On sequences of projections of the cubic lattice

Antonio Campello
Institute of Mathematics, Statistics
and Computer Science
University of Campinas
13083-859, Campinas-SP, Brazil
campello@ime.unicamp.br

João Strapasson
School of Applied Sciences
University of Campinas
13484-350, Limeira-SP, Brazil
joao.strapasson@fca.unicamp.br

Abstract

In this paper we study sequences of lattices which are, up to similarity, projections of $\mathbb{Z}^{n+1}$ onto hyperplanes $v^\perp$, with $v \in \mathbb{Z}^{n+1}$. We show a sufficient condition to construct sequences converging at rate $O(1/\|v\|^{2/n})$ to integer lattices and exhibit explicit constructions for some important families of lattices. The problem addressed here arises from a question of communication theory.

Keywords: Projections - Lattices - Dense Packings.

1 Introduction

It was recently proved [3] that any $n$-dimensional lattice can be approximated by a sequence of lattices such that each element is, up to similarity, the orthogonal projection of the cubic lattice $\mathbb{Z}^{n+1}$ onto a hyperplane determined by a linear equation with integer coefficients. Given a target lattice $\Lambda \subset \mathbb{R}^n$, it is possible to find a vector $v \in \mathbb{Z}^{n+1}$ from the construction in [3], such that the distance between $\Lambda$ and a lattice which is equivalent to the projection of $\mathbb{Z}^{n+1}$ onto $v^\perp$ has order $O(1/\|v\|^{1/n})$, where $\|v\|$ is the Euclidean norm of $v$. A natural question that arises from that result is whether it is possible to improve this convergence. We give a positive answer to this question by showing a sufficient condition to obtain sequences converging to an integer lattice with order $O(1/\|v\|^{2/n})$.
We also show explicit constructions of such sequences for some families of lattices (\(D_n\), odd \(n\), \(D^*_n\)) and exhibit a table of which is, to our knowledge, the best sequences of projection lattices in the sense of the tradeoff between density and \(\|v\|\).

Apart from the purely geometric interest, the problem of finding sequences of projection lattices with a better order of convergence is motivated by an application in joint source-channel coding of a Gaussian channel [6]. In the aforementioned paper, the authors propose a coding scheme based on curves on flat tori and show that the efficiency of this scheme is closely related to the “small-ball radius” of these curves, which can be approximated by the packing radius of a lattice obtained by projecting \(\mathbb{Z}^{n+1}\) onto the subspace \(v^\perp\) for \(v \in \mathbb{Z}^{n+1}\). Given a value \(l_0 > 0\), a worth objective to the design of good codes in the sense of [6] is the one of choosing a vector \(v \in \mathbb{Z}^{n+1}\) with \(\|v\| = l_0\) in such a way to maximize

\[
r(v) = \min_{n \in \mathbb{Z}^{n+1}} \min_{t \in \mathbb{R}} \|vt - n\|,
\]

which is the length of the shortest vector of \(\Lambda_v\), the projection of \(\mathbb{Z}^{n+1}\) onto \(v^\perp\). Let \(\delta_{\Lambda_v}\) be the center density of these lattices (for undefined terms see Section II). Since the volume of \(\Lambda_v\) is given by \(1/\|v\|\) (see [4]), we have:

\[
\delta_{\Lambda_v} = \frac{r(v)^n \|v\|}{2^n},
\]

therefore maximizing \(r(v)\) implies maximizing \(\delta_{\Lambda_v}\).

Another geometrical formulation to this problem is the so-called fat strut problem. A “strut” is defined as a cylinder anchored at two points in \(\mathbb{Z}^{n+1}\) such that its interior does not contain any other integer point. Given \(l_0 > 0\), the fat strut problem asks for a vector \(v \in \mathbb{Z}^{n+1}\) of length \(l_0\) that maximizes the radius of the strut anchored at \(0\) and \(v\). This problem is shown to be equivalent to the one of finding dense projections of \(\mathbb{Z}^{n+1}\) [4]. Therefore, projection lattices with higher densities imply fat-struts with larger radii, and the problem addressed in this work is related to finding small vectors that attain high density projection lattices. This is done by considering families of projections of \(\mathbb{Z}^{n+1}\).

This paper is organized as follows. In Section 2 we summarize some
relevant concepts and results on lattices. In Section 3, we derive a sufficient condition to construct good sequences of projection lattices and in Section 4 we exhibit explicit constructions for some well-known lattices. Finally, in Section 5 we present our conclusions.

2 Preliminaries and Notation

In this section we give a brief review of some relevant concepts concerning lattices and establish the notation to be used from now on.

Given \( m \) linearly independent vectors \( b_1, \ldots, b_m \) in \( \mathbb{R}^n \), a lattice \( \Lambda \) is the set of all integer linear combinations of these vectors. The matrix \( G \) whose rows are the vectors \( b_i \) is called a generator matrix for \( \Lambda \) and the matrix \( A = GG^t \) is said to be a Gram matrix for \( \Lambda \). The determinant or discriminant of \( \Lambda \) is defined as \( \det \Lambda = \det A \) and corresponds to the square of the volume of any fundamental region for the lattice \( \Lambda \). We say that two lattices with generator matrices \( G_1 \) and \( G_2 \) are equivalent if there exists an unimodular matrix \( U \), an orthogonal matrix \( Q \) and a real number \( c \) such that \( G_1 = cU G_2 Q \). The density \( \Delta \) of a lattice is the ratio between the volume of a sphere of radius \( \rho \) (half of the minimal distance between two distinct lattice points) and the volume of a fundamental region, while the center density is defined as \( \delta = \Delta / V_n \) where \( V_n \) is the volume of the unitary sphere in \( \mathbb{R}^n \). Sometimes we will refer to the center density of a specific lattice \( \Lambda \) as \( \delta_{\Lambda} \).

