A Note on Projecting the Cubic Lattice

N. J. A. Sloane, Vinay A. Vaishampayan, AT&T Shannon Labs, 180 Park Avenue, Florham Park, NJ 07932-0971, USA.
and
Sueli I. R. Costa, University of Campinas, Campinas, SP 13083-970, Brazil.

Email: njas@research.att.com, vinay@research.att.com, sueli@ime.unicamp.br.

(a) To whom correspondence should be addressed.

April 5, 2010; revised April 24, 2010, May 25 2010, July 14 2010

Abstract

It is shown that, given any \((n-1)\)-dimensional lattice \(\Lambda\), there is a vector \(v \in \mathbb{Z}^n\) such that the orthogonal projection of \(\mathbb{Z}^n\) onto \(v^\perp\) is, up to a similarity, arbitrarily close to \(\Lambda\). The problem arises in attempting to find the largest cylinder anchored at two points of \(\mathbb{Z}^n\) and containing no other points of \(\mathbb{Z}^n\).

Keywords: projections, shadows, dense packings

AMS 2010 Classification: Primary 11H55, 52C17

1. Introduction

Let \(\mathbb{Z}^n\) denote the cubic lattice with basis \(e_1 := (1, 0, \ldots, 0), \ldots, e_n := (0, 0, \ldots, 1)\). If we project \(\mathbb{Z}^n\) onto the \((n-1)\)-dimensional subspace

\[ v^\perp := \{ x \in \mathbb{R}^n : x \cdot v = 0 \} \]

perpendicular to a vector \(v \in \mathbb{Z}^n\), we obtain an \((n-1)\)-dimensional lattice that we denote by \(\Lambda_v\). We will show that, given any \((n-1)\)-dimensional lattice \(\Lambda\), we can choose \(v \in \mathbb{Z}^n\) so that \(\Lambda_v\) is arbitrarily close to a lattice that is geometrically similar to \(\Lambda\). More precisely, we will establish:

**Theorem 1.** Let \(\Lambda\) be an \((n-1)\)-dimensional lattice with Gram matrix \(A\) (with respect to some basis for \(\mathbb{R}^{n-1}\)). For any \(\epsilon > 0\), there exist a nonzero vector \(v \in \mathbb{Z}^n\), a basis \(B\) for the \((n-1)\)-dimensional lattice \(\Lambda_v\), and a number \(c\) such that if \(A_v\) denotes the Gram matrix of \(B\), then

\[ \| A - cA_v \|_\infty < \epsilon. \]

The theorem is at first surprising, since \(A\) has \(\frac{n+1}{2}\) degrees of freedom, whereas \(v\) has only \(n\) degrees of freedom (for the explanation see the remark following the proof of Theorem 2).

The problem arises from a question in communication theory (see [3]), which calls for projections \(\Lambda_v\) with high packing density. Since both the determinant and minimal norm of a lattice are continuous functions of the entries in the Gram matrix, so is the packing density. The theorem

\footnote{The minimal norm \(\mu\) of a \(d\)-dimensional lattice with Gram matrix \(A\) is the minimum over all \(z \in \mathbb{Z}^d, z \neq 0\), of the quadratic form \(zA^Tz\). It is enough to consider the finite set of \(z\) in some ball around the origin. For a given \(z \neq 0\), \(zA^Tz\) is a continuous function of the entries of \(A\), and since the minimum of a finite set of continuous functions is continuous, \(\mu\) is a continuous function of the entries of \(A\).}
recovered as a projection of $K \leq k$.

We begin with some preliminary remarks about the projection lattice $\Lambda$. Proof of Theorem 1

Notation. $\Lambda^*$ denotes the dual lattice to $\Lambda$, $A^T$ is the transpose of $A$, and $\|A\|_\infty = \max_{i,j} |A_{i,j}|$. Our vectors are row vectors. For undefined terms from lattice theory see [3].

2. Proof of Theorem 1

We begin with some preliminary remarks about the projection lattice $\Lambda_v$ and its dual $\Lambda_v^*$. For simplicity we will only consider projections that use vectors of the form $v = (1, v_1, v_2, \ldots, v_{n-1}) \in \mathbb{Z}^n$. Let $\tilde{v} := (v_1, v_2, \ldots, v_{n-1})$, $M := \|v\|^2 = 1 + \sum v_i^2$.

