1-1-2014

On the Geometry of Cyclic Lattices

Lenny Fukshansky
Claremont McKenna College

Xun Sun
Claremont Graduate University

ON THE GEOMETRY OF CYCLIC LATTICES

LENNY FUKSHANSKY AND XUN SUN

Abstract. Cyclic lattices are sublattices of $\mathbb{Z}^N$ that are preserved under the rotational shift operator. Cyclic lattices were introduced by D. Micciancio in [16] and their properties were studied in the recent years by several authors due to their importance in cryptography. In particular, Peikert and Rosen [19] showed that on cyclic lattices in prime dimensions, the shortest independent vectors problem SIVP reduces to the shortest vector problem SVP with a particularly small loss in approximation factor, as compared to general lattices. In this paper, we further investigate geometric properties of cyclic lattices. Our main result is a counting estimate for the number of well-rounded cyclic lattices, indicating that well-rounded lattices are more common among cyclic lattices than generically. We also show that SVP is equivalent to SIVP on a positive proportion of Minkowskian well-rounded cyclic lattices in every dimension. As an example, we demonstrate an explicit construction of a family of such lattices on which this equivalence holds. To conclude, we introduce a class of sublattices of $\mathbb{Z}^N$ closed under the action of subgroups of the permutation group S_N, which are a natural generalization of cyclic lattices, and show that our results extend to all such lattices closed under the action of any N-cycle.

1. Introduction

Define the rotational shift operator on $\mathbb{R}^N$, $N \geq 2$, by

$$\mathrm{rot}(x_1, x_2, \ldots, x_{N-1}, x_N) = (x_N, x_1, x_2, \ldots, x_{N-1})$$

for every $\boldsymbol{x} = (x_1, x_2, \ldots, x_{N-1}, x_N) \in \mathbb{R}^N$. We will write rot^k for iterated application of rot k times for each $k \in \mathbb{Z}_{>0}$ (then rot^0 is just the identity map, and $\mathrm{rot}^k = \mathrm{rot}^{N+k}$). It is also easy to see that rot (and hence each iteration rot^k) is a linear operator. A sublattice Γ of $\mathbb{Z}^N$ is called *cyclic* if $\mathrm{rot}(\Gamma) = \Gamma$, i.e. if for every $\boldsymbol{x} \in \Gamma$, $\mathrm{rot}(\boldsymbol{x}) \in \Gamma$. Clearly, $\mathbb{Z}^N$ itself is a cyclic lattice. In fact, cyclic lattices come from ideals in the quotient polynomial ring $\mathbb{Z}[x]/(x^N-1)$. Let $p(x) \in \mathbb{Z}[x]/(x^N-1)$, then $p(x) = \sum_{n=0}^{N-1} a_n x^n$ for some $a_0, \ldots, a_{N-1} \in \mathbb{Z}$. Define a $\mathbb{Z}$-module isomorphism $\rho : \mathbb{Z}[x]/(x^N-1) \to \mathbb{Z}^N$ given by

$$\rho(p(x)) = (a_0, \ldots, a_{N-1}) \in \mathbb{Z}^N,$$

then for any ideal $I \subseteq \mathbb{Z}[x]/(x^N-1)$, $\Gamma_I := \rho(I)$ is a sublattice of $\mathbb{Z}^N$. Notice that for every $p(x) = \sum_{n=0}^{N-1} a_n x^n \in I$,

$$xp(x) = a_{N-1} + a_0 x + a_1 x^2 + \cdots + a_{N-2} x^{N-1} \in I,$$

2010 *Mathematics Subject Classification.* Primary: 11H06, 11H55; Secondary: 68Q17.

Key words and phrases. cyclic lattices, well-rounded lattices, shortest vector problem.

The first author was partially supported by NSA Young Investigator Grant #1210223 and Simons Foundation grants #208969, 279155.

and so

$$\rho(xp(x)) = (a_{N-1}, a_0, a_1, \dots, a_{N-2}) = \mathrm{rot}(\rho(p(x))) \in \Gamma_I,$$

and for any $(a_0, \dots, a_{N-1}) \in \Gamma_I$,

$$\mathrm{rot}(a_0, \dots, a_{N-1}) = \rho\left(x \sum_{n=0}^{N-1} a_n x^n\right) \in \Gamma_I,$$

since $x\sum_{n=0}^{N-1} a_n x^n \in I$. In other words, $\Gamma \subseteq \mathbb{Z}^N$ is a cyclic lattice if and only if $\Gamma = \Gamma_I$ for some ideal $I \subseteq \mathbb{Z}[x]/(x^N - 1)$. Cyclic lattices were introduced by D. Micciancio in [16] and [17] in the context of cryptographic algorithms and were further studied in [12], [19], among other sources. In fact, cyclic lattices are used in the well known NTRU cryptosystem [10], [9] (also see, for instance [22] and [23] for some details) and are further discussed in the context of post-quantum cryptography [3].

On the other hand, given a lattice $\Gamma \subset \mathbb{R}^N$ of rank r, we define its successive minima by

$$\lambda_i = \lambda_i(\Gamma) := \inf\{\lambda \in \mathbb{R}_{>0} : \Gamma \cap \lambda B_N \text{ contains } i \text{ linearly independent vectors}\},$$

where B_N is a unit ball centered at the origin in $\mathbb{R}^N$, and so

$$0 < \lambda_1 \leq \cdots \leq \lambda_r.$$

Let us write $\| \ \|$ for the usual Euclidean norm on $\mathbb{R}^N$. There exists a collection of linearly independent vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_r$ in Γ such that $\|\boldsymbol{x}_i\| = \lambda_i$ for each $1 \leq i \leq r$; we will refer to them as vectors *corresponding* to successive minima. When $r \leq 4$, there exists a basis for Γ consisting of vectors corresponding to successive minima, which is a *Minkowski reduced basis* for Γ; this is not necessarily true for $r \geq 5$ (see for instance [20]), but there are many lattices in higher dimensions as well for which it is true; following J. Martinet, we call such lattices *Minkowskian*. Notice also that λ_1 is the minimal norm of nonzero vectors in Γ and define the *set of minimal vectors*

$$S(\Gamma) = \{\boldsymbol{x} \in \Gamma : \|\boldsymbol{x}\| = \lambda_1\}.$$

The lattice Γ is called *well-rounded* (abbreviated WR) if $\lambda_1 = \cdots = \lambda_r$, which is equivalent to saying that $S(\Gamma)$ spans a subspace of $\mathbb{R}^N$ of dimension r. A strictly stronger condition in general is: $\Gamma = \mathrm{span}_{\mathbb{Z}} S(\Gamma)$; we will refer to it by saying that Γ is WR$'$. WR lattices are important in discrete optimization, in particular in the investigation of sphere packing, sphere covering, and kissing number problems (see [14]), as well as in coding theory (see [1]). Properties of WR lattices have also been investigated in [15] in connection with Minkowski's conjecture and in [8] in connection with the linear Diophantine problem of Frobenius.

Let $\mathcal{C}_N$ be the set of full-rank cyclic sublattices of $\mathbb{Z}^N$. In this paper we discuss some geometric properties of lattices from $\mathcal{C}_N$, in particular establishing the following counting estimate on the number of well-rounded cyclic lattices.

Theorem 1.1. *Let $R \in \mathbb{R}_{>0}$, then there exists a constant $\alpha_N > 0$ depending only on dimension N such that*

$$\#\left\{\Gamma \in \mathcal{C}_N : \lambda_N(\Gamma) \leq R, \ \Gamma \text{ is WR}'\right\} \geq \alpha_N R^N \tag{1}$$

as $R \to \infty$.

