Electronic Colloquium on Computational Complexity, Report No. 113 (2004)

ECCC

Lattices with Many Cycles Are Dense

Mårten Trolin

Department of Numerical Analysis and Computer Science,
Royal Institute of Technology, Stockholm, Sweden
marten@nada.kth.se

Abstract We give a method for approximating any n-dimensional lattice with a lattice Λ whose factor group $\mathbb{Z}^n/\Lambda$ has $n-1$ cycles of equal length with arbitrary precision. We also show that a direct consequence of this is that the Shortest Vector Problem and the Closest Vector Problem cannot be easier for this type of lattices than for general lattices.
Keywords: lattices, shortest vector problem, closest vector problem

1 Introduction

The interest in the computational complexity of lattice problems started in the beginning of the 1980s, when van Emde Boas published the first **NP**-completeness result for lattice problems [18]. Several hardness results for different variants of this problems and for different subsets of lattices have followed. One such way of classifying lattices is according to the cycle structure of Abelian group $\mathbb{Z}^n/\Lambda$, which is the main focus of this paper. Previous results on the complexity of lattice problems that either explicitly or implicitly consider lattices with a certain cycle structure include [1,3,15,17].

There are two reasons to study the hardness of certain lattice problems in different subclasses of lattices rather than for general lattices. The first reason is purely theoretical — it gives us a better understanding of how the computational complexity of lattice problems behaves if we restrict ourselves to certain lattice classes. The second reason is more practical — most hardness results are worst-case results for general lattices. The lattices that appear in many applications may have certain structural properties. It would be desired to have results that show that these properties cannot be used to solve lattice problem more efficiently.

The first result on the cycle structure was published by Paz and Schnorr [15]. In that paper it is shown that any lattice can be approximated arbitrarily well by a lattice with one cycle. In other words, the lattices with one cycle form a hard core. On the other hand, the lattices Cai and Nerurkar [3] prove to be hard in the improved version of Ajtai [1] have up to n/c cycles. Although the results are different in nature (the latter is not an **NP**-hardness result), it is interesting to note that they give hardness results for lattices with different cycle structure. This gives rise to the question of the role of the cycle structure in the complexity of lattice problems.

ISSN 1433-8092

The influence of the cycle structure on the hardness of lattice problems has practical implications. For some crypto systems (e.g., NTRU [7]) there are attacks based on finding short vectors in certain lattices. The lattices used in some of these attacks have a cycle structure that differs from the cycle structure of the lattices that previously have been shown to be **NP**-hard.

Since a lattice with n cycles always can be transformed into a lattice with fewer cycles by a simple rescaling, the maximum number of cycles that is meaningful to analyze is $n-1$. Trolin showed that the exact version SVP under the max-norm is **NP**-complete for n-dimensional lattices with $n-1$ cycles of equal length [17].

In this paper we investigate the importance of the cycle structure further. Our main result is a polynomial-time transformation that with arbitrary precision approximates any n-dimensional lattice with a lattice that has $n-1$ cycles of equal length, showing that these lattices form a hard core. A consequence of this is that short vectors and close vectors cannot be computed more efficiently in this class of lattices than in general lattices, except possibly for a polynomial factor. As our transformation only changes the size of the coordinates of the basis vectors and not the dimension of the lattice, the transformation is rather tight.

2 Background

2.1 Lattices

A *lattice* is a discrete additive subgroup $\Lambda \subseteq \mathbb{R}^n$. A lattice Λ can be defined by its basis, a set of independent vectors $\{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_m}\}$, $\mathbf{b_i} \in \mathbb{R}^n$, such that $\mathbf{u} \in \Lambda$ if and only if there exist integers $t_1, t_2, \ldots, t_m$ such that $\mathbf{u} = \sum_{i=1}^{m} t_i \mathbf{b_i}$. If $m = n$ the lattice is said to be full-dimensional. Only lattices that are subsets of $\mathbb{Q}^n$ (and often $\mathbb{Z}^n$) are considered in this paper. For each vector $\mathbf{v} \in \mathbb{R}^n$ and $p \geq 1$ the ℓ_p-norm is defined as $\|\mathbf{v}\|_p = \sqrt[p]{\sum_{i=1}^{n} |v_i|^p}$. The ℓ_∞-norm, also called the maximum norm, is defined as $\|\mathbf{v}\|_\infty = \max_{i=1}^{n} |v_i|$. When no index is given, $\|\mathbf{v}\| = \|\mathbf{v}\|_2$.

A *basis matrix* of a lattice is a matrix whose rows form a basis of the lattice. The *determinant* of a lattice is the absolute value of the determinant of a basis matrix. For lattices that are not full-dimensional, the determinant is defined as $\det(\Lambda) = \sqrt{\det(\mathbf{B}\mathbf{B}^T)}$. It is not difficult to see that the determinant is independent of the choice of basis.

2.2 Basis representations

In different situations different bases may be suitable. Two such representations are the Hermite Normal Form and LLL-reduced bases.

A basis $\{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}\}$ is said to be on Hermite Normal Form (HNF) if the basis matrix is upper triangular, and $b_{ii} > b_{ji} \geq 0$ for $j < i$. The Hermite Normal Form can be computed efficiently [8]. In [12] Micciancio gives some results on the use of HNF in cryptographic applications.

An LLL-reduced basis is defined as follows. Every lattice basis $\{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_m}\}$ has an associated *orthogonal* basis $\left\{\hat{\mathbf{b}}_\mathbf{1}, \hat{\mathbf{b}}_\mathbf{2}, \ldots, \hat{\mathbf{b}}_\mathbf{m}\right\}$ defined by

$$\hat{\mathbf{b}}_\mathbf{i} = \mathbf{b_i} - \sum_{j=1}^{i-1} \mu_{ij} \hat{\mathbf{b}}_\mathbf{i}$$

where $\mu_{ij} = \left\langle \mathbf{b_i}, \hat{\mathbf{b}}_\mathbf{j} \right\rangle / \left\| \hat{\mathbf{b}}_\mathbf{j} \right\|^2$ for $i > j$. Extending the definition, we let $\mu_{ii} = 1$ and $\mu_{ij} = 0$ for $i < j$. It holds that $\prod_{i=1}^{m} \left\| \hat{\mathbf{b}}_\mathbf{i} \right\| = \det(\Lambda)$. A lattice basis is called *LLL-reduced* (after Lenstra, Lenstra and Lovász) with δ, $1/4 \leq \delta < 1$, if $|\mu_{ij}| \leq 1/2$ for $1 \leq j < i \leq m$ and $\delta \left\| \hat{\mathbf{b}}_{\mathbf{i-1}} \right\|^2 \leq \left\| \hat{\mathbf{b}}_\mathbf{i} \right\|^2 + \mu_{i,i-1}^2 \left\| \hat{\mathbf{b}}_{\mathbf{i-1}} \right\|^2$ for $i = 2, \ldots, m$. An LLL-reduced basis can be found in polynomial time [11].

The two most studied lattice problems are the closest vector problem, CVP, and the shortest vector problem, SVP. The input to the closest vector problem is a lattice Λ, $\mathbf{y} \in \mathbb{R}^n$ and $d > 0$. The problem is to determine whether or not there exists $\mathbf{x} \in \Lambda$ such that $\|\mathbf{y} - \mathbf{x}\| < d$. SVP is the homogeneous variant of the same problem, where we want to determine whether or not there exists $\mathbf{x} \in \Lambda$ such that $0 < \|\mathbf{x}\| < d$. As a matter of fact, these are both families of problems, since every norm gives a different problem.

