Mastermath, Spring 2018
Intro to Lattice Algs & Crypto

Lecture 2

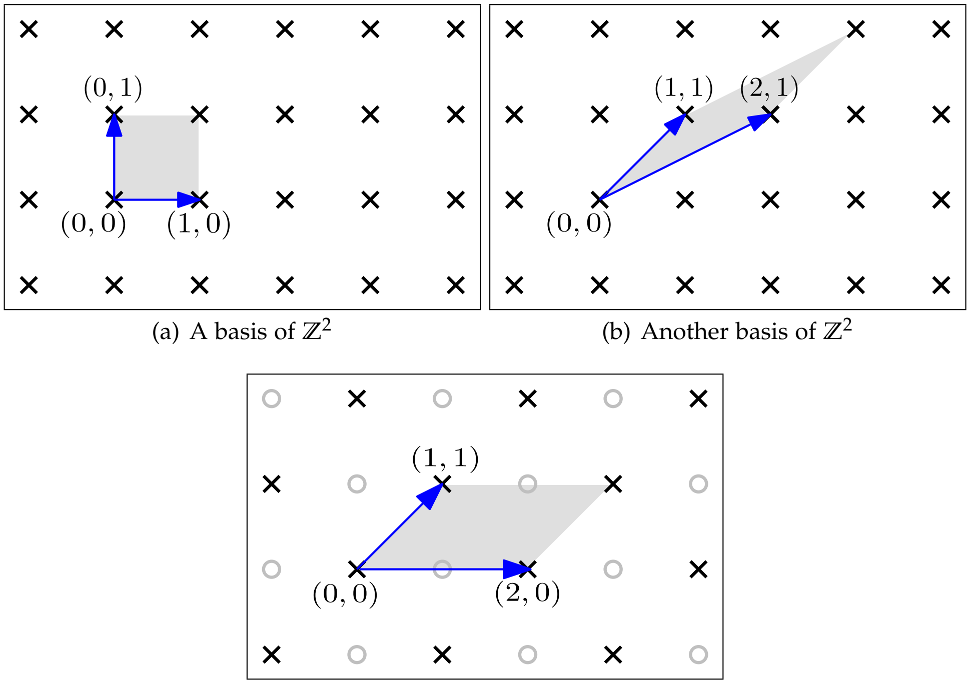
Lecturers: D. Dadush, L. Ducas
Scribe: D. Dadush

# Determinants, Packing and Covering, and the Minkowski Theorems

## 1 Fundamental Parallelepiped and the Determinant

Definition 1 (Fundamental Parallelepiped) *Let $\mathcal{L} = \mathcal{L}(B) \subseteq \mathbb{R}^n$ for some basis matrix $\mathbf{B} \in \mathbb{R}^{n \times k}$. We define the fundamental parallelepiped of $\mathcal{L}$ with respect to $\mathbf{B}$ as $\mathcal{P}(\mathbf{B}) = \mathbf{B}[0,1)^k \overset{\text{def}}{=} \{\mathbf{B}\mathbf{x} : \mathbf{x} \in [0,1)^k\}$.*

Examples of fundamental parallelepipeds are shown by the gray areas in Figure 1. Notice that $\mathcal{P}(\mathbf{B})$ depends on the basis $\mathbf{B}$. As is easily seen in the pictures, if we place one copy of $\mathcal{P}(\mathbf{B})$ at each lattice point in $\mathcal{L}(\mathbf{B})$ we obtain a tiling of the entire span$(\mathcal{L}(\mathbf{B}))$ (we prove this in Lemma 4). See Figure 2.



(a) A basis of $\mathbb{Z}^2$

(b) Another basis of $\mathbb{Z}^2$

(c) Not a basis of $\mathbb{Z}^2$

Figure 1: Some lattice bases

Now that we know that every lattice admits a basis, a next fundamental question is: given linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathcal{L}$ how can we tell if they form a basis of $\mathcal{L}$? As we have seen previously, not every set of $n$ linearly vectors in $\mathbb{Z}^n$ is a basis of $\mathbb{Z}^n$. One possible answer is given in the following lemma.

It says that the basic parallelepiped generated by the vectors should not contain any lattice points, except the origin. As an example, notice that the basic parallelepiped shown in Figure 1(c) contains the lattice point $(1, 0)$ whereas those in Figures 1(a) and 1(b) do not contain any nonzero lattice points.

Lemma 2 *Let $\mathcal{L}$ be a lattice of rank $n$, and let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathcal{L}$ be $n$ linearly independent lattice vectors. Then $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ form a basis of $\mathcal{L}$ if and only if $\mathcal{P}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) \cap \mathcal{L} = \{0\}$.*

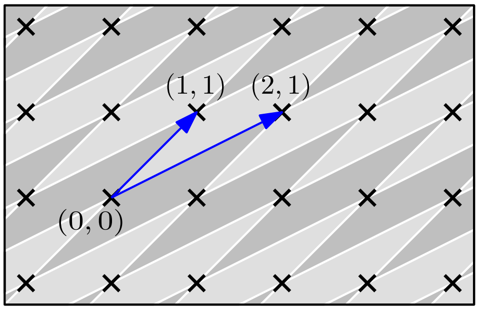


Figure 2: Tiling span($\mathcal{L}(\mathbf{B})$) with $\mathcal{P}(\mathbf{B})$

PROOF: Assume first that $\mathbf{b}_1, \ldots, \mathbf{b}_n$ form a basis of $\mathcal{L}$. Then, by definition, $\mathcal{L}$ is the set of all their integer combinations. Since $\mathcal{P}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is defined as the set of linear combinations of $\mathbf{b}_1, \ldots, \mathbf{b}_n$ with coefficients in $[0,1)$, the intersection of the two sets is $\{\mathbf{0}\}$.

For the other direction, assume that $\mathcal{P}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) \cap \mathcal{L} = \{\mathbf{0}\}$. Since $\mathcal{L}$ is a rank $n$ lattice and $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are linearly independent, we can write any lattice vector $\mathbf{x} \in \mathcal{L}$ as $\sum y_i \mathbf{b}_i$ for some $y_i \in \mathbb{R}$. Since by definition a lattice is closed under addition, the vector $\mathbf{x}' = \sum (y_i - \lfloor y_i \rfloor) \mathbf{b}_i$ is also in $\mathcal{L}$. By our assumption, $\mathbf{x}' = \mathbf{0}$. This implies that all $y_i$ are integers and hence $\mathbf{x}$ is an integer combination of $\mathbf{b}_1, \ldots, \mathbf{b}_n$. □

Given that a lattice $\mathcal{L}$ lives in an ambient space, one interesting question to ask is how can we measure the "density" of $\mathcal{L}$ within its ambient space? In particular, the length of the shortest-vector $\lambda_1(\mathcal{L})$, certainly gives one such measure, i.e. the smaller $\lambda_1$, the denser the lattice. However, this provides only a one dimensional notion of density. Another measure, which plays a crucial role in the theory of lattices, is given by the following quantity.

