldots, 0, -t\theta_{12}, -t\theta_{22}, -t\theta_{32}, \ldots, -t\theta_{n2})\\
\vec{b}_{n+3}^* &= (0, 0, 1, \ldots, 0, -t\theta_{13}, -t\theta_{23}, -t\theta_{33}, \ldots, -t\theta_{n3})\\
&\vdots\\
\vec{b}_{n+m}^* &= (0, 0, 0, \ldots, 1, -t\theta_{1m}, -t\theta_{2m}, -t\theta_{3m}, \ldots, -t\theta_{nm}).
\end{aligned}$$

Thus for a vector $\vec{v}=\sum_{j=1}^{n+m} c_j \vec{b}_j^*$ we have that $(\vec{v}, \vec{\alpha})=\sum_{j=1}^{m} c_{j+n}\alpha_j$ and clearly $\|\vec{v}\| \geqq t\left(\sum_{i=1}^{n}\left\{\sum_{j=1}^{m} c_{j+n}\theta_{ij}\right\}^2\right)^{1/2}$. The results by Khinchin now follows from $\max_{\vec{v}\in L^*} |\{(\vec{\alpha}, \vec{v})\}|/\|\vec{v}\| \geqq c_n d(\vec{\alpha}, L)$.

In this paper we are interested in the best possible value of the constant c_n. Khinchin did not explicitly calculate his lower bound for c_n, Cassels [2] got the bound $c_n \geq (n!)^{-2}$ which was improved by Babai [1] to c^n. We prove that $c_n \geq (6n^2+1)^{-1}$. Examples show that $c_n \leq c/n$. The question whether c_n could be chosen to be of the form $1/p(n)$ for a polynomial $p(n)$ was posed as an open problem by Lovász [9].

Taking the view of complexity theory we are studying the following computational problem. Given a lattice $L \subset Q^n$ and a point $\vec{x} \in Q^n$ what is the distance from $\vec{x}$ to L (i.e. $\min_{\vec{y} \in L} \|\vec{x}-\vec{y}\|$). This problem is *NP*-complete [3]. To make it be in *NP* we have to make it into a decision problem by asking: Is $d(\vec{x}, L) \leq K$?

A "yes" answer to this question can easily be verified by giving a vector $\vec{y} \in L$ such that $\|\vec{x}-\vec{y}\| \leq K$. The only nontrivial part to check, before concluding that the problem is in *NP*, is that $\vec{y} \in L$ can be checked in polynomial time. This is however not hard. A "no" answer to the above question can probably not be verified in polynomial time since a *NP*-complete problem is not in *co-NP* unless *co-NP=NP*. However by our result (and previous results) the problem is in an approximate version of *co-NP*. By this we mean that if $d(\vec{x}, L)=K$ then it is possible to prove that $d(\vec{x}, L) \geq K/(6n^2+1)$ by displaying a suitable vector $\vec{v} \in L^*$. The best known solution to this approximate lower bounds was given by Lagarias, Lenstra and Schnorr [7]. By showing the existence of a nice basis for any lattice L they show by using this basis it is possible to produce a vector $\vec{y} \in L$ and a certificate that $d(\vec{x}, L) \geq cn^{-3/2}\|\vec{x}-\vec{y}\|$.

Our existential proof is nonconstructive and we know of no subexponential time algorithm that finds the vector $\vec{v}$. We would like to point out that Babai [1] using Lovász' lattice reduction algorithm (from [8]) has given a polynomial time algorithm that finds a vector $\vec{v}$ that satisfies $|\{(\vec{x}, \vec{v})\}|/\|\vec{v}\| \geq 9^{-n} d(\vec{x}, L)$.

2. Preliminaries and notation

Let L be a lattice with basis $(\vec{b}_i)_{i=1}^n$. In general we will work with several different bases for the same lattice. We will in general not change notation. Let L^* be the dual lattice of L with basis $(\vec{b}_i^*)_{i=1}^n$ satisfying $(\vec{b}_i, \vec{b}_j^*)=\delta_{ij}$.

For $i=1, 2, \ldots, n$, let *i*th *successive minima* λ_i be the radius of the smallest sphere around the origin containing i linearly independent points of L. We let λ_i^* be the corresponding numbers for the dual lattice. We will let $\|\vec{x}\|$ denote the euclidean length of a vector $\vec{x}$.