Remark 1.1. By Minkowski Successive Minima Theorem (see, for instance Theorem 2.6.8 on p. 50 of [14]),

$$\det(\Gamma) \gg\ll_N \lambda_N(\Gamma)^N.$$

Hence

$$\#\left\{\Gamma \in \mathcal{C}_N : \lambda_N(\Gamma) \leq R\right\} \gg\ll_N \#\left\{\Gamma \in \mathcal{C}_N : \det(\Gamma) \leq R^{\frac{1}{N}}\right\},$$

and analogously for subsets of $\mathcal{C}_N$ consisting of WR or WR$'$ lattices.

When $N = 2$ a direct argument can be applied to obtain a more explicit bound.

Theorem 1.2. *Let $R \in \mathbb{R}_{>0}$, then*

$$\begin{aligned} 0.200650... \times R^2 - 3.742382... \times R &\leq \#\left\{\Gamma \in \mathcal{C}_2 : \lambda_2(\Gamma) \leq R,\ \Gamma \textit{ is } \mathrm{WR}'\right\} \\ &\leq 0.267638... \times R^2 + 1.673031... \times R. \end{aligned} \tag{2}$$

Remark 1.2. The estimate of Theorems 1.1 and 1.2 is of the same order of magnitude as the number of *all* (not only WR) ideal lattices from polynomial rings $\mathbb{Z}[x]/f(x)$ for irreducible polynomials $f(x)$ under the same map ρ as above (see [4]). On the other hand, the number of all cyclic lattices with successive minima $\leq R$ grows like $O(R^N(\log R)^{d(N)-1})$ as $R \to \infty$, where $d(N)$ is the number of divisors of N: this is a special case of an estimate of the number of ideal lattices in a forthcoming paper by S. Kühnlein and the first author.

Lattice-based cryptographic algorithms heavily rely on the fact that the problem of finding $\lambda_1(\Gamma)$, given an arbitrary basis matrix for Γ, is NP-hard. For most lattices, the problem of finding all successive minima is strictly harder, however if the lattice is WR then the two problems are the same. On the other hand, the set of WR lattices has measure zero in the space of all lattices in a given dimension N. The advantage of using cyclic lattices is that many of them can be constructed from a single vector (using its rotations), and hence the size of the input for a basis matrix of the lattice reduces from N^2 to N. While it is not clear whether the problem of finding $\lambda_1(\Gamma)$ still remains NP-hard, there are reasons to expect that for many cyclic lattices this problem is the same as that of finding all successive minima, i.e. many cyclic lattices are WR. In particular, in [19] the authors proved that in *prime* dimensions N, the shortest independent vectors problem SIVP on cyclic lattices reduces to (a slight variant of) the shortest vector problem SVP by a polynomial-time algorithm with only a factor of 2 loss in approximation factor (compare to the factor of $\sqrt{N}$ loss on general lattices; see Figure 1 on p. 140 of [18]). As a corollary of our proof of Theorem 1.1, we show that SVP and SIVP are equivalent on a positive proportion of Minkowskian well-rounded cyclic lattices in every dimension N and exhibit a construction of a family of such lattices for which this equivalence holds. These results are given by Lemma 3.4, Remark 3.4 and Corollary 3.5.

The paper is organized as follows. In Section 2 we establish some preliminary results on distribution properties of cyclic lattices. In Section 3 we give a lower bound on the number of WR$'$ cyclic lattices with bounded successive minima, proving Theorem 1.1. Among WR cyclic lattices spanned by their shortest vectors, we specifically focus on those that are in fact spanned by rotations of a single shortest vector: for many such lattices all rotations of any shortest vector are linearly independent, and hence SIVP on these lattices is solved by taking a solution to SVP and all of its rotations. We prove Theorem 1.2 in Section 4. Here we follow the tactic of Section 3, but make the estimates more precise in dimension 2.

In Section 5 we extend our results to a more general class of lattices. Specifically, let S_N be the group of permutations on $N \geq 2$ elements. We can define an action of S_N on $\mathbb{R}^N$ by

$$\tau \boldsymbol{x} = \begin{pmatrix} x_{\tau(1)} \\ \vdots \\ x_{\tau(N)} \end{pmatrix} \tag{3}$$

for each $\tau \in S_N$ and $\boldsymbol{x} = (x_1, \dots, x_N)^t \in \mathbb{R}^N$. We say that a lattice $\Lambda \subset \mathbb{R}^N$ is *τ-invariant* (or invariant under τ) for a fixed $\tau \in S_N$ if $\tau\Lambda = \Lambda$. In particular, cyclic lattices are precisely the full-rank sublattices of $\mathbb{Z}^N$ invariant under the N-cycle $(1\ 2 \dots N)$. The following statement about lattices invariant under arbitrary N-cycles follows from our Theorem 1.1.

Corollary 1.3. *Let $N \geq 2$, let $\tau \in S_N$ be an N-cycle, and let $\mathcal{C}_N(\tau)$ be the set of all τ-invariant full-rank sublattices of $\mathbb{Z}^N$. Then*

$$\#\left\{\Gamma \in \mathcal{C}_N(\tau) : \lambda_N(\Gamma) \leq R,\ \Gamma \textit{ is } \mathrm{WR}'\right\} \geq \alpha_N R^N, \tag{4}$$

as $R \to \infty$, for the same value of α_N as in (1).

We prove Corollary 1.3 in Section 5 and conclude with some further questions about more general permutation invariant lattices. We are now ready to proceed.

2. Basic properties of cyclic lattices

Let $\mathcal{G}_N$ be the set of full-rank cyclic sublattices of $\mathbb{Z}^N$ spanned by vectors corresponding to their successive minima (when $N \leq 4$, $\mathcal{G}_N = \mathcal{C}_N$). In this section we start out by looking at the cyclic lattices generated by rotations of a single vector. Notice that for every $\boldsymbol{a} \in \mathbb{Z}^N$, $\|\boldsymbol{a}\| = \|\operatorname{rot}(\boldsymbol{a})\|$, therefore if $\Gamma \subseteq \mathbb{Z}^N$ is a cyclic lattice and $\boldsymbol{a} \in S(\Gamma)$, then $\operatorname{rot}^n(\boldsymbol{a}) \in S(\Gamma)$ for every $1 \leq n \leq N-1$ (clearly $\operatorname{rot}^N(\boldsymbol{a}) = \boldsymbol{a}$). Therefore cyclic lattices have large sets of minimal vectors, and so it is natural to expect that they are WR fairly often. In fact, it is clear that if $\boldsymbol{a} \in S(\Gamma)$ and $\boldsymbol{a}, \operatorname{rot}(\boldsymbol{a}), \dots, \operatorname{rot}^{N-1}(\boldsymbol{a})$ are linearly independent, then Γ is WR. To state our first observation in this direction, we need some more notation.

Let $\boldsymbol{a} = (a_0, \dots, a_{N-1})^t \in \mathbb{R}^N$, and define $\boldsymbol{a}(x) = \sum_{n=0}^{N-1} a_n x^n$ to be the polynomial of degree $\leq N-1$ in x whose coefficient vector is $\boldsymbol{a}$. Let also

$$M(\boldsymbol{a}) = (\boldsymbol{a}\ \operatorname{rot}(\boldsymbol{a})\ \dots\ \operatorname{rot}^{N-1}(\boldsymbol{a}))$$

be an $N \times N$ matrix. Consider the lattice

$$\Lambda(\boldsymbol{a}) = \operatorname{span}_{\mathbb{Z}}\left\{\boldsymbol{a}, \operatorname{rot}(\boldsymbol{a}), \dots, \operatorname{rot}^{N-1}(\boldsymbol{a})\right\} = M(\boldsymbol{a})\mathbb{Z}^N,$$

and define the *cyclic order* of $\boldsymbol{a}$, denoted $\operatorname{co}(\boldsymbol{a})$, to be the rank of $\Lambda(\boldsymbol{a})$. This means that precisely $\operatorname{co}(\boldsymbol{a})$ of the vectors $\boldsymbol{a}, \operatorname{rot}(\boldsymbol{a}), \dots, \operatorname{rot}^{N-1}(\boldsymbol{a})$ are linearly independent, and so $M(\boldsymbol{a})$ is a matrix of rank $\operatorname{co}(\boldsymbol{a})$. While not every $\Lambda(\boldsymbol{a})$ is necessarily generated by the vectors corresponding to its successive minima, lattices of the form $\Lambda(\boldsymbol{a})$ for $\boldsymbol{a} \in \mathbb{Z}^N$ are very common among cyclic lattices.