DEFINITION 3 (DETERMINANT) *Let $\mathcal{L} = \mathcal{L}(\mathbf{B}) \subseteq \mathbb{R}^n$ for some basis $\mathbf{B} \in \mathbb{R}^{n \times k}$. Define the determinant of $\mathcal{L}$ to be* $\det(\mathcal{L}) = \sqrt{\det(\mathbf{B}^\intercal \mathbf{B})}$.

For the above definition, we first note that $\det(\mathcal{L})$ is invariant under the choice of basis. To see this, note that any other basis of $\mathcal{L}$ has the form $\mathbf{BU}$ for some unimodular matrix $\mathbf{U} \in \mathbb{Z}^{k \times k}$. Therefore

$$\sqrt{\det((\mathbf{BU})^\intercal \mathbf{BU})} = \sqrt{\det(\mathbf{U}^\intercal \mathbf{B}^\intercal \mathbf{BU})} = \sqrt{\det(\mathbf{B}^\intercal \mathbf{B}) \det(\mathbf{U})^2} = \sqrt{\det(\mathbf{B}^\intercal \mathbf{B})},$$

as needed. In the special case where $k = n$, note that $\det(\mathcal{L}) = |\det(\mathbf{B})|$.

We now show that the determinant corresponds to inverse density of lattice within its ambient space. In particular, we show that for a lattice $\mathcal{L}(\mathbf{B})$, the fundamental parallelepiped $\mathcal{P}(\mathbf{B})$ tiles space with respect to $\mathcal{L}$ and has volume exactly $\det(\mathcal{L})$. Hence every lattice point can be associated with $\det(\mathcal{L})$ distinct units of volume in the ambient space, which justifies the interpretation of inverse density.

LEMMA 4 *Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_k)$ denote a basis for a lattice $\mathcal{L}$. Then for $\mathcal{P}(\mathbf{B})$, the following holds:*

1. $\mathrm{vol}_k(\mathcal{P}(\mathbf{B})) = \det(\mathcal{L})$.
2. $\forall \mathbf{x} \in \mathrm{span}(\mathcal{L})$, *there is a unique* $\mathbf{y} \in \mathcal{L}$ *such that* $\mathbf{x} \in \mathbf{y} + \mathcal{P}(\mathbf{B})$. *In particular,* $\mathrm{span}(\mathcal{L}) = \mathcal{L} + \mathcal{P}(\mathbf{B})$, *i.e.* $\mathcal{P}(\mathbf{B})$ *tiles space with respect to* $\mathcal{L}$.

PROOF:

**Proof of 1.** Let $\mathbf{O} \in \mathbb{R}^{n \times k}$ be a matrix whose columns form an orthonormal basis of $\mathrm{span}(\mathcal{L})$. Clearly, the linear transformation $\mathbf{O}^\mathsf{T}$ is an isometry (preserves distances) when restricted to $\mathrm{span}(\mathcal{L})$, and hence preserves volumes. Therefore $\mathrm{vol}_k(\mathbf{O}^\mathsf{T}\mathcal{P}(\mathbf{B})) = \mathrm{vol}_k(\mathcal{P}(\mathbf{B}))$. Since $\mathbf{O}^\mathsf{T}\mathcal{P}(\mathbf{B}) = \mathbf{O}^\mathsf{T}\mathbf{B}[0,1)^k$, where $\mathbf{O}^\mathsf{T}\mathbf{B}$ is a $k \times k$ matrix, we have that $\mathrm{vol}_k(\mathbf{O}^\mathsf{T}\mathbf{B}[0,1)^k) = |\det(\mathbf{O}^\mathsf{T}\mathbf{B})|\mathrm{vol}_k([0,1)^k) = |\det(\mathbf{O}^\mathsf{T}\mathbf{B})|$. Since for any $\mathbf{x} \in \mathrm{span}(\mathcal{L})$ we have $\mathbf{O}\mathbf{O}^\mathsf{T}\mathbf{x} = \mathbf{x}$, we see that

$$\det(\mathbf{O}^\mathsf{T}\mathbf{B})^2 = \det(\mathbf{B}^\mathsf{T}\mathbf{O})\det(\mathbf{O}^\mathsf{T}\mathbf{B}) = \det(\mathbf{B}^\mathsf{T}\mathbf{O}\mathbf{O}^\mathsf{T}\mathbf{B}) = \det(\mathbf{B}^\mathsf{T}\mathbf{B}) = \det(\mathcal{L})^2.$$

Therefore $\mathrm{vol}_k(\mathcal{P}(\mathbf{B})) = |\det(\mathbf{O}^\mathsf{T}\mathbf{B})| = \det(\mathcal{L})$.

**Proof of 2.** Take $\mathbf{x} \in \mathrm{span}(\mathcal{L})$. Let $\mathbf{b}_1, \ldots, \mathbf{b}_k$ be the columns of $\mathbf{B}$. Since they form a basis of $\mathrm{span}(\mathcal{L})$, there is a unique way to express $\mathbf{x} = \sum_{i=1}^k a_i \mathbf{b}_i$ for $a_1, \ldots, a_k \in \mathbb{R}$. Let $\mathbf{y} = \sum_{i=1}^k \lfloor a_i \rfloor \mathbf{b}_i \in \mathcal{L}$. Since $a_i - \lfloor a_i \rfloor \in [0,1)$, we have that $\mathbf{x} - \mathbf{y} \in \mathcal{P}(\mathbf{B}) \Rightarrow \mathbf{x} \in \mathcal{P}(\mathbf{B}) + \mathbf{y}$. Since this holds for any vector $\mathrm{span}(\mathcal{L})$, and $\mathcal{P}(\mathbf{B}) \subseteq \mathrm{span}(\mathcal{L})$, we get that $\mathrm{span}(\mathcal{L}) = \mathcal{L} + \mathcal{P}(\mathbf{B})$.

It remains to show that $\mathbf{y}$ is the unique lattice vector such that $\mathbf{x} \in \mathcal{P}(\mathbf{B}) + \mathbf{y}$ with this property. In particular for $\mathbf{x} \in \mathcal{L}$ distinct from $\mathbf{y}$, we wish to show that $(\mathcal{P}(\mathbf{B}) + \mathbf{y}) \cap (\mathcal{P}(\mathbf{B}) + \mathbf{x}) = \emptyset$. Assume not, then by rearranging we must have that $\mathbf{x} - \mathbf{y} \in \mathcal{P}(\mathbf{B}) - \mathcal{P}(\mathbf{B}) = \mathbf{B}([0,1)^n - [0,1)^n) = \mathbf{B}(-1,1)^n$. Since $\mathbf{x} - \mathbf{y} \in \mathcal{L}$, we must be able to write $\mathbf{x} - \mathbf{y} = \sum_{i=1}^n z_i \mathbf{b}_i$ for $z_1, \ldots, z_n \in \mathbb{Z}$. Since $\mathbf{B}$ is non-singular, from the inclusion $\mathbf{x} - \mathbf{y} \in \mathbf{B}(-1,1)^n$, we must have that $z_1, \ldots, z_n \in (-1,1) \cap \mathbb{Z} = \{0\}$. Therefore $z_1 = \cdots = z_n = 0$, and hence $\mathbf{x} = \mathbf{y}$, a clear contradiction. □