For a basis $(\vec{b}_i)_{i=1}^n$ let $\vec{\beta}_i$ be the projection of $\vec{b}_i$ onto the space orthogonal to $\vec{b}_1, \ldots, \vec{b}_{i-1}$. A Korkine—Zolotarev (in future KZ) basis is defined recursively as follows.

(1) $\vec{b}_1$ is one of the shortest vectors in L.

(2) $\vec{b}_i$ is one of the vectors giving a minimal $\|\vec{\beta}_i\|$.

Ties are resolved in any arbitrary way. Interesting to note is that such a basis can be found in exponential time by an algorithm by Kannan [4]. This type of basis has some useful properties.

Lemma 1. *For any vector $\vec{z}$ in the linear span of of L there is a vector $\vec{y} \in L$ such*

that

$$\|\vec{z}-\vec{y}\| \leqq \frac{1}{2}\left(\sum_{i=1}^{n} \|\vec{\beta}_i\|^2\right)^{1/2}.$$

Proof. The $\vec{\beta}_i$ are clearly mutually orthogonal and $\vec{b}_i$ can be written in the form $\vec{b}_i = \sum_{j=1}^{i-1} \mu_{ij}\vec{\beta}_j + \vec{\beta}_i$. Write $\vec{z} = \sum_{i=1}^{n} \gamma_i \vec{\beta}_i$ and we will now find a $\vec{y} = \sum_{i=1}^{n} c_i \vec{\beta}_i = \sum_{i=1}^{n} a_i \vec{b}_i$ such that $|c_i - \gamma_i| \leqq 1/2$. This can be done be making the unique choice for a_i starting with $i=n$ and going towards lower indices. This clearly proves Lemma 1. ∎

Observe that the procedure is completely effective once the basis is given. By applying the above procedure to the basis vectors we can assume that $|\mu_{ij}| \leqq 1/2$ and thus we have the following lemma.

Lemma 2. *We can find a KZ-basis such that* $\|\vec{b}_i\|^2 \leqq \sum_{j=1}^{i-1} \|\vec{\beta}_j\|^2/4 + \|\vec{\beta}_i\|^2$.

3. Main theorem

Having done away with the preliminaries we can now state and prove our main theorem.

Theorem. *Given a lattice L in $\mathbf{R}^n$. For every $\vec{z} \in \mathbf{R}^n$ there is a vector $\vec{v} \in L^*$ such that*

$$\frac{|\{(\vec{v}, \vec{z})\}|}{\|\vec{v}\|} \geqq \frac{1}{6n^2+1} d(\vec{z}, L)$$

Loosely speaking for every vector which is far from the lattice there is a reasonable onedimensional reason for this.

Proof. Suppose that $|\{(\vec{z}, \vec{v})\}| \leqq \varepsilon \|\vec{v}\|$ for all $\vec{v} \in L^*$. We have to prove that $\vec{z}$ is close to L. We will quite explicitly construct a vector in the lattice that is close to $\vec{z}$. For all short vectors $\vec{v} \in L^*$ it is true that $(\vec{v}, \vec{z})$ is very close to an integer. The idea of the proof is to pick the vector in the lattice which has the same inner products rounded to integers with all short vectors. We have to prove that this vector is well defined. Let $\vec{b}_i^*$, $i=1, 2, \ldots, n$ be a KZ basis of L^* which are as short as described by Lemma 2. Let r be the largest integer such that $\|\vec{\beta}_i^*\| \leqq (12\varepsilon n^{1/2})^{-1}$ for $i=1, 2, \ldots, r$. We will keep this value of r fixed from now on. Observe that this in particular implies that $\|\vec{b}_i^*\| \leqq 1/(12\varepsilon)$ for $i=1, 2, \ldots, r$.

For a real number x let $[x]$ denote the closest integer to x and let $\tilde{z}$ be a vector in L satisfying

$$(\tilde{z}, \vec{b}_i^*) = [(\vec{z}, \vec{b}_i^*)] \quad i = 1, \ldots, r$$

such a $\tilde{z}$ always exist and is unique if $r=n$. We will now prove the following lemma:

Lemma 3. *For any vector $\vec{v} \in L^*$ in the linear span of $\vec{b}_1^*, \vec{b}_2^*, \ldots, \vec{b}_r^*$, with $\|\vec{v}\| \leqq 1/(6\varepsilon)$ it is true that $(\tilde{z}, \vec{v}) = [(\vec{z}, \vec{v})]$.*

For the proof of Lemma 3 we will need some machinery.