The matrix that orthogonally projects $\mathbb{R}^n$ onto $v^\perp$ is $P := I_n - \frac{1}{M} v^T v$. As a generator matrix $G$ for $\mathbb{Z}^n$ (expressed in terms of $e_1, \ldots, e_n$) we take $I_n$ with its first row replaced by $v$. Let $G_v$ be obtained by omitting the first (zero) row of $GP$. Then $G_v$ is an $(n-1) \times n$ generator matrix for the projection lattice $\Lambda_v$, and $A_v := G_v G_v^T = I_{n-1} - \frac{1}{M} \tilde{v}^T \tilde{v}$ is its Gram matrix, with $\det \Lambda_v = \det A_v = \frac{1}{M}$.

It is often easier to work with the dual lattice $\Lambda_v^*$. This is the intersection of $\mathbb{Z}^n$ with the subspace $v^\perp$, and has generator matrix

$$
\begin{bmatrix}
-v_1 & 1 & 0 & \ldots & 0 \\
-v_2 & 0 & 1 & \ldots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
-v_{n-1} & 0 & 0 & \ldots & 1
\end{bmatrix},
$$

(2)

Gram matrix $A_v^* = I_{n-1} + \tilde{v}^T \tilde{v}$, and determinant $M$.

If a sequence of matrices $T_i$ converges in the $\| \cdot \|_\infty$ norm to a positive-definite matrix $T$, then $T_i^{-1}$ converges to $T^{-1}$. So the following theorem is equivalent to Theorem 1.

Theorem 2. Let $\Lambda$ be an $(n-1)$-dimensional lattice with Gram matrix $A$ (with respect to some basis for $\mathbb{R}^{n-1}$). For any $\epsilon > 0$, there exist a nonzero vector $v \in \mathbb{Z}^n$, a basis $B$ for the $(n-1)$-dimensional lattice $\Lambda_v^*$ and a number $c$ such that if $A_v^*$ denotes the Gram matrix of $B$, then

$$
\|A - c A_v^*\|_\infty < \epsilon.
$$

(3)

Proof of Theorem 2. We may write $A = LL^T$ where $L = [L_{i,j}]$ is an $(n-1) \times (n-1)$ lower triangular matrix. For $w = 1, 2, \ldots$ let us form the $(n-1) \times n$ matrix

$$
L_w := -\left[\begin{array}{c} wL_1 \vspace{10pt} \hline wL_2 \vspace{10pt} \hline \vdots \vspace{10pt} \hline -wL_{n-1} \end{array} \right] + \left[\begin{array}{c} 0 \vspace{10pt} \hline 0 \vspace{10pt} \hline \vdots \vspace{10pt} \hline I_{n-1} \end{array} \right]
$$

$$
= \left[\begin{array}{cccccc}
-wL_{1,1} & 1 & 0 & \ldots & 0 & 0 \\
-wL_{2,1} & -wL_{2,2} & 1 & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
-wL_{n-1,1} & -wL_{n-1,2} & -wL_{n-1,3} & \ldots & -wL_{n-1,n-1} & 1
\end{array} \right],
$$

(4)
where \( \mathbf{0} \) denotes a column of \( n - 1 \) zeros. We call \( L_w \) a “lifted” version of \( L \).

We apply elementary row operations to \( L_w \) so as to put it in the form

\[
\tilde{L}_w := \begin{bmatrix}
-v_1 & 1 & 0 & \ldots & 0 & 0 \\
-v_2 & 0 & 1 & \ldots & 0 & 0 \\
0 & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 0 & 1 \\
0 & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 0 & 1
\end{bmatrix},
\]  

and take \( v = (1, v_1, \ldots, v_{n-1}) \). Then \( \Lambda_v^* \) has generator matrix \( \tilde{L}_w \). But \( \tilde{L}_w \) and \( L_w \) generate the same lattice. It follows that \( \Lambda_v^* \) has a Gram matrix

\[
A_v^* = L_wL_w^t = w^2A + B = w^2\left(A + \frac{1}{w^2}B\right),
\]  

using (4), where the entries in \( B \) are of order \( O(w) \) as \( w \to \infty \). This implies (3) (with \( c = 1/w^2 \)).

