On lattice extensions

Lenny Fukshansky
Claremont McKenna College

(*joint work with Maxwell Forst*)

Modern Problems in Number Theory
Sirius University of Science and Technology
July 8 - 13, 2024

Unimodular matrices

Let $A = (a_{ij})$ be an $m \times n$ integer matrix, $1 \leq m < n$. A is called **unimodular** if there exists an $(n-m) \times n$ integer matrix $B = (b_{ij})$ so that the $n \times n$ integer matrix

$$\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \\ b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{(n-m)1} & \cdots & b_{(n-m)n} \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z}),$$

meaning that $\det \begin{pmatrix} A \\ B \end{pmatrix} = \pm 1$.

Unimodular matrices

Let $A = (a_{ij})$ be an $m \times n$ integer matrix, $1 \leq m < n$. A is called **unimodular** if there exists an $(n-m) \times n$ integer matrix $B = (b_{ij})$ so that the $n \times n$ integer matrix

$$\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \\ b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{(n-m)1} & \dots & b_{(n-m)n} \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z}),$$

meaning that $\det \begin{pmatrix} A \\ B \end{pmatrix} = \pm 1$.

Question 1

How can we tell if a given matrix A is unimodular?

Unimodular criterion

Theorem 1 (I. Heger - 1856)

*An $m \times n$ integer matrix A is unimodular if and only if the $m \times m$ minors of A (**Plücker coordinates**) are relatively prime.*

Unimodular criterion

Theorem 1 (I. Heger - 1856)

*An $m \times n$ integer matrix A is unimodular if and only if the $m \times m$ minors of A (**Plücker coordinates**) are relatively prime.*

One can ask how often unimodular matrices occur, or –

Question 2

What is the "probability" that a given $m \times n$ matrix A is unimodular?

Unimodular criterion

Theorem 1 (I. Heger - 1856)

*An $m \times n$ integer matrix A is unimodular if and only if the $m \times m$ minors of A (**Plücker coordinates**) are relatively prime.*

One can ask how often unimodular matrices occur, or –

Question 2

What is the "probability" that a given $m \times n$ matrix A is unimodular?

To make this question precise, we write

$$\mathcal{U}(T) = \left\{ A = (a_{ij}) \in \mathbb{Z}^{m \times n} : A \text{ is unimodular and } |A| \leq T \right\},$$

where $|A| := \max_{i,j} |a_{ij}|$, and define the **natural density** of $m \times n$ unimodular matrices to be

$$d_{m,n} = \lim_{T \to \infty} \frac{\#\mathcal{U}(T)}{T^{mn}}.$$

Unimodular probability

Theorem 2 (Maze, Rosenthal, Wagner - 2011)

$$d_{m,n} = \left(\prod_{j=n-m+1}^{n} \zeta(j) \right)^{-1},$$

where ζ stands for the Riemann ζ-function.

Unimodular probability

Theorem 2 (Maze, Rosenthal, Wagner - 2011)

$$d_{m,n} = \left(\prod_{j=n-m+1}^{n} \zeta(j) \right)^{-1},$$

where ζ stands for the Riemann ζ-function.

In other words, this quantity can be viewed as the "probability" that a "random" $m \times n$ integer matrix is unimodular.

Unimodular probability

Theorem 2 (Maze, Rosenthal, Wagner - 2011)

$$d_{m,n} = \left(\prod_{j=n-m+1}^{n} \zeta(j) \right)^{-1},$$

where ζ stands for the Riemann ζ-function.

In other words, this quantity can be viewed as the "probability" that a "random" $m \times n$ integer matrix is unimodular.

For the special case of $1 \times n$ integer matrices, we have

$$d_{1,n} = 1//\zeta(n),$$

which (via Heger's theorem) follows from the classical result of Cesáro (1884) about coprimality of a random n-tuple of integers. Cesáro's theorem has been independently rediscovered several times by different mathematicians since.

Extending a basis

On the other hand, A is unimodular if and only if its rows form a **primitive collection** of vectors, i.e. extendable to a basis for $\mathbb{Z}^n$. If there is one such extension, there are infinitely many.

Extending a basis

On the other hand, A is unimodular if and only if its rows form a **primitive collection** of vectors, i.e. extendable to a basis for $\mathbb{Z}^n$. If there is one such extension, there are infinitely many.