Lemma 2.1. *The vectors $\boldsymbol{a}, \operatorname{rot}(\boldsymbol{a}), \dots, \operatorname{rot}^{N-1}(\boldsymbol{a}) \in \mathbb{Z}^N$ are linearly independent if and only if the polynomial $\boldsymbol{a}(x)$ does not have any common factors with $x^N - 1$.*

Proof. In this case $M(\boldsymbol{a})$ is an $N \times N$ circulant matrix corresponding to a vector $\boldsymbol{a} \in \mathbb{Z}^N$. It is a well-known fact (see for instance [24]) that

$$\det(M(\boldsymbol{a})) = \prod_{n=0}^{N-1} \boldsymbol{a}(\omega_j),$$

where $\omega_j = e^{\frac{2\pi i j}{N}}$ is an N-th root of unity. Hence $\det(M(\boldsymbol{a})) = 0$ if and only if $\boldsymbol{a}(\omega_j) = 0$ for some $0 \leq j \leq N-1$, which happens if and only if $\boldsymbol{a}(x)$ is divisible by the minimal polynomial of ω_j – that is, by some cyclotomic polynomial dividing $x^N - 1$. □

Remark 2.1. An immediate consequence of Lemma 2.1 is that when N is prime, the vectors $\boldsymbol{a}, \mathrm{rot}(\boldsymbol{a}), \ldots, \mathrm{rot}^{N-1}(\boldsymbol{a}) \in \mathbb{Z}^N$ are linearly independent if and only if $\boldsymbol{a}(x)$ is not a multiple of $x-1$ or $\sum_{n=0}^{N-1} x^n$. See Section 2 of [19] for further results of this kind.

Let

$$C_R^N = \{\boldsymbol{x} \in \mathbb{R}^N \ : \ |\boldsymbol{x}| := \max\{|x_1|, \ldots, |x_N|\} \leq R\}$$

for every $R \in \mathbb{R}_{>0}$, i.e., C_R^N is a cube of side-length $2R$ centered at the origin in $\mathbb{R}^N$. Recall that d-th cyclotomic polynomial $\Phi_d(x)$ divides $x^N - 1$ if and only if d is a divisor of N. For each divisor d of N, define the *d-th cyclotomic subspace* to be

$$H_{\Phi_d} = \left\{\boldsymbol{a} \in \mathbb{R}^N : \Phi_d(x) \text{ divides } \boldsymbol{a}(x) \text{ in } \mathbb{R}[x]\right\}. \tag{5}$$

By Lemmas 2.3 and 2.4 of [19], H_{Φ_d} is a subspace of $\mathbb{R}^N$ of dimension

$$\dim_{\mathbb{R}}(H_{\Phi_d}) = N - \deg(\Phi_d) = N - \varphi(d),$$

where φ is Euler's φ-function. Then $\Lambda_{\Phi_d} := H_{\Phi_d} \cap \mathbb{Z}^N$ is a sublattice of $\mathbb{Z}^N$ of rank $N - \varphi(d)$. Therefore

$$\begin{aligned}
\left| C_R^N \cap \left(\mathbb{Z}^N \setminus \bigcup_{d|N} \Lambda_{\Phi_d} \right) \right| &= \left| C_R^N \cap \mathbb{Z}^N \right| - \sum_{d|N} \left| C_R^N \cap \Lambda_{\Phi_d} \right| \\
&\geq \left| C_R^N \cap \mathbb{Z}^N \right| - \sum_{d|N} \left| C_R^{N-\varphi(d)} \cap \mathbb{Z}^{N-\varphi(d)} \right| \\
&\geq \left| C_R^N \cap \mathbb{Z}^N \right| - \left| C_R^{N-1} \cap \mathbb{Z}^{N-1} \right| \sum_{d|N} \varphi(d) \\
&= (2R+1)^N - N(2R+1)^{N-1} \\
&= (2R+1-N)(2R+1)^{N-1}. \qquad (6)
\end{aligned}$$

The lattice $\Lambda(\boldsymbol{a}) \subseteq \mathbb{Z}^N$ has rank N if and only if the vectors $\boldsymbol{a}, \mathrm{rot}(\boldsymbol{a}), \ldots, \mathrm{rot}^{N-1}(\boldsymbol{a})$ are linearly independent, which happens if and only if the polynomial $\boldsymbol{a}(x)$ is not divisible by any cyclotomic polynomial $\Phi_d(x)$ for any $d \mid N$, by Lemma 2.1. How often does this happen?

Lemma 2.2. *Let $R > \frac{N-1}{2}$, then*

$$\mathrm{Prob}_{\infty,R}\left(\mathrm{rk}(\Lambda(\boldsymbol{a})) = N\right) \geq 1 - \frac{N}{2R+1}, \tag{7}$$

where probability $\mathrm{Prob}_{\infty,R}(\cdot)$ is with respect to the uniform distribution among all points $\boldsymbol{a}$ in the set $C_R^N \cap \mathbb{Z}^N$.

Proof. By Lemma 2.1,

$$\mathrm{Prob}_{\infty,R}\left(\mathrm{rk}(\Lambda(\boldsymbol{a}))=N\right)=\frac{\left|C_R^N\cap\left(\mathbb{Z}^N\setminus\bigcup_{d|N}\Lambda_{\Phi_d}\right)\right|}{\left|C_R^N\cap\mathbb{Z}^N\right|},$$

and the statement of the lemma follows by (6) combined with the observation that $\left|C_R^N\cap\mathbb{Z}^N\right|=(2R+1)^N$. □

3. General cyclic lattices

The main goal of this section is to prove Theorem 1.1. Recall that $\mathcal{C}_N$ is the set of all cyclic full-rank sublattices of $\mathbb{Z}^N$, while $\mathcal{G}_N\subset\mathcal{C}_N$ is the subset consisting of all lattices in $\mathcal{C}_N$ which are spanned by the vectors corresponding to successive minima. Naturally, every lattice $\Gamma\in\mathcal{C}_N$ has a sublattice $\Gamma_1\in\mathcal{G}_N$ which is spanned by the vectors corresponding to successive minima of Γ; it is called a *Minkowskian sublattice* of Γ. While Minkowskian sublattice may not be unique, there can only be finitely many of them, where an upper bound on this number depends only on N. On the other hand, the index $|\Gamma:\Gamma_1|$ of a Minkowskian sublattice is also bounded above by a constant depending only on N, and hence a given lattice in $\mathcal{G}_N$ can be a Minkowskian sublattice for only finitely many lattices in $\mathcal{C}_N$ (see [13] and subsequent works of J. Martinet and his co-authors for more information on the index of Minkowskian sublattices). This means that the numbers of WR lattices in $\mathcal{C}_N$ and $\mathcal{G}_N$ have the same asymptotic order. Here we will construct large families of WR lattices in $\mathcal{G}_N$.