Given the above, we can define the following operation which will be important in the segway:

Definition 5 (Parallelepiped Mod) *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice with basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_k) \in \mathbb{R}^{n \times k}$. For a vector $\mathbf{x} \in \mathrm{span}(\mathcal{L})$, where $\mathbf{x} = \sum_{i=1}^k a_i \mathbf{b}_i$, we define $\mathbf{x} \pmod{\mathcal{P}(\mathbf{B})}$ to the vector $\sum_{i=1}^k (a_i - \lfloor a_i \rfloor)\mathbf{b}_i \in \mathcal{P}(\mathbf{B})$.*

We note that the above operation is well-defined from Lemma 4. Furthermore, it is easy to check that for $\mathbf{x}, \mathbf{y} \in \mathrm{span}(\mathcal{L}(\mathbf{B}))$, that $\mathbf{x} - \mathbf{y} \in \mathcal{L}(\mathbf{B})$ iff $\mathbf{x} \pmod{\mathcal{P}(\mathbf{B})} = \mathbf{y} \pmod{\mathcal{P}(\mathbf{B})}$.

## 2 Packing, Covering and Tiling

In the previous section, we saw how any fundamental parallelepiped of a lattice $\mathcal{L}$ tiles space with respect to $\mathcal{L}$. We shall now examine generalizations of the tiling concept, and show how they imply some very useful integral and volume inequalities.

Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice and let $F \subseteq \mathrm{span}(\mathcal{L})$ be a measurable set (with respect to Lesbegue measure on $\mathrm{span}(\mathcal{L})$). We define $F$ to be

1. $\mathcal{L}$-packing if $\forall \mathbf{x}, \mathbf{y} \in \mathcal{L}$, $\mathbf{x} \neq \mathbf{y}$, $(\mathbf{x} + F) \cap (\mathbf{y} + F) = \emptyset$
2. $\mathcal{L}$-covering if $\mathcal{L} + F = \mathrm{span}(\mathcal{L})$.
3. $\mathcal{L}$-tiling (or a fundamental domain of $\mathcal{L}$) if $F$ is both $\mathcal{L}$-packing and $\mathcal{L}$-covering.

Remark 6 From the above definitions, by Lemma 4 we see that for a lattice $\mathcal{L}$ and any basis $\mathbf{B}$ of $\mathcal{L}$ that $\mathcal{P}(\mathbf{B})$ is a fundamental domain of $\mathcal{L}$.

We derive the following simple equivalence.

Lemma 7 *$F \subseteq \mathrm{span}(\mathcal{L})$ is $\mathcal{L}$-(packing, covering, tiling) if and only if*

$$\forall \mathbf{x} \in \mathrm{span}(\mathcal{L}), \quad |(\mathcal{L} + \mathbf{x}) \cap F| \quad (\leq, \geq, =) \quad 1. \tag{1}$$

*Furthermore $F \subseteq \mathrm{span}(\mathcal{L})$ is non-empty and $\mathcal{L}$-packing $\Leftrightarrow (F - F) \cap \mathcal{L} = \{\mathbf{0}\}$.*

Proof: Assume $F$ is $\mathcal{L}$-packing. Take $\mathbf{x} \in \mathrm{span}(\mathcal{L})$. If $|(\mathcal{L} + \mathbf{x}) \cap F| \geq 2$, then we can pick distinct $\mathbf{w}, \mathbf{z} \in F$ such that $\mathbf{w}, \mathbf{z} \in \mathcal{L} + \mathbf{x}$. Now note that $\mathbf{w} \in F = F + \mathbf{0}$ and $\mathbf{w} = \mathbf{z} + (\mathbf{w} - \mathbf{z}) \in F + (\mathbf{w} - \mathbf{z})$. Therefore $(F + \mathbf{0}) \cap (F + \mathbf{w} - \mathbf{z}) \neq \emptyset$. But $\mathbf{0}$ and $\mathbf{w} - \mathbf{z}$ are distinct points in $\mathcal{L}$, a contradiction to our assumption on $F$. Hence $|(\mathcal{L} + \mathbf{x}) \cap F| \leq 1$ as needed. Assume $F$ is $\mathcal{L}$-covering. Take $\mathbf{x} \in \mathrm{span}(\mathcal{L})$. Since $\mathcal{L} + F = \mathbb{R}^n$, there exists $\mathbf{y} \in \mathcal{L}$ such that $\mathbf{x} \in \mathbf{y} + F$. Therefore $\mathbf{x} - \mathbf{y} \in F$, and since $-\mathbf{y} \in \mathcal{L}$ we get that $|(\mathcal{L} + \mathbf{x}) \cap F| \geq 1$ as needed. The claim for $F$ an $\mathcal{L}$-tiling follows directly from the previous assertions.

We prove the furthermore. We first note that $\exists \mathbf{x} \in \mathrm{span}(\mathcal{L})$ such that $|(\mathcal{L} + \mathbf{x}) \cap F| \geq 2 \Leftrightarrow \exists \mathbf{x}_1, \mathbf{x}_2 \in F$, such that $\mathbf{x}_1 - \mathbf{x}_2 \in \mathcal{L} \setminus \{\mathbf{0}\} \Leftrightarrow ((F - F) \cap \mathcal{L}) \setminus \{\mathbf{0}\} \neq \emptyset$. Therefore $F$ is not $\mathcal{L}$-packing if and only if $((F - F) \cap \mathcal{L}) \setminus \{\mathbf{0}\} \neq \emptyset$, as needed. □

The following theorem, gives us some fundamental properties of packing, covering and tiling sets. In particular, it shows that every fundamental domain of a lattice has the same volume (which we currently only knew for fundamental parallelipipeds).

Theorem 8 *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a $k \geq 1$ dimensional lattice and let $W = \mathrm{span}(\mathcal{L})$. Let $F \subseteq W$ be measurable set and $g : \mathrm{span}(\mathcal{L}) \to \mathbb{R}_+$ be a measurable function with respect to the k-dimensional Lesbesgue measure on W. If F is a $\mathcal{L}$-(packing, covering, tiling) we have that*

$$\int_F \sum_{\mathbf{y} \in \mathcal{L}} g(\mathbf{y} + \mathbf{x}) \mathrm{dvol}_k(\mathbf{x}) \quad (\leq, \geq, =) \quad \int_W g(\mathbf{x}) \mathrm{dvol}_k(\mathbf{x}),$$