Let \( G \) be a full-rank generator matrix for \( \Lambda \). The dual lattice \( \Lambda^* \) of \( \Lambda \) is the set of all \( x \in \text{span}(G) \) such that \( \langle x, y \rangle \) is an integer number for all \( y \in \Lambda \), where \( \text{span}(G) \) is the row space of \( G \). One can easily verify that \( (GG^t)^{-1}G \) generates \( \Lambda^* \). We say that \( \Lambda \) is an integer (or rational) lattice if its generator matrix has integer (rational) entries. All rational lattices are integers up to scale. The cubic lattice \( \mathbb{Z}^n \) is the full-dimensional integer self-dual lattice that has the canonical vectors \( e_1 = (1,0,\ldots,0), \ldots, e_n = (0,\ldots,0,1) \) as a basis. A list of the densest known packings in some dimensions as well as many other information about lattices can be found in [1].

We say that a sequence of lattices \( \Lambda_w \) converges to \( \Lambda \) if there exist Gram matrices \( A \) for \( \Lambda \) and \( A_w \) for \( \Lambda_w \) such that \( \|A_w - A\|_\infty \to 0 \) as
where $w \to \infty$ where $\|M\|_\infty = \max_{i,j} |M_{ij}|$. Of course, if $\Lambda_w$ converges in that sense it also converges in any matrix norm. Another matrix norm we use in this work is the Frobenius norm, given by $\|M\|_F = \sqrt{\text{tr}(MM^T)}$.

Finally, we call $\Lambda_1$ a projection lattice of $\Lambda_2$ if it is obtained by projecting $\Lambda_2$ onto the subspace orthogonal to a vector $v \in \Lambda_2$, the projection vector. In this paper, a projection lattice will always be a projection of the cubic lattice onto $v^\perp$ for $v \in \mathbb{Z}^{n+1}$ a primitive vector (i.e., whose entries have greatest common divisor equal to 1). In the context of the projection lattices, the results in [4] and [3] are remarkable. The first one gives an achievable bound for the density of the projection lattices comparable to the so-called Minkowski-Hlawka bound while the second one states that every lattice can be approximated by a sequence of lattices that are equivalent to projection lattices. More formally, given a $n$-dimensional lattice $\Lambda$, it is shown that for every $\varepsilon > 0$, there is a vector $v \in \mathbb{Z}^{n+1}$ and a constant $c$ such that there is a Gram matrix $A_v$ for the lattice obtained by projecting $\mathbb{Z}^{n+1}$ onto $v^\perp$ and a Gram matrix $A$ for $\Lambda$ satisfying $\|A - cA_v\| \leq \varepsilon$. In this work we make a slight modification on the construction in [3] that leads to many other projection lattices sequences converging to a target lattice. We then make an error analysis for these sequences and show a sufficient condition for achieving a faster order of convergence, as well as explicit constructions for some important lattices.

3 Motivation

Considering the coding scheme mentioned in Section 1, there are two problems that can arise:

1. Given a certain radius $r_0$, what is the vector $v \in \mathbb{Z}^{n+1}$ that maximizes $\|v\|$ s.t. $r(v) = r_0$? Equivalently: given a minimum distance for the projection lattice, what is the vector $v \in \mathbb{Z}^{n+1}$ s.t. the projection of $v \in \mathbb{Z}^{n+1}$ has maximal density? In this case, we want to solve the following maximization problem:

$$\max_{v \in \mathbb{Z}^{n+1}} \|v\| \quad \text{subject to } r(v) = r_0. \quad (3)$$
2. Conversely, given a length $l_0$ what is the vector $v \in \mathbb{Z}^{n+1}$ with $\|v\| = l_0$ for which $r(v)$ is a maximum? Equivalently, we want to find the solution to:

$$\max_{v \in \mathbb{Z}^{n+1}} r(v) \quad \text{subject to} \quad \|v\| = l_0. \quad (4)$$

We illustrate these two problems in the case $n = 4$. We run an exhaustive search to solve the maximization problem (4) for $2 \leq l_0 \leq \sqrt{270478}$ (i.e., fixing $\|v\| = l_0$). Some examples are illustrated in Table 3.

From this table, we can guess a good solution for the problem (3), where $r_0$ is fixed.

For instance, take $r_0 = 0.16385$. The fourth element of the family of projection lattices onto $(1, 2w^2 - w + 1, 2w^2 + w + 1, 4w^3 + 3w)^\perp$ has minimal distance 0.163858, center density 0.164452 and squared norm 89425. Among the vectors of similar norm, we can find similar performances (e.g., the lattice produced by the vector $(1, 157, 164, 195)$ has minimal distance, center density and squared norm equal to 0.16386, 0.164594 and 89571 respectively).

