

ON LATTICE EXTENSIONS

MAXWELL FORST AND LENNY FUKSHANSKY

ABSTRACT. A lattice Λ is said to be an extension of a sublattice L of smaller rank if L is equal to the intersection of Λ with the subspace spanned by L . The goal of this paper is to initiate a systematic study of the geometry of lattice extensions. We start by proving the existence of a small-determinant extension of a given lattice, and then look at successive minima and covering radius. To this end, we investigate extensions (within an ambient lattice) preserving the successive minima of the given lattice, as well as extensions preserving the covering radius. We also exhibit some interesting arithmetic properties of deep holes of planar lattices.

1. INTRODUCTION AND STATEMENT OF RESULTS

Let $n \geq m \geq 2$ be integers and let Λ be a lattice of rank m in \mathbb{R}^n , then

$$\Lambda = AZ^m$$

for an $n \times m$ basis matrix A of rank m and *determinant* of Λ is

$$\det \Lambda = \sqrt{\det(A^\top A)},$$

which is its co-volume in $\text{span}_{\mathbb{R}} \Lambda$: this definition is independent of the choice of the basis matrix A for Λ . Let $B_m(1)$ be the m -dimensional unit ball centered at $\mathbf{0}$ in $\text{span}_{\mathbb{R}} \Lambda$ and write ω_m for the m -dimensional volume of $B_m(1)$. Then $B_m(r)$ is a ball of radius r and volume $\omega_m r^m$. We briefly recall the standard notation from the geometry of numbers (see [11] for the detailed exposition of the subject). First, the *successive minima* of Λ are real numbers

$$0 < \lambda_1(\Lambda) \leq \dots \leq \lambda_m(\Lambda),$$

given by

$$\lambda_i(\Lambda) = \min \{r \in \mathbb{R} : \dim_{\mathbb{R}} \text{span}_{\mathbb{R}}(B_m(r) \cap \Lambda) \geq i\}.$$

Then $\frac{1}{2}\lambda_1(\Lambda)$ is the radius of a ball in the sphere packing associated to Λ and the product of successive minima is bounded as follows by the Minkowski's Successive Minima Theorem:

$$\frac{2^m \det \Lambda}{m! \omega_m} \leq \prod_{i=1}^m \lambda_i(\Lambda) \leq \frac{2^m \det \Lambda}{\omega_m}.$$

Additionally, the *covering radius* of Λ is defined as

$$\mu(\Lambda) = \min \{r \in \mathbb{R} : \Lambda + B_m(r) = \text{span}_{\mathbb{R}} \Lambda\}.$$

2020 *Mathematics Subject Classification*. Primary: 11H06, 11H31, 52C05, 52C07, 52C15, 52C17.

Key words and phrases. lattice, successive minima, covering radius, deep hole.
Fukshansky was partially supported by the Simons Foundation grant #519058.

The classical inequality of Jarnik asserts that

$$\frac{1}{2}\lambda_m(\Lambda) \leq \mu(\Lambda) \leq \frac{1}{2} \sum_{i=1}^m \lambda_i(\Lambda).$$

Now, let $L \subset \Lambda$ be a sublattice of rank $k < m$. We say that Λ is an *extension* lattice of L if

$$\Lambda \cap \text{span}_{\mathbb{R}} L = L.$$

As a first example of lattice extensions, we demonstrate the following construction of a small-determinant extension of a sublattice inside of the integer lattice \mathbb{Z}^n .

Theorem 1.1. *Let $\mathbf{x}_1, \dots, \mathbf{x}_k$ be linearly independent vectors in \mathbb{Z}^n and let*

$$\Omega = \text{span}_{\mathbb{Z}} \{\mathbf{x}_1, \dots, \mathbf{x}_k\} \subset \mathbb{Z}^n$$

be the sublattice of rank k spanned by these vectors. Then there exists a full-rank extension $\Omega' \subseteq \mathbb{Z}^n$ of Ω so that

$$\det \Omega' = \gcd(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k).$$

Further, if $k = n - 1$ then there exists $\mathbf{y} \in \mathbb{Z}^n$ so that $\Omega' = \text{span}_{\mathbb{Z}} \{\Omega, \mathbf{y}\}$ and

$$\|\mathbf{y}\| \leq \left\{ \left(\frac{\gcd(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k)}{\det \Omega} \right)^2 + \mu(\Omega)^2 \right\}^{1/2}.$$

Throughout this paper, the wedge product of vectors, $\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k$ as above in the Grassmann algebra, is identified with the corresponding vector of Grassmann-Plücker coordinates; see Chapter 1 of [16] for details. We prove Theorem 1.1 in Section 2, where we also explain how it can be generalized to any lattice in \mathbb{R}^n (Remark 2.1). Lattice extensions play an implicit important role in a variety of contexts, for instance in lattice packing and covering constructions such as lamination (see [6], [13]), in reduction theory when constructing Minkowski or HKZ reduced bases (see [11], [13]), as well as in constructions of primitive collections in a lattice (see [7]). Further, the idea of lattice extensions was recently used to construct a family of counterexamples to the famous covering conjecture of Woods (see [14]). This being said, we have not seen lattice extensions studied explicitly. Our main goal in this note is to explore lattice extensions with control over their geometric invariants. In particular, we say that Λ is a *successive minima extension* of L if Λ is an extension of L such that

$$\lambda_j(\Lambda) = \lambda_j(L) \quad \forall 1 \leq j \leq k.$$

Also, we call Λ an *equal covering extension* of L if Λ is an extension of L such that

$$\mu(\Lambda) = \mu(L).$$

Given a lattice L of rank $k < n$ in \mathbb{R}^n , it is easy to construct a rank- $(k+1)$ successive minima extension Λ of L : we can simply take $\mathbf{u} \in \mathbb{R}^n$ to be a vector perpendicular to $\text{span}_{\mathbb{R}} L$ of norm $> \lambda_k(L)$ and define $\Lambda = \text{span}_{\mathbb{Z}} \{L, \mathbf{u}\}$. It is a more delicate problem to construct such an extension inside of a given full-rank lattice in \mathbb{R}^n , since such a perpendicular vector \mathbf{u} may simply not exist inside of our given lattice. Our next result addresses this problem while controlling the $(k+1)$ -st successive minimum of the constructed extension.

Theorem 1.2. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice of full rank, and let $L_k \subset \Lambda$ be a sublattice of rank $1 \leq k < n$. There exists a sublattice $L_{k+1} \subset \Lambda$ of rank $k+1$ such that $L_k \subset L_{k+1}$ is a lattice extension, $\lambda_j(L_{k+1}) = \lambda_j(L_k)$ for all $1 \leq j \leq k$ and*

$$(1) \quad \lambda_{k+1}(L_{k+1}) \leq \frac{\lambda_k(L_k)(v_*^2 + \sqrt{1 - v_*^2})}{\sqrt{1 - v_*^4}} + 2\mu,$$

where μ is the covering radius of Λ and v_* is the smallest root of the polynomial

$$p(v) = \left(\frac{\mu^2}{\lambda_k^2} (1 - v^4) - v^2(v^4 - v^2 + 1) \right)^2 - \left(\frac{2\mu^2}{\lambda_k^2} v(1 - v^4) + 2v^4 \right)^2 (1 - v^2)$$

in the interval $(0, 1)$: such v_* necessarily exists.

We prove Theorem 1.2 in Section 3. We also include an alternate version of the bound for Theorem 1.2 suggested to us by one of the referees (Remark 3.1). The situation is more complicated with equal covering extensions: they do not necessarily exist inside of a given lattice. Our next result is a full characterization of planar lattices that are equal covering extensions of some lattice of rank one. Let $\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{R}^2$ and $E_1 = \mathbb{Z}\mathbf{e}_1 \subset \mathbb{R}^2$ be a lattice of rank one in the plane. Then the covering radius of E_1 is $\mu(E_1) = 1/2$. More generally, for a rank-one lattice $\mathbb{Z}\mathbf{u} \in \mathbb{R}^n$ its covering radius is $\frac{1}{2}\|\mathbf{u}\|$.

Theorem 1.3. *A lattice $\Lambda \subset \mathbb{R}^2$ is an equal covering extension of E_1 if and only if*

$$(2) \quad \Lambda = \Lambda(\alpha) := \left(\begin{array}{cc} \alpha & \alpha - 1 \\ \sqrt{\alpha - \alpha^2} & \sqrt{\alpha - \alpha^2} \end{array} \right) \mathbb{Z}^2$$

for some real number $0 < \alpha < 1$. More generally, a lattice $\Lambda \subset \mathbb{R}^n$ of rank 2 is an equal covering extension of a rank-one lattice $L \subset \Lambda$ if and only if it is isometric to some lattice of the form $\det(L)\Lambda(\alpha)$, where $\Lambda(\alpha)$ is as in (2).