It is known that CVP is **NP**-complete for any ℓ_p-norm (including the max-norm, ℓ_∞) [18] and that it is **NP**-hard to approximate within $n^{\frac{c_p}{\log \log n}}$ for some constants c_p [5]. It is also known that SVP is **NP**-complete in the ℓ_∞-norm [10] and under randomized reductions also for any ℓ_p-norm [2]. It has been shown that SVP is **NP**-hard to approximate within any factor smaller than $\sqrt{p}$ under randomized reductions [13] in ℓ_p-norm. Khot has improved that inapproximability bound to $p^{1-\varepsilon}$ for large values of p under randomized reductions [9] and Dinur has improved the bound for ℓ_∞-norm to $n^{1/\log \log n}$ [4].

2.3 The cycle structure

In this paper we focus on the role of the *cycle structure* of a lattice in the complexity of lattice problems. The cycle structure is defined as the algebraic structure of the group $\mathbb{Z}^n/\Lambda$ for a full-dimensional lattice Λ.

Definition 1 (Cycle structure). *A lattice Λ is said to have the* cycle structure *$k_1 \times k_2 \times \cdots \times k_m$, if the additive factor group $\mathbb{Z}^n/\Lambda \sim \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_m}$ and k_i divides k_{i+1} for $i = 1, 2, \ldots, m-1$.*

Cycles of length one are called trivial. In the cases where it is not clear from the context we specify whether non-trivial cycles should be considered. A lattice with only one non-trivial cycle is called *cyclic*. Depending on context, it may be more convenient to number the cycle lengths in increasing or decreasing order.

There are other ways to look upon the cycle structure that may be useful in certain situations. One is to consider the Smith Normal Form [16] of a basis

matrix, and another to examine the set of modular equations whose solutions are precisely the lattice points.

Definition 2 (Smith Normal Form). *Let* $\mathbf{B}$ *be an integral square matrix. The* Smith Normal Form, SNF*, of* $\mathbf{B}$ *is the diagonal matrix* $\mathbf{S}$ *are such that* $\mathbf{S} = \mathbf{UBV}$*, with* $\mathbf{U}$ *and* $\mathbf{V}$ *integral and* $|\det(\mathbf{U})| = |\det(\mathbf{V})| = 1$ *and diagonal elements* s_i *of* $\mathbf{S}$ *such that* s_{i+1}/s_i *all are integers.*

Such a diagonal matrix exists for every integral square matrix, see, e.g., [14]. The following theorem from [15] shows the relation between the Smith Normal Form and the cycle structure.

Theorem 1. *Let* Λ *be an* n*-dimensional lattice, and let* $\mathbf{B}$ *be a basis matrix of* Λ*. Let* $\mathbf{S}$ *be the Smith Normal Form of* $\mathbf{B}$*. Let the diagonal elements of* $\mathbf{S}$ *be* $s_1, s_2, \ldots, s_n$*. Then the cycle structure of* Λ *is* $s_1 \times s_2 \times \cdots \times s_n$*.*

We also give a theorem showing a connection between the subdeterminants of a lattice and its Smith Normal Form. An i-minor of $\mathbf{B}$ is an $i \times i$ matrix formed by taking i rows and i columns of $\mathbf{B}$.

Theorem 2. *Let* $\mathbf{B}$ *be an integral square matrix. Then the diagonal elements of the Smith Normal Form,* $s_1, s_2, \ldots, s_n$ *can be computed as*

$$s_i = \frac{d_i}{d_{i-1}}$$

where d_i *is* gcd *of the determinants of all* i*-minors of* $\mathbf{B}$*, and* $d_0 = 1$*.*

Although this method of computing the Smith Normal Form and hence the cycle structure is quite inefficient (we need consider all the i-minors, not only the principal), it turns out to be useful in certain proofs in this paper. There are other, more efficient methods to compute the Smith Normal Form [8].

Another way to describe the number of cycles of a lattice is to use a different representation of the lattice, namely as a set of modular equations. Every lattice can be described in this way.

Theorem 3. *Let* $\Lambda \subseteq \mathbb{Z}^n$ *be a lattice. Then there exist* n*-dimensional vectors* $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_m}$ *and integers* $b_1, b_2, \ldots, b_m$*,* $b_i > 1$*, such that*

$$\Lambda = \{\mathbf{x} : \langle \mathbf{a_1}, \mathbf{x} \rangle \equiv 0 \bmod b_1 \wedge \langle \mathbf{a_2}, \mathbf{x} \rangle \equiv 0 \bmod b_2 \wedge \ldots \wedge \langle \mathbf{a_m}, \mathbf{x} \rangle \equiv 0 \bmod b_m\} \ .$$

The essence of this theorem is that any lattice can be expressed as a system of modular linear equations whose solutions form the lattice.

The connection to the cycle structure is that the number of nontrivial cycles is m, and the length of cycle i is b_i, provided that the system of equations has been reduced to minimize the number of equations and that the gcd of the coefficients and the modulus is 1 in each equation.

In the transformations we approximate lattices in $\mathbb{Z}^n$ with lattices in $\mathbb{Q}^n$. The standard definition of cycle structure cannot be applied to general lattices

in $\mathbb{Q}^n$. Since multiplication by a constant does not affect lattice problems such as SVP and CVP, we will define the cycle structure of a lattice $\Lambda \subset \mathbb{Q}^n$ as the cycle structure of $k\Lambda$, where k is the smallest integer such that $k\Lambda \subseteq \mathbb{Z}^n$.

We now state three simple lemmas on the cycle structure. They follow directly from Theorem 1.

Lemma 1. *Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice with cycle structure $k_1 \times k_2 \times \cdots \times k_m$. Then* $\det(\Lambda) = \prod_{i=1}^{m} k_i$.

Lemma 2. *Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice with cycle structure $k_1 \times k_2 \times \cdots \times k_n$ (not necessarily all nontrivial). Then the lattice $t \cdot \Lambda$ has cycle structure $t \cdot k_1 \times t \cdot k_2 \times \cdots \times t \cdot k_n$*

Lemma 3. *Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice with cycle structure $k_1 \times k_2 \times \cdots \times k_n$, $k_1 \geq k_2 \geq \cdots \geq k_n$. Then the lattice $\frac{1}{k_n} \cdot \Lambda$ has cycle structure $\frac{k_1}{k_n} \times \frac{k_2}{k_n} \times \cdots \times \frac{k_n}{k_n}$.*

Because of the divisibility requirement, the lattice $\frac{1}{k_n}\Lambda$ in Lemma 3 is in $\mathbb{Z}^n$. Should k_n be greater than one, we can always remove it as shown in the theorem. Hence we can assume without loss of generality that the number of cycles is less than n.

2.4 Previous results on the cycle structure

In [15] the following theorem is proved.

Theorem 4. *Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice. Then for every $\varepsilon > 0$ we can efficiently construct a linear transformation $\sigma_{\Lambda,\varepsilon} : \Lambda \to \mathbb{Z}^n$ such that $\sigma_{\Lambda,\varepsilon}(\Lambda)$ is a lattice and for some integer k*

1. $\forall \mathbf{u} \in \Lambda : \|\mathbf{u} - \sigma_{\Lambda,\varepsilon}(\mathbf{u})/k\| \leq \varepsilon \|\mathbf{u}\|$
2. *$\sigma_{\Lambda,\varepsilon}(\Lambda)$ is cyclic.*

This theorem implies that if we can solve a lattice problem for cyclic lattices, we can get an approximative solution for the same problem for any with arbitrary precision. In other words, the cyclic lattices form a hard core.

In his celebrated paper [1], Ajtai showed how to generate lattices with a connection between the average case and the worst case of variants of SVP. The lattices in the constructions in Cai's and Nerurkar's improved version of Ajtai's result [3] have n/c cycles. Although this result is not an **NP**-hardness result, it raises the question of whether the hardness of lattice problems does or does not in general decrease with a higher number of cycles. In [17] it is shown that SVP in the maximum norm is **NP**-complete for lattices with $n-1$ cycles, giving further evidence that hardness results of lattice problems extend to many cycle structures. The result of the current paper gives the main result of [17] as a consequence.