Question 3

If $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m \in \mathbb{Z}^n$ is a primitive collection, then how many collections $\boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-m} \in \mathbb{Z}^n$ there exist so that

$$\boldsymbol{a}_1, \dots, \boldsymbol{a}_m, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-m}$$

is a basis for $\mathbb{Z}^n$, $|\boldsymbol{b}_i| \leq T \ \forall\ 1 \leq i \leq n-m$ as $T \to \infty$?

Counting basis extensions - I

Theorem 3 (M. Forst, L.F. - 2022)

Let $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m \in \mathbb{Z}^n$ be a primitive collection of vectors.

1. *If $m < n-1$, the number of vectors $\boldsymbol{b} \in \mathbb{Z}^n$ with $|\boldsymbol{b}| \leq T$ such that the collection $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m, \boldsymbol{b}$ is again primitive is equal to $\Theta(T^n)$ as $T \to \infty$.*
2. *If $m = n-1$, the number of vectors $\boldsymbol{b} \in \mathbb{Z}^n$ with $|\boldsymbol{b}| \leq T$ such that the collection $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m, \boldsymbol{b}$ is a basis for $\mathbb{Z}^n$ is equal to $\Theta(T^{n-1})$ as $T \to \infty$.*

As a result, for any $1 \leq k < n-m$ there exist $\Theta(T^{nk})$ collections of vectors $\boldsymbol{b}_1, \dots, \boldsymbol{b}_k \in \mathbb{Z}^n$ with $|\boldsymbol{b}_i| \leq T$, $1 \leq i \leq k$, such that $\{\boldsymbol{a}_i, \boldsymbol{b}_j : 1 \leq i \leq m, 1 \leq j \leq k\}$ is again primitive. Further, there are $\Theta(T^{n^2-nm-1})$ such collections $\boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-m}$ so that

$$\mathbb{Z}^n = \operatorname{span}_{\mathbb{Z}} \{\boldsymbol{a}_1, \dots, \boldsymbol{a}_m, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-m}\}.$$

Counting basis extensions - II

Any lattice $\Lambda \subset \mathbb{R}^n$ is of the form $\Lambda = U\mathbb{Z}^n$ for some matrix $U \in \mathrm{GL}_n(\mathbb{R})$. As such, bases in Λ are in bijective correspondence with bases in $\mathbb{Z}^n$, given by multiplication by U. This correspondence allows to extend Theorem 3 to arbitrary lattices, where we call a collection of vectors in Λ primitive if it is a basis or can be extended to a basis of Λ.

Counting basis extensions - II

Any lattice $\Lambda \subset \mathbb{R}^n$ is of the form $\Lambda = U\mathbb{Z}^n$ for some matrix $U \in \mathrm{GL}_n(\mathbb{R})$. As such, bases in Λ are in bijective correspondence with bases in $\mathbb{Z}^n$, given by multiplication by U. This correspondence allows to extend Theorem 3 to arbitrary lattices, where we call a collection of vectors in Λ primitive if it is a basis or can be extended to a basis of Λ.

Corollary 4

Let $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m$ be a primitive collection of vectors in a full-rank lattice $\Lambda \subset \mathbb{R}^n$ with $1 \leq m < n$. Then there are $\Theta(T^{n^2-nm-1})$ collections of vectors $\boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-m} \in \Lambda$ such that $|\boldsymbol{b}_i| \leq T$ for each $1 \leq i \leq n-m$ and

$$\Lambda = \mathrm{span}_{\mathbb{Z}} \{\boldsymbol{a}_1, \dots, \boldsymbol{a}_m, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-m}\}.$$