We discuss covering radii of planar lattices and prove Theorem 1.3 with some corollaries in Section 5. In particular, we show that the lattice coming from the ring of integers of a quadratic number field $\mathbb{Q}(\sqrt{D})$, for a squarefree rational integer D , via Minkowski embedding into \mathbb{R}^2 is an equal covering extension of a rank-one sublattice if and only if $D \not\equiv 1 \pmod{4}$. We also construct orthogonal equal covering extensions in any dimension, proving the following result.

Theorem 1.4. *Let $\Lambda_k \subset \mathbb{R}^n$ be an orthogonal lattice of rank $k < n$. There exists an orthogonal lattice $\Lambda_{k+1} \subset \mathbb{R}^n$ of rank $k+1$ so that $\Lambda_k \subset \Lambda_{k+1}$ is a lattice extension and $\mu(\Lambda_{k+1}) = \mu(\Lambda_k)$. Further, if \mathbf{z} is a deep hole of Λ_k it is also a deep hole of Λ_{k+1} .*

Recall that, given a lattice $\Lambda \subset \mathbb{R}^n$ a vector $\mathbf{z} \in \text{span}_{\mathbb{R}} \Lambda$ is called a *deep hole* of Λ if it is furthest from the lattice, i.e.

$$d(\mathbf{z}, \Lambda) = \max \{ d(\mathbf{y}, \Lambda) : \mathbf{y} \in \text{span}_{\mathbb{R}} \Lambda \},$$

where $d(\mathbf{y}, \Lambda) := \min \{ \|\mathbf{x} - \mathbf{y}\| : \mathbf{x} \in \Lambda \}$. Thus the covering radius of the lattice is the distance from the origin to the nearest deep hole. We discuss deep holes of lattices in some detail in Section 4 with a special focus on the two-dimensional situation. In particular, we obtain necessary and sufficient conditions for the deep

holes of a lattice $\Lambda \subset \mathbb{R}^2$ to have finite order as elements of the torus quotient group \mathbb{R}^2/Λ and give a bound on this order (Theorem 4.3).

Before we proceed, let us recall a few more standard notions of lattice theory. The isometries of a Euclidean space are given by real orthogonal matrices, and two lattices are *isometric* if there exists an isometry taking one to the other. Two lattices are *similar* if their scalar multiples are isometric for some choice of scalars. Both, isometry and similarity are equivalence relations on lattices of the same rank. A lattice is called *well-rounded* (abbreviated WR) if all of its successive minima are equal; this property is preserved under similarity.

2. SMALL-DETERMINANT EXTENSIONS IN \mathbb{Z}^n

In this section we present the first example of lattice extensions, proving Theorem 1.1. Let $\mathbf{x}_1, \dots, \mathbf{x}_k$ be k vectors in \mathbb{R}^n , $1 \leq k < n$. As we mentioned above, the wedge product $\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k$ can be identified with the vector of Plücker coordinates in $\mathbb{R}^{\binom{n}{k}}$, i.e. determinants of $k \times k$ submatrices of the $n \times k$ matrix $(\mathbf{x}_1 \dots \mathbf{x}_k)$.

Proposition 2.1. *Let $\mathbf{x}_1, \dots, \mathbf{x}_k$ be linearly independent vectors in \mathbb{Z}^n and let*

$$\Omega = \text{span}_{\mathbb{Z}} \{\mathbf{x}_1, \dots, \mathbf{x}_k\} \subset \mathbb{Z}^n$$

be the sublattice of rank m spanned by these vectors. Then there exists a full-rank extension $\Omega' \subseteq \mathbb{Z}^n$ of Ω so that

$$\det \Omega' = \gcd(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k).$$

Proof. Let $\bar{\Omega} = \mathbb{Z}^n \cap \text{span}_{\mathbb{R}} \Omega$, then $\bar{\Omega} \subset \mathbb{Z}^n$ is a sublattice of rank k containing Ω such that $\mathbb{Z}^n/\bar{\Omega}$ is torsion free. Hence any basis of $\bar{\Omega}$ is extendable to \mathbb{Z}^n . Let $\mathbf{y}_1, \dots, \mathbf{y}_k$ be a basis for $\bar{\Omega}$ extended to a basis for \mathbb{Z}^n by $\mathbf{y}_{k+1}, \dots, \mathbf{y}_n$. Since $\mathbf{x}_1, \dots, \mathbf{x}_k$ and $\mathbf{y}_1, \dots, \mathbf{y}_k$ are two collections of integer vectors spanning the same subspace of \mathbb{R}^n , the vectors of Plücker coordinates represent the same rational projective point. Further, since the collection $\mathbf{y}_1, \dots, \mathbf{y}_k$ is extendable to a basis of \mathbb{Z}^n , the Plücker coordinates of this collection must be relatively prime (Lemma 2 on p.15 of [5]). Hence

$$\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k = g(\mathbf{y}_1 \wedge \dots \wedge \mathbf{y}_k)$$

for some integer g , and so $g = \gcd(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k)$. Define

$$\Omega' = \text{span}_{\mathbb{Z}} \{\mathbf{x}_1, \dots, \mathbf{x}_k, \mathbf{y}_{k+1}, \dots, \mathbf{y}_n\}.$$

By the bi-linearity of the wedge product,

$$\det \Omega' = \mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k \wedge \mathbf{y}_{k+1} \wedge \dots \wedge \mathbf{y}_n = g(\mathbf{y}_1 \wedge \dots \wedge \mathbf{y}_k \wedge \mathbf{y}_{k+1} \wedge \dots \wedge \mathbf{y}_n),$$

and since $\mathbf{y}_1 \wedge \dots \wedge \mathbf{y}_k \wedge \mathbf{y}_{k+1} \wedge \dots \wedge \mathbf{y}_n = \det \mathbb{Z}^n = 1$, we have that $\det \Omega' = g$. \square

Corollary 2.2. *Let the notation be as in Proposition 2.1 with $k = n - 1$. Then there exists $\mathbf{y} \in \mathbb{Z}^n$ so that $\Omega' = \text{span}_{\mathbb{Z}} \{\Omega, \mathbf{y}\}$ and*

$$\|\mathbf{y}\| \leq \left\{ \left(\frac{\gcd(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k)}{\det \Omega} \right)^2 + \mu(\Omega)^2 \right\}^{1/2}.$$

Proof. Write $A = (\mathbf{x}_1 \ \dots \ \mathbf{x}_{n-1})$ for the corresponding basis matrix of Ω and let Ω' be as given by Proposition 2.1. This means that there exists $\mathbf{z} \in \mathbb{Z}^n$ such that $\Omega' = \text{span}_{\mathbb{Z}}\{\Omega, \mathbf{z}\}$, so $\det \Omega' = \gcd(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_m)$. Let $\rho_{\Omega} = A(A^{\top}A)^{-1}A^{\top}$ be the orthogonal projection onto $\text{span}_{\mathbb{R}} \Omega$. Let

$$\mathcal{P} = \left\{ \sum_{i=1}^{n-1} a_i \mathbf{x}_i : 0 \leq a_i < 1 \ \forall 1 \leq i \leq n-1 \right\}, \quad \mathcal{P}' = \{\mathbf{u} + a\mathbf{z} : \mathbf{u} \in \mathcal{P}, 0 \leq a < 1\}$$

be fundamental parallelepipeds for Ω and Ω' , respectively. Then

$$\begin{aligned} \gcd(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k) &= \det \Omega' = \text{Vol}_n(\mathcal{P}') \\ &= \text{Vol}_{n-1}(\mathcal{P}) \|(I_n - \rho_{\Omega})\mathbf{z}\| = \det \Omega \|(I_n - \rho_{\Omega})\mathbf{z}\|, \end{aligned}$$

hence

$$\|(I_n - \rho_{\Omega})\mathbf{z}\| = \frac{\gcd(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k)}{\det \Omega}.$$

On the other hand, $\rho_{\Omega}\mathbf{z} \in \text{span}_{\mathbb{R}} \Omega$, and by definition of the covering radius μ of Ω , there exists $\mathbf{v} \in \Omega$ such that $\|\rho_{\Omega}\mathbf{z} - \mathbf{v}\| \leq \mu$. Let $\mathbf{y} = \mathbf{z} - \mathbf{v}$, then $\mathbf{y} \in \mathbb{Z}^n$ and

$$\rho_{\Omega}\mathbf{y} = \rho_{\Omega}\mathbf{z} - \rho_{\Omega}\mathbf{v} = \rho_{\Omega}\mathbf{z} - \mathbf{v},$$

since $\mathbf{v} \in \text{span}_{\mathbb{R}} \Omega$. Then $(I_n - \rho_{\Omega})\mathbf{y} = (I_n - \rho_{\Omega})\mathbf{z}$ and

$$\Omega' = \text{span}_{\mathbb{Z}}\{\Omega, \mathbf{z}\} = \text{span}_{\mathbb{Z}}\{\Omega, \mathbf{y}\}.$$

Therefore, by Pythagorean theorem,

$$\begin{aligned} \|\mathbf{y}\|^2 &= \|(I_n - \rho_{\Omega})\mathbf{y}\|^2 + \|\rho_{\Omega}\mathbf{y}\|^2 = \|(I_n - \rho_{\Omega})\mathbf{z}\|^2 + \|\rho_{\Omega}\mathbf{z} - \mathbf{v}\|^2 \\ &\leq \left(\frac{\gcd(\mathbf{x}_1 \wedge \dots \wedge \mathbf{x}_k)}{\det \Omega} \right)^2 + \mu^2. \end{aligned}$$

The result follows. \square

Now Theorem 1.1 follows by combining Proposition 2.1 with Corollary 2.2.