3 The approximation

Let $\Lambda \subseteq \mathbb{Z}^n$ be an arbitrary lattice. To adapt this into a lattice with $n-1$ cycles that is arbitrarily close to the original lattice we go through the following five steps:

1. Inflate the lattice by a factor k and perturb to achieve a lattice with Hermite Normal Form of a certain form.
2. Reduce the sublattice spanned by the first $n-1$ vectors of the Hermite Normal Form using the LLL algorithm.
3. Factor the partly reduced basis matrix into two matrices, where the second has its determinant equal to one.
4. Perform modifications to the first matrix to give it $n-1$ cycles of equal length.
5. Multiply the two matrices to get a basis for an $(n-1)$-cyclic lattice that is close to the original lattice.

In Sections 3.1 to 3.4 these steps are described in detail. It is also shown that the modifications have the desired effect on the cycle structure. In Section 3.5 we analyze the disturbance from the perturbation and show that it does not move a lattice vector more than a small multiple of the original length. All the transformations are linear, and extend through linearity to any point in $\mathbb{R}^n$.

3.1 Acquiring a lattice with a good Hermite Normal Form

For the modification to work we need the lattice to have a Hermite Normal Form of a certain form. In this section we describe how we efficiently can modify a general lattice slightly to get the Hermite Normal Form we need.

Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice, and let $\mathbf{H}$ be its basis in Hermite Normal Form. For the coming steps, we need the basis of the lattice to be of the following form:

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1} \\ 0 & 0 & \cdots & 0 & d \end{pmatrix} \tag{1}$$

where $d = \det(\Lambda)$ and $0 \leq a_i < d$. We show how to perturb Λ so that we get a lattice whose Hermite Normal Form as is in equation (1). The method we use is based on the following theorem.

Lemma 4. *Let* $\mathbf{H}$ *be a matrix on Hermite Normal Form, i.e.,*

$$\mathbf{H} = \begin{pmatrix} h_{11} & h_{12} & h_{13} & \dots & h_{1(n-1)} & h_{1n} \\ 0 & h_{22} & h_{23} & \dots & h_{2(n-1)} & h_{2n} \\ 0 & 0 & h_{33} & \dots & h_{3(n-1)} & h_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & h_{(n-1)(n-1)} & h_{(n-1)n} \\ 0 & 0 & 0 & \dots & 0 & h_{nn} \end{pmatrix}.$$

Then the matrix $\tau(\mathbf{H})$ given by

$$\tau(\mathbf{H}) = \begin{pmatrix} h_{11} & h_{12} & h_{13} & \dots & h_{1(n-1)} & h_{1n} \\ 1 & h_{22} & h_{23} & \dots & h_{2(n-1)} & h_{2n} \\ 0 & 1 & h_{33} & \dots & h_{3(n-1)} & h_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & h_{(n-1)(n-1)} & h_{(n-1)n} \\ 0 & 0 & 0 & \dots & 1 & h_{nn} \end{pmatrix} \tag{2}$$

has a Hermite Normal Form as in equation (1). The transformation can be computed in time polynomial in the size of the input data.

Proof. We show how to transform the matrix $\tau(\mathbf{H})$ into the Hermite Normal Form using row operations. We begin by placing the topmost vector at the bottom. This gives a matrix that is upper triangular except for the last row. Since all elements on the diagonal are one, we can cancel the $n-1$ first elements of the last row. We then cancel all non-diagonal elements except for the rightmost column, which gives a matrix on HNF. Since the determinant is preserved, the bottom right entry must be $\det(\mathbf{H})$.

We also define the transformation when the input is a vector as

$$\tau_{\Lambda,k}\left(\sum_{i=1}^{n} t_i \mathbf{u_i}\right) = \sum_{i=1}^{n} t_i \mathbf{u'_i} \tag{3}$$

where $\mathbf{u_1}, \mathbf{u_2}, \dots, \mathbf{u_n}$ are the rows of $\mathbf{U}$ and $\mathbf{u'_1}, \mathbf{u'_2}, \dots, \mathbf{u'_n}$ are the rows of $\tau(k\mathbf{U})$.

As the reader may have noticed, this step actually implies the result from [15], although we not only achieve a cyclic lattice, but a lattice whose Hermite Normal Form is as defined above.

3.2 Factoring the basis

Now that we have a basis with the Hermite Normal Form we need, we proceed by finding a more orthogonal basis and factoring the basis matrix.

Let the operation $\rho(\mathbf{B})$ be defined as follows: First the LLL-reduction is applied to the first $n-1$ vectors of $\mathbf{B}$ using $\delta = 3/4$, keeping the last vector unchanged. Let us call this intermediate step ρ'. Assuming that the input is a basis matrix $\mathbf{B}$ of the form (1), this gives a matrix of the form

$$\rho'(\mathbf{B}) = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1(n-1)} & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2(n-1)} & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{(n-1)1} & b_{(n-1)2} & \cdots & b_{(n-1)(n-1)} & b_{(n-1)n} \\ 0 & 0 & \cdots & 0 & d \end{pmatrix}. \tag{4}$$

From the LLL-reduced basis the $(n-1)$'th vector is placed first, keeping the internal order of the other vectors. The complete transformation is called ρ. The matrix $\rho(\mathbf{B})$ can be factored into

$$\begin{pmatrix} 1\,0\,0\cdots 0\,0 \\ 0\,1\,0\cdots 0\,0 \\ 0\,0\,1\cdots 0\,0 \\ \vdots\,\vdots\,\vdots\,\ddots\,\vdots\,\vdots \\ 0\,0\,0\cdots 1\,0 \\ 0\,0\,0\cdots 0\,d \end{pmatrix} \cdot \begin{pmatrix} b_{(n-1)1} & b_{(n-1)2} & \cdots & b_{(n-1)n} \\ b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{(n-2)1} & b_{(n-2)2} & \cdots & b_{(n-2)n} \\ 0 & 0 & \cdots & 1 \end{pmatrix} \tag{5}$$

Since the determinant of the right factor is 1, the cycle structure of the product only depends on the left factor. This follows since, as pointed out in [15], unimodular transformations do not change the cycle structure.

3.3 Modifying the cycle structure

Let $\mathbf{B}_l$ be the left factor in the basis factorization (5) and $\mathbf{B}_r$ the right factor. We create a new lattice Λ' by inflating the lattice spanned by $\mathbf{B}_l$ by a factor d^{n-2}. Put differently, the matrix $d^{n-2} \cdot \mathbf{B}_l$ is a basis matrix of Λ'. By Lemma 2, this lattice has $n-1$ cycles of length d^{n-2} and one cycle of length d^{n-1}.

By modifying the lattice Λ' slightly, we get a new lattice that has $n-1$ cycles of length d^{n-1}. We call the new lattice Λ''. The modification is defined by the function γ':

$$\gamma'_n(d) = \begin{pmatrix} d^{n-2} & d^{n-3} & d^{n-4} & \cdots & d^2 & d & 1 & 0 \\ 0 & d^{n-2} & d^{n-3} & \cdots & d^3 & d^2 & d & 0 \\ 0 & 0 & d^{n-2} & \cdots & d^4 & d^3 & d^2 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & d^{n-2} & d^{n-3} & d^{n-4} & 0 \\ 0 & 0 & 0 & \cdots & 0 & d^{n-2} & d^{n-3} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & d^{n-2} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & d^{n-1} \end{pmatrix}.$$

Theorem 5. *The lattice Λ'' with basis matrix $\gamma'_n(\det(\mathbf{B}_l))$ has $n-1$ nontrivial cycles, each of which has length d^{n-1}.*

Proof. Set $\mathbf{C} = \gamma'(\mathbf{B}_l)$. We describe why this lattice has the cycle structure mentioned above by examining the quotient

$$k_1 = \frac{m_n}{m_{n-1}}$$

where $m_n = |\det(\mathbf{C})| = d^{(n-1)(n-1)}$ and m_{n-1} is the gcd of all $(n-1)$-minors of $\mathbf{C}$. We know that k_1 is the length of the longest cycle.