Definition. A $(\vec{b}_i^*)_{i=1}^r$-*walk* be a sequence of points $\vec{u}_i$, $i=1, 2, \ldots, s$ such that for each i, there exists a $j(i)$ such that $1 \leqq j(i) \leqq r$ and $\vec{u}_i - \vec{u}_{i-1} = \pm \vec{b}_{j(i)}^*$.

Using this notation let us prove the following lemma.

Lemma 4. *Given $\vec{v} \in L^*$ in the linear span of b_i^*, $i=1, 2, \ldots, r$ there exist a $(\vec{b}_i^*)_{i=1}^r$-walk from 0 to $\vec{v}$ never leaving the ball of radius* $\|\vec{v}\| + (3/2)\left(\sum_{i=1}^r \|\beta_i^*\|^2\right)^{1/2}$.

Proof. We will define the walk recursively from $\vec{v}$ to 0. Make $\vec{u}_1 = \vec{v}$ and suppose $\vec{u}_j = \sum_{i=1}^r c_i^j \vec{\beta}_i$. Find the smallest i such that $(c_i^j) \geqq 1$ and define $u_{j+1} = u_j - \operatorname{sign}(c_i)\vec{b}_i$. We need to verify that we eventually get to 0 and that we stay within a relatively small ball on the way. Let us first prove that we eventually reach 0. Define $d_j = \sum_{i=1}^r |c_i^j| 2^i$.

Fact. $d_{j+1} \leqq d_j - 1$.

Proof. If i is the chosen index in the definition of $\vec{u}_{j+1}$ then $|c_i^{j+1}| = |c_i^j| - 1$ while $c_k^{j+1} = c_k^j$ for $k > i$ and $|c_k^{j+1}| \leqq |c_k^j| + 1/2$ for $k < i$.

Using this fact, to prove that we eventually get to 0 we only have to prove that if $\vec{u}_j$ is nonzero then there exist an i such that $|c_i^j| \geqq 1$. This follows from the observation that for the largest i such that c_i^j is nonzero c_i^j is an integer.

To get the estimate for how far from the origin $\vec{u}_j$ can be we need only observe that $|c_i^j| \leqq \max(3/2, c_i^1)$. The proof of Lemma 4 is complete. ∎

Let us return to the proof of Lemma 3. By Lemma 4 there exist a walk $(\vec{u}_i)$ from 0 to $\vec{v}$ by the vectors $\vec{b}_i^*$ which stays inside the ball of radius $1/(3\varepsilon)$. We prove that $(\vec{z}, \vec{u}_i) = [(\vec{z}, \vec{u}_i)]$ by induction over i. Number the walk such that $0 = \vec{u}_1$ and $\vec{v} = \vec{u}_s$ Clearly the induction hypothesis holds for $i=1$. For the induction step use $\vec{u}_i = \vec{u}_{i-1} \pm b_j^*$ giving

$$[(\vec{z}, \vec{u}_i)] - (\vec{z}, \vec{u}_i) = [(\vec{z} - \vec{z}, \vec{u}_{i-1} \pm \vec{b}_j^*)].$$

Using the induction hypothesis and $\|\vec{u}_{i-1}\| \leqq 1/(3\varepsilon)$ we get $|(\vec{z} - \vec{z}, \vec{u}_{i-1})| \leqq 1/3$ and $|(\vec{z} - \vec{z}, \vec{b}_j^*)|$ is bounded by 1/12 since $\|\vec{b}_j^*\| \leqq 1/(12\varepsilon)$ and $[(\vec{z} - \vec{z}, \vec{b}_j^*)] = 0$ by the definition of $\vec{z}$. Thus $[(\vec{z} - \vec{z}, \vec{u}_{i-1} + \vec{b}_j^*)] = 0$ and this completes the proof of Lemma 3. ∎

Remark. We feel that apart from being of use in the present proof Lemma 4 is of interest of its own.