Remark 2.1. Let $\Lambda = A\mathbb{Z}^m \subset \mathbb{R}^n$ be a lattice of rank $m \leq n$ and let $\mathbf{z}_1, \dots, \mathbf{z}_k$, $k \leq m$, be linearly independent vectors in Λ . Then for each $1 \leq i \leq k$, $\mathbf{z}_i = A\mathbf{x}_i$, where $\mathbf{x}_1, \dots, \mathbf{x}_k \in \mathbb{Z}^m$ are also linearly independent. Let

$$\Omega = \text{span}_{\mathbb{Z}}\{\mathbf{x}_1, \dots, \mathbf{x}_k\} \subset \mathbb{Z}^m$$

be the sublattice of rank k spanned by these vectors and let Ω' be an extension of Ω in \mathbb{Z}^m guaranteed by Proposition 2.1. Then $A\Omega = \text{span}_{\mathbb{Z}}\{\mathbf{z}_1, \dots, \mathbf{z}_k\} \subseteq \Lambda$ and $A\Omega' \subseteq \Lambda$ is an extension of $A\Omega$ with

$$\det A\Omega' = \sqrt{\det(A^{\top}A)} \det \Omega' = \det \Lambda \det \Omega'.$$

Further, if $k = m - 1$ then there exists $\mathbf{y} \in \mathbb{Z}^m$ so that $A\Omega' = \text{span}_{\mathbb{Z}}\{A\Omega, A\mathbf{y}\}$ and $\|\mathbf{y}\|$ bounded as in Corollary 2.2.

3. SUCCESSIVE MINIMA EXTENSIONS

In this section, we prove Theorem 1.2. We want to construct a sublattice $L_{k+1} \subset \Lambda$ of rank $k+1$ such that $L_k \subset L_{k+1}$, $\lambda_j(L_{k+1}) = \lambda_j(L_k)$ for all $1 \leq j \leq k$ and $\lambda_{k+1}(L_{k+1})$ is as small as possible. To prove the theorem, we first need an auxiliary lemma. Write $\lambda_1, \dots, \lambda_k$ for the successive minima of L_k and let $V_k = \text{span}_{\mathbb{R}} L_k$, $\theta \in (0, \pi/2]$, and

$$(3) \quad C_\theta(V_k) = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{a}(\mathbf{x}, \mathbf{y}) \in [\theta, \pi - \theta] \forall \mathbf{y} \in V_k\},$$

where $\mathbf{a}(\mathbf{x}, \mathbf{y})$ stands for the angle between two vectors.

Lemma 3.1. *If $\mathbf{x} \in C_\theta(V_k)$ and*

$$\|\mathbf{x}\| \geq \frac{\lambda_k(\cot \theta \cos \theta + 1)}{\sqrt{1 + \cos^2 \theta}},$$

then $\|\mathbf{x} + \mathbf{y}\| \geq \lambda_k$ for every $\mathbf{y} \in V_k$.

Proof. For $\mathbf{x} \in C_\theta(V_k)$ and $\mathbf{y} \in V_k$, define

$$f(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} + \mathbf{y}\|^2 = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 + 2\|\mathbf{x}\|\|\mathbf{y}\| \cos \mathbf{a}(\mathbf{x}, \mathbf{y}).$$

We want to guarantee that $f(\mathbf{x}, \mathbf{y}) \geq \lambda_k^2$ for all $\mathbf{y} \in V_k$. Let us write $t = \|\mathbf{x}\|$, $z = \|\mathbf{y}\|$, and notice that

$$f(\mathbf{x}, \mathbf{y}) - \lambda_k^2 \geq g(t, z) := t^2 + z^2 - 2tz \cos \theta - \lambda_k^2,$$

thus we want to find a lower bound on t that would guarantee $g(t, z) \geq 0$ for all $z > 0$. In other words, we want

$$t \geq h(z) := z \cos \theta + \sqrt{\lambda_k^2 - z^2 \sin^2 \theta}$$

for all $z > 0$. Notice that $h(z)$ is real-valued if and only if $z \leq \frac{\lambda_k}{\sin \theta}$, then let us find the value of z that maximizes $h(z)$. Differentiating $h(z)$ and setting the derivative equal to zero, we obtain

$$z_* = \frac{\lambda_k \cot \theta}{\sqrt{1 + \cos^2 \theta}},$$

the point at which $h(z)$ assumes its maximum value of

$$h(z_*) = \frac{\lambda_k(\cot \theta \cos \theta + 1)}{\sqrt{1 + \cos^2 \theta}}.$$

Thus, taking $t = \|\mathbf{x}\|$ to be \geq than this value ensures that $\|\mathbf{x} + \mathbf{y}\| \geq \lambda_k$ for every $\mathbf{y} \in V_k$, as required. \square

Proof of Theorem 1.2. Let us write $B_n(r)$ for the ball of radius $r > 0$ centered at the origin in \mathbb{R}^n . Let $\theta \in (0, \pi/2]$ and

$$(4) \quad r(\theta) = \frac{\lambda_k(\cot \theta \cos \theta + 1)}{\sqrt{1 + \cos^2 \theta}}.$$

Then Lemma 3.1 guarantees that for any vector $\mathbf{x} \in \Lambda \cap (C_\theta(V_k) \setminus B_n(r(\theta)))$ the lattice $M = \text{span}_{\mathbb{Z}} \{L_k, \mathbf{x}\}$ satisfies $\lambda_j(M) = \lambda_j(L_k)$ for all $1 \leq j \leq k$ and $\lambda_{k+1}(M) \leq \|\mathbf{x}\|$. Hence we want to minimize

$$\lambda_{k+1}(\theta) := \min \{\|\mathbf{x}\| : \mathbf{x} \in \Lambda \cap (C_\theta(V_k) \setminus B_n(r(\theta)))\}$$

as a function of θ .

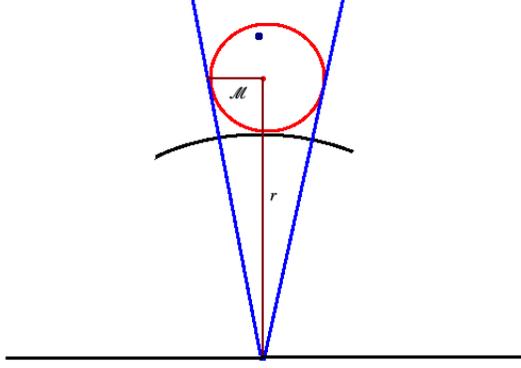


FIGURE 1. Cone construction with the lattice point (in blue) caught in the ball (red) of covering radius.