For a subspace $V\subseteq\mathbb{R}^N$ which is closed under the rotational shift operator, define the set

$$\mathcal{D}_N^V=\left\{\boldsymbol{a}\in V:\mathrm{co}(\boldsymbol{a})=\dim_{\mathbb{R}}(V),\ \boldsymbol{a}\in S(\Lambda(\boldsymbol{a})),\ \Lambda(\boldsymbol{a})\text{ spanned by }S(\Lambda(\boldsymbol{a}))\right\},\tag{8}$$

and let us write $\mathcal{D}_N$ for $\mathcal{D}_N^{\mathbb{R}^N}$.

Lemma 3.1. *A lattice $\Lambda(\boldsymbol{a})\subset V\subseteq\mathbb{R}^N$ is of rank $=\dim_{\mathbb{R}}(V)$ with $\boldsymbol{a}\in S(\Lambda(\boldsymbol{a}))$ if and only if $\boldsymbol{a}\in\mathcal{D}_N^V$. Moreover, $\Lambda(\boldsymbol{a})=\Lambda(\boldsymbol{b})$ for only finitely many $\boldsymbol{b}\in\mathcal{D}_N^V$ with an upper bound on their number, call it $\beta(V)$, depending only on the dimension of V; we will write β_N for $\beta(\mathbb{R}^N)$.*

Proof. The first assertion is clear from the definition of $\mathcal{D}_N^V$. The second assertion follows from a well known fact in the reduction theory of positive definite quadratic forms (see, for instance, Theorems 1.1-1.2 in Chapter 12 of [5]). □

For each $R\in\mathbb{R}_{>0}$, let $B_N^V(R)$ be a ball of radius R centered at the origin in V, and let

$$\mathcal{D}_N^V(R)=\left\{\boldsymbol{a}\in\mathcal{D}_N^V:\|\boldsymbol{a}\|\le R\right\}=\mathcal{D}_N^V\cap B_N^V(R).$$

It is easy to notice that $\boldsymbol{a}\in\mathcal{D}_N^V$ if and only if $R\boldsymbol{a}\in\mathcal{D}_N^V$, and hence $\mathcal{D}_N^V(R)=R\mathcal{D}_N^V(1)$ is a homogeneously expanding domain. Moreover, $\mathcal{D}_N^V(R)$ is a symmetric bounded star body, and hence is Jordan-measurable. We write $\mathcal{D}_N(R)$ for $\mathcal{D}_N\cap B_N(R)$, where $B_N(R)$ is a ball of radius R centered at the origin in $\mathbb{R}^N$.

Given a vector $\boldsymbol{a}\in\mathbb{R}^N$ with $\mathrm{co}(\boldsymbol{a})=k$, let $\boldsymbol{a}_1,\dots,\boldsymbol{a}_k$ be some fixed ordering of the vectors $\boldsymbol{a},\mathrm{rot}(\boldsymbol{a}),\dots,\mathrm{rot}^{k-1}(\boldsymbol{a})$. Define the angle sequence $\{\theta_1,\dots,\theta_{k-1}\}$ of this ordering as follows: for each $1\le i\le k-1$, let θ_i be the angle between $\boldsymbol{a}_{i+1}$ and the subspace spanned by $\boldsymbol{a}_1,\dots,\boldsymbol{a}_i$.

Lemma 3.2. *Let $V \subseteq \mathbb{R}^N$ be an L-dimensional subspace closed under the rotational shift operator. Assume that V contains a vector $\boldsymbol{a}$ with $\mathrm{co}(\boldsymbol{a}) = L$ such that some ordering of its L linearly independent rotations has the corresponding angle sequence satisfying the condition*

$$\pi/3 + \varepsilon \leq \theta_i \leq 2\pi/3 - \varepsilon \tag{9}$$

for each $1 \leq i \leq k-1$, for some $\varepsilon > 0$. Then $\mathrm{Vol}_L(\mathcal{D}_N^V(R)) = O(R^L)$, where the constant in the O-notation depends on V, L, and N.

Proof. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_L$ be the ordering of L linearly independent rotations of $\boldsymbol{a}$ with the corresponding angle sequence as in (9). Notice that $\|\boldsymbol{a}_1\| = \cdots = \|\boldsymbol{a}_L\| = \|\boldsymbol{a}\|$, and so Theorem 1 of [2] guarantees that $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_L$ are minimal vectors in $\Lambda(\boldsymbol{a})$, hence $\boldsymbol{a} \in \mathcal{D}_N^V$.

Let $\delta > 0$ and let

$$B(V, \delta) = \{\boldsymbol{x} \in V : \|\boldsymbol{x}\| \leq \delta\}$$

be the closed ball of radius δ centered at the origin in V. Let $\boldsymbol{t} \in B(V, \delta)$ and $\boldsymbol{a}' = \boldsymbol{a} + \boldsymbol{t}$. Let $\boldsymbol{a}'_1, \ldots, \boldsymbol{a}'_L$ be the rotations of $\boldsymbol{a}'$ corresponding to the rotations $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_L$ of $\boldsymbol{a}$. There exists a $\delta > 0$, depending on ε, small enough so that for every $\boldsymbol{t} \in B(V, \delta)$ the angle sequence $\{\theta'_1, \ldots, \theta'_{k-1}\}$ of $\boldsymbol{a}'_1, \ldots, \boldsymbol{a}'_L$ still satisfies (9) with ε replaced by some $\varepsilon' > 0$. Then, as above, Theorem 1 of [2] guarantees that $\boldsymbol{a}' \in \mathcal{D}_N^V$, i.e., $\boldsymbol{a} + B(V, \delta) \subseteq \mathcal{D}_N^V$, and so $\mathcal{D}_N^V$ must have positive L-dimensional volume. Since $\mathcal{D}_N^V$ is a homogeneously expanding domain, we must have

$$0 < \mathrm{Vol}_L(\mathcal{D}_N^V(R)) = \mathrm{Vol}_L(R\mathcal{D}_N^V(1)) = O(R^L),$$

which completes the proof of the lemma. □

Remark 3.1. We will apply Lemma 3.2 to $\mathbb{R}^N$. Notice that the angle sequence of the rotations of the first standard basis vector $\boldsymbol{e}_1 \in \mathbb{R}^N$ satisfies the assumption of Lemma 3.2. Hence $\mathrm{Vol}_N(\mathcal{D}_N(R)) = O(R^N)$ for every $N \geq 2$, by Lemma 3.2.

Remark 3.2. There is also another way to look at the set $\mathcal{D}_N^V$ with V as in the statement of Lemma 3.2. For each $\boldsymbol{a} \in V$, all rotations of $\boldsymbol{a}$ have to be in V, and so $\mathrm{co}(\boldsymbol{a}) \leq L$. Let

$$M_V(\boldsymbol{a}) = (\boldsymbol{a} \ \mathrm{rot}(\boldsymbol{a}) \ \ldots \ \mathrm{rot}^{L-1}(\boldsymbol{a})), \tag{10}$$

and notice that $M_V(\boldsymbol{a}) = M(\boldsymbol{a})$ when $V = \mathbb{R}^N$. Define the corresponding $L \times L$ Gram matrix

$$Q_V(\boldsymbol{a}) = M_V(\boldsymbol{a})^t M_V(\boldsymbol{a}),$$

and let us write q_{ij} for the entires of this matrix, then

$$q_{ij} = q_{ij}^V(\boldsymbol{a}) := \mathrm{rot}^{i-1}(\boldsymbol{a}) \cdot \mathrm{rot}^{j-1}(\boldsymbol{a}).$$