Now, take $r_0 = 0.1721$ and the fourth element of the sequence of projections determined by the vectors $(1, 2w^2 - w + 1, 2w^2 + w + 1, 4w^3 + 3w)$ (which is an “optimal” sequence in the sense discussed in this paper). It has minimal distance, center density and squared norm equal to 0.172147, 0.173511 and 74035. Comparing this to the vector $(1, 13, 75, 244)$, which is “close” to $(1, 29, 37, 268)$ in the sense of these parameters, we find out that although the last one has a slightly smaller norm (65331), its center density is much smaller (0.163112). There is clearly a tradeoff between these parameters. Finally, let us fix the vector length around $\|v\|_2^2 = 89425$.

The fourth element of the first family above-cited produces a projection lattice with parameters “close” to the ones of the vector $(1, 31, 38, 295)$ (minimal distance, center density and squared norm equal to 0.163988, 0.164852 and 89431). On the other hand, there is no vector (with norm up to 89425) producing denser lattices than the fourth element of the optimal sequence, but within the interval 74035 and 89425 there are many other vectors that generate lattices with density superior to 0.163858, as shown in Table 1.
### Table 1: Dense projection lattices of $\mathbb{Z}^4$ onto $v^\perp$, for $74035 \leq \|v\| \leq 89425$.

| Center density | Minimal norm | $\|v\|^2$ |
|----------------|--------------|-----------|
| 0.173511       | 0.172147     | 74035     |
| 0.16502       | 0.168637     | 75778     |
| 0.170589       | 0.170362     | 76180     |
| 0.16473       | 0.16783      | 774035    |
| 0.166423       | 0.167331     | 80751     |
| 0.165716       | 0.166535     | 82390     |
| 0.164198       | 0.164612     | 86725     |
| 0.166189       | 0.165065     | 87442     |
| 0.165562       | 0.16484      | 87442     |
| 0.16497       | 0.164493     | 87922     |
| 0.164452       | 0.163858     | 89425     |

### 4 Convergence rate analysis

Let $\Lambda \subset \mathbb{R}^n$ be a lattice with a $n \times n$ generator matrix $\tilde{G}$ and consider $n \times n$ generator matrix $\tilde{G}^*$ to $\Lambda^*$. Let $G^* = \begin{bmatrix} \tilde{G}^* & 0_{n \times 1} \end{bmatrix}$ and $G = \begin{bmatrix} \tilde{G} & 0_{n \times 1} \end{bmatrix}$. We define $\Lambda^*_w, w \in \mathbb{N}$ as the sequence of $n$-dimensional lattices in $\mathbb{R}^{n+1}$ associated to the generator matrices

$$G^*_w = wG^* + P,$$

where $P$ is an $n \times (n+1)$ integer matrix which we will call a perturbation matrix. The correspondent Gram matrices for $\Lambda^*_w$ are

$$A^*_w = w^2 A^* + w(G^* P^t + PG^*) + PP^t \cong w^2 A^* + wQ_1 + Q_0,$$

where $A^* = G^* G^{*t}$ is a Gram matrix for $\Lambda^*$. We define $H_w = (G^*_w)(1,...,n),(2,...,n+1)$ as the matrix consisting on the last $n$ columns of $G^*_w$. If $\tilde{G}$ is a lower triangular matrix and $P = [0_{n \times 1} I_{n \times n}]$ it is shown in [3] that each $\Lambda^*_w$ (dual of $\Lambda^*_w$) is the projection of $\mathbb{Z}^{n+1}$ onto the subspace orthogonal to some vector $v \in \mathbb{Z}^{n+1}$ and the sequence of Gram matrices $(A^*_w)/c = (G^*_w G^*_w)/c \to A^*$
as $w \to \infty$ (hence, $cA_w \to A$), for $c = w^2$. A natural extension of this result is the following:

**Lemma 4.1.** Let $G_w^*$ and $H_w$ be the matrices defined above. If $H_w$ is unimodular for all $w \in \mathbb{N}$ then the lattices $\Lambda_w$ associated to the generator matrices $G_w$ are projection lattices.

**Proof.** Since $H_w$ is unimodular so is its inverse and $\Lambda_w^*$ is also generated by $H_w^{-1}G_w^*$. On the other hand, $H_w^{-1}G_w^* = [\tilde{v}_w \ I_{n \times n}]$ and for the same arguments of [4], $\Lambda_w^*$ is the intersection of $\mathbb{Z}^{n+1}$ with the subspace orthogonal to the vector $v_w = (1, -\tilde{v}_w)$, which is the dual of the projection of $\mathbb{Z}^{n+1}$ onto $v_w^\perp$. $\square$

In the sequel we will consider the analysis of the convergence order of the sequence $w^2A_w$ (i.e., the sequence of duals of (5)). We start by analysing the sequence (5). It is straightforward to show that $1/w^2A_w^* \to A^*$ with order $O(1/w)$ since

$$\|A^* - \left(1/w^2\right)A_w^*\|_\infty = \left\|\frac{Q_1}{w} + \frac{Q_0}{w^2}\right\|_\infty = O(1/w).$$

If $Q_1 = 0$, we obtain an $O(1/w^2)$ convergence order, as it happens in the example of [3], Section 4. More generally, if $Q_1 = \alpha A^*$, we can evaluate $A_w^*$ as follows:

$$A_w^* = w^2A^* + \alpha wA^* + Q_0 = A^*\left(w + \frac{\alpha}{2}\right)^2 - \frac{\alpha^2A^*}{4} + PP^t,$$

therefore the sequence $A_w^*/(w + \alpha/2)^2$ (i.e., taking $c = (w + \alpha/2)^2$) converges to $A_w^*$ with rate $O(1/w^2)$. Nevertheless, our main objective is the analysis of the sequence $\Lambda_w$. In what follows, we will show that the asymptotic behavior of $\Lambda_w$ is essentially the same as $\Lambda_w^*$, although for finite $w$ they may differ. In order to show this, we will need the following lemma.