Let μ be the covering radius of Λ , then any translated copy of the ball of radius μ in \mathbb{R}^n must contain a point of Λ . Suppose that $\theta \in (0, \pi/2]$ is such that

$$(5) \quad B'_n(\mu) \subset (C_\theta(V_k) \cap B_n(r(\theta) + 2\mu)) \setminus B_n(r(\theta)),$$

where $B'_n(\mu)$ is such a translated copy. Then $C_\theta(V_k) \setminus B_n(r(\theta))$ would be guaranteed to contain a point \mathbf{x} of Λ with

$$(6) \quad \|\mathbf{x}\| \leq r(\theta) + 2\mu,$$

so that we can take $L_{k+1} = \text{span}_{\mathbb{Z}}\{L_k, \mathbf{x}\}$. Notice that θ satisfying condition (5) exists. Indeed, for any θ the set $B_n(r(\theta) + 2\mu) \setminus B_n(r(\theta))$ contains a ball of radius μ , and hence θ can always be chosen small enough so that the cone $C_\theta(V_k)$ is sufficiently wide to contain this ball. In fact, we can choose θ so that the line segment from $\mathbf{0}$ to the center of this ball $B'_n(\mu)$ has length $r(\theta) + \mu$ and makes the angle $\pi/2 - \theta$ with any line in the boundary of $C_\theta(V_k)$ emanating from the center and tangent to the ball $B'_n(\mu)$. These conditions result in a right triangle with legs $r(\theta) + \mu$ and μ and the angle $\pi/2 - \theta$ opposite to the second leg (see Figure 1 for a graphical illustration of this argument). Hence we have the equation

$$\tan(\pi/2 - \theta) = \frac{\mu}{r(\theta) + \mu}.$$

Using (4), along with the fact that $\tan(\pi/2 - \theta) = \cot \theta$, writing $v = \cos \theta$ and simplifying, we obtain the following relation in terms of v :

$$\mu \left(\sqrt{1 - v^2} - v \right) = \frac{\lambda_k (v^2 + \sqrt{1 - v^2}) v}{\sqrt{1 - v^4}},$$

which transforms into the following polynomial equation:

$$(7) \quad \left(\frac{\mu^2}{\lambda_k^2} (1 - v^4) - v^2 (v^4 - v^2 + 1) \right)^2 = \left(\frac{2\mu^2}{\lambda_k^2} v (1 - v^4) + 2v^4 \right)^2 (1 - v^2).$$

It follows from our construction that this equation has at least one solution v in the interval $(0, 1)$. Then $r(\theta)$ as a function of v becomes

$$r(v) = \frac{\lambda_k(v^2 + \sqrt{1-v^2})}{\sqrt{1-v^4}},$$

which is an increasing function of v in the interval $(0, 1)$. Hence, to minimize the bound (6), we can pick v_* to be the smallest root of the equation (7) in the interval $(0, 1)$. In other words, we are maximizing our choice of the angle θ for which the condition (5) holds. The inequality (1) follows. \square

Remark 3.1. We also present here an alternate bound for the $(k+1)$ -st successive minimum of an extension lattice L_{k+1} of L_k in Λ with $\lambda_j(L_{k+1}) = \lambda_j(L_k)$ for all $1 \leq j \leq k$ as in Theorem 1.2, as suggested to us by one of the anonymous referees:

$$(8) \quad \lambda_{k+1}(L_{k+1}) \leq (\max\{\lambda_{k+1}(\Lambda), 2\lambda_k(L_k)\}^2 + \mu(L_k)^2)^{1/2}.$$

To prove this bound, let $\mathbf{u}_1, \dots, \mathbf{u}_{k+1}$ be linearly independent vectors in Λ corresponding to the successive minima $\lambda_1(\Lambda), \dots, \lambda_{k+1}(\Lambda)$, respectively. Since $\dim V_k = k$, there must exist some \mathbf{u}_i among these vectors which is not in V_k . Let \mathbf{x} be the projection of \mathbf{u}_i into V_k^\perp , the orthogonal complement of V_k . First assume that $\|\mathbf{x}\| \geq \lambda_k(L_k)$, then $\|\mathbf{x} + \mathbf{y}\| \geq \lambda_k(L_k)$ for any $\mathbf{y} \in V_k$. To see this, notice that

$$(9) \quad \|\mathbf{x} + \mathbf{y}\|^2 = \|\mathbf{x}\|^2 + 2\mathbf{x}^\top \mathbf{y} + \|\mathbf{y}\|^2 = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 \geq \|\mathbf{x}\|^2,$$

since $\mathbf{x} \in V_k^\perp$, $\mathbf{y} \in V_k$, and so $\mathbf{x}^\top \mathbf{y} = 0$. The translated subspace $\mathbf{x} + V_k$ contains an affine copy of the lattice L_k , and hence there must exist a point of the lattice Λ , call it \mathbf{x}_{k+1} , in the set $\mathbf{x} + B_{V_k}(\mu(L_k))$, where $B_{V_k}(\mu(L_k))$ is the ball of radius $\mu(L_k)$ centered at the origin in V_k . Set $L_{k+1} = \text{span}_{\mathbb{Z}}\{L_k, \mathbf{x}_{k+1}\}$, then (9) implies that for every $\mathbf{z} \in L_{k+1} \setminus L_k$, $\|\mathbf{z}\| \geq \|\mathbf{x}\| \geq \lambda_k(L_k)$. Hence, $\lambda_j(L_{k+1}) = \lambda_j(L_k)$ for all $1 \leq j \leq k$ and

$$\lambda_{k+1}(L_{k+1})^2 \leq \|\mathbf{x}_{k+1}\|^2 \leq \|\mathbf{x}\|^2 + \mu(L_k)^2 \leq \|\mathbf{u}_i\|^2 + \mu(L_k)^2 \leq \lambda_{k+1}(\Lambda)^2 + \mu(L_k)^2,$$

implying (8). On the other hand, suppose that $\|\mathbf{x}\| < \lambda_k(L_k)$. We can then replace \mathbf{x} by its integer multiple \mathbf{x}' , chosen in such a way that $\lambda_k(L_k) \leq \|\mathbf{x}'\| \leq 2\lambda_k(L_k)$, and proceed as above. We thank the referee for suggesting this elegant argument.

Remark 3.2. We also want to discuss Theorem 1.2 in the general context of reduction theory. This result can be loosely compared to the construction of a *canonical filtration* of a lattice as originally defined by Grayson and Stuhler (see Casselman's survey paper [4] for a detailed discussion, as well as [15] for a recent application of the canonical filtration). This is a unique flag of sublattices

$$\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \dots \subset \Lambda_n = \Lambda$$

in a lattice Λ such that $\text{rk}(\Lambda_k) = k$ and $\det(\Lambda_n)^{1/n} > \det(\Lambda_k)^{1/k}$ for every $k < n$, where

$$\det(\Lambda_k) = \min \{ \det(\Omega) : \Omega \subset \Lambda, \text{rk}(\Omega) = k \}.$$

A lattice Λ is called *semi-stable* if the canonical filtration is $\Lambda_0 \subset \Lambda_n$, i.e. if for each sublattice $\Omega \subseteq \Lambda$,

$$(10) \quad \det(\Lambda)^{1/\text{rk}(\Lambda)} \leq \det(\Omega)^{1/\text{rk}(\Omega)}.$$

This family of lattices is important in reduction theory. Y. Andre explains in [1]:

Reduction theory aims at estimating the length of short vectors, and more generally the (co)volumes of small sublattices of lower ranks, of lattices of given rank and (co)volume, and at combining lower and upper bounds to get finiteness results. A better grasp on lower bounds comes from the more recent part of reduction theory which deals with semistability and slope filtrations (heuristically, semistability means that the Minkowski successive minima are not far from each other, cf. [3])

On the other hand, our Theorems 1.1 and 1.2 give constructions of lattice extensions of a given sublattice within an ambient lattice with small determinant (= (co)volume) and successive minima, respectively, while preserving the geometric properties of the sublattice that is being extended.

Additionally, if we start with a rank-one sublattice $L_1 \subset \Lambda$ and recursively apply the construction described in the proof of Theorem 1.2] to obtain a sublattice $L_n \subseteq \Lambda$ of full rank, the collection of vectors we build to bound the successive minima at every step will be a basis, call this basis $\mathbf{x}_1, \dots, \mathbf{x}_n$. We can choose the angle θ_k between \mathbf{x}_{k+1} and $V_k = \text{span}_{\mathbb{R}} L_k = \text{span}_{\mathbb{R}}\{\mathbf{x}_1, \dots, \mathbf{x}_k\}$ for each $1 \leq k \leq n-1$ to be in the interval $[\pi/3, \pi/2]$ instead of the interval $(0, \pi/2]$ we used in the proof of Theorem 1.2]: this is always possible at the expense of the $(k+1)$ -st successive minimum λ_{k+1} being larger, since the cone $C_{\theta_k}(V_k)$ eventually becomes wide enough to contain a ball of radius μ . Then we can ensure that the resulting lattice L_n is weakly nearly orthogonal in the sense of [2] and [10]. Specifically, a lattice is called weakly nearly orthogonal if it contains an ordered basis with the angles between the $(k+1)$ -st basis vector and the subspace spanned by the previous k falling in the interval $[\pi/3, \pi/2]$. Weakly nearly orthogonal lattices have applications in image compression and digital communications.

4. DEEP HOLES OF PLANAR LATTICES

We start this section with the following simple but useful technical lemma.