Notice that

$$\mathrm{rot}^{i-1}(\boldsymbol{a}) \cdot \mathrm{rot}^{j-1}(\boldsymbol{a}) = \mathrm{rot}^{i}(\boldsymbol{a}) \cdot \mathrm{rot}^{j}(\boldsymbol{a}), \tag{11}$$

and so all the distinct entries q_{ij} are represented in the first row. Furthermore,

$$\boldsymbol{a} \cdot \mathrm{rot}^{i-1}(\boldsymbol{a}) = \boldsymbol{a} \cdot \mathrm{rot}^{N-i+1}(\boldsymbol{a}) \tag{12}$$

for each $2 \leq i \leq N-1$, and hence the total number of distinct off-diagonal entries in the matrix $Q_V(\boldsymbol{a})$ is at most $[N/2]$; all the diagonal entries $q_{ii} = \|\boldsymbol{a}\|^2$. Now, $\boldsymbol{a} \in \mathcal{D}_N^V$ if and only if $Q_V(\boldsymbol{a})$ is in the corresponding Minkowski reduction domain, which is known to be a convex polyhedral cone in $\mathbb{R}^{\frac{L(L+1)}{2}}$ with a finite number of

facets (see, for instance, Chapter 12 of [5] or [21]), and conditions (10), (11), (12) imply that $Q_V(\boldsymbol{a})$ would have to be in a specific section of this cone. On the other hand, given a Gram matrix Q, the basis matrix M such that $Q = M^t M$ is uniquely determined up to an orthogonal transformation.

Lemma 3.3. *Let $R \in \mathbb{R}_{>0}$, and define*

$$f_N(R) = \#\left\{\Lambda(\boldsymbol{a}) \in \mathcal{C}_N : \|\boldsymbol{a}\| = \lambda_1(\Lambda(\boldsymbol{a})) = \lambda_N(\Lambda(\boldsymbol{a})) \le R\right\}, \tag{13}$$

then

$$O(R^N) \le f_N(R) \le O(R^N), \tag{14}$$

where the constants in the O-notation depend only on N.

Proof. Let β_N be as in Lemma 3.1, then

$$\frac{1}{\beta_N} \#\left(\mathbb{Z}^N \cap \mathcal{D}_N(R)\right) \le f_N(R) \le \#\left(\mathbb{Z}^N \cap \mathcal{D}_N(R)\right) \tag{15}$$

by Lemma 3.1. Theorem 2 on p. 128 of [11] asserts that

$$\#\left(\mathbb{Z}^N \cap \mathcal{D}_N(R)\right) = \mathrm{Vol}_N(\mathcal{D}_N(R)) + O(R^{N-1}). \tag{16}$$

and so (14) follows by combining (16) with Lemma 3.2 and (15). □

Remark 3.3. The boundary of the set $\mathcal{D}_N(R)$ is Lipschitz parameterizable, however that is not important for the application of Theorem 2 on p. 128 of [11] in the argument above, since we are only using the main term of the asymptotic formula in our inequalities, and Lemma 3.2 implies that there exist sets C_1, C_2 with Lipschitz parameterizable boundaries (in fact, convex sets) such that $RC_1 \subseteq \mathcal{D}_N^V(R) \subseteq RC_2$ for all $R > 0$.

Proof of Theorem 1.1. The theorem now follows from the estimates of Lemma 3.3. □

Now we comment on the connection of our results to the equivalence of SVP and SIVP. Let

$$\mathcal{R}_N = \left\{\Lambda(\boldsymbol{a}) \in \mathcal{C}_N : \|\boldsymbol{a}\| = \lambda_1(\Lambda(\boldsymbol{a})) = \lambda_N(\Lambda(\boldsymbol{a}))\right\},$$

and let $\Gamma \in \mathcal{R}_N$. Suppose that $\boldsymbol{c}, \mathrm{rot}(\boldsymbol{c}), \ldots, \mathrm{rot}^{N-1}(\boldsymbol{c})$ are linearly independent for every $\boldsymbol{c} \in S(\Gamma)$, then SIVP is equivalent to SVP on Γ. In the next lemma we prove that this is true for a positive proportion of lattices in $\mathcal{R}_N$. Specifically, let

$$\mathcal{R}'_N = \left\{\Gamma \in \mathcal{R}_N : \mathrm{co}(\boldsymbol{c}) = N \ \forall\ \boldsymbol{c} \in S(\Gamma)\right\},$$

and define

$$f'_N(R) = \#\left\{\Gamma \in \mathcal{R}'_N : \lambda_N(\Gamma) \le R\right\}$$

for any $R \in \mathbb{R}_{>0}$.

Lemma 3.4. *As $R \to \infty$, we have*

$$\frac{f'_N(R)}{f_N(R)} \ge O(1),$$

where the constant in O-notation depends only on N.

Proof. Let $\Gamma \in \mathcal{R}_N$, and suppose that $\boldsymbol{c} \in S(\Gamma)$ is such that $\mathrm{co}(\boldsymbol{c}) < N$. Then $\boldsymbol{c} \in \Gamma \cap H_{\Phi_d}$ for some $d \mid N$. In other words, $\Gamma \in \mathcal{R}_N \setminus \mathcal{R}'_N$ if and only if

$$S(\Gamma) \cap \left(\bigcup_{d|N} H_{\Phi_d} \right) \neq \emptyset. \tag{17}$$

Then

$$f'_N(R) \asymp \#\left\{ \boldsymbol{a} \in \mathbb{Z}^N \cap \mathcal{D}_N(R) : \Gamma = \Lambda(\boldsymbol{a}) \text{ does not satisfy (17)} \right\},$$

and since (17) is given by finitely many polynomial conditions, we have $f'_N(R) \asymp f_N(R)$. □

Remark 3.4. Lemma 3.4 then guarantees that

$$\frac{\#\left\{\Gamma \in \mathcal{R}'_N : \lambda_N(\Gamma) \leq R\right\}}{\#\left\{\Gamma \in \mathcal{R}_N : \lambda_N(\Gamma) \leq R\right\}} \geq O(1) \text{ as } R \to \infty. \tag{18}$$

By our observation above, SVP and SIVP are equivalent on $\mathcal{R}'_N$, and so the two problems are equivalent on a positive proportion of cyclic lattices in $\mathcal{R}_N$.

In fact, we can use the idea in the proof of Lemma 3.2 and Remark 3.1 to explicitly construct full-rank WR lattices of the form $\Lambda(\boldsymbol{a})$ in $\mathbb{R}^N$ on which SVP and SIVP are equivalent.

Corollary 3.5. *Let $k_1, \ldots, k_{N-1} \in \mathbb{Z}$ be nonzero integers, $m = \mathrm{lcm}(k_1, \ldots, k_{N-1})$, and*

$$\boldsymbol{a} = \left(m, \frac{m}{k_1}, \ldots, \frac{m}{k_{N-1}} \right)^t \in \mathbb{Z}^N.$$

There exists a sufficiently large positive integer l, depending only on the dimension N, such that whenever $|k_1|, \ldots, |k_{N-1}| \geq l$, the lattice $\Lambda(\boldsymbol{a}) \in \mathcal{R}'_N$.

Proof. Let l be a positive integer, the choice of which is to be specified below, and let the rest of the notation be as in the statement of the corollary. Let $\boldsymbol{b} = \frac{1}{m}\boldsymbol{a} = \boldsymbol{e}_1 + \boldsymbol{\varepsilon}$, where

$$\boldsymbol{\varepsilon} = (0, 1/k_1, \ldots, 1/k_{N-1}).$$

Taking l sufficiently large, we can ensure that the angle sequence of the rotations of the vector $\boldsymbol{b}$ satisfies condition (9) for some $\varepsilon > 0$, in which case $\Lambda(\boldsymbol{b})$ is a lattice of rank N with minimal norm equal to $\|\boldsymbol{b}\|$ by the same argument as in the proof of Lemma 3.2 and Remark 3.1.