Defining a lattice extension

So far, we only talked about extending a collection of vectors to a basis in a lattice. Now, let Λ be a lattice of rank n in $\mathbb{R}^n$ and let $\Omega \subset \Lambda$ be a sublattice of rank $m < n$. We say that Λ is an **extension** lattice of Ω if

$$\Lambda \cap \operatorname{span}_{\mathbb{R}} \Omega = \Omega.$$

Defining a lattice extension

So far, we only talked about extending a collection of vectors to a basis in a lattice. Now, let Λ be a lattice of rank n in $\mathbb{R}^n$ and let $\Omega \subset \Lambda$ be a sublattice of rank $m < n$. We say that Λ is an **extension** lattice of Ω if

$$\Lambda \cap \operatorname{span}_{\mathbb{R}} \Omega = \Omega.$$

As a first example, we can demonstrate a construction of a small-determinant extension of a sublattice inside of the integer lattice $\mathbb{Z}^n$. We identify the wedge product of vectors $\boldsymbol{x}_1 \wedge \cdots \wedge \boldsymbol{x}_m$ in the Grassmann algebra with the corresponding vector of Plücker coordinates in $\mathbb{R}^{\binom{n}{m}}$ with respect to a lexicographic embedding.

Defining a lattice extension

So far, we only talked about extending a collection of vectors to a basis in a lattice. Now, let Λ be a lattice of rank n in $\mathbb{R}^n$ and let $\Omega \subset \Lambda$ be a sublattice of rank $m < n$. We say that Λ is an **extension** lattice of Ω if

$$\Lambda \cap \operatorname{span}_{\mathbb{R}} \Omega = \Omega.$$

As a first example, we can demonstrate a construction of a small-determinant extension of a sublattice inside of the integer lattice $\mathbb{Z}^n$. We identify the wedge product of vectors $\boldsymbol{x}_1 \wedge \cdots \wedge \boldsymbol{x}_m$ in the Grassmann algebra with the corresponding vector of Plücker coordinates in $\mathbb{R}^{\binom{n}{m}}$ with respect to a lexicographic embedding.

Additionally, define the **covering radius** of Ω to be

$$\mu(\Omega) = \min \left\{ r \in \mathbb{R} : \Omega + B_m(r) = \operatorname{span}_{\mathbb{R}} \Omega \right\},$$

where $B_m(r) \subset \operatorname{span}_{\mathbb{R}} \Omega$ is a ball of radius r centered at $\mathbf{0}$.

Small-determinant lattice extension

Theorem 5 (Forst, L.F. - 2024)

Let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ *be linearly independent vectors in* $\mathbb{Z}^n$ *and let*

$$\Omega = \operatorname{span}_{\mathbb{Z}} \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\} \subset \mathbb{Z}^n$$

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*

$$\det \Omega' = \gcd(\boldsymbol{x}_1 \wedge \cdots \wedge \boldsymbol{x}_m). \tag{1}$$

Further, if $m = n - 1$ *then there exists* $\boldsymbol{y} \in \mathbb{Z}^n$ *so that* $\Omega' = \operatorname{span}_{\mathbb{Z}} \{\Omega, \boldsymbol{y}\}$ *and*

$$\|\boldsymbol{y}\| \leq \left\{ \left(\frac{\gcd(\boldsymbol{x}_1 \wedge \cdots \wedge \boldsymbol{x}_m)}{\det \Omega} \right)^2 + \mu(\Omega)^2 \right\}^{1/2}. \tag{2}$$

Idea of proof

Any basis of the lattice $\Lambda = \mathbb{Z}^n \cap \operatorname{span}_{\mathbb{R}} \Omega$ is extendable to a basis of $\mathbb{Z}^n$. Let $\boldsymbol{y}_1, \dots, \boldsymbol{y}_m$ be a basis of Λ, extended to a basis of $\mathbb{Z}^n$ by $\boldsymbol{y}_{m+1}, \dots, \boldsymbol{y}_n$. Then,

$$\operatorname{span}_{\mathbb{R}}\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_m\} = \operatorname{span}_{\mathbb{R}}\{\boldsymbol{y}_1, \dots, \boldsymbol{y}_m\},$$

and, by Heger's theorem, Plücker coordinates of $\boldsymbol{y}_1 \wedge \dots \wedge \boldsymbol{y}_m$ are relatively prime. Hence

$$\boldsymbol{x}_1 \wedge \dots \wedge \boldsymbol{x}_m = \gcd(\boldsymbol{x}_1 \wedge \dots \wedge \boldsymbol{x}_m)(\boldsymbol{y}_1 \wedge \dots \wedge \boldsymbol{y}_m).$$

Define $\Omega' = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_m, \boldsymbol{y}_{m+1}, \dots, \boldsymbol{y}_n\}$, then (1) follows by the bilinearity of the wedge product.