Lemma 4.1. *Let $\mathbf{x}_1, \dots, \mathbf{x}_m$ be linearly independent points in \mathbb{R}^n , $m \leq n$. There exist points $\mathbf{z} \in \mathbb{R}^n$ so that $\|\mathbf{z}\| = \|\mathbf{z} - \mathbf{x}_i\|$ for all $1 \leq i \leq m$, and these points are solutions to*

$$(11) \quad \begin{pmatrix} \mathbf{x}_1^\top \\ \vdots \\ \mathbf{x}_m^\top \end{pmatrix} \mathbf{z} = \frac{1}{2} \begin{pmatrix} \|\mathbf{x}_1\|^2 \\ \vdots \\ \|\mathbf{x}_m\|^2 \end{pmatrix}.$$

Proof. If \mathbf{z} is equidistant from \mathbf{x}_i and $\mathbf{0}$ then \mathbf{z} lies in the hyperplane orthogonal to \mathbf{x}_i that passes through the point $\mathbf{x}_i/2$. That is

$$\mathbf{z} \cdot \mathbf{x}_i = \text{proj}_{\mathbf{x}_i}(\mathbf{z}) \cdot \mathbf{x}_i = \frac{\|\mathbf{x}_i\|^2}{2}.$$

Since this is true for each $1 \leq i \leq m$ this gives the linear system in (11). \square

Our main goal here is to describe some properties of the deep holes of lattices, focusing especially on the two-dimensional case. Our first basic observation is that if \mathbf{z} is a deep hole of a lattice $\Lambda \subset \mathbb{R}^n$, then so is $-\mathbf{z}$: this follows by the fact that $-\Lambda = \Lambda$, since lattices are symmetric about the origin. Recall that every 2-dimensional lattice has a basis consisting of vectors corresponding to successive minima, and such a basis can always be chosen so that the angle between the basis

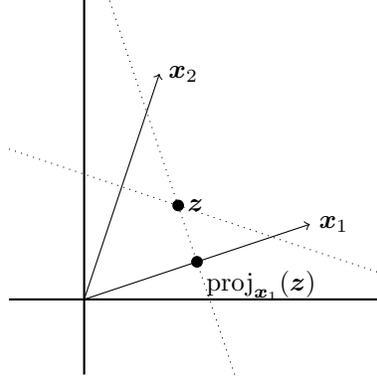


FIGURE 2. Point z , equidistant from $\mathbf{0}, \mathbf{x}_1, \mathbf{x}_2$, to illustrate the proof of Lemma 4.1.

vectors is in the interval $[\pi/3, \pi/2]$; we call this basis a *minimal basis* for the lattice (see, e.g., [8] for details). Then we have the following observation.

Lemma 4.2. *Let $\Lambda \subset \mathbb{R}^2$ be a lattice of rank 2 with minimal basis \mathbf{x}, \mathbf{y} and angle $\theta \in [\pi/3, \pi/2]$ between these basis vectors. Write λ_1, λ_2 for the successive minima of Λ , so that $0 < \lambda_1 = \|\mathbf{x}\| \leq \lambda_2 = \|\mathbf{y}\|$. Then the fundamental parallelogram*

$$\mathcal{P} = \{s\mathbf{x} + t\mathbf{y} : 0 \leq s, t < 1\}$$

contains two deep holes $\mathbf{z}_1, \mathbf{z}_2$ with $\mathbf{z}_1 + \mathbf{z}_2 \in \Lambda$. If the angle $\theta = \pi/2$, then $\mathbf{z}_1 = \mathbf{z}_2$ is the center of \mathcal{P} , and we say that this deep hole has multiplicity 2.

Proof. Let us label the vertices of \mathcal{P} as follows: O for the origin, X for the endpoint of the vector \mathbf{x} , Y for the endpoint of the vector \mathbf{y} , and Q for the endpoint of the vector $\mathbf{x} + \mathbf{y}$. The parallelogram \mathcal{P} can be split into two congruent triangles: OXY and QYX . Then the endpoints of the deep holes of Λ contained in \mathcal{P} are the centers of the circles circumscribed around these two triangles, call them Z_1 and Z_2 , respectively, and let $\mathbf{z}_1, \mathbf{z}_2$ be vectors with the endpoints Z_1, Z_2 (see [12]). The two triangles are symmetric to each other about the center C of \mathcal{P} , which means that reflection with respect to C maps the line segment OZ_1 onto the line segment QZ_2 . This means that OZ_1QZ_2 is a parallelogram with OQ as its longer diagonal, and hence the corresponding vector is the sum $\mathbf{z}_1 + \mathbf{z}_2$. Since its endpoint is Q , a vertex of \mathcal{P} , this vector is in Λ (see Figure 3 for a graphical illustration of this argument). If $\theta = \pi/2$, then the deep hole of each of the triangles is in the center of the hypotenuse of its corresponding right triangle, i.e. at the center point C of \mathcal{P} ; in this case, the two deep holes coincide, so $Z_1 = Z_2 = C$. \square

An immediate implication of Lemma 4.2 is that deep holes $\mathbf{z}_1, \mathbf{z}_2$ are each other's inverses in the additive abelian group \mathbb{R}^2/Λ . Further, \mathbf{z}_1 is an element of order two in this group if and only if the angle $\theta = \pi/2$; in this case $\mathbf{z}_1 = \mathbf{z}_2$. On the other hand, $\mathbf{z}_1, \mathbf{z}_2$ can be elements of finite order in other situations too. For instance, in the hexagonal lattice

$$L_{\pi/3} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} \mathbb{Z}^2$$

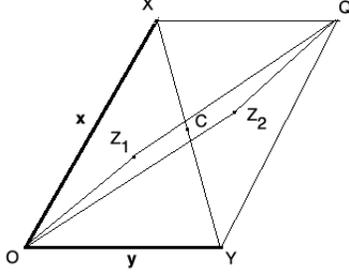


FIGURE 3. Fundamental parallelogram \mathcal{P} of Λ with deep holes \mathbf{z}_1 and \mathbf{z}_2 .

the deep holes are $\mathbf{z}_1 = (1/2, 1/(2\sqrt{3}))$, $\mathbf{z}_2 = (1, 1/\sqrt{3})$ have order three in the group $\mathbb{R}^2/L_{\pi/3}$, while the lattice

$$L' = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \sqrt{3} \end{pmatrix} \mathbb{Z}^2$$

has a deep hole $\mathbf{z}_1 = (1/2, 11\sqrt{3}/24)$ satisfying the condition

$$48\mathbf{z}_1 = 13(1, 0) + 22(1/2, \sqrt{3}) \in L',$$

which makes \mathbf{z}_1 an element of order dividing 48 in the group \mathbb{R}^2/L' . These observations raise a natural question: when does a deep hole of $\Lambda \subset \mathbb{R}^2$ have finite order as an element of the group \mathbb{R}^2/Λ ?

Theorem 4.3. *Let $\Lambda \subset \mathbb{R}^2$ be a full-rank lattice with successive minima λ_1, λ_2 and corresponding minimal basis vectors $\mathbf{x}_1, \mathbf{x}_2$. A deep hole \mathbf{z} of Λ has finite order in the group \mathbb{R}^2/Λ if and only if Λ is orthogonal or there exist rational numbers p, q so that $p\lambda_1^2 = \mathbf{x}_1 \cdot \mathbf{x}_2 = q\lambda_2^2$. Moreover, if $\lambda_1^2, \lambda_2^2, \mathbf{x}_1 \cdot \mathbf{x}_2 \in \mathbb{Z}$ then the order of \mathbf{z} in \mathbb{R}^2/Λ is $\leq 12\sqrt{3} \lambda_2^4$.*

Proof. As we discussed above, if Λ is orthogonal then the deep hole always has order 2 in \mathbb{R}^2/Λ , hence we assume Λ is not orthogonal. As we indicated above, we can assume that the minimal basis vectors $\mathbf{x}_1, \mathbf{x}_2$ are chosen so that the angle θ between them satisfies $\pi/3 \leq \theta \leq \pi/2$. If \mathbf{z} is the equidistant from $\mathbf{x}_1, \mathbf{x}_2$ and the origin then \mathbf{z} is a deep hole of Λ and is contained in the convex hull of $\{0, \mathbf{x}_1, \mathbf{x}_2\}$. By Lemma 4.1,

$$(12) \quad \mathbf{z} \cdot \mathbf{x}_1 = \frac{\lambda_1^2}{2}, \quad \mathbf{z} \cdot \mathbf{x}_2 = \frac{\lambda_2^2}{2}.$$