**Lemma 4.2.** Let $A_w^*$ be Gram matrices for $\Lambda_w^*$ as in Equation (6). There exists $w_o$ such that, for $w \geq w_o$, the projection lattices $\Lambda_w$ have Gram
matrix

\[ A_w = \sum_{k=0}^{\infty} \left[ \frac{A}{w^2} (-wQ_1 - Q_0) \right]^k \frac{A}{w^2}. \]  \hspace{1cm} (7)

**Proof.** According to the matrix Neumann series \[2\] Ch. 3, Eq. (3.8.3):

\[ A_w = (A_w^*)^{-1} = (w^2A^* + wQ_1 + Q_0)^{-1} = \sum_{k=0}^{\infty} \left[ \frac{A}{w^2} (-wQ_1 - Q_0) \right]^k \frac{A}{w^2} \]  \hspace{1cm} (8)

provided that \( \lim_{k \to \infty} \left\| (w^2A^*)^{-1}(wQ_1 + Q_0)^k \right\| = 0 \) for any matrix norm. Since all entries of \((wQ_1 + Q_0)\) have order \(O(w)\) and the entries of \((w^2A)^{-1}\) are \(O(w^2)\), there exists \(w_o\) such that, for \(w \geq w_o\), each entry of the matrix \((w^2A^*)^{-1}(wQ_1 + Q_0)\) is arbitrarily close to zero. Taking the matrix power, we can make \(\left\| (w^2A^*)^{-1}(wQ_1 + Q_0)^k \right\| < \varepsilon\) for any \(\varepsilon > 0\) and the result follows.

As a consequence of the above lemma, we have:

\[ \left\| A - w^2A_w \right\| = \left\| \sum_{k=1}^{\infty} \left[ \frac{A}{w^2} (-wQ_1 - Q_0) \right]^k A \right\| \approx \left\| \frac{AQ_1A}{w} + \frac{AQ_0A}{w^2} \right\| = O(1/w). \]

Again, if \(Q_1 = \alpha A^* \) (\(\Leftrightarrow AQ_1A = \alpha A\)), we obtain an \(O(1/w^2)\) convergence through the evaluation

\[ \frac{A}{w^2} - \frac{\alpha A}{w^2} + \frac{AQ_0A}{w^4} = A \left( \frac{1}{w} - \frac{\alpha}{2w^2} \right)^2 + \frac{\alpha^2 A}{4w^4} + \frac{AQ_0A}{w^4} \]

so that the distance from \(A_w/(1/w - \alpha/2w^2)^2\) to \(A\) has order \(O(1/w^2)\).

**Remark 4.3.** Since \(\lim_{w \to \infty} \left( \frac{1}{w} - \frac{\alpha}{2w^2} \right)^2 = 1\), we have:

\[ \left( A_w/(1/w - \alpha/2w^2)^2 \right)^{-1} \approx A_w^*/(w + \alpha/2)^2. \]
We can now prove our main theorem concerning the convergence analysis of projection lattices sequences.

**Theorem 4.4.** Let $\Lambda$ be an $n$-dimensional lattice with generator matrix $\bar{G}$ and Gram matrix $A$ and $\Lambda^* \subseteq \mathbb{Z}^n$ its dual with generator and Gram matrices $\bar{G}^*$ and $A^*$ respectively. Now, let $\Lambda_w^*$ be the sequence of lattices with generator matrices given by (5) satisfying:

$$\det(H_w) = \pm 1, \forall w \in \mathbb{N} \text{ and}$$

$$\exists \alpha \text{ such that } Q_1 = \alpha A^*, \quad (10)$$

with $H_w$, $A_w^*$, $Q_1$ as previously defined and $A_w = (A_w^*)^{-1}$. Then each $\Lambda_w^*$ is a projection lattice of $\mathbb{Z}^{n+1}$ onto the orthogonal subspace of a vector $v_w \in \mathbb{Z}^{n+1}$ whose infinity norm satisfies

$$\|v_w\|_\infty = \sqrt{\det \Lambda^* w^n + O(w^{n-1})} \quad (11)$$

for sufficiently large $w$, and there exists a $c_w \in \mathbb{R}$ such that

$$\|A - c_w A_w\|_\infty = O\left(\frac{1}{w^2}\right) = O\left(\frac{1}{\|v_w\|_{\infty}^{2/n}}\right) \to 0, \text{ as } w \to \infty. \quad (12)$$

**Proof.** We will first show the validity of the Equation (11) and then (12) will hold for $c_w = (1/w - \alpha/2w^2)^2$ provided Lemma 4.2 and previous arguments. Let $\vec{v}_w$ be the generalized cross product of the rows of $G_w^*$ (see [5]) i.e., $(\vec{v}_w)_i = (-1)^{n+i} |(G_w^*)_i|$, where $|(G_w^*)_i|$ denotes the determinant of the matrix obtained excluding the $i$-th column of $G_w^*$. According to Lemma 4.1 the projection vector $v_w$ will be given by $v_w = (1, -\hat{v}_w)$ for

$$\hat{v}_w = (H_w)^{-1}(G_w^*)_1 \Rightarrow (G_w^*)_1 = H_w \hat{v}_w = -\sum_{j=2}^{n} (v_w)_j (G_w^*)_j.$$