We can assume that $l > 10N$ so that $(1 - N/l)^2 > 81/100$. We will now show that

$$S(\Lambda(\boldsymbol{b})) = \{\pm\boldsymbol{b}, \pm \mathrm{rot}(\boldsymbol{b}), \ldots, \pm \mathrm{rot}^{N-1}(\boldsymbol{b})\}. \tag{19}$$

Indeed, suppose

$$\boldsymbol{c} = \sum_{i=1}^{N} \alpha_i \, \mathrm{rot}^{i-1}(\boldsymbol{b}) \in S(\Lambda(\boldsymbol{b})),$$

where $\alpha_1, \ldots, \alpha_N \in \mathbb{Z}$, not all zero. Let $\alpha = \max_{1 \leq i \leq N} |\alpha_i|$, so for each $1 \leq n \leq N$

$$|\alpha_1 + \cdots + \alpha_{n-1} + \alpha_{n+1} + \cdots + \alpha_N| \leq N\alpha.$$

Then c_n, the n-th coordinate of $\boldsymbol{c}$, satisfies the inequalities

$$\max\{0, |\alpha_n| - N\alpha/l\} \leq |c_n| \leq |\alpha_n| + N\alpha/l,$$

and so we have

$$\|\boldsymbol{c}\|^2 \geq \alpha^2(1-N/l)^2.$$

Assume first that $\alpha > 1$, then we have

$$\|\boldsymbol{c}\|^2 > 2 > 1 + (N-1)/l^2 \geq \|\boldsymbol{b}\|^2.$$

Therefore we must have $\alpha = 1$. If $\alpha_n = \pm 1$ for only one n, then $\boldsymbol{c} = \pm \operatorname{rot}^{n-1}(\boldsymbol{b})$. Hence assume there exist $1 \leq j < n \leq N$ such that $\alpha_j, \alpha_n = \pm 1$, then

$$\|\boldsymbol{c}\|^2 \geq 2(1-N/l)^2 > 1 + (N-1)/l^2 = \|\boldsymbol{b}\|^2,$$

which establishes (19). Then $\Lambda(\boldsymbol{a}) = m\Lambda(\boldsymbol{b})$, and hence

$$S(\Lambda(\boldsymbol{a})) = \{\pm\boldsymbol{a}, \pm\operatorname{rot}(\boldsymbol{a}), \ldots, \pm\operatorname{rot}^{N-1}(\boldsymbol{a})\},$$

meaning that each vector in $S(\Lambda(\boldsymbol{a}))$ has cyclic order $= N$. Thus $\Lambda(\boldsymbol{a}) \in \mathcal{R}'_N$. $\square$

Remark 3.5. To summarize, the main idea of Corollary 3.5 is to pick a rational vector $\boldsymbol{b}$ from a small ball centered at $\boldsymbol{e}_1$. Then the set of minimal vectors of $\Lambda(\boldsymbol{b})$ will consist only of $\pm$ rotations of $\boldsymbol{b}$ due to the fact that one coordinate of $\boldsymbol{b}$ strongly dominates others. Hence SVP and SIVP are equivalent on $\Lambda(\boldsymbol{b})$, and $\Lambda(\boldsymbol{b})$ is similar to some full-rank WR cyclic sublattice of $\mathbb{Z}^N$ because coordinates of $\boldsymbol{b}$ are rational. Since a ball of positive radius centered at $\boldsymbol{e}_1$ contains infinitely many rational points, infinitely many mutually non-similar lattices with this equivalence property can be constructed this way.

4. Cyclic lattices in the plane

In this section we prove Theorem 1.2. Recall that every planar cyclic lattice is spanned by vectors corresponding to its successive minima. Furthermore, for a sublattice Γ of $\mathbb{Z}^2$, $|S(\Gamma)| = 2$ or 4, and Γ is WR if and only if $|S(\Gamma)| = 4$. If Γ is not WR, then $|S(\Gamma)| = 2$ and the vectors corresponding to first and second successive minima are unique (up to $\pm$ sign): this follows, for instance, from the second Theorem and discussion after it on p. 203 of [6].

Lemma 4.1. *A lattice $\Gamma \in \mathcal{C}_2$ is WR if and only if either $\Gamma = \Lambda(\boldsymbol{a})$ for some $\boldsymbol{a} \in S(\Gamma)$ or $\Gamma = \alpha \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \mathbb{Z}^2$ for some $\alpha \in \mathbb{Z}_{>0}$. On the other hand, $\Gamma \in \mathcal{C}_2$ is not WR if and only if $\Gamma = \begin{pmatrix} \alpha & \beta \\ \alpha & -\beta \end{pmatrix} \mathbb{Z}^2$ for some distinct positive integers α, β.*

Proof. If $\Gamma = \Lambda(\boldsymbol{a})$ for some $\boldsymbol{a} \in S(\Gamma)$, then $S(\Gamma) = \{\pm\boldsymbol{a}, \pm\operatorname{rot}(\boldsymbol{a})\}$ and the vectors $\boldsymbol{a}, \operatorname{rot}(\boldsymbol{a})$ are linearly independent. If $\Gamma = \alpha \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \mathbb{Z}^2$ for some $\alpha \in \mathbb{Z}$, then

$$S(\Gamma) = \left\{ \pm\alpha \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \pm\alpha \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}.$$

In both cases, it is clear that Γ is WR.

Suppose then that Γ is WR, then $|S(\Gamma)| = 4$ and $S(\Gamma)$ contains a basis for Γ. Let $\boldsymbol{a} \in S(\Gamma)$. First assume $\Lambda(\boldsymbol{a})$ has rank 2, then $\boldsymbol{a}, \operatorname{rot}(\boldsymbol{a}) \in S(\Gamma)$ are linearly independent, and hence form a basis for Γ. Therefore $\Gamma = \Lambda(\boldsymbol{a})$. Next suppose that $\Lambda(\boldsymbol{a})$ has rank 1, then $\boldsymbol{a} = c\operatorname{rot}(\boldsymbol{a})$ for some $c \in \mathbb{Z}$, which easily implies that

$a_1 = a_2$, and so $\boldsymbol{a} = \alpha \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ for some $\alpha \in \mathbb{Z}$. Since Γ is WR, there must exist $\boldsymbol{c} \in S(\Gamma)$ such that $\boldsymbol{c} \neq \pm \boldsymbol{a}$. Then $\mathrm{rot}(\boldsymbol{c})$ is also in $S(\Gamma)$, and since $|S(\Gamma)| = 4$, we must have $-\boldsymbol{c} = \mathrm{rot}(\boldsymbol{c})$ and $\|\boldsymbol{c}\| = \|\boldsymbol{a}\|$, meaning that $\boldsymbol{c} = \alpha \begin{pmatrix} -1 \\ 1 \end{pmatrix}$. Then $S(\Gamma) = \{\pm \boldsymbol{a}, \pm \boldsymbol{c}\}$, and so

$$\Gamma = \alpha \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \mathbb{Z}^2.$$

This completes the proof of the first statement.

The second statement follows immediately from the observation that $\mathbb{R}^2$ has precisely two cyclotomic subspaces:

$$H_{\Phi_1} = \mathrm{span}_{\mathbb{R}} \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}, \; H_{\Phi_2} = \mathrm{span}_{\mathbb{R}} \left\{ \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}.$$

□

For $R \in \mathbb{R}_{>0}$, let $f_2(R)$ be as in (13) for $N = 2$, and define

$$g_2(R) = \# \left\{ \Gamma \in \mathcal{C}_2 : \Gamma \neq \Lambda(\boldsymbol{a}) \; \forall \; \boldsymbol{a} \in \mathbb{Z}^2, \; \lambda_1(\Gamma) = \lambda_2(\Gamma) \leq R \right\}.$$

We can now use Lemma 4.1 to estimate the functions $f_2(R)$ and $g_2(R)$.