We determine m_{n-1} by systematically examining the $(n-1)$-minors of $\mathbf{C}$. Let $\mathbf{C}^{i,j}$ be the $(n-1)\times(n-1)$-matrix where the i'th row and the j'th column

of $\mathbf{C}$ have been removed. First consider $\mathbf{C}^{i,j}$, where $i < j$. These matrices are triangular with one or more zeroes on the diagonal. Therefore, the determinants of these matrices are all zero. The matrices $\mathbf{C}^{i,i}$ are also triangular, but with non-zero elements on the diagonal. For $i < n$, $\det\left(\mathbf{C}^{i,i}\right) = d^{(n-2)(n-1)+1}$, and $\det\left(\mathbf{C}^{n,n}\right) = d^{(n-2)(n-1)}$. Next we consider $\det\left(\mathbf{C}^{i,j}\right)$ where $n > i > j$. These matrices are block-triangular, as below.

$$\mathbf{C}^{i,j} = \begin{pmatrix} \mathbf{D_{j-1}} & \cdot & \cdot & \cdot \\ \mathbf{0} & \mathbf{L_{i-j}} & \cdot & \cdot \\ \mathbf{0} & \mathbf{0} & \mathbf{D_{n-i-1}} & \cdot \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & d^{n-1} \end{pmatrix}$$

where $\mathbf{D_k}$ is the $k \times k$ triangular matrix

$$\mathbf{D_k} = \begin{pmatrix} d^{n-2} & d^{n-3} & d^{n-4} & \cdots & d^{n-k} & d^{n-k-1} \\ 0 & d^{n-2} & d^{n-3} & \cdots & d^{n-k+1} & d^{n-k} \\ 0 & 0 & d^{n-2} & \cdots & d^{n-k+2} & d^{n-k+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & d^{n-2} & d^{n-3} \\ 0 & 0 & 0 & \cdots & 0 & d^{n-2} \end{pmatrix}$$

and $\mathbf{L_k}$ is the $k \times k$ matrix

$$\mathbf{L_k} = \begin{pmatrix} d^{n-3} & d^{n-4} & d^{n-5} & \cdots & d^{n-k} & d^{n-k-1} & d^{n-k-2} \\ d^{n-2} & d^{n-3} & d^{n-4} & \cdots & d^{n-k+1} & d^{n-k} & d^{n-k-1} \\ 0 & d^{n-2} & d^{n-3} & \cdots & d^{n-k+2} & d^{n-k+1} & d^{n-k} \\ 0 & 0 & d^{n-2} & \cdots & d^{n-k+3} & d^{n-k+2} & d^{n-k+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & d^{n-2} & d^{n-3} & d^{n-4} \\ 0 & 0 & 0 & \cdots & 0 & d^{n-2} & d^{n-3} \end{pmatrix}.$$

To compute $\det\left(\mathbf{L_k}\right)$, we notice that the last two columns are linearly dependent, since the leftmost column multiplied by d gives the $(k-1)$'th column. This means that $\det\left(\mathbf{L_k}\right) = 0$, and that $\det\left(\mathbf{C}^{i,j}\right) = 0$ for $i < j < n$.

What remains to be checked is $\det\left(\mathbf{C}^{n,j}\right)$ for $j = 1, 2, \ldots, n-1$. These matrices, where we have removed the last row, have only zeroes in their rightmost column and hence the determinant is 0.

Combining these results, we see that $d^{(n-2)(n-1)}$ is a factor of all the $(n-1)$-minors. Also, there are $(n-1)$-minors whose determinant is precisely $d^{(n-2)(n-1)}$. Hence we have that $m_{n-1} = d^{(n-2)(n-1)}$, and consequently $k_1 = d^{n-1}$. Since gcd of all 1-minors (in other words, all the elements) is 1, $m_1 = 1$. This means that we have $n-1$ cycles whose product is $d^{(n-1)(n-1)}$ (the determinant) and that the longest one has length d^{n-1}. Because of the divisibility requirement on the lengths of the cycles, the only possibility is that there are $(n-1)$ cycles of length d^{n-1}.

3.4 Returning to the original representation

Returning to the original representation is just a matter of multiplying by $\mathbf{B}_r$. Since this does not change the cycle structure ($\mathbf{B}_r$ is unimodular), we still have a lattice with the required cycle structure.

We denote the transformation described in Sections 3.2 to 3.4 by γ. More precisely,

$$\gamma(\mathbf{B}) = \gamma'_n\left(\det\left(\mathbf{B}_l\right)\right) \cdot \mathbf{B}_r$$

where $\mathbf{B}_l$ and $\mathbf{B}_r$ are the left and right factors of $\rho(\mathbf{B})$ as in (5) and n is the dimension of the lattice.

We also define the transformation when applied to a vector $\mathbf{v} = \sum_{i=1}^{n} t_i \mathbf{b_i}$ in a lattice Λ where $\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}$ is a basis. The transformation is then defined as

$$\gamma_\Lambda(\mathbf{v}) = \sum_{i=1}^{n} t_i \mathbf{b'_i}$$

where $\mathbf{b'_1}, \mathbf{b'_2}, \ldots, \mathbf{b'_n}$ are the rows of $\gamma(\mathbf{B})$.

Since LLL-reduction can be performed in polynomial time ρ can be computed in polynomial time. It is obvious that also γ' and the factorization in $\mathbf{B}_l$ and $\mathbf{B}_r$ require at most polynomial time. Hence γ can be computed in time polynomial in the size of the input data.

3.5 Completing the approximation

Now we have the necessary steps to complete the approximation. Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice. Our goal is to prove that for any $\varepsilon > 0$ there exist a transformation $\sigma_{\Lambda,\varepsilon}$ and an integer k such that

1. $\forall \mathbf{u} \in \mathbb{Z}^n : \|\mathbf{u} - \sigma_{\Lambda,\varepsilon}(\mathbf{u})/k\| \leq \varepsilon \|\mathbf{u}\|$.
2. $\sigma_{\Lambda,\varepsilon}(\Lambda)$ has $n-1$ non-trivial cycles of equal length.

The transformations we use are $\tau_{\Lambda,k}$ and γ_Λ as described above. Since the displacement for these transformations (as we will see) depends on the determinant, we need to find an appropriate k that makes the determinant large enough. In the final approximation we will begin by applying τ and then apply γ. This composed transformation is called $\sigma_{\Lambda,\varepsilon}(\mathbf{u})$ and can be computed in polynomial time since both τ and γ can be computed in polynomial time.

We bound the displacement introduced by the two transformations τ and γ described above.

Lemma 5. *Let Λ be a lattice and let $\tau_{\Lambda,k}$ be defined as in (3). Then* $\forall \mathbf{u} \in \mathbb{Z}^n : \left\|\mathbf{u} - \frac{1}{k}\tau_{\Lambda,k}(\mathbf{u})\right\| \leq \frac{1}{k} 2^n \|\mathbf{u}\|$.

Proof. The proof of this lemma follows the proof in [15] closely. Let $\mathbf{B}$ be the basis matrix on HNF of the lattice Λ, let $\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}$ be its rows and b_{ij} its elements. Assume $\mathbf{u} = \sum_{i=1}^{n} t_i \mathbf{b_i}$. We first show that

$$|t_i| \leq \|\mathbf{u}\| 2^{i-1} \tag{6}$$

for any ℓ_p-norm (including ℓ_∞). Since $\mathbf{B}$ is upper-triangular, $\sum_{i=1}^{j} |t_i|\,|b_{ij}| \geq |u_j|$. Dividing with $|b_{jj}|$ and using the property of the HNF that $b_{ij} \leq b_{jj}$ for $i < j$ we get

$$|t_j| \leq \frac{\sum_{i=1}^{j-1} |t_i|\,|b_{ij}| + |u_j|}{|b_{jj}|} \leq \sum_{i=1}^{j-1} |t_i| + \|\mathbf{u}\| \ .$$

Induction (on j) gives (6).