Remark. The apparent paradox mentioned in §1 is explained by the fact that we use \( \binom{n}{2} \) degrees of freedom in going from (4) to (5).

3. Examples

3.1. The lattice \( 2\mathbb{Z} \oplus \mathbb{Z} \)

We start with a concrete example. If we take \( v = (1, 1, 0) \) then \( \Lambda_v \) has Gram matrix \( \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \), and is geometrically similar to \( \sqrt{2}\mathbb{Z} \oplus \mathbb{Z} \). Similarly \( v = (1, 1, 1) \) produces the hexagonal (or \( A_2 \)) lattice, and in general \( v = (1, 1, \ldots, 1) \) gives \( A_{n-1} \). On the other hand, there is no \( v = (1, v_1, v_2) \in \mathbb{Z}^3 \) such that \( \Lambda_v \) is geometrically similar to \( 2\mathbb{Z} \oplus \mathbb{Z} \) (see Proposition 3). However, we can find projections which converge to a lattice that is geometrically similar to \( 2\mathbb{Z} \oplus \mathbb{Z} \). Since any two-dimensional lattice is geometrically similar to its dual, we can apply Theorem 2 with \( \Lambda = 2\mathbb{Z} \oplus \mathbb{Z} \). Then \( L = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \),

the lifted generator matrix is \( L_w = \begin{bmatrix} -2w & 1 & 0 \\ 0 & -w & 1 \end{bmatrix}, \tilde{L}_w = \begin{bmatrix} -2w & 1 & 0 \\ -2w^2 & 0 & 1 \end{bmatrix}, v = (1, 2w, 2w^2) \), and a Gram matrix for \( \Lambda_v^* \) is \( I_2 + \tilde{v}^t \tilde{v} = \begin{bmatrix} 4w^2 + 1 & 4w^3 \\ 4w^3 & 4w^4 + 1 \end{bmatrix} \). If we subtract \( w \) times the first generator from the second, this becomes

\[
\begin{bmatrix} 4w^2 + 1 & -w \\ -w & w^2 + 1 \end{bmatrix} = w^2 \begin{bmatrix} 4 + 1/w^2 & -1/w \\ -1/w & 1 + 1/w^2 \end{bmatrix},
\]

which converges to \( w^2 \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix} \) as \( w \to \infty \).

**Proposition 3.** There is no vector \( v = (1, a, b) \in \mathbb{Z}^3 \) such that \( \Lambda_v^* \) is geometrically similar to \( 2\mathbb{Z} \oplus \mathbb{Z} \).
Proof. From (2), $\Lambda_v^*$ has Gram matrix $A := \begin{bmatrix} a^2 + 1 & ab \\ ab & b^2 + 1 \end{bmatrix}$. If $\Lambda_v^*$ is geometrically similar to $2\mathbb{Z} \oplus \mathbb{Z}$ then there is a matrix $T := \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL_2(\mathbb{Z})$ and $\lambda \in \mathbb{R}$ such that 

\[ A = \lambda T \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix} T^{tr} = \lambda \begin{bmatrix} 4r^2 + s^2 & 4rt + su \\ 4rt + su & 4t^2 + u^2 \end{bmatrix}. \]

This implies $\lambda \in \mathbb{Q}$, and taking the determinant and trace of both sides we obtain $a^2 + b^2 + 1 = 4\lambda^2$, $a^2 + b^2 + 2 = 4\lambda^2 + 1 = \lambda\sigma$, where $\sigma := 4r^2 + 4t^2 + s^2 + u^2 \in \mathbb{Z}$. Hence the discriminant of the quadratic for $\lambda$, $\sigma^2 - 16$, is a perfect square, so $\sigma = 4$ or 5, $\lambda = \frac{1}{2}$, $\frac{1}{4}$ or 1, $a^2 + b^2 + 1 = 1$, $\frac{1}{4}$ or 3, none of which are possible.