Now suppose that \mathbf{z} has finite order in \mathbb{R}^2/Λ . Then there are integers a, b, c so that $c \neq 0$ and

$$a\mathbf{x}_1 + b\mathbf{x}_2 = c\mathbf{z}.$$

In fact, the pairs \mathbf{z}, \mathbf{x}_1 and \mathbf{z}, \mathbf{x}_2 are linearly independent so a, b, c are all nonzero. Taking scalar products of both sides of this equation with \mathbf{x}_1 and \mathbf{x}_2 , and applying (12), we obtain

$$\begin{aligned} a\lambda_1^2 + b\mathbf{x}_1 \cdot \mathbf{x}_2 &= \frac{c\lambda_1^2}{2} \\ b\lambda_2^2 + a\mathbf{x}_1 \cdot \mathbf{x}_2 &= \frac{c\lambda_2^2}{2}. \end{aligned}$$

Notice that since Λ is not orthogonal, $\mathbf{x}_1 \cdot \mathbf{x}_2 \neq 0$ and

$$\mathbf{x}_1 \cdot \mathbf{x}_2 = \frac{c - 2a}{2b} \lambda_1^2 = \frac{c - 2b}{2a} \lambda_2^2.$$

Now suppose that there are there are rational numbers p, q so that

$$p\lambda_1^2 = \mathbf{x}_1 \cdot \mathbf{x}_2 = q\lambda_2^2.$$

Then, by (12), there exist rational, and hence integer solutions a, b, c to the linear system

$$(13) \quad \begin{cases} a\mathbf{x}_1 \cdot \mathbf{x}_1 + b\mathbf{x}_1 \cdot \mathbf{x}_2 + c\mathbf{x}_1 \cdot \mathbf{z} = 0 \\ a\mathbf{x}_1 \cdot \mathbf{x}_2 + b\mathbf{x}_2 \cdot \mathbf{x}_2 + c\mathbf{x}_2 \cdot \mathbf{z} = 0, \end{cases}$$

which factors as

$$(14) \quad \begin{pmatrix} \mathbf{x}_1^\top \\ \mathbf{x}_2^\top \end{pmatrix} (\mathbf{x}_1 \quad \mathbf{x}_2 \quad \mathbf{z}) \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \mathbf{0}.$$

Since the matrix $\begin{pmatrix} \mathbf{x}_1^\top \\ \mathbf{x}_2^\top \end{pmatrix}$ is of full rank, $(a, b, c)^\top$ solves (14) if and only if it solves

$$(15) \quad (\mathbf{x}_1 \quad \mathbf{x}_2 \quad \mathbf{z}) \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \mathbf{0}.$$

On the other hand, \mathbf{z} being an integer solution of (15) is equivalent to \mathbf{z} having finite order in \mathbb{R}^2/Λ . In fact, the order of \mathbf{z} in \mathbb{R}^2/Λ is $\leq |c|$. By combining (13) with (12), we obtain the linear system

$$(16) \quad \begin{pmatrix} 2\lambda_1^2 & 2\mathbf{x}_1 \cdot \mathbf{x}_2 & \lambda_1^2 \\ 2\mathbf{x}_1 \cdot \mathbf{x}_2 & 2\lambda_2^2 & \lambda_2^2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \mathbf{0}.$$

If $\lambda_1^2, \lambda_2^2, \mathbf{x}_1 \cdot \mathbf{x}_2 \in \mathbb{Z}$, then by Siegel's lemma (see, for instance, Lemma 4D in Chapter 1 of [16]) there exists a nontrivial integer solution to this system with

$$\max\{|a|, |b|, |c|\} \leq 3\sqrt{3} (\max\{2\lambda_1^2, 2\lambda_2^2, |\mathbf{x}_1 \cdot \mathbf{x}_2|\})^2 = 12\sqrt{3} \lambda_2^4,$$

since $\lambda_1^2 \leq |\mathbf{x}_1 \cdot \mathbf{x}_2| \leq \lambda_2^2$. □

5. EQUAL COVERING EXTENSIONS

In this section we investigate the covering radii of lattices in the plane, in particular proving Theorem 1.3 and its corollaries. Let $\Lambda \subset \mathbb{R}^2$ be a lattice of rank 2 with minimal basis \mathbf{x}, \mathbf{y} and angle $\theta \in [\pi/3, \pi/2]$ between these basis vectors. Then the successive minima of Λ are

$$(17) \quad 0 < \lambda_1 = \|\mathbf{x}\| \leq \lambda_2 = \|\mathbf{y}\|.$$

See, for instance, [8] for the details on the existence of such a minimal basis. We will use the following result in this section.

Theorem 5.1 (Theorem 3.2 of [12]). *Consider the parallelogram generated by minimal basis vectors of Λ , as above. Then deep holes of Λ in this parallelogram are the circumcenters of the two acute (right) triangles comprising this parallelogram and the covering radius of Λ is the circumradius of the triangles.*

We start with the following formula for the covering radius.

Lemma 5.2. *The covering radius of Λ is*

$$(18) \quad \mu = \frac{\sqrt{\lambda_1^2 + \lambda_2^2 - 2\lambda_1\lambda_2 \cos \theta}}{2 \sin \theta}.$$

Proof. The vectors \mathbf{x}, \mathbf{y} correspond to successive minima in Λ , and hence form a reduced basis. Then Theorem 5.1 asserts that the covering radius of Λ is equal to the circumradius of the triangle with sides corresponding to the vectors \mathbf{x} and \mathbf{y} . The length of the third side of this triangle is

$$(19) \quad \sqrt{\lambda_1^2 + \lambda_2^2 - 2\lambda_1\lambda_2 \cos \theta},$$

and the area of this triangle is

$$(20) \quad A = \frac{1}{2} \lambda_1 \lambda_2 \sin \theta.$$

Now, the circumradius of a triangle with sides a, b, c and area A is given by the formula

$$(21) \quad R = \frac{abc}{4A}.$$

Putting together (19), (20) and (21) produces (18). \square

The similarity classes of WR lattices in the plane are parameterized by the angle $\theta \in [\pi/3, \pi/2]$, and each similarity class is represented by

$$L_\theta = \begin{pmatrix} 1 & \cos \theta \\ 0 & \sin \theta \end{pmatrix} \mathbb{Z}^2,$$

see [9], [8] for details. The following corollary follows immediately from Lemma 5.2 by substituting $\lambda_1 = \lambda_2 = 1$ into (18).

Corollary 5.3. *The covering radius $\mu = \mu(\theta)$ of the lattices L_θ is a continuous function on the interval $[\pi/3, \pi/2]$, given by*

$$\mu(\theta) = \frac{\sqrt{1 - \cos \theta}}{\sqrt{2} \sin \theta}.$$

The endpoints of the interval are represented by the hexagonal lattice and the square lattice \mathbb{Z}^2 with the covering radii $1/\sqrt{3}$ and $1/\sqrt{2}$, respectively.

We are now ready to prove Theorem 1.3. We first want to build an extension $E_1 \subset \Lambda \subset \mathbb{R}^2$ with $\text{rk } \Lambda = 2$ so that $\mu(\Lambda) = \mu(E_1)$. Our argument characterizes all possible such extensions, showing that they must be rectangular lattices, i.e. lattices containing an orthogonal basis.

Proof of Theorem 1.3. First notice that each $\Lambda(\alpha)$ as in (2) is a rectangular lattice, thus its successive minima are

$$\lambda_{1,2} = \sqrt{\alpha}, \sqrt{1-\alpha},$$

i.e. norms of the orthogonal basis vectors given in (2). By Lemma 5.2, the covering of $\Lambda(\alpha)$ is

$$\mu = \frac{\sqrt{\alpha + (1-\alpha) - 2\sqrt{\alpha(1-\alpha)} \cos(\pi/2)}}{2 \sin(\pi/2)} = \frac{1}{2}.$$