We can now compute the actual displacement for a vector $\mathbf{u} = \sum_{i=1}^{n} t_i \mathbf{b_i}$ as

$$\begin{aligned} \left\| \mathbf{u} - \frac{1}{k} \tau_{\Lambda,k}(u) \right\| &= \frac{1}{k} \left\| \sum_{i=2}^{n} t_i \mathbf{e_{i-1}} \right\| \\ &\leq \frac{1}{k} \sum_{i=2}^{n} 2^{i-1} \|\mathbf{u}\| \\ &\leq \frac{1}{k} 2^n \|\mathbf{u}\| \end{aligned} \tag{7}$$

where $\mathbf{e_i}$ are the unit vectors.

We need some bounds on the basis (4) before we can complete the proof. We give these bounds as two lemmas. The first lemma shows that the coordinates of a vector are bounded in a way similar to Lemma 5, and the second that the basis vectors are bounded.

Lemma 6. *Let* $\mathbf{B}$ *be the basis matrix of* Λ *given on the form (4), let* $\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}$ *be its rows. Assume* $\mathbf{u} = \sum_{i=1}^{n} t_i \mathbf{b_i}$. *Then*

$$|t_i| \leq 2^{\frac{3}{2}n-i} \|\mathbf{u}\| \tag{8}$$

for $i < n$ *and for any* ℓ_p*-norm (including* ℓ_∞*).*

Proof. Since the first $n-1$ rows of $\mathbf{B}$ are LLL-reduced, there is an orthogonal basis $\hat{\mathbf{b}}_\mathbf{i}$ given by $\hat{\mathbf{b}}_\mathbf{i} = \mathbf{b_i} - \sum_{j=1}^{i-1} \mu_{ij} \hat{\mathbf{b}}_\mathbf{j}$, or $\mathbf{b_i} = \sum_{j=1}^{i} \mu_{ij} \hat{\mathbf{b}}_\mathbf{j}$, where $|\mu_{ij}| \leq 1/2$ except for $\mu_{ii} = 1$. We can rewrite $\mathbf{u}$ as

$$\begin{aligned} \mathbf{u} &= \sum_{i=1}^{n} t_i \mathbf{b_i} \\ &= \sum_{i=1}^{n} t_i \left(\sum_{j=1}^{i} \mu_{ij} \hat{\mathbf{b}}_\mathbf{j} \right) \end{aligned}$$

$$= \sum_{i=1}^{n} \hat{\mathbf{b}}_\mathbf{i} \left(\sum_{j=i}^{n} t_j \mu_{ji} \right)$$
$$= \sum_{i=1}^{n} \hat{t}_i \hat{\mathbf{b}}_\mathbf{i}$$

where

$$\hat{t}_i = \sum_{j=i}^{n} t_j \mu_{ji} \ .$$

Assume that the lemma is not true, and let i be the largest index such that $|t_i| > 2^{\frac{3}{2}n-i}\|\mathbf{u}\|$. Then

$$\begin{aligned}
|\hat{t}_i| &= \sum_{j=i}^{n} \mu_{ji} t_j \\
&\geq |t_i| - \left| \sum_{j=i+1}^{n} \mu_{ji} t_j \right| \\
&> 2^{\frac{3}{2}n-i}\|\mathbf{u}\| - \frac{1}{2}\|\mathbf{u}\| \sum_{j=i+1}^{n} 2^{\frac{3}{2}n-j} \\
&\geq 2^{\frac{n}{2}}\|\mathbf{u}\| \left(2^{n-i} - \frac{1}{2} \sum_{j=0}^{n-i-1} 2^j \right) \\
&\geq 2^{\frac{n}{2}}\|\mathbf{u}\|
\end{aligned}$$

However, since $\mathbf{u} = \sum_{i=1}^{n} \hat{t}_i \hat{\mathbf{b}}_\mathbf{i}$, the vectors $\hat{\mathbf{b}}_\mathbf{i}$ are pairwise orthogonal and $\left\|\hat{\mathbf{b}}_\mathbf{i}\right\| \geq 2^{-\frac{i-1}{2}}$, this would imply that $\|\mathbf{u}\| > \|\mathbf{u}\|$. As this is a contradiction, the assumption must be false. This proves the lemma.

Lemma 7. *Let* $\mathbf{B}$ *be a basis matrix of the form (1), and let* $\mathbf{b}_\mathbf{i}$ *be the row vectors of the matrix* $\rho(\mathbf{B})$*. Then it holds that*

$$\|\mathbf{b}_\mathbf{i}\| \leq n 2^{\frac{n^2}{8}} \sqrt[4]{d^2 n}$$

for $i = 2, 3, \ldots, n-1$.

The idea of the proof is that in an LLL-reduced basis $\mathbf{B}$ the length of every vector except the last one has an upper bound of the order $\sqrt{\det(\mathbf{B})}$. We then need to renumber the vectors since the can only afford the first vector to remain unbounded in order to bound $\gamma(\mathbf{B})$. It is essential that the bound is $o(\det(\mathbf{B}))$ because of the displacement of γ. The full proof is as follows.

Proof. If we are able to prove that the condition holds for $\mathbf{b'_1}, \mathbf{b'_2}, \ldots, \mathbf{b'_{n-2}}$, where $\mathbf{b'_i}$ are the row vectors of $\rho'(\mathbf{B})$, the lemma obviously follows by renumbering.

We are interested in the $(n-1)$-dimensional lattice $\mathbf{S} \subset \mathbb{Z}^n$ spanned by $\mathbf{b'_1}, \mathbf{b'_2}, \ldots, \mathbf{b'_{n-1}}$. A basis (in fact the basis given in (1)) of the $(n-1)$-dimensional lattice is

$$\mathbf{C} = \begin{pmatrix} 1\,0\cdots 0 & a_1 \\ 0\,1\cdots 0 & a_2 \\ \vdots\,\vdots\,\ddots\,\vdots & \vdots \\ 0\,0\cdots 1 & a_{n-1} \end{pmatrix} \tag{9}$$

with $0 \leq a_i < d$.

The determinant for this not full-dimensional lattice is given by

$$\det(\mathbf{S}) = \sqrt{\det\left(\mathbf{C}\mathbf{C}^T\right)}\ .$$

Let $\mathbf{G} = \mathbf{C}\mathbf{C}^T$. It holds that

$$\mathbf{G} = \begin{pmatrix} 1\,0\cdots 0 & a_1 \\ 0\,1\cdots 0 & a_2 \\ \vdots\,\vdots\,\ddots\,\vdots & \vdots \\ 0\,0\cdots 1 & a_{n-1} \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_{n-1} \end{pmatrix} =$$

$$= \begin{pmatrix} 1+a_1^2 & a_1a_2 & a_1a_3 & \cdots & a_1a_{n-2} & a_1a_{n-1} \\ a_2a_1 & 1+a_2^2 & a_2a_3 & \cdots & a_2a_{n-2} & a_2a_{n-1} \\ a_3a_1 & a_3a_2 & 1+a_3^2 & \cdots & a_3a_{n-2} & a_3a_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-2}a_1 & a_{n-2}a_2 & a_{n-2}a_3 & \cdots & 1+a_{n-2}^2 & a_{n-2}a_{n-1} \\ a_{n-1}a_1 & a_{n-1}a_2 & a_{n-1}a_3 & \cdots & a_{n-1}a_{n-2} & 1+a_{n-1}^2 \end{pmatrix} =$$

$$= \mathbf{a}\mathbf{a}^T + \mathbf{I_{n-1}}$$

where $\mathbf{I_{n-1}}$ is the $(n-1)$-dimensional unit matrix. Since

$$\mathbf{G}\cdot\mathbf{a} = \left(\mathbf{a}\mathbf{a}^T + \mathbf{I_{n-1}}\right)\mathbf{a} = \mathbf{a}\mathbf{a}^T\mathbf{a} + \mathbf{a} = \mathbf{a}\left(\mathbf{a}^T\mathbf{a} + 1\right) = \mathbf{a}\left(1 + \sum_{i=1}^{n-1} a_i^2\right)$$