3.2. The lattice $5_1$

For an example where the floor operations in (4) are actually needed, consider the lattice $\Lambda$ with Gram matrix $\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}$ and determinant 5 (this is the lattice $5_1$ in the notation of [1]). Again there is no $v = (1, v_1, v_2) \in \mathbb{Z}^3$ such that $\Lambda_v$ is geometrically similar to $\Lambda$. We take $L = \begin{bmatrix} \sqrt{3} & 0 \\ \frac{1}{\sqrt{3}} & \sqrt{5/3} \end{bmatrix}$, and find that 

\[ v = (1, \lfloor \sqrt{3} \rfloor w, \lfloor \sqrt{3} \rfloor w \lfloor \sqrt{5/3} \rfloor w) + \lfloor w/\sqrt{3} \rfloor) . \]

3.3. The lattice $D_m$, $m \geq 3$

As generator matrix for $D_m^*$ we take ([3, p. 120])

\[ \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 1/2 & 1/2 & 1/2 & \ldots & 1/2 & 1/2 \end{bmatrix} \]

We set $w = 2t$, $t \in \mathbb{Z}$, and obtain 

\[ v = \begin{pmatrix} 1, 2t, (2t)^2, \ldots, (2t)^{m-1}, t^2 + 1 \end{pmatrix}. \]

In particular, when $m = 3$, we have 

\[ v = (1, 2t, 4t^2, 4t^3 + 2t^2 + t), \]

for which $\Lambda_v^*$ converges to the body-centered cubic lattice $D_3^*$ and $\Lambda_v$ to the face-centered cubic lattice $D_3$.

3.4. The lattice $E_8$

Using the generator matrix given in ([3, p. 121]), we find that $v = (1, v_1, v_2, \ldots, v_8)$ is given by 

\[ v_1 = 2w, v_2 = 2w^2 - w, v_i = w(v_{i-1} - v_{i-2}) \text{ for } i = 3, 4, \ldots, 7, \text{ and } v_8 = (w/2)(1 + \sum_{i=1}^{7} v_i), \]

where $w$ is even.
3.5. The Leech lattice

Using [3, Fig. 4.12], we find that $v = (1, v_1, v_2, \ldots, v_{24})$ is given by

\[
\begin{align*}
v_1 &= 8w, \\
v_i &= 4w(v_{i-1} + 1), \text{ for } i = 2, \ldots, 7, 9, 10, 11, 13, 17, \\
v_i &= 2w(\sum_{j\in S_i} v_j + 1), \text{ for } i = 8, 12, 14, 15, 16, 18, 19, 20, \\
v_i &= 2\sum_{j\in S_i} v_j, \text{ for } i = 21, 22, 23, \\
v_{24} &= w(\sum_{i=1}^{23} v_i - 3),
\end{align*}
\]

where $S_8 = \{1, 2, \ldots, 7\}$, $S_{12} = \{1, 2, 3, 8, 9, 10, 11\}$, $S_{14} = \{1, 4, 5, 8, 9, 12, 13\}$, $S_{15} = \{2k, 1 \leq k \leq 7\}$, $S_{16} = \{3, 4, 7, 8, 11, 12, 15\}$, $S_{18} = \{2, 4, 7, 8, 9, 16, 17\}$, $S_{19} = \{3, 4, 5, 8, 10, 16, 18\}$, $S_{20} = \{1, 4, 6, 8, 11, 16, 19\}$, $S_{21} = \{1, 2, 3, 4, 8, 12, 16, 20\}$, $S_{22} = \{8, 9, 12, 13, 16, 17, 20, 21\}$, $S_{23} = \{2k, k = 4, 5, \ldots, 11\}$.

4. Faster convergence

The construction in Theorem [2] produces a vector $v$ of length $\|v\| = O(w^n)$, while from [3] we have $\|A - \frac{1}{w^*}A_v^*\|_\infty = O\left(\frac{1}{\|v\|^{1/4}}\right)$. It is sometimes possible to obtain a faster rate of convergence. Suppose $\Lambda$ is $D_3$, and instead of (2) let us take the following generator matrix for $D_3^*$:

\[
L := \begin{bmatrix}
-1 & -1 & 1 \\
1 & -1 & 1 \\
1 & 1 & 1
\end{bmatrix}.
\]