Hence:

$$|(G_w^*)_i| = \det \begin{bmatrix} -\sum_{j=2}^{n} (v_w)_j (G_w^*)_j & (G_w^*)_2 & \ldots & (G_w^*)_i & \ldots & (G_w^*)_n \end{bmatrix}$$

$$= \det \begin{bmatrix} -(v_w)_i (G_w^*)_i & (G_w^*)_2 & \ldots & (G_w^*)_i & \ldots & (G_w^*)_n \end{bmatrix}$$

$$= (-1)^{i} |H_w| (v_w)_i \quad \therefore \quad \hat{v}_w = (-1)^{n} |H_w| v_w.$$
where $\left(G_w^*\right)_i$ means the exclusion of the $i$-th column from the matrix. Thus, up to a change of sign, the projection vector is the cross product of the rows of $G^*_w$. Considering that, it is easy to show that each entry of $v_w$ is a polynomial of degree up to $n - 1$, excepting for the last one, whose absolute value is $|\det(G^*_w)_n|$ or $|(v_w)_n| = |\det(wG^* + (P)_n)| = |w^n \det G^* + O(w^{n-1})|$ and this completes the proof.

In what follows, we show that the vectors $v_w$, the densities of the projection lattices and the convergence rate of the sequence $\|A - c_w A_w\|_\infty$ do not depend on the basis choice for $\Lambda^*$.

**Proposition 4.5.** Let $G^*_1$ and $G^*_2$ be two generator matrices for $\Lambda^*$ with $A^*_1$ and $A^*_2$ the correspondent Gram matrices. Let $G^*_1 = \left[G^*_1 \ 0_{n \times 1}\right]$ and $G^*_2 = \left[G^*_2 \ 0_{n \times 1}\right]$. Now, take the sequence of lattices $\Lambda^*_w, 1$ associated to the generator matrices $G^*_w, 1 = wG^*_1 + P_1$ and let $H^*_w, 1 = (G^*_w, 1)_{(1, \ldots, n), (2, \ldots, n+1)}$ such that conditions (9) and (10) hold. There exists $P_2 \in \mathbb{Z}^{n \times (n+1)}$ such that the sequence $G^*_w, 2 = wG^*_2 + P_2$ satisfies conditions (9), (10) and

$$H^{-1}_{w, 1} G^*_1 = H^{-1}_{w, 2} G^*_2. \quad (13)$$

**Proof.** Since $G^*_1$ and $G^*_2$ generate the same lattice, there exists an unimodular matrix $U$ such that $G^*_1 = U G^*_2$. We will show that $P_2 = U^{-1}P_1$ satisfies the three properties above.

For condition (9), we have:

$$G^*_2 P^t_2 + P^*_2 G^*_1 = U^{-1} G^*_1 P^t_1 U^{-t} + U^{-1} P^*_2 G^*_1 U^{-t} =$$

$$= U^{-1}(G^*_1 P^t_1 + P_1 G^*_1 t) U^{-t} = \alpha U^{-1} A^*_1 U^{-t} = \alpha A^*_2. \quad (14)$$

For condition (10) and Equation (13), just observe that $H^*_w, 2 = U^{-1} H^*_w, 1$.

Although the search for good sequences is independent of the basis choice, distinct representations (i.e., geometrically similar) for the same lattice can yield substantially different sequences in terms of the densities of $\Lambda_w$ and the norm of each $v_w$, as shown in Equation (11) and illustrated in examples 3.1 and 3.4.
When there is no perturbation matrix such that $Q_1 = \alpha A^*$, the convergence of the sequence $A_w/w^2$ is related to the coefficient $A(Q_1 - \alpha A^*)A$. We can thus try the solution of the problem

$$\min \| A(G^*P^t + PG^*t - \alpha A^*)A \|$$

s. t. $| \det H_w | = 1$, $\forall w \in \mathbb{N}$

$$P \in \mathbb{Z}^{n \times (n+1)}$$

$$\alpha \in \mathbb{Z}$$

which is a non-linear problem of $n^2 + n$ integer variables. In fact, the constraint $\alpha \in \mathbb{Z}$ can be relaxed to $\alpha \text{gcd}((A^*)_{ij}) \in \mathbb{Z}$ and the complexity of this problem is mainly caused by the constraint $| \det H_w | = 1$. Hence, sometimes it is worth considering sub-optimal solutions. One possibility is to take a lower triangular matrix $G^*$ and consider the problem:

$$\min \| A(G^*P^t + PG^*t - \alpha A^*)A \|$$

s. t. $P \in \mathbb{Z}^{n \times (n+1)}$

$$P_{ij} = 1, \text{ if } j = i + 1$$

$$P_{ij} = 0, \text{ if } j > i + 1,$$

with $\alpha$ constrained as above. In this case, the perturbation matrix $P$ will have the structure

$$P = \begin{bmatrix}
P_{11} & 1 & 0 & \cdots & 0 & 0 \\
P_{21} & P_{22} & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
P_{n1} & P_{n2} & P_{n3} & \cdots & P_{nn} & 1
\end{bmatrix}$$

and we can drop the constraint $| \det H_w | = 1$ out.
5 Explicit Constructions

In the following examples we employ different strategies to generate the projection lattices families, depending on the structure of each target lattice and the feasibility of finding integer solutions satisfying conditions (9) and (10) or solving the non-linear problem (16).