the vector $\mathbf{a}$ is an eigenvector of $\mathbf{G}$ with eigenvalue $\lambda_1 = 1 + \sum_{i=1}^{n-1} a_i^2$. Now let $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_{n-2}}$ be $n-2$ linearly independent vectors orthogonal to $\mathbf{a}$. Then

$$\mathbf{G}\cdot\mathbf{v_i} = \left(\mathbf{a}\mathbf{a}^T + \mathbf{I_{n-1}}\right)\mathbf{v_i} = \mathbf{a}\cdot\left(\mathbf{a}^T\mathbf{v_i}\right) + \mathbf{v_i} = \mathbf{a}\cdot 0 + \mathbf{v_i} = \mathbf{v_i}$$

which shows that $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_{n-2}}$ also are eigenvectors of $\mathbf{G}$ with eigenvalues $\lambda_i = 1, i = 2, 3, \ldots, n-1$. From this it follows that

$$\det(\mathbf{G}) = \prod_{i=1}^{n-1} \lambda_i = 1 + \sum_{i=1}^{n-1} a_i^2$$

which gives an upper bound for the determinant of $\mathbf{S}$ as

$$\det(\mathbf{S}) = \sqrt{\det\left(\mathbf{C}\mathbf{C}^T\right)} = \sqrt{\det(\mathbf{G})} = \sqrt{1 + \sum_{i=1}^{n-1} a_i^2} \leq d\sqrt{n} \ .$$

Our next step is to prove an upper bound for $\left\|\hat{\mathbf{b}'}_\mathbf{i}\right\|$, $i < n-1$, where $\hat{\mathbf{b}'}_\mathbf{i}$ are the vectors of the corresponding orthogonal system. Using a contradiction argument, we show that

$$\left\|\hat{\mathbf{b}'}_\mathbf{i}\right\| < 2^{\frac{n^2}{8}} \sqrt{\det \mathbf{S}} \ .$$

Assume this is not the case, i.e., that there exists an index $j \in \{1, 2, \ldots, n-2\}$ such that

$$\left\|\hat{\mathbf{b}'}_\mathbf{j}\right\| \geq 2^{\frac{n^2}{8}} \sqrt{\det \mathbf{S}} \ .$$

Since the basis is LLL-reduced with $\delta = 3/4$,

$$\frac{1}{2}\left\|\hat{\mathbf{b}'}_{\mathbf{i-1}}\right\|^2 \leq \left\|\hat{\mathbf{b}'}_\mathbf{i}\right\|^2$$

and

$$\prod_{i=1}^{n-1} \left\|\hat{\mathbf{b}'}_\mathbf{i}\right\| = \det(\mathbf{S}) \tag{10}$$

Since $\left\|\hat{\mathbf{b}'}_\mathbf{1}\right\| = \|\mathbf{b}'_\mathbf{1}\| \geq 1$, it holds that $\left\|\hat{\mathbf{b}'}_\mathbf{i}\right\| \geq 2^{-\frac{i-1}{2}}$ for $i = 1, 2, \ldots, j-1$ and $\left\|\hat{\mathbf{b}'}_\mathbf{i}\right\| \geq 2^{\frac{n^2}{8}} \sqrt{\det(\mathbf{S})} 2^{-\frac{i-j}{2}}$ for $i = j, j+1, \ldots, n-1$. Using equation (10) we can compute the determinant as

$$\det(\mathbf{S}) = \prod_{i=1}^{n-1} \left\|\hat{\mathbf{b}'}_\mathbf{i}\right\| \geq \prod_{i=1}^{j-1} 2^{-\frac{i-1}{2}} \cdot \prod_{i=j}^{n-1} 2^{\frac{n^2}{8}} \sqrt{\det(\mathbf{S})} 2^{-\frac{i-j}{2}} =$$

$$2^{-\frac{(j-2)(j-1)}{4}} (\det(\mathbf{S}))^{\frac{n-j}{2}} 2^{\frac{n^2}{8}n - j} 2^{-\frac{(n-j)(n-j-1)}{2}} \ .$$

For $\det(\mathbf{S})$ large enough this is a decreasing function, so it takes its minimum over j when $j = n-2$ as

$$2^{-\frac{(n-4)(n-3)}{4}} \det(\mathbf{S}) 2^{\frac{n^2}{8}} 2^{-\frac{2 \cdot 1}{2}} > 2^{-\frac{n^2}{4}} \det(\mathbf{S}) 2^{\frac{n^2}{4}} = \det(\mathbf{S})$$

which gives the contradiction $\det(\mathbf{S}) > \det(\mathbf{S})$. Hence the assumption must be incorrect and $\|\hat{\mathbf{b}'}_\mathbf{i}\| < 2^{\frac{n^2}{8}} \sqrt{\det \mathbf{S}} \leq 2^{\frac{n^2}{8}} \sqrt[4]{d^2 n}$ for $i = 1, 2, \ldots, n-2$.

Since we have the relation that $\mathbf{b}'_\mathbf{k} = \hat{\mathbf{b}'}_\mathbf{k} + \sum_{i=1}^{k-1} \mu_{ij} \hat{\mathbf{b}'}_\mathbf{i}$ and $|\mu_{ij}| \leq 1/2$, it holds that

$$\|\mathbf{b}_\mathbf{k}\| = \left\|\hat{\mathbf{b}'}_\mathbf{k} + \sum_{i=1}^{k-1} \mu_{ij} \hat{\mathbf{b}'}_\mathbf{i}\right\|$$

$$\leq \left\|\hat{\mathbf{b}'}_{\mathbf{k}}\right\| + \sum_{i=1}^{k-1} \left\|\mu_{ij}\hat{\mathbf{b}'}_{\mathbf{i}}\right\|$$
$$\leq 2^{\frac{n^2}{8}} \sqrt[4]{d^2 n} + \frac{1}{2} n 2^{\frac{n^2}{8}} \sqrt[4]{d^2 n}$$
$$\leq n 2^{\frac{n^2}{8}} \sqrt[4]{d^2 n} \ .$$

from which the lemma follows.

Now we have the necessary tools to find a bound for the transformation γ_Λ.

Lemma 8. *Let Λ be an n-dimensional lattice and let γ_Λ be as defined in Section 3.4. Then $\forall \mathbf{u} \in \mathbb{Z}^n$*

$$\left\|\mathbf{u} - \frac{1}{\det(\Lambda)^{n-2}} \gamma_\Lambda(\mathbf{u})\right\| \leq \frac{n^{9/4} 2^{\frac{3}{2}n + \frac{n^2}{8}}}{\sqrt{\det(\Lambda)}} \|\mathbf{u}\|$$

for $\det(\Lambda) = \Omega\left(2^{n^2}\right)$.