Lemma 4.2. *Let $R \in \mathbb{R}_{>0}$, then*

$$0.200650... \times R^2 - 3.742382... \times R \leq f_2(R) \leq 0.267638... \times R^2 + 0.965925... \times R, \tag{20}$$

$$g_2(R) = \left[\frac{R}{\sqrt{2}} \right]. \tag{21}$$

Proof. First assume $\Gamma = \Lambda(\boldsymbol{a})$ for some $\boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \in S(\Gamma)$. Notice that we can assume without loss of generality that $|a_1| > |a_2|$. The condition that $\boldsymbol{a}, \mathrm{rot}(\boldsymbol{a})$ form a Minkowski reduced basis amounts to satisfying the following condition (see, for instance, Note 1 on p. 257 of [5]):

$$a_1^2 + a_2^2 \geq 4|a_1 a_2|.$$

This means that either

$$a_1^2 + a_2^2 - 4a_1 a_2 \geq 0, \; a_1 a_2 \geq 0, \tag{22}$$

or

$$a_1^2 + a_2^2 + 4a_1 a_2 \geq 0, \; a_1 a_2 < 0. \tag{23}$$

First consider the (22) situation, then there are the following two options:

(1) $a_1 \geq [(2+\sqrt{3})a_2] + 1 > a_2 \geq 0$,
(2) $0 \geq a_2 > [(2+\sqrt{3})a_2] - 1 \geq a_1$.

Notice that a_1, a_2 satisfy option (1) if and only if $-a_1, -a_2$ satisfy option (2), hence they correspond to the same lattice $\Lambda(\boldsymbol{a})$. Next consider the (23) situation, then there are the following two options:

(3) $a_1 \leq -[(2+\sqrt{3})a_2] - 1 < 0 < a_2$,
(4) $a_1 \geq -[(2+\sqrt{3})a_2] + 1 > 0 > a_2$.

Again, a_1, a_2 satisfy option (3) if and only if $-a_1, -a_2$ satisfy option (4), hence they correspond to the same lattice $\Lambda(\boldsymbol{a})$. Notice also that for each pair a_1, a_2 satisfying options (1) and (2), there is precisely one pair satisfying options (3) and (4). Hence we will only count vectors $\boldsymbol{a} \in \mathbb{Z}^2$ with $\|\boldsymbol{a}\| \leq R$ satisfying (1) and multiply this number by 2. Therefore:

$$f_2(R) = 2\sum_{a_2=1}^{A(R)} \left(\left[\sqrt{R^2 - a_2^2} \right] - \left[(2+\sqrt{3})a_2 \right] - 1 \right), \tag{24}$$

where

$$A(R) = \left[\frac{R}{2\sqrt{2+\sqrt{3}}} \right].$$

Using (24), we now give quick estimates on $f_2(R)$. A higher degree of precision is easily possible here, but we choose in favor of simplicity. Notice that

$$\begin{aligned} f_2(R) &\geq 2RA(R) - 2(3+\sqrt{3})\sum_{a_2=1}^{A(R)} a_2 - 2A(R) \\ &= 2RA(R) - (3+\sqrt{3})A(R)^2 - (5+\sqrt{3})A(R) \\ &\geq \frac{\left(4\sqrt{2+\sqrt{3}} - 3 - \sqrt{3}\right)R^2}{8+4\sqrt{3}} - \frac{\left(5+\sqrt{3}+4\sqrt{2+\sqrt{3}}\right)R}{2\sqrt{2+\sqrt{3}}} \\ &= 0.200650... \times R^2 - 3.742382... \times R. \end{aligned} \tag{25}$$

On the other hand,

$$\begin{aligned} f_2(R) &\leq 2RA(R) - (2+\sqrt{3})A(R)(A(R)+1) \\ &\leq \frac{R^2}{\sqrt{2+\sqrt{3}}} - \frac{R^2}{4} + \frac{\sqrt{2+\sqrt{3}}\ R}{2} \\ &= 0.267638... \times R^2 + 0.965925... \times R. \end{aligned} \tag{26}$$

Next suppose $\Gamma \in \mathcal{C}_2$ is WR, but not of the form $\Gamma = \Lambda(\boldsymbol{a})$ for some $\boldsymbol{a} \in S(\Gamma)$, then $\Gamma = \alpha \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \mathbb{Z}^2$ for some $\alpha \in \mathbb{Z}_{>0}$, by Lemma 4.1. Now, $\lambda_1(\Gamma) \leq R$ if and only if

$$0 < \alpha \leq \frac{R}{\sqrt{2}},$$

and so α can be equal to $1, 2, \ldots, [R/\sqrt{2}]$. Since α identifies Γ uniquely, (21) follows. This completes the proof. □

We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2. Notice that

$$\#\left\{\Gamma \in \mathcal{C}_2 : \lambda_2(\Gamma) \leq R,\ \Gamma \text{ is WR}\right\} = f_2(R) + g_2(R).$$

The result now follows directly from Lemma 4.2. □

5. Permutation invariance

Let S_N be the group of permutations on $N \geq 2$ elements and define the action of S_N on $\mathbb{R}^N$ as in (3). In fact, for each $\tau \in S_N$ define E_τ to be the $N \times N$ matrix obtained from the $N \times N$ identity matrix I_N by permuting its rows with τ; in other words, $E_\tau = (e_{ij})_{1 \leq i,j \leq N}$ where $e_{ij} = 1$ whenever $j = \tau(i)$ and $e_{ij} = 0$ otherwise. These are the well-known permutation matrices. Then for every $\boldsymbol{x} \in \mathbb{R}^N$,

$$\tau \boldsymbol{x} = E_\tau \boldsymbol{x}.$$

It is easy to check that the map $\psi : S_N \to \mathrm{GL}_N(\mathbb{Z})$ given by $\tau \mapsto E_\tau$ is a faithful representation of S_N in $\mathrm{GL}_N(\mathbb{R})$, and we write $\psi(S_N)$ for its image. Notice that the rotational shift operator is given precisely by the N-cycle $(1\ 2 \ldots N) \in S_N$:

$$\mathrm{rot}(\boldsymbol{x}) = E_{(1\ 2 \ldots N)} \boldsymbol{x} = \begin{pmatrix} 0 & \ldots & 0 & 1 \\ 1 & \ldots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \ldots & 1 & 0 \end{pmatrix} \boldsymbol{x}. \tag{27}$$

Observe also that each matrix E_τ is orthogonal, and hence lattices Λ and $\tau\Lambda := E_\tau \Lambda$ are isometric. This in particular means that Λ is WR if and only if $\tau\Lambda$ is invariant for every $\tau \in S_N$.

As in Section 1, we say that a lattice $\Lambda \subset \mathbb{R}^N$ is *τ-invariant* (or invariant under τ) for a fixed $\tau \in S_N$ if $E_\tau \Lambda = \Lambda$. It is clear that Λ is τ-invariant if and only if it is σ-invariant for every permutation σ in $\langle \tau \rangle$, the cyclic group generated by τ. This observation together with (27) readily implies that cyclic lattices are precisely the sublattices of $\mathbb{Z}^N$ which are invariant under the cyclic permutation group $\langle (1\ 2 \ldots N) \rangle$. Further notice that if Λ is τ-invariant and σ-invariant for some two elements $\sigma, \tau \in S_N$, then it is $(\sigma\tau)$-invariant. Recall that the transposition $(1\ 2)$ and N-cycle $(1\ 2 \ldots N)$ together generate S_N, and hence any cyclic lattice that is also $(1\ 2)$-invariant is invariant under the entire group S_N. We can now extend our results on cyclic lattices to τ-invariant full-rank sublattices of $\mathbb{Z}^N$ for any N-cycle τ.