5.1 The lattice $a\mathbb{Z} \oplus b\mathbb{Z}$

As a first example, consider the lattice generated by the matrix $\bar{G} = \begin{pmatrix} 1 & ab \\ \end{pmatrix} \text{diag}(a,b), \ a,b \neq 0$, a scaled version of the $\mathbb{Z}^2$ lattice. We can assume w.l.o.g. that $(a,b) = 1$. As a generator matrix for its dual, we choose $\bar{G}^* = \text{diag}(a,b)$, and hence, taking a general perturbation $P$, we have:

$$G_w = \begin{bmatrix} aw + P_{1,1} & P_{1,2} & P_{1,3} \\ P_{2,1} & bw + P_{2,2} & P_{2,3} \end{bmatrix}$$  \quad (17)

In this case, the condition (10) is equivalent to:

$$P_{11} = \frac{a\alpha}{2}, P_{21} = -\frac{bP_{12}}{a} \text{ and } P_{22} = \frac{ab}{2}$$  \quad (18)

Since $a$ and $b$ have no common factors, $\alpha$ must be even ($\alpha = 2\beta, \text{ for } \beta \in \mathbb{Z}$) and $P_{12} = ka$. Under these conditions, we calculate the determinant of $H_w$:

$$\det(H_w) = akP_{23} - b\beta P_{13} - bwP_{13}$$  \quad (19)

and condition (9) will be satisfied iff

$$P_{13} = 0 \text{ and } akP_{23} = \pm 1.$$  \quad (20)

Hence, by Theorem (4.4), any lattice of the form $\mathbb{Z} \oplus b\mathbb{Z}, b \neq 0$ can be recovered as a sequence (5) or projection lattices whose order of convergence is $O(1/\|v\|)$, while for $a \neq 1$ it is not possible to find a perturbation matrix such that the hypotheses of Theorem (4.4) hold.

As an interesting consequence of this fact, it is not possible to ensure conditions (9) and (10) to the Example 1 of [4] scaled by 1/2 i.e., for $a = 2$ and $b = 1$. Nevertheless, for the equivalent lattice $\Lambda = (1/2)\mathbb{Z} \oplus 2\mathbb{Z}$
and its dual $\Lambda^* = \mathbb{Z} \oplus 2\mathbb{Z}$, the sequence of projection lattices associated to the dual of the lattices generated by the matrices

$$G_w^* = \begin{bmatrix} w + c & 1 & 0 \\ -2 & 2w + 2c & 1 \end{bmatrix}, \quad c \in \mathbb{Z} \tag{21}$$

and projection vectors $v_w = [1, -w - c, 2w^2 + 4wc + 2c^2 + 2]$ converges to $\Lambda$ at rate $O(\|v\|)$.

5.2 The lattice $D_n$ (for odd $n$)

A possible $O(1/w^2)$ convergence is shown in [3] for $n = 3$. We here extend this result for any odd $n$. As the matrix $G^*$ (generator matrix for $2D_n^*$ with a zero column added to the right) we choose:

$$G^* = \begin{bmatrix} 2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 2 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 2 & 0 & 0 \\ 1 & 1 & \cdots & 1 & 0 & \end{bmatrix}$$

We have then the following proposition:

**Proposition 5.1.** There is a sequence of projection lattices that converges to a lattice which is equivalent to $D_n$, for odd $n$, at the rate $O(1/\|v\|^{2/n})$.

**Proof.** The proof follows by choosing a suitable perturbation matrix. In this case, take $P$ such that

$$P_{ij} = \begin{cases} (-1)^i & \text{if } j = n - i \text{ and } 1 \leq i \leq n, \\ (-1)^{i+1} & \text{if } j = n - i + 2 \text{ and } 2 \leq i \leq n - 1, \\ 1 & \text{if } (i, j) \in \{(n-1, n+1), (n, n+1)\} \\ 1 & \text{if } (i, j) = (1, n) \\ 0 & \text{otherwise} \end{cases} \tag{22}$$

By direct multiplication, one can prove that $G^* P^t + P G^{*t} = 0$ and by elementary operations on the matrix $H_w$ it is possible to prove that $\det H_w = 1 \forall w$ provided that $n$ is an odd number, thus ensuring that the hypotheses of Theorem (4.4) hold and the result follows. $\square$
To illustrate this example, we exhibit below the matrices $G_w^*, A_w^*$ and $P$ as well as the vector $v_w$ for $n = 5$.