Proof. Let $\mathbf{b_i}$ be the vectors of the partly LLL-reduced basis in (4) and let $\mathbf{b'_i} = \gamma_\Lambda(\mathbf{b_i})$ be the vectors of the modified basis. If we let the lattice determinant be d, using Lemma 6 we get a displacement for the vector $\mathbf{u} = \sum_{i=1}^{n} t_i \mathbf{b_i}$ of (remember the last two basis vectors are not modified in the transformation)

$$\left\|\mathbf{u} - \frac{1}{d^{n-2}} \gamma_\Lambda(\mathbf{u})\right\| = \frac{1}{d^{n-2}} \left\| \sum_{i=1}^{n-2} t_i \left(d^{n-3} \mathbf{b_{i+1}} + o\left(d^{n-3}\right) \sum_{j=i+2}^{n-2} \mathbf{b_j} \right) \right\|$$
$$\leq \frac{1}{d} 2^{\frac{3}{2}n} \|\mathbf{u}\| \sum_{i=2}^{n-1} \|\mathbf{b_i}\| + o\left(d^{-1}\right) 2^{\frac{3}{2}n} \sum_{i=2}^{n-2} \|\mathbf{b_i}\| \ . \tag{11}$$

To show that this displacement remains bounded, we use Lemma 7 to get an upper bound for $\|\mathbf{b_i}\|$. Inequality (11) can be written as

$$\left\|\mathbf{u} - \frac{1}{d^{n-2}} \gamma_{\Lambda,\varepsilon}(\mathbf{u})\right\| \leq \frac{1}{d} 2^{\frac{3}{2}n} \|\mathbf{u}\| \sum_{i=2}^{n-1} \|\mathbf{b_i}\| + o\left(d^{-1}\right) 2^{\frac{3}{2}n} \sum_{i=2}^{n-2} \|\mathbf{b_i}\|$$
$$\leq \frac{1}{d} 2^{\frac{3}{2}n} \|\mathbf{u}\| n \cdot n 2^{\frac{n^2}{8}} \sqrt[4]{d^2 n}$$
$$= \frac{n^{9/4} 2^{\frac{3}{2}n + \frac{n^2}{8}}}{\sqrt{d}} \|\mathbf{u}\| \tag{12}$$

for d large enough, which proves the lemma.

We combine these two lemmas in order to show a bound for the composed transformation $\sigma_{\Lambda,\varepsilon}$.

Theorem 6. *Let Λ be an n-dimensional lattice. For every choice of $\varepsilon > 0$ there exist integers k and s, at most of size polynomial in $\log\left(\varepsilon^{-1}\right)$ and n, such that the transformation $\sigma_{\Lambda,\varepsilon} = \gamma_{\tau_s(\Lambda)} \circ \tau_{\Lambda,s}$ generates a lattice with $n-1$ cycles of equal length and for any vector $\mathbf{u}$*

$$\left\| \mathbf{u} - \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{u}) \right\| \leq \varepsilon \|\mathbf{u}\|$$

Proof. Let $d = \det(\Lambda)$. According to the triangle inequality, the displacement for $\mathbf{u}$ is at most the sum of the displacement for τ and γ. According to Lemma 5 τ_s gives a displacement of at most $\frac{1}{s}2^n\|\mathbf{u}\|$ whereas according to Lemma 8 γ gives a displacement of at most $n^{9/4}2^{\frac{3}{2}n+\frac{n^2}{8}}\sqrt{\det(\Lambda')}\|\mathbf{u}\|$ where Λ' is the lattice $\tau_s(\Lambda)$. Since $\det(\Lambda') = \Omega\left(ds^n\right)$ the total displacement is

$$\left\| \mathbf{u} - \frac{1}{(ds^n)^{n-2}}\sigma_{\Lambda,\varepsilon}(\mathbf{u}) \right\| \leq \frac{1}{s}2^n\|\mathbf{u}\| + n^2 2^{\frac{3}{2}n+\frac{n^2}{8}} \frac{\sqrt[4]{n}}{\sqrt{\Omega\left(ds^n\right)}}\|\mathbf{u}\|$$

By picking $s = O\left(2^n\varepsilon^{-1}\right)$ and $k = (ds^n)^{n-2}$ we fulfill the approximation requirements.

The requirements on the cycle structure follow from the construction of the transformations.

4 Applications to CVP and SVP

In this section we will outline how the transformation can be used to find a solution to CVP and SVP, should these problems be easier to solve in lattices with many cycles.

In CVP our goal, given a lattice $\Lambda \subseteq \mathbb{Z}^n$ and a point $\mathbf{y} \in \mathbb{Z}^n$, is to find $\mathbf{x} \in \Lambda$ such that $\|\mathbf{x}-\mathbf{y}\|_p$ is minimized in some ℓ_p-norm. If (a slightly perturbed) $\mathbf{x}$ remains the lattice point closest to (a slightly perturbed) $\mathbf{y}$ after the transformation, we can reduce the instance of CVP to an instance of CVP in a lattice with many cycles. The following theorem shows how to choose the transformation parameters. The proof is given in the full version.

Theorem 7. *Let $\Lambda \subseteq \mathbb{Z}^n$, and let $\mathbf{y} \in \mathbb{Z}^n$. Let $\mathbf{x} \in \Lambda$ and $\mathbf{z} \in \Lambda$. Assume that all coordinates are in the interval $0, \ldots, \det(\Lambda) - 1$. It holds that if*

$$\|\mathbf{x}-\mathbf{y}\|_p < \|\mathbf{z}-\mathbf{y}\|_p$$

then

$$\left\| \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{x}) - \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{y}) \right\|_p < \left\| \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{z}) - \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{y}) \right\|_p$$

for

$$0 < \varepsilon < \frac{1}{2pn^{1+1/p}\det(\Lambda)^{p+1}}$$

if $p < \infty$ *and*

$$0 < \varepsilon < \frac{1}{2\det(\Lambda)}$$

if $p = \infty$ *and* k *is polynomial in* ε^{-1}.

Proof. The influence of the transformation on the distance between $\mathbf{x}$ and $\mathbf{y}$ is

$$\left| \|\mathbf{x}-\mathbf{y}\|_p - \left\| \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{x}) - \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{y}) \right\|_p \right| = \left| \|\mathbf{x}-\mathbf{y}\|_p - \left\| \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{x}-\mathbf{y}) \right\|_p \right| \leq$$

$$\left| \left\| (\mathbf{x}-\mathbf{y}) - \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{x}-\mathbf{y}) \right\|_p \right| \leq \varepsilon \|\mathbf{x}-\mathbf{y}\|_p \ .$$

In the same way we can compute $\left| \|\mathbf{z}-\mathbf{y}\|_p - \left\|\frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{z}) - \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{y})\right\|_p \right| \leq \varepsilon \|\mathbf{z}-\mathbf{y}\|_p$.

Using this we get

$$\left\| \frac{1}{k}\sigma(\mathbf{z}) - \frac{1}{k}\sigma(\mathbf{y}) \right\| - \left\| \frac{1}{k}\sigma(\mathbf{x}) - \frac{1}{k}\sigma(\mathbf{y}) \right\| \geq$$

$$(\|\mathbf{z}-\mathbf{y}\| - \|\mathbf{x}-\mathbf{y}\|) - \varepsilon(\|\mathbf{z}-\mathbf{y}\| + \|\mathbf{x}-\mathbf{y}\|) \ .$$

We want to pick ε to ensure this expression is greater than 0. For $p < \infty$ we have a lower bound for the first part of the expression as

$$\|\mathbf{z}-\mathbf{y}\| - \|\mathbf{x}-\mathbf{y}\| \geq \sqrt[p]{n \cdot \det(\Lambda)^p - 1} - \sqrt[p]{n \cdot \det(\Lambda)^p - 2} \geq \frac{1}{p} \left(n \det(\Lambda)^p\right)^{1/p-1}$$

and an upper bound for the second part as

$$\|\mathbf{z}-\mathbf{y}\| + \|\mathbf{x}-\mathbf{y}\| \leq 2\sqrt[p]{n}\det(\Lambda)$$

we have the necessary condition fulfilled if we pick

$$0 < \varepsilon < \frac{1}{p} \frac{1}{n \cdot \det(\Lambda)^p} \frac{1}{2\sqrt[p]{n}\det(\Lambda)}$$

If, on the other hand, $p = \infty$, we have $\|\mathbf{z}-\mathbf{y}\| - \|\mathbf{x}-\mathbf{y}\| \geq 1$ and $\|\mathbf{z}-\mathbf{y}\| + \|\mathbf{x}-\mathbf{y}\| \leq 2\det(\Lambda)$ so the condition holds if

$$0 < \varepsilon < \frac{1}{2\det(\Lambda)} \ .$$

The following two lemmas show how to use Theorem 7 to reduce CVP to a lattice with $n-1$ cycles. The first lemma follows directly from the fact that every lattice repeats itself in cubes with side $\det(\Lambda)$.