*where $\mathrm{vol}_k$ denotes the k-dimensional Lebesgue measure on W. Furthermore, if F is a $\mathcal{L}$-(packing, covering, tiling) we have that*

$$\mathrm{vol}_k(F) \quad (\leq, \geq, =) \quad \det(\mathcal{L}).$$

Proof: By choosing an orthormal basis for $W$ and applying a change of coordinates, we may assume that $W = \mathbb{R}^n$ and that $k = n$. Since $g \geq 0$ and measurable, we have that $m(A) = \int_A g(\mathbf{x}) \mathrm{d}\mathbf{x}$, for $A \subseteq \mathbb{R}^n$ measurable, defines a measure on $\mathbb{R}^n$. Let $1_{\mathbf{y}+F}$, $\mathbf{y} \in \mathcal{L}$, denote the indicator function of $\mathbf{y} + F$. Since $\mathbf{y} + F$ is measurable, we get that $1_{F+\mathbf{y}}$ is non-negative measurable function. Since $\mathcal{L}$ is countable, by the monotone convergence theorem we have that

$$\begin{aligned} \sum_{\mathbf{y} \in \mathcal{L}} m(\mathbf{y} + F) &= \sum_{\mathbf{y} \in \mathcal{L}} \int_{\mathbb{R}^n} 1_{\mathbf{y}+F}(\mathbf{x}) g(\mathbf{x}) \mathrm{d}\mathbf{x} = \sum_{\mathbf{y} \in \mathcal{L}} \int_{\mathbb{R}^n} 1_F(\mathbf{x}) g(\mathbf{x} + \mathbf{y}) \mathrm{d}\mathbf{x} \\ &= \int_{\mathbb{R}^n} \sum_{\mathbf{y} \in \mathcal{L}} 1_F(\mathbf{x}) g(\mathbf{x} + \mathbf{y}) \mathrm{d}\mathbf{x} = \int_F \sum_{\mathbf{y} \in \mathcal{L}} g(\mathbf{x} + \mathbf{y}) \mathrm{d}\mathbf{x} \end{aligned}$$

If $F$ is $\mathcal{L}$-packing, then collections of sets $\mathbf{y} + F \subseteq \mathbb{R}^n$, for $\mathbf{y} \in \mathcal{L}$, are all disjoint. Therefore we have that

$$\int_{\mathbb{R}^n} g(\mathbf{x}) \mathrm{d}\mathbf{x} = m(\mathbb{R}^n) \geq m(\mathcal{L} + F) = \sum_{\mathbf{y} \in \mathcal{L}} m(\mathbf{y} + F) = \int_F \sum_{\mathbf{y} \in \mathcal{L}} g(\mathbf{x} + \mathbf{y}) \mathrm{d}\mathbf{x}$$

as needed. If $F$ is $\mathcal{L}$-covering, we have that $\mathbb{R}^n \subseteq \mathcal{L} + F$, and hence

$$m(\mathbb{R}^n) = m(\mathcal{L} + F) \leq \sum_{\mathbf{y} \in \mathcal{L}} m(\mathbf{y} + F) = \int_F \sum_{\mathbf{y} \in \mathcal{L}} g(\mathbf{x} + \mathbf{y}) \mathrm{d}\mathbf{x}$$

as needed. If $F$ is $\mathcal{L}$-tiling, we get the desired equality by combining the above two inequalities.

We now prove the furthermore. Let $B \in \mathbb{R}^{n \times n}$ denote a basis for $\mathcal{L}$. From Lemma 4, we know that $B[0,1)^n$ is $\mathcal{L}$-tiling and satisfies $\mathrm{vol}_n(B[0,1)^n) = \det(\mathcal{L})$. From the first part of the lemma, we have that

$$\mathrm{vol}_n(F) = \int_{\mathbb{R}^n} 1_F(\mathbf{x}) \mathrm{d}\mathbf{x} = \int_{B[0,1)^n} \sum_{\mathbf{y} \in \mathcal{L}} 1_F(\mathbf{x} + \mathbf{y}) \mathrm{d}\mathbf{x} = \int_{B[0,1)^n} |(\mathcal{L} + \mathbf{x}) \cap F| \mathrm{d}\mathbf{x}$$

If $F$ is $\mathcal{L}$-(packing, covering, tiling) we have that $\forall \mathbf{x} \in \mathbb{R}^n$, $|(\mathcal{L} + \mathbf{x}) \cap F| \ (\leq, \geq, =) \ 1$. Therefore if $F$ is $\mathcal{L}$-(packing, covering, tiling) we have that

$$\mathrm{vol}_n(F) = \int_{\mathbf{B}[0,1)^n} |(\mathcal{L} + \mathbf{x}) \cap F| \mathrm{d}\mathbf{x} \ \ (\leq, \geq, =) \ \ \int_{\mathbf{B}[0,1)^n} 1 \mathrm{d}\mathbf{x} = \mathrm{vol}_n(\mathbf{B}[0,1)^n) = \det(\mathcal{L})$$

as needed. □

## 3 Sublattices and Quotient Groups

For a lattice $\mathcal{L} \subseteq \mathbb{R}^n$ of rank $k$, we define the quotient group $\mathrm{span}(\mathcal{L})/\mathcal{L} = \{\mathbf{x} + \mathcal{L} : \mathbf{x} \in \mathrm{span}(\mathcal{L})\}$. It is easy to check that $\mathrm{span}(\mathcal{L})/\mathcal{L}$ forms a group under addition, where $(\mathbf{x} + \mathcal{L}) + (\mathbf{y} + \mathcal{L}) = (\mathbf{x} + \mathbf{y}) + \mathcal{L}$. Note that $\mathbf{x} + \mathcal{L} = \mathbf{y} + \mathcal{L} \Leftrightarrow \mathbf{x} - \mathbf{y} \in \mathcal{L}$. For convenience of notation, we will write $\mathbf{x} \equiv \mathbf{y} \pmod{\mathcal{L}}$ if $\mathbf{x} - \mathbf{y} \in \mathcal{L}$. Note that while $\mathrm{span}(\mathcal{L})/\mathcal{L}$ is infinite, the "correct" notion of size is from the volumetric standpoint where it makes sense to interpret $\det(\mathcal{L})$ as the "size" of the group. Here we justify this by the fact that any fundamental domain $F$ of $\mathcal{L}$ contains a unique representative from every element of $\mathrm{span}(\mathcal{L})/\mathcal{L}$ and $\mathrm{vol}_k(F) = \det(\mathcal{L})$. The geometry of the group $\mathrm{span}(\mathcal{L})/\mathcal{L}$ will play an important role in many of the lattice structure results. It is easy to see (we prove it in Lemma 9) that the $\mathrm{span}(\mathcal{L})/\mathcal{L}$ is isomorphic (algebraically speaking) to the torus $\mathbb{R}^k/\mathbb{Z}^k$, i.e. the group of real vectors under addition modulo 1.

For a lattice $\mathcal{L} \subseteq \mathbb{R}^n$, a lattice $\mathcal{L}' \subseteq \mathcal{L}$ is a called a sublattice of $\mathcal{L}'$. For example, the lattice $\mathcal{L}' = \{(x, y) \in \mathbb{Z}^2 : x + y \equiv 0 \pmod{2}\}$ is a sublattice of $\mathbb{Z}^2$. Analogous to the above construction, we define the quotient group $\mathcal{L}/\mathcal{L}' = \{\mathbf{x} + \mathcal{L}' : \mathbf{x} \in \mathcal{L}\}$. As opposed to the previous setting, $|\mathcal{L}/\mathcal{L}'|$ is generally finite (as long as $\mathrm{span}(\mathcal{L}') = \mathrm{span}(\mathcal{L})$). Perhaps the simplest class of sublattices of $\mathcal{L}$ that will occur frequently throughout this course are of the form $m\mathcal{L}$ for $m \in \mathbb{N}$.