In the reverse direction, assume $\Lambda \subset \mathbb{R}^2$ is a full rank lattice so that $\mathbf{e}_1 \in \Lambda$ and $\mu(\Lambda) = 1/2$. The vector $\mathbf{a} := \frac{1}{2}\mathbf{e}_1$ is a deep hole of E_1 . First we show that \mathbf{a} is a deep hole of the lattice Λ as well. Suppose not, then there exists a point $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \Lambda$ such that

$$\|\mathbf{x} - \mathbf{a}\| < 1/2.$$

Then the vector $\mathbf{z} = \mathbf{e}_1 - \mathbf{x} = \begin{pmatrix} 1-x_1 \\ -x_2 \end{pmatrix}$ is also in Λ , and

$$\|\mathbf{z} - \mathbf{a}\| = \|\mathbf{x} - \mathbf{a}\| < 1/2.$$

Let $\Lambda' = \text{span}_{\mathbb{Z}}\{\mathbf{x}, \mathbf{z}\} \subseteq \Lambda$, then $\mu(\Lambda') \geq \mu(\Lambda)$. The triangle with sides corresponding to the basis vectors \mathbf{x}, \mathbf{z} of Λ' is contained in the interior of the circle of radius $1/2$ with center at \mathbf{a} , thus the circumradius R of this triangle is $< 1/2$. On the other hand, by Theorem 5.1 the covering radius of Λ' is equal to the circumradius of the triangle with sides corresponding to the shortest basis vectors, which has to be $\leq R$. Hence $\mu(\Lambda) \leq \mu(\Lambda') < 1/2$, which is a contradiction, so \mathbf{a} is a deep hole of the lattice Λ . This means that there exists a basis $\mathbf{x}, \mathbf{z} \in \Lambda$ with $\|\mathbf{x}\| = \lambda_1$, $\|\mathbf{z}\| = \lambda_2$ so that the point \mathbf{a} is the center of the circle circumscribed around the triangle with sides \mathbf{x}, \mathbf{z} , meaning in particular that

$$(22) \quad (1/2)^2 = \|\mathbf{x} - \mathbf{a}\|^2 = (x_1 - 1/2)^2 + x_2^2 = x_1^2 + x_2^2 - x_1 + (1/2)^2.$$

Also, $2\mathbf{a} = \mathbf{e}_1$ is a diagonal of the fundamental parallelogram of Λ spanned by \mathbf{x}, \mathbf{z} , meaning that

$$\mathbf{x} + \mathbf{z} = \mathbf{e}_1.$$

Hence $\mathbf{z} = \begin{pmatrix} 1-x_1 \\ -x_2 \end{pmatrix}$, and

$$\cos \theta = \frac{\mathbf{x} \cdot \mathbf{z}}{\|\mathbf{x}\| \|\mathbf{z}\|} = \frac{x_1 - x_1^2 - x_2^2}{\lambda_1 \lambda_2},$$

where θ is the angle between \mathbf{x} and \mathbf{z} , which lies in the interval $[\pi/3, \pi/2]$. Hence $\cos \theta = 0$ by (22). Letting $x_1 = \alpha$, we obtain

$$x_2 = \sqrt{\alpha - \alpha^2},$$

and (2) follows by replacing \mathbf{z} with $-\mathbf{z}$.

Next, suppose that $L \subset \mathbb{R}^n$ be a lattice of rank 1 and let $\mathbf{u} \in \mathbb{R}^n$ be such that $L = \mathbb{Z}\mathbf{u}$, so the covering radius of L is $\mu = \|\mathbf{u}\|/2$. Let Λ be a lattice of

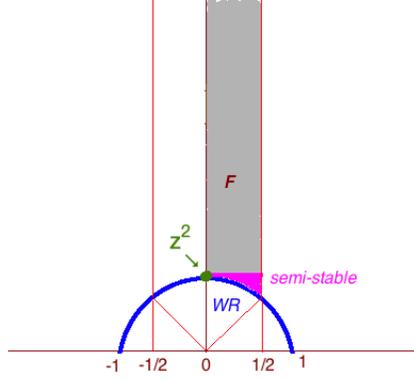


FIGURE 4. Similarity classes of planar lattices with \mathbb{Z}^2 representing the only equal covering extension class that is WR and semi-stable.

rank 2 in \mathbb{R}^n containing L and let $V = \text{span}_{\mathbb{R}} \Lambda$ be the 2-dimensional subspace spanned by this lattice. Applying a suitable isometry of \mathbb{R}^n , we can identify V with $C_2 := \{\mathbf{x} \in \mathbb{R}^n : x_i = 0 \ \forall \ 2 < i \leq n\}$. In fact, we can choose such an isometry τ so that \mathbf{u} maps to $\beta \mathbf{e}_1$ for $\beta = \|\mathbf{u}\|$. Then $\Lambda' = \frac{1}{\beta} \tau(\Lambda)$ is a lattice isometric to $\frac{1}{\beta} \Lambda$ in \mathbb{R}^n , and Λ' contains \mathbf{e}_1 . Identifying C_2 with \mathbb{R}^2 we see that Theorem 1.3 implies that Λ' is an equal covering extension of $\mathbb{Z} \mathbf{e}_1$ in \mathbb{R}^2 if and only if it is of the form (2). Finally, notice that

$$\det(L) = \sqrt{\det(\mathbf{u}^T \mathbf{u})} = \|\mathbf{u}\| = \beta.$$

This completes the proof of the theorem. \square

Remark 5.1. An immediate implication of Theorem 1.3 is that the only well-rounded equal covering extension of E_1 is

$$(23) \quad \Lambda(1/2) = \begin{pmatrix} 1/2 & -1/2 \\ 1/2 & 1/2 \end{pmatrix} \mathbb{Z}^2,$$

which is a square lattice in the plane containing \mathbb{Z}^2 as a sublattice of index 2. More generally, a rank-two equal covering extension $\Lambda \subset \mathbb{R}^n$ of a rank-one lattice $L \subset \Lambda$ is well-rounded if and only if it is isometric to $\det(L)\Lambda(1/2)$. Further, the set of all similarity classes of planar lattices is parameterized by

$$F = \{(a, b) \in \mathbb{R}^2 : 0 \leq a \leq 1/2, a^2 + b^2 \geq 1\},$$

see Figure 4. The set of semi-stable classes in \mathbb{R}^2 contains the WR classes: from (10) it follows that a lattice Λ in \mathbb{R}^2 is semi-stable if and only if $\lambda_1(\Lambda) \geq \det(\Lambda)^{1/2}$ (see [9] for more details). Thus the only semi-stable equal covering extensions are also those similar to $\Lambda(1/2)$ as in (23), i.e. similar to \mathbb{Z}^2 as demonstrated in Figure 4.

Let D be a squarefree integer and $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field with embeddings $\sigma_1, \sigma_2 : K \rightarrow \mathbb{C}$. Let $\Sigma_K : K \rightarrow \mathbb{R}^2$ be the Minkowski embedding of K ,

defined for every $x \in K$ as

$$\Sigma_K(x) = \begin{pmatrix} \sigma_1(x) \\ \sigma_2(x) \end{pmatrix},$$

if $D > 0$ and

$$\Sigma_K(x) = \begin{pmatrix} \Re(\sigma_1(x)) \\ \Im(\sigma_1(x)) \end{pmatrix},$$

if $D < 0$. We write Ω_K for the planar lattice $\Sigma_K(\mathcal{O}_K)$, where \mathcal{O}_K is the ring of integers of the number field K .

Corollary 5.4. *Assume $D \not\equiv 1 \pmod{4}$, then Ω_K is an equal covering extension of the rank-one lattice $\mathbb{Z}\Sigma_K(1 + \sqrt{D})$.*

Proof. If $D \not\equiv 1 \pmod{4}$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$, and so

$$\Omega_K = \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix} \mathbb{Z}^2 \text{ if } D > 0, \quad \Omega_K = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{|D|} \end{pmatrix} \mathbb{Z}^2 \text{ if } D < 0.$$

In either case, the lattice Ω_K is rectangular. If $D > 0$, then $\lambda_1 = \sqrt{2}$, $\lambda_2 = \sqrt{2D}$, and so Lemma 5.2 implies that $\mu(\Omega_K) = \sqrt{D+1}/\sqrt{2}$, while

$$\Sigma_K(1 + \sqrt{D}) = \begin{pmatrix} 1 + \sqrt{D} \\ 1 - \sqrt{D} \end{pmatrix},$$

and so $\mu(\mathbb{Z}\Sigma_K(1 + \sqrt{D})) = \sqrt{D+1}/\sqrt{2}$. If $D < 0$, then $\lambda_1 = 1$, $\lambda_2 = \sqrt{|D|}$, and so Lemma 5.2 implies that $\mu(\Omega_K) = \sqrt{|D|+1}/2$, while

$$\Sigma_K(1 + \sqrt{D}) = \begin{pmatrix} 1 \\ \sqrt{|D|} \end{pmatrix},$$

and so $\mu(\mathbb{Z}\Sigma_K(1 + \sqrt{D})) = \sqrt{|D|+1}/2$. □

Corollary 5.5. *Assume $D \equiv 1 \pmod{4}$, then Ω_K is not an equal covering extension of any rank-one lattice.*

Proof. If $D \equiv 1 \pmod{4}$ then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$, and so

$$\Omega_K = \begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix} \mathbb{Z}^2 \text{ if } D > 0, \quad \Omega_K = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \sqrt{|D|} \end{pmatrix} \mathbb{Z}^2 \text{ if } D < 0.$$

In both cases it is not difficult to check that Ω_K does not have an orthogonal basis, and hence cannot be similar to a lattice of the form $\Lambda(\alpha)$ as in (2). The conclusion follows from Theorem 1.3. □

Finally, we discuss a construction of orthogonal equal covering extensions in any dimension.