Finally we return to the proof of the theorem. Define M_r to be the r-dimensional subspace spanned by $\vec{b}_1^*, \vec{b}_2^*, \ldots, \vec{b}_r^*$. We are going to decompose $\vec{z} - \tilde{z}$ in two components $z^{(1)} + z^{(2)}$ where $z^{(1)} \in M_r$ and $z^{(2)}$ is orthogonal to M_r. We will prove that $z^{(1)}$ is short and that $z^{(2)}$ can be approximated well by a vector in L orthogonal to M_r.

Lemma 5. $\|z^{(1)}\| \leqq 2\varepsilon$.

Proof. For any $\vec{v}$ in $M_r \cap L^*$ with $\|\vec{v}\| \leq 1/(6\varepsilon)$ we know that $\varepsilon\|\vec{v}\| \geq |\{(\vec{z}-\vec{z}, \vec{v})\}| = |(z^{(1)}, \vec{v})|$. Suppose that $\|z^{(1)}\| \geq 2\varepsilon$, then for any such $\vec{v}$, the (acute) angle between $z^{(1)}$ and $\vec{v}$ must be at least 60°. Thus points of L^* are excluded from the shaded region in Figure 1.

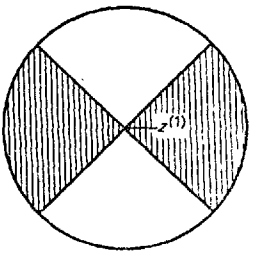

Fig. 1. Ball of radius $\frac{1}{6\varepsilon}$ in M_r

Observe that the region contains a ball of radius $1/(18\varepsilon)$ and by Lemma 1 and the choice of r there is always a point of L^* in every ball of radius $\geq 1/(24\varepsilon)$. This is a contradiction and we have proved the lemma. ∎

Next we proceed to find a lattice point which is close to $z^{(2)}$. Let L' be the $n-r$ dimensional sublattice of L which is orthogonal to M_r. We have

Lemma 6. *There is a* $z' \in L'$ *such that* $\|z^{(2)}-z'\| \leq 6n^2\varepsilon$.

Proof. Let the dual of L' be $L^{*\prime}$. Observe that $L^{*\prime}$ is L^* projected onto the orthogonal complement of M_r. By the definition of r and of KZ basis there is no vector in $L^{*\prime}$ which is shorter than $(12n^{1/2}\varepsilon)^{-1}$.

Let $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_{n-r}$ be a KZ basis for L'. Then we know by [7] that

$$\|\vec{\beta}_i\| \leq \frac{n}{\lambda_1'^*} \leq 12n^{3/2}\varepsilon.$$

Thus by Lemma 1 any vector can be approximated within $6n^2\varepsilon$ and the proof is complete. ∎

Theorem 1 now clearly follows from Lemmas 5 and 6. Observe that if ε is small enough we do not get any component $z^{(2)}$ and hence we can drop the factor n^{-2} in the theorem.

Acknowledgment. I thank Jeff Lagarias for many fruitful discussions about lattices.

References

[1] L. Babai, On Lovász' lattice reduction and the nearest lattice point problem, *Combinatorica*, 6 (1986), 1—13.
[2] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer Verlag, Heidelberg 1971.
[3] P. Van Emde Boas, Another *NP*-complete problem and the complexity of computing short vectors in a lattice, *Math. Dept. Report 81—04. Univ. of Amsterdam*, April 1981.

[4] R. KANNAN, Minkowski's convex body theorem and integer programming, *to appear in Mathematics of Operations Research.*
[5] A. I. KHINCHIN, A quantitative formulation of Kronecker's theory of approximation, *Inv. Akad. Nauk. SSSR (ser. Mat),* **12** 113—122 *(in russian).*
[6] A. KORKINE and G. ZOLOTAREV, Sur les formes quadratiques, *Mathematiche Annalen,* **6** (1973), 366—389.
[7] J. C. LAGARIAS, H. W. LENSTRA and C. P. SCHNORR, Korkine—Zolotarev bases and the successive minima of a lattice and its reciprocal lattice, *to appear in Combinatorica.*
[8] A. K. LENSTRA, H. W. LENSTRA and L. LOVÁSZ, Factoring polynomials with rational coefficients, *Math. Ann.*, **261** (1982), 515—534.
[9] L. LOVÁSZ, *personal communication.*

Johan Hastad

Laboratory for Comp. Science
M. I. T.
545 Technology Square
Cambridge, MA 02139
U.S.A.