Idea of proof

Any basis of the lattice $\Lambda = \mathbb{Z}^n \cap \operatorname{span}_{\mathbb{R}} \Omega$ is extendable to a basis of $\mathbb{Z}^n$. Let $\boldsymbol{y}_1, \dots, \boldsymbol{y}_m$ be a basis of Λ, extended to a basis of $\mathbb{Z}^n$ by $\boldsymbol{y}_{m+1}, \dots, \boldsymbol{y}_n$. Then,

$$\operatorname{span}_{\mathbb{R}}\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_m\} = \operatorname{span}_{\mathbb{R}}\{\boldsymbol{y}_1, \dots, \boldsymbol{y}_m\},$$

and, by Heger's theorem, Plücker coordinates of $\boldsymbol{y}_1 \wedge \cdots \wedge \boldsymbol{y}_m$ are relatively prime. Hence

$$\boldsymbol{x}_1 \wedge \cdots \wedge \boldsymbol{x}_m = \gcd(\boldsymbol{x}_1 \wedge \cdots \wedge \boldsymbol{x}_m)(\boldsymbol{y}_1 \wedge \cdots \wedge \boldsymbol{y}_m).$$

Define $\Omega' = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_m, \boldsymbol{y}_{m+1}, \dots, \boldsymbol{y}_n\}$, then (1) follows by the bilinearity of the wedge product.
The proof of (2) is more involved: it uses the orthogonal projection $\rho_\Omega = A(A^\top A)^{-1}A^\top$ onto $\operatorname{span}_{\mathbb{R}} \Omega$, where $A = \begin{pmatrix} \boldsymbol{x}_1 & \dots & \boldsymbol{x}_{n-1} \end{pmatrix}$.

Successive minima extensions

The **successive minima** of a rank-n lattice Λ are real numbers

$$0 < \lambda_1(\Lambda) \leq \cdots \leq \lambda_n(\Lambda),$$

given by $\lambda_i(\Lambda) = \min \left\{ r \in \mathbb{R} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}} \left(B_n(r) \cap \Lambda \right) \geq i \right\}$.

Successive minima extensions

The **successive minima** of a rank-n lattice Λ are real numbers

$$0 < \lambda_1(\Lambda) \leq \cdots \leq \lambda_n(\Lambda),$$

given by $\lambda_i(\Lambda) = \min \left\{ r \in \mathbb{R} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}} \left(B_n(r) \cap \Lambda \right) \geq i \right\}$.
Our main goal is to explore lattice extensions with control over their geometric invariants. In particular, we say that Λ is a **successive minima extension** of Ω if Λ is an extension of Ω such that

$$\lambda_j(\Lambda) = \lambda_j(\Omega) \ \forall \ 1 \leq j \leq m.$$

Successive minima extensions

The **successive minima** of a rank-n lattice Λ are real numbers

$$0 < \lambda_1(\Lambda) \leq \cdots \leq \lambda_n(\Lambda),$$

given by $\lambda_i(\Lambda) = \min\left\{r \in \mathbb{R} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}} \left(B_n(r) \cap \Lambda\right) \geq i\right\}$.
Our main goal is to explore lattice extensions with control over their geometric invariants. In particular, we say that Λ is a **successive minima extension** of Ω if Λ is an extension of Ω such that

$$\lambda_j(\Lambda) = \lambda_j(\Omega) \ \forall\ 1 \leq j \leq m.$$

To construct a rank-$(m+1)$ successive minima extension Λ of Ω, take $\boldsymbol{u} \in \mathbb{R}^n$ to be a vector perpendicular to $\operatorname{span}_{\mathbb{R}} \Omega$ of norm $> \lambda_m(\Omega)$ and define $\Lambda = \operatorname{span}_{\mathbb{Z}}\{\Omega, \boldsymbol{u}\}$. It is a more delicate problem to construct such an extension inside of a given full-rank lattice in $\mathbb{R}^n$: a perpendicular vector $\boldsymbol{u}$ may not exist inside of our given lattice.