Here we describe the simple algebraic structure of the quotient group for two of the cases mentioned above.

Lemma 9 *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a $k \geq 1$ dimensional lattice. The following holds:*

1. $\mathrm{span}(\mathcal{L})/\mathcal{L} \cong \mathbb{R}^k/\mathbb{Z}^k$.
2. *For $m \in \mathbb{N}$, $\mathcal{L}/m\mathcal{L} \cong \mathbb{Z}_m^k$ and $|\mathcal{L}/m\mathcal{L}| = m^k$. Furthermore $\det(m\mathcal{L}) = m^k \det(\mathcal{L})$.*

Proof:

**Proof of** 1**:** Let $\mathbf{b}_1, \ldots, \mathbf{b}_k$ denote any basis for $\mathcal{L}$. For $\mathbf{x} \in \mathrm{span}(\mathcal{L})$, let $T : \mathrm{span}(\mathcal{L}) \to \mathbb{R}^k$ be the coordinate map which sends $\mathbf{x} = \sum_{i=1}^k a_i \mathbf{b}_i \in \mathrm{span}(\mathcal{L})$ to $(a_1, \ldots, a_k)$. Given that $T$ is linear and bijective, and since $T(\mathrm{span}(\mathcal{L})) = \mathbb{R}^k$ and $T(\mathcal{L}) = \mathbb{Z}^n$, we have that $\mathrm{span}(\mathcal{L})/\mathcal{L} \cong T(\mathrm{span}(\mathcal{L})/T(\mathcal{L}) = \mathbb{R}^k/\mathbb{Z}^k$ as needed.

**Proof of** 2**:** Let $\mathbf{b}_1, \ldots, \mathbf{b}_k$ denote any basis for $\mathcal{L}$. Clearly $\mathcal{L}(m\mathbf{b}_1, \ldots, m\mathbf{b}_k) = m\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k) = m\mathcal{L}$, and hence $m\mathbf{b}_1, \ldots, m\mathbf{b}_k$ is a basis for $m\mathcal{L}$. Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_k)$ denote the associated basis matrix. Then by definition

$$\det(m\mathcal{L}) = \sqrt{\det((m\mathbf{B})^\mathsf{T}(m\mathbf{B}))} = m^k\sqrt{\det(\mathbf{B}^\mathsf{T}\mathbf{B})} = m\det(\mathcal{L}).$$

Let $\tau : \mathcal{L} \to \mathbb{Z}_m^k$ denote the map which sends $\mathbf{x} = \sum_{i=1}^k a_i \mathbf{b}_i \in \mathcal{L}$ to $(a_1 \pmod{m}, \ldots, a_k \pmod{m})$. Clearly this map is well defined since $\mathbf{b}_1, \ldots, \mathbf{b}_k$ are a basis of $\mathcal{L}$. Furthermore, by the properties of addition mod $m$ we clearly have that $\tau(\mathbf{x} + \mathbf{y}) = \tau(\mathbf{x}) + \tau(\mathbf{y})$ for any $\mathbf{x}, \mathbf{y} \in \mathcal{L}$, and hence $\tau$ is a homomorphism from $\mathcal{L}$ to $\mathbb{Z}_m^k$. Next, we note that the $\tau$ is surjective onto $\mathbb{Z}_m^k$ since $\tau(\mathbf{B}\{0, 1, \ldots, m-1\}^k) = \mathbb{Z}_m^k$. Lastly, for $\mathbf{x} = \sum_{i=1}^k a_i \mathbf{b}_i$, we see that $\tau(\mathbf{x}) \equiv 0 \pmod{\mathbb{Z}_m^k} \Leftrightarrow a_i \equiv 0 \pmod{m}\ \forall i \in [k] \Leftrightarrow \mathbf{x} \in m\mathcal{L}$. Hence the kernel of $\tau$ is $m\mathcal{L}$, and therefore $\mathcal{L}/m\mathcal{L} \cong \mathbb{Z}_m^k$ as needed. □

In the above Lemma, we saw that $|\mathcal{L}/m\mathcal{L}| = \det(m\mathcal{L})/\det(\mathcal{L})$. In the following theorem, we show that this is also the case for general sublattices.

Lemma 10 *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a $k \geq 1$ dimensional lattice, and let $\mathcal{L}'$ be a sublattice of $\mathcal{L}$. The following holds:*

1. $|\mathcal{L}/\mathcal{L}'| < \infty$ *if and only if* $\mathrm{span}(\mathcal{L}) = \mathrm{span}(\mathcal{L}')$.
2. *Assume $|\mathcal{L}/\mathcal{L}'| < \infty$. Then $|\mathcal{L}/\mathcal{L}'| = |\mathcal{L} \cap \mathcal{P}(\mathbf{B}')| = \det(\mathcal{L}')/\det(\mathcal{L})$, for any basis $\mathbf{B}'$ of $\mathcal{L}'$.*

Proof:

**Proof of** 1**.** We prove the first assertion. First, assume that $|\mathcal{L}/\mathcal{L}'| < \infty$. Take $\mathbf{x} \in \mathcal{L}$. Since $\mathcal{L}/\mathcal{L}'$ is a finite group, we must that $k\mathbf{x} \equiv \mathbf{0} \pmod{\mathcal{L}'}$ for some $k \in \mathbb{N}$. Hence $k\mathbf{x} \in \mathcal{L}' \Rightarrow \mathbf{x} \in \mathrm{span}(\mathcal{L}')$. Assume that $\mathrm{span}(\mathcal{L}) = \mathrm{span}(\mathcal{L}')$. Let $\mathbf{B}'$ denote a basis of $\mathcal{L}'$. Note that for any $\mathbf{x} \in \mathcal{L}$, since $\mathbf{x} \in \mathrm{span}(\mathcal{L}')$, by Lemma 4 we have that the map $\mathbf{x} \to \mathbf{x} \pmod{\mathcal{P}(\mathbf{B}')}$ (see Definition 5) sends $\mathbf{x}$ to the unique representative of $\mathbf{x} + \mathcal{L}'$ in $\mathcal{P}(\mathbf{B}')$. From this reasoning, we see that $|\mathcal{L}/\mathcal{L}'| = |\mathcal{P}(\mathbf{B}') \cap \mathcal{L}|$. Since $\mathcal{P}(\mathbf{B}')$ is a bounded region and since $\mathcal{L}$ is a lattice, we have that $|\mathcal{P}(\mathbf{B}') \cap \mathcal{L}| < \infty$ as needed.