$$G_w^* = \begin{bmatrix} 2w & 0 & 0 & -1 & 1 & 0 \\ 0 & 2w & 1 & 0 & -1 & 0 \\ 0 & -1 & 2w & 1 & 0 & 0 \\ 1 & 0 & -1 & 2w & 0 & 1 \\ w & w & w & w & w & 1 \end{bmatrix} \quad (23)$$

$$A_w^* = \begin{bmatrix} 4w^2 + 2 & -1 & -1 & 0 & 2w^2 \\ -1 & 4w^2 + 2 & 0 & -1 & 2w^2 \\ -1 & 0 & 4w^2 + 2 & 0 & 2w^2 \\ 0 & -1 & 0 & 4w^2 + 3 & 2w^2 + 1 \\ 2w^2 & 2w^2 & 2w^2 & 2w^2 + 1 & 5w^2 + 1 \end{bmatrix},$$

$$P = \begin{bmatrix} 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and $v_w = \begin{bmatrix} 1 \\ 4w^3 + 2w^2 + 3w + 1 \\ -4w^3 + 2w^2 - 3w + 1 \\ 8w^4 + 8w^2 + w + 1 \\ 8w^4 + 8w^2 - w + 1 \\ 16w^5 + 20w^3 + 5w \end{bmatrix}$

Remark 5.2. For $n = 3$ and a suitable change of basis, the perturbation given by Equation (23) is precisely the same as the one described in [3], Section 4.

5.3 $D_n^*$

Here is a case where $\alpha \neq 0$ is actually necessary. Let us start with the lattice $D_3^*$. As a basis to $(D_3^*)^* = D_3$ we take:

$$\tilde{G}^* = \begin{bmatrix} -2 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{bmatrix}, \quad (24)$$
and we want to find a perturbation matrix \( P \in \mathbb{Z}_{3 \times 4} \) in order to ensure conditions (9) and (10) of Theorem (4.4). Again, starting with a general perturbation, condition (9) with \( \alpha = 0 \) is equivalent to:

\[
P_{11} = 0, P_{12} = -2P_{23} + 2P_{31} - 2P_{33}, P_{21} = P_{23} - P_{31} + P_{33},
\]

\[
P_{22} = P_{23} - P_{31} + P_{33}, P_{13} = -2P_{23} - 2P_{33}, P_{32} = P_{33}
\]

Besides, by explicit calculating the determinant of \( H_w \) (which is a polynomial of degree 2 in \( w \)), it is easy to show that \( P_{1,4} \) (coefficient of \( w^2 \)) must vanish. Under that condition, we have:

\[
H_w = \begin{bmatrix}
-2P_{23} + 2P_{31} - 2P_{33} & -2P_{23} - 2P_{33} & 0 \\
-w + P_{23} - P_{31} + P_{33} & P_{23} & P_{24} \\
w + P_{33} & P_{33} - w & P_{34}
\end{bmatrix}
\]

and clearly \( \det H_w \) is even i.e., \( \det H_w \neq \pm 1 \) what shows that there is no \( P \) such that, for \( \alpha = 0 \), the conditions (9) and (10) simultaneously hold. However, following an analogous argument for \( \alpha = 1 \), we find the perturbation matrix:

\[
P = \begin{bmatrix}
-1 & 1 & 1 & 0 \\
0 & -1 & 0 & 1 \\
0 & 0 & -1 & -2
\end{bmatrix}
\]

We extended this result for any \( n \) through the following proposition:

**Proposition 5.3.** There is a sequence of projection lattices that converges to \( D^*_n \) for any \( n \geq 1 \) at the rate \( O(1/\|\psi\|^2/n) \).

**Proof.** Here, the perurbation matrix is given by

\[
P_{ij} = \begin{cases} 
(-1)^i \binom{n-1}{i-1} & \text{if } j = n+1 \text{ and } i \geq 2, \\
-1 & \text{if } i = j, \\
1 & \text{if } i = 1 \text{ and } j \leq n, \\
0 & \text{otherwise}
\end{cases}
\]

Again, by direct multiplication we can see that \( G^*P^t + PG^*t = A^* (\alpha = 1) \) and by applying elementary operations to the matrix \( H_w \) we see that \( \det H_w = (-1)^{n+1} \) proving the statement. \( \square \)
For \( n = 3 \) the projection family associated to the vectors
\[
\mathbf{v}_w = [1, -2w^2 + w + 1, -2w^2 - 3w - 2, 2w^3 + 3w^2 + 3w + 1]
\]
converges to the famous body-centered cubic lattice, which has the best covering density in three dimensions \([3]\), at a rate \( O(1/\|\mathbf{v}\|^{2/3}) \).

5.4 The lattice \( E_8 \)

For the lattice \( E_8 \), the problem of finding a perturbation matrix that speeds the convergence rate up to \( O(1/w^2) \) has 72 integer variables. After some simplifications (by explicitly solving equation (9)) we can reduce this problem to 36 integer variables and 7 non-linear restrictions, corresponding to the polynomial equality (10), which has a high computational complexity. We do not know if there exists an exact solution to this problem. Hence, we generate sub-optimal solutions, considering the problem (16) and the Frobenius norm, which yields to a quadratic integer problem (IQP), and show that these solutions have good (exponential) gains in comparison to the sequences in \([3]\). We also compare different equivalent integer representations for the \( E_8 \) lattice. It is worth reminding that \( \|M\|_F \geq \|M\|_\infty \) for any matrix \( M \).