Successive minima extensions

Theorem 6 (Forst, L.F. - 2024)

Let $\Lambda \subset \mathbb{R}^n$ be a lattice of full rank, and let $\Omega_m \subset \Lambda$ be a sublattice of rank $1 \leq m < n$. Write $\mu = \mu(\Lambda)$, $\lambda_m = \lambda_m(\Omega_m)$. There exists a sublattice $\Omega_{m+1} \subset \Lambda$ of rank $m+1$ such that $\Omega_m \subset \Omega_{m+1}$ is a lattice extension, $\lambda_j(\Omega_{m+1}) = \lambda_j(\Omega_m)$ for all $1 \leq j \leq m$ and

$$\lambda_{m+1}(\Omega_{m+1}) \leq \frac{\lambda_m(\Omega_m)(v_*^2 + \sqrt{1-v_*^2})}{\sqrt{1-v_*^4}} + 2\mu(\Lambda), \qquad (3)$$

where v_* is the smallest root of the polynomial $p(v) =$

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

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

Sketch of proof

Let $V_m = \operatorname{span}_{\mathbb{R}} \Omega_m$, $\theta \in (0, \pi/2]$, and define the cone

$$C_\theta(V_m) = \{\boldsymbol{x} \in \mathbb{R}^n : \mathfrak{a}(\boldsymbol{x}, \boldsymbol{y}) \in [\theta, \pi - \theta] \; \forall \; \boldsymbol{y} \in V_m\},$$

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

Sketch of proof

Let $V_m = \operatorname{span}_{\mathbb{R}} \Omega_m$, $\theta \in (0, \pi/2]$, and define the cone

$$C_\theta(V_m) = \{\boldsymbol{x} \in \mathbb{R}^n : \mathfrak{a}(\boldsymbol{x}, \boldsymbol{y}) \in [\theta, \pi - \theta] \ \forall\ \boldsymbol{y} \in V_m\},$$

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

Lemma 7

If $\boldsymbol{x} \in C_\theta(V_m)$ *and*

$$\|\boldsymbol{x}\| \geq \frac{\lambda_m(\Omega_m)(\cot\theta\cos\theta + 1)}{\sqrt{1 + \cos^2\theta}},$$

then $\|\boldsymbol{x} + \boldsymbol{y}\| \geq \lambda_m(\Omega_m)$ *for every* $\boldsymbol{y} \in V_m$.

Sketch of proof

Let $V_m = \operatorname{span}_{\mathbb{R}} \Omega_m$, $\theta \in (0, \pi/2]$, and define the cone

$$C_\theta(V_m) = \{\boldsymbol{x} \in \mathbb{R}^n : \mathfrak{a}(\boldsymbol{x}, \boldsymbol{y}) \in [\theta, \pi - \theta] \ \forall \ \boldsymbol{y} \in V_m\},$$

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

Lemma 7

If $\boldsymbol{x} \in C_\theta(V_m)$ and

$$\|\boldsymbol{x}\| \geq \frac{\lambda_m(\Omega_m)(\cot\theta\cos\theta + 1)}{\sqrt{1 + \cos^2\theta}},$$

then $\|\boldsymbol{x} + \boldsymbol{y}\| \geq \lambda_m(\Omega_m)$ for every $\boldsymbol{y} \in V_m$.

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

$$r(\theta) = \frac{\lambda_m(\Omega_m)(\cot\theta\cos\theta + 1)}{\sqrt{1 + \cos^2\theta}}.$$

Sketch of proof

Then Lemma 7 guarantees that for any vector

$$\boldsymbol{x} \in \Lambda \cap (C_\theta(V_m) \setminus B_n(r(\theta))),$$

the lattice $L = \text{span}_{\mathbb{Z}} \{\Omega_m, \boldsymbol{x}\}$ satisfies $\lambda_j(L) = \lambda_j(\Omega_m)$ for all $1 \leq j \leq m$ and $\lambda_{m+1}(L) \leq \|\boldsymbol{x}\|$.