**Proof of** 2**.** Assume that $|\mathcal{L}/\mathcal{L}'| < \infty$. Let $\mathbf{B}$ and $\mathbf{B}'$ denote a basis for $\mathcal{L}$ and $\mathcal{L}'$ respectively. From here, we have that $\mathcal{P}(\mathbf{B})$ and $\mathcal{P}(\mathbf{B}')$ are fundamental domains of $\mathcal{L}$ and $\mathcal{L}'$ respectively. That $|\mathcal{P}(\mathbf{B}') \cap \mathcal{L}| = |\mathcal{L}/\mathcal{L}'|$ follows directly from the proof of 1, so it remains to show that $|\mathcal{L}/\mathcal{L}'| = \det(\mathcal{L}')/\det(\mathcal{L})$. Letting $W = \mathrm{span}(\mathcal{L})$, from the first part, we know that $W = \mathrm{span}(\mathcal{L}')$. Therefore by Theorem 8, and since $\mathcal{P}(\mathbf{B})$ is a fundamental domain of $\mathcal{L}$, we have that

$$\det(\mathcal{L}') = \mathrm{vol}_k(\mathcal{P}(\mathbf{B}')) = \int_W 1_{\mathcal{P}(\mathbf{B}')}(\mathbf{x})\mathrm{dvol}_k(\mathbf{x}) = \int_{\mathcal{P}(\mathbf{B})} \sum_{\mathbf{y} \in \mathcal{L}} 1_{\mathcal{P}(\mathbf{B}')}(\mathbf{y} + \mathbf{x})\mathrm{dvol}_k(\mathbf{x})$$

$$= \int_{\mathcal{P}(\mathbf{B})} |(\mathcal{L} + \mathbf{x}) \cap \mathcal{P}(\mathbf{B}')|\mathrm{dvol}_k(\mathbf{x}).$$

Let $A = \mathcal{P}(\mathbf{B}') \cap \mathcal{L}$. From the first part of the lemma, we know that $|A| = |\mathcal{L}/\mathcal{L}'|$, and in particular that $\mathcal{L}' + A = \mathcal{L}$. Since each coset $\mathcal{L}' + \mathbf{a}$, $\mathbf{a} \in A$, is disjoint and since $\mathcal{P}(\mathbf{B}')$ is a fundamental domain of $\mathcal{L}'$ we have that for any $\mathbf{x} \in \mathbb{R}^n$, $|(\mathcal{L} + \mathbf{x}) \cap \mathcal{P}(\mathbf{B}')| = |(\mathcal{L}' + A + \mathbf{x}) \cap \mathcal{P}(\mathbf{B}')| = |A| = |\mathcal{L}/\mathcal{L}'|$. Therefore

$$\det(\mathcal{L}') = \int_{\mathcal{P}(\mathbf{B})} |(\mathcal{L} + \mathbf{x}) \cap \mathcal{P}(\mathbf{B}')| \mathrm{dvol}_k(\mathbf{x}) = |\mathcal{L}/\mathcal{L}'| \int_{\mathcal{P}(\mathbf{B})} \mathrm{dvol}_k(\mathbf{x}) = |\mathcal{L}/\mathcal{L}'| \det(\mathcal{L}),$$

as needed. □

The following exercise gives a simple bound on how "far" a sublattice is from the full lattice.

**Exercise 1** Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice, and let $\mathcal{L}' \subseteq \mathcal{L}$ be a full-rank sublattice of $\mathcal{L}$. Letting $m = |\mathcal{L}/\mathcal{L}'|$, show that $m\mathcal{L} \subseteq \mathcal{L}'$.

# 4 Lattice Geometry

## 4.1 The Successive Minima and the Covering Radius

In terms of measurable lattice parameters, we have so far seen the shortest non-zero vector and the determinant. Here we give some other geometric lattice parameters that encode much useful information about a lattice. We begin with generalizations of the $\lambda_1$ parameter known as the successive minima. These parameters help us attain a finer understanding of the geometry of the lattice.

Definition 11 (Successive Minima) *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a rank $k \geq 1$ lattice. For $1 \leq i \leq k$, we define the $i^{th}$ minima of $\mathcal{L}$ with as*

$$\lambda_i(\mathcal{L}) = \inf\{s \geq 0 : \dim(\mathcal{L} \cap s\mathcal{B}_2^n) \geq i\}.$$

Remark 12 We first note that for $i = 1$, the above definition of $\lambda_1 = \inf\{s \geq 0 : \dim(s\mathcal{B}_2^n \cap \mathcal{L}) \geq 1\}$ seems somewhat different from the original definition $\lambda_1(\mathcal{L}) = \inf_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{y}\|$. To see that the definitions are equivalent, note that $\dim(s\mathcal{B}_2^n \cap \mathcal{L}) \geq 1 \Leftrightarrow \exists \mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}$ s.t. $\|\mathbf{y}\| \leq s$. From this, it is direct to see that both definitions yield exactly the same value.

By definition, it is clear that $\lambda_1(\mathcal{L}) \leq \lambda_2(\mathcal{L}) \leq \cdots \leq \lambda_k(\mathcal{L})$. We now show that successive minima are in fact well-defined, and that there are lattice vectors that attain them.

Lemma 13 *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a $k \geq 1$ dimensional lattice. Then there exists linearly independent vectors $\mathbf{y}_1, \dots, \mathbf{y}_k \in \mathcal{L}$ such that $\|\mathbf{y}_i\| = \lambda_i(\mathcal{L})$. In particular, $\lambda_i(\mathcal{L}) < \infty$ for all $i \in [k]$.*

Proof: Let $\mathbf{b}_1, \dots, \mathbf{b}_k$ denote a basis for $\mathcal{L}$. Let $R = \max_{1 \leq i \leq k} \|\mathbf{b}_i\|$. Clearly $\dim(R\mathcal{B}_2^n \cap \mathcal{L}) = \dim(\mathcal{L}) = k$. Therefore, $\lambda_i(\mathcal{L}) \leq R$ for all $i \in [k]$. Hence, if there exists $\mathbf{y} \in \mathcal{L}$ such that $\|\mathbf{y}\| = \lambda_i(\mathcal{L})$, for any $i \in [k]$, we must have that $\mathbf{y} \in R\mathcal{B}_2^n$.

We recursively choose $\mathbf{y}_1, \dots, \mathbf{y}_k \in \mathcal{L} \setminus \{\mathbf{0}\}$ as follows. Let $V_0 = \{\mathbf{0}\}$, and let $\mathbf{y}_1$ be a shortest vector in $(\mathcal{L} \cap R\mathcal{B}_2^n) \setminus V_0$. For $i$, $2 \leq i \leq k$, let $\mathbf{y}_i$ be the shortest vector in $\mathcal{L} \cap R\mathcal{B}_2^n \setminus V_{i-1}$ where $V_{i-1} = \mathrm{span}(\mathbf{y}_1, \dots, \mathbf{y}_{i-1})$. We note that $\mathbf{y}_1, \dots, \mathbf{y}_k$ exist since $\mathcal{L} \cap R\mathcal{B}_2^n$ is finite (by discreteness of $\mathcal{L}$) and since $\dim(\mathcal{L} \cap R\mathcal{B}_2^n) = k$.