The first representation for \( \Lambda^* = E_8 \) is the matrix \([1\text{, p. 121}]\), the same as in \([3]\). The second one is the matrix obtained by applying Construction A \([1\text{, ch.5}]\) to the extended Hamming code \( \mathcal{H}(8, 4) \) \([1\text{, ch 3, sec 2.3}]\). We show the perturbation matrices found in both cases (respectively, \( P_1 \) and \( P_2 \)) and compare the curves of center density versus the the logarithm to the basis 2 of the euclidean norm of the projection vector (Figure 4). For all these constructions, the rate of convergence of the produced sequences is \( O(1/w) \).
In this paper we address the problem of finding sequences of projection lattices with a good rate “density versus length of the projection vector”. With a subtle modification of the Lifting Construction [4], we prove a sufficient condition for constructing projection lattices sequences that converge with order $O(1/\|v\|^{2/n})$ to target lattices whose dual are integer. We then construct explicit examples of such sequences for some well-known lattices, such as $D_n$ (odd $n$) and $D^*_n$. We also show examples of good projection lattices sequences for the $E_8$ lattice that do not satisfy condition (10).

The question whether it is always possible to speed the convergence rate up to $O(1/\|v\|^{2/n})$ remains open. Also explicit constructions for $D_n$ (even $n$) as well as other important lattices are let for further work. These constructions, however, seem to require totally different techniques. For instance, it is possible to verify computationally through an exhaustive

\[ P_1 = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & -1 & -1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & -1 & -1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
\end{bmatrix}, \]

\[ P_2 = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & -1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 1 \\
\end{bmatrix}. \]
Figure 1: The first two curves from the bottom to the top were obtained with the same generator matrix for $E_8$ as in [3] and perturbation matrices $[0 I_8]$ and $P_1$, respectively. The last two correspond to representation $G_2$ above and perturbation matrices $[0 I_8]$ and $P_2$, respectively.

search that there is no simultaneous solution for equations (9) and (10) for the lattice $D_4$.

We finish by exhibiting a table of which is, to our knowledge, the best projection lattices sequences in dimensions from 3 to 8, in the sense discussed in this paper (except $n = 6$).

Acknowledgments

The authors would like to thank the anonymous referees for pointing out some mistakes in the first version of the paper. The authors also acknowledge Prof. Sueli Costa for fruitful discussions on projection lattices. This work was supported by São Paulo Research Foundation (FAPESP) under grant 2009/18337-6 for Antonio Campello and 2011/01096-6 for João Strapasson.

To our knowledge, there is no integer representation in $\mathbb{R}^6$ for the best 6-dimensional lattice packing $E_6$, hence the approach here cannot be employed. The projections of $\mathbb{Z}^7$ onto $v^\perp$ for the vector presented here converge to $D_6$. 

1
Table 2: Best families of projection lattices of $\mathbb{Z}^{n+1}$ $n = 3$ to 8 (except $n = 6$), converging to the target lattice $\Lambda$.

| $n$ (A) | Vector |
|-----|--------|
| 3 ($D_3$) | $(1,2w^2 + w + 1,2w^2 - w + 1,-4w^3 - 3w)$ |
| 4 ($D_4$) | $(1, -1 + 2w, 4w^2 - 2w + 1,8w^3 - 4w^2 + 1,8w^4 - 8w^3 + 4w^2)$ |
| 5 ($D_5$) | $(1,4w^3 + 2w^2 + 3w + 1,-4w^3 + 2w^2 - 3w + 1,8w^4 + 8w^3 + 8w^2 - w + 1,16w^5 + 20w^4 + 5w)$ |
| 6 ($D_6$) | $(1,2w - 1,4w^2 - 2w + 1,8w^3 - 4w^2 + 1,16w^4 - 8w^3 + 4w^2 + 1,32w^5 - 16w^4 + 4w^2 + 2w - 1,32w^6 - 32w^5 + 16w^4 + 2w^2 - 2w + 1)$ |
| 7 ($E_7$) | $(1,1 - 2w, 4w^2 - 4w + 2,-8w^3 + 12w^2 - 10w + 3,8w^4 - 16w^3 + 18w^2 - 10w + 2,-8w^5 + 16w^4 - 30w^3 + 28w^2 - 16w + 4,8w^6 - 16w^5 + 38w^4 - 44w^3 + 36w^2 - 16w + 3,-8w^7 + 16w^6 - 46w^5 + 60w^4 - 70w^3 + 50w^2 - 24w + 5)$ |
| 8 ($E_8$) | $(1,-2w,4w^2,-8w^3,16w^4 + 8w^3 - 2w,-16w^5 - 8w^4 - 4w^3 + 4w^2 + w,16w^6 + 8w^5 + 12w^4 - 3w^2,-16w^7 - 8w^6 - 28w^5 + 7w^3 + 6w^2,16w^8 + 8w^7 + 44w^6 + 8w^5 - 3w^4 - 10w^3 - 3w^2 + w)$ |

References

[1] J. H. Conway and N. J. A. Sloane, *Sphere-packings, lattices, and groups*, Springer-Verlag, New York, NY, USA, 1998.

[2] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*, Society for Industrial Mathematics (SIAM), Philadelphia PA, USA, 2000.

[3] N. J. A. Sloane, V. Vaishampayan, and S. I. R. Costa, *A note on projecting the cubic lattice*, Discrete & Computational Geometry 46 (2011), 472–478.

[4] N. J. A. Sloane, V. A. Vaishampayan, and S. I. R. Costa, *The lifting construction: A general solution for the fat strut problem*, IEEE international symposium on information theory proceedings (isit), 2010, pp. 1037–1041.

[5] M. Spivak, *Calculus on manifolds: A modern approach to classical theorems of advanced calculus*, Westview Press, New York, NY, 1971.

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