Sketch of proof

Then Lemma 7 guarantees that for any vector

$$\boldsymbol{x} \in \Lambda \cap \left(C_\theta(V_m) \setminus B_n(r(\theta)) \right),$$

the lattice $L = \operatorname{span}_{\mathbb{Z}} \{\Omega_m, \boldsymbol{x}\}$ satisfies $\lambda_j(L) = \lambda_j(\Omega_m)$ for all $1 \leq j \leq m$ and $\lambda_{m+1}(L) \leq \|\boldsymbol{x}\|$.
Hence we want to minimize

$$\lambda_{m+1}(\theta) := \min \left\{ \|\boldsymbol{x}\| : \boldsymbol{x} \in \Lambda \cap \left(C_\theta(V_m) \setminus B_n(r(\theta)) \right) \right\}$$

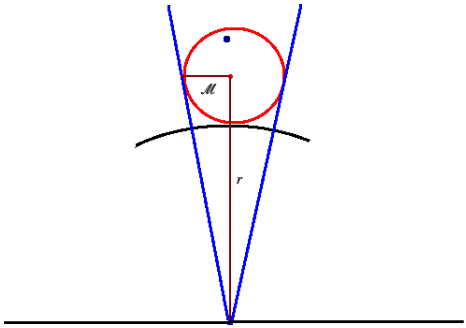
as a function of θ.
Any translated copy of the ball of radius $\mu(\Lambda)$ in $\mathbb{R}^n$ must contain a point of Λ. Suppose that $\theta \in (0, \pi/2]$ is such that

$$B_n'(\mu(\Lambda)) \subset \left(C_\theta(V_m) \cap B_n(r(\theta) + 2\mu(\Lambda)) \right) \setminus B_n(r(\theta)),$$

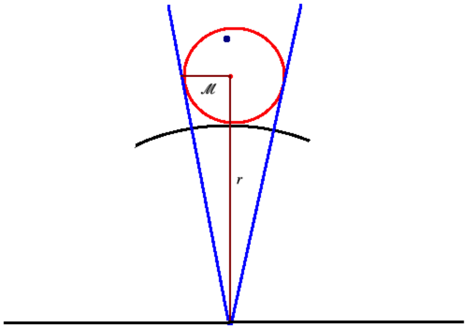
where $B_n'(\mu(\Lambda))$ is such a translated copy. Then $C_\theta(V_m) \setminus B_n(r(\theta))$ would be guaranteed to contain a point $\boldsymbol{x}$ of Λ with

$$\|\boldsymbol{x}\| \leq r(\theta) + 2\mu(\Lambda).$$

Sketch of proof



Sketch of proof



As shown in the picture, we have a right triangle with legs $r(\theta)+\mu(\Lambda)$ and $\mu(\Lambda)$ and the angle $\pi/2-\theta$ opposite to the second leg. Hence we have the equation

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

Sketch of proof

Writing $v = \cos\theta$, $\mu = \mu(\Lambda)$, and $\lambda_m = \lambda_m(\Omega_m)$, we obtain the following relation in terms of v:

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

which transforms into the polynomial equation $p(v) = 0$. It follows from our construction that this equation has at least one solution v in the interval $(0, 1)$.

Sketch of proof

Writing $v = \cos\theta$, $\mu = \mu(\Lambda)$, and $\lambda_m = \lambda_m(\Omega_m)$, we obtain the following relation in terms of v:

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

which transforms into the polynomial equation $p(v) = 0$. 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

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

which is an increasing function of v in the interval $(0, 1)$, so we pick the root v_* of $p(v)$ as small as possible.

Equal covering extensions

Λ is an **equal covering extension** of Ω if Λ is an extension of Ω such that

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

Equal covering extensions

Λ is an **equal covering extension** of Ω if Λ is an extension of Ω such that

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

Equal covering extensions may not exist inside of a given lattice.

Equal covering extensions

Λ is an **equal covering extension** of Ω if Λ is an extension of Ω such that

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

Equal covering extensions may not exist inside of a given lattice.

Theorem 8 (Forst, L.F. - 2024)

A lattice $\Lambda \subset \mathbb{R}^2$ is equal covering extension of $\mathbb{Z}\boldsymbol{e}_1$ if and only if

$$\Lambda = \Lambda(\alpha) := \begin{pmatrix} \frac{\alpha}{\sqrt{\alpha - \alpha^2}} & \frac{\alpha - 1}{\sqrt{\alpha - \alpha^2}} \end{pmatrix} \mathbb{Z}^2 \tag{4}$$

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 $\Omega \subset \Lambda$ if and only if it is isometric to some lattice of the form $\det(\Omega)\Lambda(\alpha)$, where $\Lambda(\alpha)$ is as in (4).