Proof of Corollary 1.3. Let $\tau \in S_N$ be an N-cycle, and let us write σ for the N-cycle $(1\ 2\ \ldots\ N)$. Since all N-cycles are in the same conjugacy class, there exists $g \in S_N$ such that $\tau = g\sigma g^{-1}$. Then a lattice Γ is τ-invariant if and only if the lattice $g^{-1}\Gamma$ is σ-invariant, i.e., cyclic. Since lattices Γ and $g^{-1}\Gamma$ are isometric, it follows that the sets

$$\{\Gamma \in \mathcal{C}_N : \lambda_N(\Gamma) \leq R\}, \ \{\Gamma \in \mathcal{C}_N(\tau) : \lambda_N(\Gamma) \leq R\}$$

are in bijective correspondence, as are the corresponding subsets of WR and WR_1 lattices, for each $R \in \mathbb{R}_{>0}$. The statement of the corollary now follows from Theorem 1.1. □

Since permutation invariant sublattices of $\mathbb{Z}^N$ are a natural generalization of cyclic lattices, we conclude with two questions about them.

Question 1. *Do permutation invariant full-rank sublattices of $\mathbb{Z}^N$ have some underlying algebraic structure? More specifically, which of them, if any, can be obtained from ideals in some polynomial rings, analogously to the construction of cyclic lattices from ideals in $\mathbb{Z}[x]/(x^N - 1)$?*

Question 2. *How many WR lattices are there among all τ-invariant sublattices of $\mathbb{Z}^N$ for an arbitrary permutation $\tau \in S_N$?*

A certain approach to Question 2 by means of extending the current method and studying automorphism groups of lattices is the subject of [7].

Both of the above questions can also be extended to *signed* permutation invariant lattices. Let $\mathcal{J}_N \cong (\mathbb{Z}/2\mathbb{Z})^N$ be the finite abelian subgroup of $\mathrm{GL}_N(\mathbb{Z})$ consisting of diagonal matrices with all diagonal entries being ± 1. For a fixed $g \in \mathcal{J}_N$ and $\tau \in S_N$, we will say that a lattice $\Lambda \subset \mathbb{R}^N$ is *g-signed τ-invariant* if $gE_\tau\Lambda = \Lambda$. Now we can ask Questions 1 and 2 for signed permutation invariant lattices. As an example, let

$$g = \begin{pmatrix} -1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \in \mathcal{J}_N, \ \tau = (1\ 2 \dots N) \in S_N,$$

then g-signed τ-invariant sublattices of $\mathbb{Z}^N$ are images of ideals in the quotient polynomial ring $\mathbb{Z}[x]/(x^N + 1)$ under the same map ρ as for cyclic lattices in Section 1; we will call these the signed cyclic lattices. For instance, the signed cyclic lattices in dimension 2 are of the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mathbb{Z}^2, \ a, b \in \mathbb{Z}.$$

These are orthogonal sublattices of $\mathbb{Z}^2$, which come from ideals in $\mathbb{Z}[x]/(x^2 + 1)$ (alternatively, from ideals in Gaussian integers $\mathbb{Z}[i]$ under the standard Minkowski embedding of $\mathbb{Q}(i)$ into the real plane), and are always WR. This observation suggests that signed cyclic lattices in higher dimensions may also have better than average chances of being WR.

Acknowledgment. We would like to thank the referees for the highly helpful suggestions, which significantly improved the quality of the paper.

References

[1] A. H. Banihashemi and A. K. Khandani. On the complexity of decoding lattices using the Korkin-Zolotarev reduced basis. *IEEE Trans. Inform. Theory*, 44(1):162–171, 1998.

[2] R. Baraniuk, S. Dash, and R. Neelamani. On nearly orthogonal lattice bases. *SIAM J. Discrete Math.*, 21(1):199–219, 2007.

[3] D. J. Bernstein, J. Buchmann, and E. Dahmen (editors). *Post-quantum cryptography.* Springer-Verlag, Berlin, 2009.

[4] Johannes A. Buchmann and Richard Lindner. Density of ideal lattices. In Johannes A. Buchmann, John Cremona, and Michael E. Pohst, editors, *Algorithms and Number Theory*, number 09221 in Dagstuhl Seminar Proceedings, Dagstuhl, Germany, 2009. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany.

[5] J. W. S. Cassels. *Rational quadratic forms.* Academic Press, Inc., 1978.

[6] J. L. Donaldson. Minkowski reduction of integral matrices. *Math. Comp.*, 33(145):201–216, 1979.

[7] L. Fukshansky, S. R. Garcia, and X. Sun. Permutation invariant lattices. *preprint: arXiv:1409.1491.*

[8] L. Fukshansky and S. Robins. Frobenius problem and the covering radius of a lattice. *Discrete Comput. Geom.*, 37(3):471–483, 2007.

[9] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, and W. Whyte. NTRUsign: Digital signatures using the NTRU lattice. In *Topics in Cryptology - CT-RSA 2003: The Cryptographers Track at the RSA Conference, volume 2612 of Lecture Notes in Computer Science*, pages 122–140. Springer-Verlag, 2003.

[10] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: a ring-based public key cryptosystem. In *Algorithmic number theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., 1423*, pages 267–288. Springer, Berlin, 1998.

[11] S. Lang. *Algebraic Number Theory*. Springer-Verlag, 1994.

[12] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *Automata, languages and programming. Part II, Lecture Notes in Comput. Sci., 4052*, pages 144–155. Springer, Berlin, 2006.

[13] J. Martinet. Sur l'indice d'un sous-réseau. In *Réseaux euclidiens, designs sphériques et formes modulaires, Monogr. Enseign. Math., 37*, pages 163–211. Enseignement Math., Geneva, 2001.

[14] J. Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag, 2003.

[15] C. McMullen. Minkowski's conjecture, well-rounded lattices and topological dimension. *J. Amer. Math. Soc.*, 18(3):711–734, 2005.

[16] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. *FOCS, IEEE Computer Society*, pages 356–365, 2002.

[17] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Comput. Complexity*, 16(4):365–411, 2007.

[18] D. Micciancio and S. Goldwasser. *Complexity of lattice problems: A cryptographic perspective*, volume 671. Kluwer Academic Publishers, 2002.

[19] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. *Theory of cryptography, Lecture Notes in Comput. Sci., 3876, Springer, Berlin,*, pages 145–166, 2006.

[20] M. Pohst. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. Technical report.

[21] A. Schürmann. *Computational geometry of positive definite quadratic forms*, volume 48 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2009.

[22] M. Schneider. Sieving for shortest vectors in ideal lattices. In *Progress in Cryptology – AFRICACRYPT 2013, Lecture Notes in Computer Science Volume 7918*, pages 375–391. Springer, Berlin, 2013.

[23] D. Stehlé and R. Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In *Advances in cryptology–EUROCRYPT 2011, Lecture Notes in Comput. Sci., 6632*, pages 27–47. Springer, Heidelberg, 2011.

[24] Wikipedia. Circulant matrix. *http://en.wikipedia.org/wiki/Circulant_matrix*.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711

E-mail address: lenny@cmc.edu

School of Mathematical Sciences, Claremont Graduate University, Claremont, CA 91711

E-mail address: foxfur_32@hotmail.com