Proof of Theorem 1.4. We will argue by induction on $k \geq 1$. Theorem 1.3 establishes the base of induction, so let $k \geq 2$. Let $\{\mathbf{x}_1, \dots, \mathbf{x}_k\} \subset \mathbb{R}^n$ be an orthogonal basis for Λ_k and let $\mathbf{e}_{k+1} \in \mathbb{R}^n$ be a vector orthogonal to $\text{span}_{\mathbb{R}} \Lambda_k$. Let

$$P_k = \left\{ \sum_{i=1}^k a_i \mathbf{x}_i : a_i \in \{0, 1\}, 1 \leq i \leq k \right\}$$

be the set of vertices of the fundamental parallelepiped spanned by $\mathbf{x}_1, \dots, \mathbf{x}_k$. The circumcenter of this orthogonal parallelepiped is the point $\mathbf{z} \in \mathbb{R}^n$ which is equidistant from the points of P_k by Lemma 4.1, and hence is a deep hole of Λ_k . Let

$$B_k = \{\mathbf{y} \in \text{span}_{\mathbb{R}}\{\mathbf{x}_1, \dots, \mathbf{x}_k\} : \|\mathbf{y} - \mathbf{z}\| = \mu(\Lambda_k)\}.$$

Let $\Lambda_{k-1} = \text{span}_{\mathbb{Z}}\{\mathbf{x}_1, \dots, \mathbf{x}_{k-1}\}$ and let

$$P_{k-1} = \left\{ \sum_{i=1}^{k-1} a_i \mathbf{x}_i : a_i \in \{0, 1\}, 1 \leq i \leq k-1 \right\}.$$

Now define

$$B_{k-1} = B_k \cap \text{span}_{\mathbb{R}} \Lambda_{k-1}$$

By construction, $P_{k-1} \subset B_{k-1}$, while B_{k-1} is a sphere in a $(k-1)$ -dimensional subspace and the points of P_{k-1} are elements of an orthogonal lattice in that subspace. Let \mathbf{z}' be the orthogonal projection of \mathbf{z} onto $\text{span}_{\mathbb{R}}(\Lambda_{k-1})$. Since $\{\mathbf{x}_1, \dots, \mathbf{x}_k\}$ is an orthogonal set, $\mathbf{z}' = \mathbf{z} - \text{proj}_{\mathbf{x}_k}(\mathbf{z})$. Moreover, \mathbf{z} is equidistant from $\{\mathbf{x}_1, \dots, \mathbf{x}_k\}$, so by Lemma 4.1

$$\begin{pmatrix} \mathbf{x}_1^\top \\ \vdots \\ \mathbf{x}_k^\top \end{pmatrix} \mathbf{z} = \frac{1}{2} \begin{pmatrix} \|\mathbf{x}_1\| \\ \vdots \\ \|\mathbf{x}_k\| \end{pmatrix},$$

and therefore

$$\begin{pmatrix} \mathbf{x}_1^\top \\ \vdots \\ \mathbf{x}_{k-1}^\top \end{pmatrix} \mathbf{z}' = \frac{1}{2} \begin{pmatrix} \|\mathbf{x}_1\| \\ \vdots \\ \|\mathbf{x}_{k-1}\| \end{pmatrix}.$$

Then \mathbf{z}' is equidistant from $\{\mathbf{x}_1, \dots, \mathbf{x}_{k-1}\}$ and Λ_{k-1} is an orthogonal lattice contained in the k -dimensional subspace $V = \text{span}_{\mathbb{R}}\{\Lambda_{k-1}, \mathbf{e}_{k+1}\}$. By the induction hypothesis, there exists a rank k orthogonal lattice $\Lambda'_k \subset V$ so that $\Lambda_{k-1} \subset \Lambda'_k$ and \mathbf{z}' is a deep hole of Λ'_k . Let $\mathbf{y}_1, \dots, \mathbf{y}_k$ be an orthogonal basis for Λ'_k so that $\mathbf{y}_1, \dots, \mathbf{y}_k$ are equidistant from \mathbf{z}' . Since $\mathbf{z} = \mathbf{z}' - \text{proj}_{\mathbf{x}_k}(\mathbf{z})$, and \mathbf{x}_k is orthogonal to V , $\mathbf{y}_1, \dots, \mathbf{y}_k$ are also equidistant from \mathbf{z} . Let $\Lambda_{k+1} = \text{span}_{\mathbb{Z}}\{\mathbf{y}_1, \dots, \mathbf{y}_k, \mathbf{x}_k\}$. Then Λ_{k+1} is an orthogonal lattice that contains Λ_k and

$$\begin{pmatrix} \mathbf{y}_1^\top \\ \vdots \\ \mathbf{y}_{k-1}^\top \\ \mathbf{x}_k^\top \end{pmatrix} \mathbf{z} = \frac{1}{2} \begin{pmatrix} \|\mathbf{y}_1\| \\ \vdots \\ \|\mathbf{y}_{k-1}\| \\ \|\mathbf{x}_k\| \end{pmatrix}.$$

Thus \mathbf{z} is equidistant from $\mathbf{0}, \mathbf{y}_1, \dots, \mathbf{y}_k$ by Lemma 4.1, and hence a deep hole of Λ_k . \square

Acknowledgement. We would like to thank the two anonymous referees for a very thorough reading of our paper and many helpful suggestions that improved the quality of exposition.

REFERENCES

- [1] Y. André. On nef and semistable hermitian lattices, and their behaviour under tensor product. *Tohoku Math. J. (2)*, 63(4):629–649, 2011.
- [2] R. Baraniuk, S. Dash, and R. Neelamani. On nearly orthogonal lattice bases. *SIAM J. Discrete Math*, 21(1):199–219, 2007.
- [3] T. Borek. Successive minima and slopes of Hermitian vector bundles over number fields. *J. Number Theory*, 113(2):380–388, 2005.
- [4] B. Casselman. Stability of lattices and the partition of arithmetic quotients. *Asian J. Math.*, 8(4):607–637, 2004.
- [5] J. W. S. Cassels. An Introduction to the Geometry of Numbers. Springer-Verlag, 1959.
- [6] J. H. Conway and N. J. A. Sloane. Sphere packings, lattices and groups, 3rd edition, Springer-Verlag, 1999.
- [7] M. Forst and L. Fukshansky. Counting basis extensions in a lattice. *Proc. Amer. Math. Soc.*, 150(8):3199–3213, 2022.
- [8] L. Fukshansky. Revisiting the hexagonal lattice: on optimal lattice circle packing. *Elem. Math.*, 66(1):1–9, 2011.
- [9] L. Fukshansky, P. Guerzhoy and F. Luca. On arithmetic lattices in the plane. *Proc. Amer. Math. Soc.*, 145(4):1453–1465, 2017.
- [10] L. Fukshansky and D. Kogan. On the geometry of nearly orthogonal lattices. *Linear Algebra Appl.*, 629:112–137, 2021.
- [11] P. M. Gruber and C. G. Lekkerkerker, Geometry of Numbers. North-Holland Publishing Co., 1987.
- [12] Y. Jiang, Y. Deng and Y. Pan. Covering radius of two-dimensional lattices. *J. Systems Sci. Math. Sci.*, 32 (2012), no. 7, pp. 908–914.
- [13] J. Martinet, Perfect lattices in Euclidean spaces, Springer-Verlag, 2003.
- [14] O. Regev, U. Shapira and B. Weiss. Counterexamples to a conjecture of Woods. *Duke Math. J.*, 166(13):2443–2446, 2017.
- [15] O. Regev and N. Stephens-Davidowitz. A reverse Minkowski theorem. In Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, pp. 941–953, Montreal, Canada, 2017. Association for Computing Machinery.
- [16] W. M. Schmidt, Diophantine approximations and Diophantine equations, Springer-Verlag, 1991.

INSTITUTE OF MATHEMATICAL SCIENCES, CLAREMONT GRADUATE UNIVERSITY, CLAREMONT, CA 91711

Email address: maxwell.forst@cgu.edu

DEPARTMENT OF MATHEMATICS, 850 COLUMBIA AVENUE, CLAREMONT MCKENNA COLLEGE, CLAREMONT, CA 91711

Email address: lenny@cmc.edu