Idea of proof

For a planar lattice L with successive minima λ_1, λ_2 and angle $\theta \in [\pi/3, \pi/2]$ between the corresponding minimal vectors, the covering radius can be computed as:

$$\mu(L) = \frac{\sqrt{\lambda_1^2 + \lambda_2^2 - 2\lambda_1\lambda_2\cos\theta}}{2\sin\theta}. \tag{5}$$

Idea of proof

For a planar lattice L with successive minima λ_1, λ_2 and angle $\theta \in [\pi/3, \pi/2]$ between the corresponding minimal vectors, the covering radius can be computed as:

$$\mu(L) = \frac{\sqrt{\lambda_1^2 + \lambda_2^2 - 2\lambda_1\lambda_2 \cos\theta}}{2\sin\theta}. \tag{5}$$

The lattices $\Lambda(\alpha)$ are orthogonal, and so

$$\theta = \pi/2, \ \lambda_{1,2} = \sqrt{\alpha}, \sqrt{1-\alpha}.$$

This implies that $\mu(\Lambda(\alpha)) = 1/2 = \mu(\mathbb{Z}\boldsymbol{e}_1)$.

Idea of proof

For a planar lattice L with successive minima λ_1, λ_2 and angle $\theta \in [\pi/3, \pi/2]$ between the corresponding minimal vectors, the covering radius can be computed as:

$$\mu(L) = \frac{\sqrt{\lambda_1^2 + \lambda_2^2 - 2\lambda_1\lambda_2 \cos\theta}}{2\sin\theta}. \tag{5}$$

The lattices $\Lambda(\alpha)$ are orthogonal, and so

$$\theta = \pi/2,\ \lambda_{1,2} = \sqrt{\alpha}, \sqrt{1-\alpha}.$$

This implies that $\mu(\Lambda(\alpha)) = 1/2 = \mu(\mathbb{Z}\boldsymbol{e}_1)$.
The reverse direction involves looking for the **fundamental deep hole** of a planar lattice L, i.e. the point $\boldsymbol{z} \in \mathbb{R}^2_{>0}$ with $\|\boldsymbol{z}\| = \mu(L)$ so that

$$\min_{\boldsymbol{x} \in L} \|\boldsymbol{z} - \boldsymbol{x}\| = \max_{\boldsymbol{y} \in \mathbb{R}^2} \min_{\boldsymbol{x} \in L} \|\boldsymbol{y} - \boldsymbol{x}\|.$$

Rings of quadratic integers

Corollary 9

Let D be a squarefree integer and $K = \mathbb{Q}(\sqrt{D})$ a quadratic number field. Let $\mathcal{O}_K$ be its ring of integers and let

$$\Omega_K = \sigma_K(\mathcal{O}_K) \subset \mathbb{R}^2$$

be the lattice that is the image of $\mathcal{O}_K$ in the plane under Minkowski embedding σ_K. Then Ω_K is an equal covering extension of a rank-one lattice if and only if $D \not\equiv 1 \pmod 4$. If this is the case, then Ω_K is an equal covering extension of the lattice

$$\mathbb{Z}\sigma_K(1 + \sqrt{D}).$$

Orthogonal equal covering extensions

While we do not have a characterization of equal covering extensions in higher dimensions, we can construct orthogonal equal covering extensions in any dimension.

Theorem 10 (Forst, L.F. - 2024)

Let $\Lambda_m \subset \mathbb{R}^n$ be an orthogonal lattice of rank $m < n$. There exists an orthogonal lattice $\Lambda_{m+1} \subset \mathbb{R}^n$ of rank $m+1$ so that $\Lambda_m \subset \Lambda_{m+1}$ is a lattice extension and $\mu(\Lambda_{m+1}) = \mu(\Lambda_m)$. Further, if $\boldsymbol{z}$ is a deep hole of Λ_m it is also a deep hole of Λ_{m+1}.