Let

\[
L_w = \begin{bmatrix}
w - 1 & w + 1 & -w & 0 \\
w - 1 & w & -w + 1 & 0 \\
w & -w & -w & 1
\end{bmatrix}
= [-wL \ 0] + [0 \ I_3] + \begin{bmatrix}
-1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix},
\]

with

\[
A_v^* = L_w L_w^\text{tr} = \begin{bmatrix}
3w^2 + 2 & w^2 + 1 & -w^2 \\
w^2 + 1 & 3w^2 + 2 & w^2 \\
-w^2 & w^2 & 3w^2 + 1
\end{bmatrix}.
\]

The last matrix in (10) is chosen so that there are no terms of order $w$ in (11). Let $H_w$ denote the $3 \times 3$ matrix formed by the last three columns of $L_w$, and define $v_1, v_2, v_3$ by

\[
H_w^{-1}L_w = \begin{bmatrix}
-v_1 & 1 & 0 \\
-v_2 & 0 & 1 \\
-v_3 & 0 & 0
\end{bmatrix}.
\]

Then

\[
v = (1, v_1, v_2, v_3) = (1, 2w^2 - w + 1, 2w^2 + w + 1, 4w^3 + 3w)
\]

has $\|v\| = O(w^3)$, and now $\|A - \frac{1}{w^*}A^*_v\|_\infty = O(\frac{1}{\|v\|^{1/4}})$, which is a faster convergence than we found in [3.3.3]. We do not know if similar speedups are always possible. Incidentally, we first found (12)—before Theorem [2] was proved—by a combination of computer search and guesswork.
5. The fat strut problem

The problem studied in this paper arose when constructing codes for a certain analog communication channel [6]. The codes require that one finds a curved tube in the sphere $S^{2n-1}$ which does not intersect itself, has a specified length and as large a volume as possible. The method used in [6] is based on finding a vector $v \in \mathbb{Z}^n$ with a specified value of $\|v\|$, such that there is a cylinder of large volume with axis $\vec{0}v$ which contains no points of $\mathbb{Z}^n$ other than $\vec{0}$ and $v$. The cross-section of the cylinder is an $(n-1)$-dimensional ball, and $\vec{0}$ and $v$ are the centers of the two end-faces. The radius of the cylinder is taken to be as large as possible subject to the condition that the interior contains no point of $\mathbb{Z}^n$. The problem is to choose $v$, for a given length $\|v\|$, so that the volume of the resulting cylinder is maximized. We call a cylinder which achieves the maximal volume a fat strut.

A fat strut has the property that the projection of the cylinder onto $v^\perp$ does not contain the image of any nonzero point of $\mathbb{Z}^n$. The radius of the cylinder is therefore equal to the radius of the largest $(n-1)$-dimensional sphere in the projection lattice $\Lambda_v$ which contains no nonzero point of $\Lambda_v$. In other words, finding a fat strut for a given length $\|v\|$ is equivalent to maximizing the density of the projection lattice $\Lambda_v$.

It is worth contrasting the fat strut problem with the result of [4] and [5] that for any lattice sphere packing in dimension three or higher there is always an infinite cylinder of nonzero radius (obviously not passing through the origin) which does not touch any of the spheres.

6. Acknowledgment

We thank the referee for some very helpful comments.

References

[1] J. H. Conway and N. J. A. Sloane, Low-dimensional lattices I: Quadratic forms of small determinant, Proc. Royal Soc. London, A 418 (1988), 17–41.

[2] J. H. Conway and N. J. A. Sloane, Low-dimensional lattices V: Integral coordinates for integral lattices, Proc. Royal Soc. London, A 425 (1989), 211–232.

[3] J. H. Conway and N. J. A. Sloane, Sphere Packings, Lattices and Groups, Springer-Verlag, New York, 3rd ed., 1998.

[4] A. Heppes, Ein satz über gitterförmige kugelpackungen, Ann. Univ. Sci. Budapest. Eötvös Sect. Math., 3–4 (1960/1961), 89–90.

[5] J. Horváth, Über die durchsichtigkeit gitterförmiger kugelpackungen, Studia Sci. Math. Hungar., 5 (1970), 421–426.

[6] V. A. Vaishampayan and S. I. R. Costa, Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources, IEEE Trans. Inform. Theory, 49 (2003), 1658–1672.