Lemma 9. *Let* $(\Lambda \subseteq \mathbb{Z}^n, \mathbf{y} \in \mathbb{Z}^n)$ *be an instance of* CVP. *Then for any* $\mathbf{u} \in \mathbb{Z}^n$ $\mathbf{x} \in \Lambda$ *is a solution if and only if* $\mathbf{x} - \det(\Lambda) \cdot \mathbf{u}$ *is a solution of the instance* $(\Lambda, \mathbf{y} - \det(\Lambda) \cdot \mathbf{u})$.

Lemma 10. *Let* $(\Lambda \subseteq \mathbb{Z}^n, \mathbf{y} \in \mathbb{Z}^n)$ *be an instance of* CVP *such that* $0 \leq y_i < \det(\Lambda)$. *Then* $\mathbf{x} \in \Lambda$ *is a solution if and only if* $\frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{x})$ *is a solution of the instance* $\left(\frac{1}{k}\sigma_{\varepsilon}(\Lambda), \frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{y})\right)$ *for* k *and* ε^{-1} *polynomial in* $\det(\Lambda)$ *and* n.

Proof. The lemma follows directly from Theorem 7. Using the two lemmas, we can construct the reduction by first reducing the target vector modulo $\det(\Lambda)$ and then apply the transformation with the appropriate value of ε.

Obviously the same technique can be used to achieve a similar result for SVP. The following lemma follows directly from the above lemmas.

Lemma 11. *Let* $\Lambda \subseteq \mathbb{Z}^n$ *be an instance of* SVP. *Then* $\mathbf{x} \in \Lambda$ *is a solution if and only if* $\frac{1}{k}\sigma_{\Lambda,\varepsilon}(\mathbf{x})$ *is a solution of the instance* $\frac{1}{k}\sigma_{\varepsilon}(\Lambda)$ *for* k *and* ε^{-1} *polynomial in* $\det(\Lambda)$ *and* n.

From this we can conclude that the inapproximability results for SVP and CVP from [13] and [5] hold also for lattices with $n-1$ cycles.

Theorem 8. SVP *is* ***NP****-hard to approximate within* $\sqrt{p} - \varepsilon$ *in* ℓ_p*-norm for* n*-dimensional lattices with* $n-1$ *non-trivial cycles of equal length.*

Theorem 9. *There exist constants* c_p *such that* CVP *is* ***NP****-hard to approximate within* $n^{\frac{c_p}{\log\log n}}$ *in* ℓ_p*-norm for* n*-dimensional lattices with* $n-1$ *non-trivial cycles of equal length.*

5 Conclusions

We have constructed a transformation that given an n-dimensional lattice of any cycle structure produces a lattice with $n-1$ cycles that is arbitrarily close to the original lattice. This closes the question of whether SVP and CVP can be easier to solve in lattices with many cycles. Using the presented result, such a solution would give a solution for the general case that is at most a polynomial factor slower in running time. Also the known inapproximability results for SVP and CVP extend to lattices with $n-1$ cycles.

By previous results, we know that any lattice can be approximated arbitrarily well by a cyclic lattice, and hence that SVP and CVP cannot be easier to solve in cyclic lattices than in general lattices, except possibly for a polynomial factor. We now have the two extremes, for one cycle and for $n-1$ cycles.

From Ajtai's and other papers we have a hardness result also for lattices with n/c cycles. Together with the results of the current paper, this gives evidence to the general hypothesis that the cycle structure have little importance in deciding the hardness of a certain lattice.

Although it does seem likely that also lattices with m non-trivial cycles form a hard core for $2 \leq m \leq n-2$, we don't have a proof for this. The current proof does not easily extend to these cycle structures. Since our method relies on inflating the lattice by a factor d^t to get a lattice with determinant d^{nt+1} and then making changes to achieve m cycles, the length of each cycle is $d^{(nt+1)/m}$.

Naturally t must be chosen so that $(nt+1)/m$ is an integer. In our case, we achieve this by setting $t = n-2$ and $m = n-1$. Since the value of t would depend on m and for certain relations between m and n no such t exists at all, our method cannot directly be generalized to create any cycle structure where the non-trivial cycles have equal length.

Even if a transformation into m cycles of equal length for $1 \leq m \leq n-1$ were found it would still be an open question whether other cycle structures, where the cycles have different lengths, remain easy. Still the current result seems to be a strong indication that the cycle structure does not play an important role for the computational complexity of lattice problems.

6 Acknowledgments

I would like to thank Johan Håstad for valuable tips and ideas in several of the proofs, as well as the anonymous referees for pointing out possible improvements.

References

1. M. Ajtai. Generating Hard Instances of Lattice Problems. *Proc. 28th ACM Symposium on Theory of Computing*, pages 99–108, 1996.
2. M. Ajtai. The shortest vector problem in ℓ_2 is **NP**-hard for randomized reductions. *Proc. 30th ACM Symposium on the Theory of Computing*, pages 10–19, 1998.
3. J-Y. Cai and A. Nerurkar. An Improved Worst-Case to Average-Case Connection for Lattice Problems. *Proc. 38th IEEE Symposium on Foundations of Computer Science*, pages 468–477, 1997.
4. I. Dinur. Approximating SVP_∞ to within almost polynomial factors is NP-hard. *CIAC 2000, volume 1767 of LNCS*, pages 263–276, 2000.
5. I. Dinur, G. Kindler, S. Safra, R.Raz. Approximating CVP to within Almost-Polynomial Factors is **NP**-hard *Combinatorica*, 23(2):205-243, 2003.
6. O. Goldreich and S. Goldwasser. On the limits of non-approximability of lattice problems. *Journal of Computer and System Sciences*, Academic Press, 60(3):540–563, 2000. Can be obtained from `http://www.eccc.uni-trier.de/eccc`.
7. J. Hoffstein, J. Pipher, and J.H. Silverman. NTRU: a ring based public key cryptosystem. *Proc. of ANTS III, volume 1423 of LNCS*, pages 267–288, 1998.
8. R. Kannan and A. Bachem. Polynomial Algorithms for Computing of the Smith and Hermite Normal Forms of an Integer Matrix. *SIAM Journal of Computing*, 8:499–507, 1979.
9. S. Khot. Hardness of Approximating the Shortest Vector Problem in High L_p Norms. *Proc. 44th IEEE Symposium on Foundations of Computer Science*, pages 290–297, 2003.
10. J.C. Lagarias. The Computational Complexity of Simultaneous Diophantine Approximation Problems. *SIAM Journal of Computing*, 14:196–209, 1985.
11. A.K. Lenstra, H.W. Lenstra and L. Lovász. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen* 261:515–534, 1982.
12. D. Micciancio. Improving Lattice Based Cryptosystems Using the Hermite Normal Form. *CaLC 2001, volume 2146 of LNCS*, pages 126–145, 2001.

13. D. Micciancio. The Shortest Vector in a Lattice is Hard to Approximate within Some Constant. *SIAM Journal of Computing*, 30:2008–2035, 2001.
14. M. Newman.*Integral Matrices*, Academic Press, 1972.
15. A. Paz and C.P. Schnorr. Approximating Integer Lattices by Lattices with Cyclic Factor Groups. *Automata, languages and programming (Karlsruhe)*, pages 386–393, 1987.
16. H.J.S. Smith. On Systems of Linear Indeterminate Equations and Congruences. *Philosophical Transactions of the Royal Society of London*, 151:293–326, 1861.
17. M. Trolin. The Shortest Vector Problem in Lattices with Many Cycles. *CaLC 2001, volume 2146 of LNCS*, pages 194–205, 2001.
18. P. van Emde Boas. Another **NP**-complete partition problem and the complexity of computing short vectors in lattices. Technical Report 81-04. Mathematics Department, University of Amsterdam, 1981. Can be obtained from `http://turing.wins.uva.nl/~peter`.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'