Deep holes in more detail

In general, a **deep hole** of a full-rank lattice $L \subset \mathbb{R}^n$ is a point $\boldsymbol{z}$ in $\mathbb{R}^n$ furthest removed from the lattice, i.e.

$$\min_{\boldsymbol{x}\in L} \|\boldsymbol{z} - \boldsymbol{x}\| = \max_{\boldsymbol{y}\in\mathbb{R}^n} \min_{\boldsymbol{x}\in L} \|\boldsymbol{y} - \boldsymbol{x}\|.$$

Deep holes in more detail

In general, a **deep hole** of a full-rank lattice $L \subset \mathbb{R}^n$ is a point $\boldsymbol{z}$ in $\mathbb{R}^n$ furthest removed from the lattice, i.e.

$$\min_{\boldsymbol{x}\in L} \|\boldsymbol{z}-\boldsymbol{x}\| = \max_{\boldsymbol{y}\in\mathbb{R}^n} \min_{\boldsymbol{x}\in L} \|\boldsymbol{y}-\boldsymbol{x}\|.$$

Lemma 11

Let $\Lambda \subset \mathbb{R}^2$ be a lattice of rank 2 with minimal basis $\boldsymbol{x}, \boldsymbol{y}$ 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 $0 < \lambda_1 = \|\boldsymbol{x}\| \leq \lambda_2 = \|\boldsymbol{y}\|$. Then the fundamental parallelogram

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

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

Deep holes in more detail

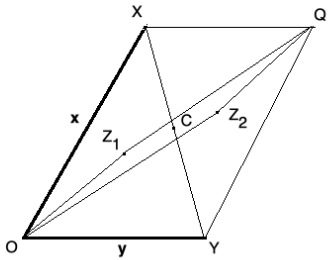


Figure: Fundamental parallelogram $\mathfrak{P}$ of Λ with deep holes $\boldsymbol{z}_1$ and $\boldsymbol{z}_2$.

An immediate implication of Lemma 11 is that deep holes $\boldsymbol{z}_1, \boldsymbol{z}_2$ are each other's inverses in the additive abelian group $\mathbb{R}^2/\Lambda$. Further, $\boldsymbol{z}_1$ is an element of order two in this group if and only if the angle $\theta = \pi/2$; in this case $\boldsymbol{z}_1 = \boldsymbol{z}_2$. On the other hand, $\boldsymbol{z}_1, \boldsymbol{z}_2$ can be elements of finite order in other situations too.

Deep holes in more detail

For instance, in the hexagonal lattice

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

the deep holes are $\boldsymbol{z}_1 = (1/2, 1/(2\sqrt{3}))$, $\boldsymbol{z}_2 = (1, 1/\sqrt{3})$ 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 $\boldsymbol{z}_1 = (1/2, 11\sqrt{3}/24)$ satisfying the condition

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

which makes $\boldsymbol{z}_1$ an element of order dividing 48 in the group $\mathbb{R}^2/L'$.

Deep holes in more detail

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 $\mathbb{R}^2/\Lambda$?

Deep holes in more detail

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 $\mathbb{R}^2/\Lambda$?

Theorem 12 (Forst, L.F. - 2024)

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

Deep holes in more detail

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 $\mathbb{R}^2/\Lambda$?

Theorem 12 (Forst, L.F. - 2024)

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

Remark 1

The proof of this theorem uses Siegel's lemma for a simple situation of a 3×2 integral linear system.

References

M. Forst and L. Fukshansky, *Counting basis extensions in a lattice*, Proceedings of the American Mathematical Society, vol. 150 no. 8 (2022), pg. 3199–3213

M. Forst and L. Fukshansky, *On lattice extensions*, Monatshefte für Mathematik, vol. 203 no. 3 (2024) pg. 613–634

Preprints are available at:

`https://www1.cmc.edu/pages/faculty/lenny/research.html`

References

M. Forst and L. Fukshansky, *Counting basis extensions in a lattice*, Proceedings of the American Mathematical Society, vol. 150 no. 8 (2022), pg. 3199–3213

M. Forst and L. Fukshansky, *On lattice extensions*, Monatshefte für Mathematik, vol. 203 no. 3 (2024) pg. 613–634

Preprints are available at:

`https://www1.cmc.edu/pages/faculty/lenny/research.html`

Thank you!