I claim that $\mathbf{y}_1, \dots, \mathbf{y}_k$ are linearly independent and that $\|\mathbf{y}_i\| = \lambda_i(\mathcal{L})$, $i \in [k]$. Since each vector is chosen outside the span of the previous vectors, we have that $\mathbf{y}_1, \dots, \mathbf{y}_k$ are linearly independent. Therefore $\dim(V_i) = \mathrm{span}(\mathbf{y}_1, \ldots, \mathbf{y}_i) = i$ for $i \in \{0, \ldots, k\}$. Furthermore, by construction, it is clear that $\|\mathbf{y}_1\| \le \|\mathbf{y}_2\| \le \cdots \le \|\mathbf{y}_k\|$. For $i \in [k]$, let $r_i = \|\mathbf{y}_i\|$. From here see that $\dim(r_i\mathcal{B}_2^n \cap \mathcal{L}) \ge \dim(V_i) = i$. Hence $r_i = \|\mathbf{y}_i\| \ge \lambda_i(\mathcal{L})$ by definition. We now show that $r_i \le \lambda_i(\mathcal{L})$. For $i \in [k]$, and $0 < \varepsilon \le r_i$, take $\mathbf{y} \in \mathcal{L} \cap (r_i - \varepsilon)\mathcal{B}_2^n$. We claim that $\mathbf{y} \in V_{i-1}$. If not, then by our choice of $\mathbf{y}_i$, we must have that $\|\mathbf{y}_i\| = r_i \le \|\mathbf{y}\| \le r_i - \varepsilon < r_i$, a clear contradiction. Therefore $\dim(\mathcal{L} \cap (r_i - \varepsilon)\mathcal{B}_2^n) \le \dim(V_{i-1})) = i - 1$, and hence $r_i \le \lambda_i(\mathcal{L})$ as needed. □

The following parameter gives us another important way to measure the sparsity of a lattice.

Definition 14 (Covering Radius) *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a k-dimensional lattice. We define the covering radius of $\mathcal{L}$ to be*

$$\mu(\mathcal{L}) = \inf\{s \ge 0 : \mathrm{span}(\mathcal{L}) \subseteq s\mathcal{B}_2^n + \mathcal{L}\}$$

*For $\mathbf{x} \in \mathbb{R}^n$, define $d(\mathcal{L}, \mathbf{x}) = \inf_{\mathbf{y} \in \mathcal{L}} \|\mathbf{x} - \mathbf{y}\|$ to be the distance from $\mathbf{x}$ to $\mathcal{L}$. Expressed equivalently, $\mu(\mathcal{L}) = \sup\{d(\mathcal{L}, \mathbf{x}) : \mathbf{x} \in \mathrm{span}(\mathcal{L})\}$.*

Remark 15 To see the equivalence above, note that $d(\mathcal{L}, \mathbf{x}) \le s \Leftrightarrow \mathbf{x} \in \mathcal{L} + s\mathcal{B}_2^n$. Therefore $\mathrm{span}(\mathcal{L}) \subseteq \mathcal{L} + s\mathcal{B}_2^n \Leftrightarrow s \ge \sup\{d(\mathcal{L}, \mathbf{x}) : \mathbf{x} \in \mathrm{span}(\mathcal{L})\}$. Since $\mu(\mathcal{L})$ corresponds to the smallest such $s$, we get that $\mu(\mathcal{L}) = \sup\{d(\mathcal{L}, \mathbf{x}) : \mathbf{x} \in \mathrm{span}(\mathcal{L})\}$, as needed.

Lemma 16 *For a full rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $\mu(\mathcal{L}) \le \sum_{i=1}^n \frac{1}{2}\lambda_i(\mathcal{L})$.*

Proof: To upper bound $\mu(\mathcal{L})$, it suffices to show that for any $\mathbf{x} \in \mathbb{R}^n$ there exists $\mathbf{y} \in \mathcal{L}$ such that $\|\mathbf{x} - \mathbf{y}\| \le \sum_{i=1}^n \frac{1}{2}\lambda_i(\mathcal{L})$. Take $\mathbf{x} \in \mathbb{R}^n$, and let $\mathbf{y}_1, \ldots, \mathbf{y}_n \in \mathcal{L}$ denote vectors attaining the successive minima of $\mathcal{L}$. Since $\mathbf{y}_1, \ldots, \mathbf{y}_n$ are linearly indepedent, we may express $\mathbf{x} = \sum_{i=1}^n a_i\mathbf{y}_i$ for $a_1, \ldots, a_n \in \mathbb{R}$. Let $\mathbf{y} = \sum_{i=1}^n \lfloor a_i \rceil \mathbf{y}_i \in \mathcal{L}$. Then note that

$$\|\mathbf{x} - \mathbf{y}\| = \|\sum_{i=1}^n (a_i - \lfloor a_i \rceil)\mathbf{y}_i\| \le \sum_{i=1}^n \frac{1}{2}\|\mathbf{y}_i\| = \sum_{i=1}^n \frac{1}{2}\lambda_i(\mathcal{L})$$

as needed.

□

## 4.2 Minkowski's First and Second Theorem

Theorem 17 (Blichfeldt's Theorem) *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a full dimensional lattice. Then for any measurable set $A \subseteq \mathbb{R}^n$ such that $\mathrm{vol}_n(A) > \det(\mathcal{L})$ there exists distinct $\mathbf{w}, \mathbf{z} \in A$ such that $\mathbf{w} - \mathbf{z} \in \mathcal{L}$.*

Proof: Let $B$ be a basis for $\mathcal{L}$. Since $\mathcal{P}(\mathbf{B})$ is a fundamental domain of $\mathcal{L}$ by Theorem 8 we have that

$$\mathrm{vol}_n(A) = \int_{\mathbb{R}^n} 1_A(\mathbf{x})\mathrm{d}\mathbf{x} = \int_{\mathcal{P}(\mathbf{B})} \sum_{\mathbf{y} \in \mathcal{L}} 1_A(\mathbf{y} + \mathbf{x})\mathrm{d}\mathbf{x} = \int_{\mathcal{P}(\mathbf{B})} |(\mathcal{L} + \mathbf{x}) \cap A|\mathrm{d}\mathbf{x}$$

Assume that for all $\mathbf{x} \in F$, $|(\mathcal{L} + \mathbf{x}) \cap A| \le 1$. Then note that

$$\mathrm{vol}_n(A) = \int_{\mathcal{P}(\mathbf{B})} |(\mathcal{L} + \mathbf{x}) \cap A|\mathrm{d}\mathbf{x} \le \int_{\mathcal{P}(\mathbf{B})} \mathrm{d}\mathbf{x} = \mathrm{vol}_n(\mathcal{P}(\mathbf{B})) = \det(\mathcal{L}),$$

a clear contradiction to the assumption that $\mathrm{vol}_n(A) > \det(\mathcal{L})$. Therefore we may pick $\mathbf{x} \in F$ such that $|(\mathcal{L} + \mathbf{x}) \cap A| \ge 2$ (since this number is an integer). Hence we may pick distinct elements $\mathbf{w}, \mathbf{z} \in (\mathcal{L} + \mathbf{x}) \cap A$, where we note that $\mathbf{x} - \mathbf{z} \in \mathcal{L}$ as needed. □

We will need the following simple lemma about convex sets.

Lemma 18 *Let $K \subseteq \mathbb{R}^n$ be a non-empty convex set. Then for any $s, t \geq 0$, $sK + tK = (s+t)K$. Furthermore, if K is symmetric, then for any $s, t \in \mathbb{R}$, $sK + tK = (|s| + |t|)K$.*

Proof: If $s = t = 0$, then since $K$ is non-empty, we clearly have that $(s+t)K = 0(K) = \{\mathbf{0}\}$ and $sK + tK = \{\mathbf{0}\} + \{\mathbf{0}\} = \{\mathbf{0}\}$, as needed. Therefore, we may assume that $s + t > 0$.

Any element in $(s+t)K$ can be written as $(s+t)\mathbf{x}$ for $\mathbf{x} \in K$. Given that $(s+t)\mathbf{x} = s\mathbf{x} + t\mathbf{x} \in sK + tK$, we get that $(s+t)K \subseteq sK + tK$ as needed.

Take $\mathbf{z} \in sK + tK$. Here $\mathbf{z} = s\mathbf{x} + t\mathbf{y}$ for some $\mathbf{x}, \mathbf{y} \in K$. By convexity and the fact that $s + t > 0$, we have that $\frac{s}{s+t}\mathbf{x} + \frac{t}{s+t}\mathbf{y} \in K$. Therefore $\mathbf{z} = (s+t)\left(\frac{s}{s+t}\mathbf{x} + \frac{t}{s+t}\mathbf{y}\right) \in (s+t)K$ as needed.

The furthermore follows directly from the first part after noting that $sK = |s|K$ if $K$ is symmetric. □

Theorem 19 (Minkowski's Convex Body Theorem) *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a full dimensional lattice. Let $K \subseteq \mathbb{R}^n$ be a symmetric convex set with $\mathrm{vol}_n(K) > 2^n \det(\mathcal{L})$. Then K contains a non-zero lattice vectors.*

Proof: We give two different proofs. One using Blichfeldt's Theorem and the second using lattice packing.

**Proof 1.** By Lemma 9, we know that $\det(2\mathcal{L}) = 2^n \det(\mathcal{L})$. Since $\mathrm{vol}_n(K) > \det(2\mathcal{L})$, by Blichfeldt's Theorem there exists distinct $\mathbf{w}, \mathbf{z} \in K$ such that $\mathbf{w} - \mathbf{z} \in \mathcal{L}$. Let $\mathbf{y} = \frac{1}{2}(\mathbf{w} - \mathbf{z})$. Note that since $\mathbf{w} - \mathbf{z} \in 2\mathcal{L} \setminus \{\mathbf{0}\}$, we have that $\mathbf{y} = \frac{1}{2}(\mathbf{w} - \mathbf{z}) \in \mathcal{L} \setminus \{\mathbf{0}\}$. Furthermore, since $K$ is symmetric, note that $\mathbf{z} \in K \Rightarrow -\mathbf{z} \in K$. Next, by convexity of $K$ we have that $\mathbf{y} = \frac{1}{2}(\mathbf{w} - \mathbf{z}) \in K$. Hence $K$ contains a non-zero lattice point as claimed.

**Proof 2.** We prove the converse, that is the $K \cap \mathcal{L} = \{\mathbf{0}\} \Rightarrow \mathrm{vol}_n(K) \leq 2^n \det(\mathcal{L})$. Assume that $K \cap \mathcal{L} = \{\mathbf{0}\}$. By Lemma 7, we know that $\frac{1}{2}K$ is $\mathcal{L}$-packing if and only if $(\frac{1}{2}K - \frac{1}{2}K) \cap \mathcal{L} = \{\mathbf{0}\}$. By Lemma 18, since $K$ is symmetric $\frac{1}{2}K - \frac{1}{2}K = K$. Since by assumption $K \cap \mathcal{L} = \{\mathbf{0}\}$, we therefore have that $\frac{1}{2}K$ is $\mathcal{L}$-packing. By Theorem 8, since $\frac{1}{2}K$ is $\mathcal{L}$-packing, $\mathrm{vol}_n(\frac{1}{2}K) \leq \det(\mathcal{L}) \Leftrightarrow \mathrm{vol}_n(K) \leq 2^n \det(\mathcal{L})$ as needed. □

Theorem 20 (Minkowski's First Theorem) *For any full-rank lattice $\mathcal{L}$ of rank n,*

$$\lambda_1(\mathcal{L}) \leq 2 \frac{\det(\mathcal{L})^{\frac{1}{n}}}{\mathrm{vol}_n(\mathcal{B}_2^n)^{\frac{1}{n}}} \leq \sqrt{n} \det(\mathcal{L})^{\frac{1}{n}}.$$

Proof: Let $s = 2\frac{\det(\mathcal{L})^{\frac{1}{n}}}{\mathrm{vol}_n(\mathcal{B}_2^n)^{\frac{1}{n}}}$. Notice that for any $\varepsilon > 0$, that $\mathrm{vol}_n(s(1+\varepsilon)\mathcal{B}_2^n) = (1+\varepsilon)^n s^n \mathrm{vol}_n(\mathcal{B}_2^n) = (1+\varepsilon)^n 2^n \det(\mathcal{L}) > 2^n \det(\mathcal{L})$. Since $s(1+\varepsilon)\mathcal{B}_2^n$ is a symmetric convex body, by Theorem 19, there exists $\mathbf{y} \in s(1+\varepsilon)\mathcal{B}_2^n \cap \mathcal{L}$, $\mathbf{y} \neq \mathbf{0}$. Since $\|\mathbf{y}\| \leq s(1+\varepsilon)$, we clearly have that $\lambda_1(\mathcal{L}) \leq \|\mathbf{y}\| \leq s(1+\varepsilon)$. Since this holds for all $\varepsilon > 0$, we have that $\lambda_1(\mathcal{L}) \leq s$, as needed. Since $[-\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}]^n \subseteq \mathcal{B}_2^n$, we have that

$$\mathrm{vol}_n(\mathcal{B}_2^n)^{\frac{1}{n}} \geq \mathrm{vol}_n([-\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}]^n)^{\frac{1}{n}} = \frac{2}{\sqrt{n}}.$$

The claim follows by plugging in the lower bound on $\mathrm{vol}_n(\mathcal{B}_2^n)$. □

The term $\det(\mathcal{L})^{1/n}$ might seem strange at first, but is in fact very natural: it makes sure that the expression scales properly. Indeed, consider the lattice $c\mathcal{L}$ obtained by scaling $\mathcal{L}$ by a factor of $c$. Then clearly $\lambda_1(c\mathcal{L}) = c\lambda_1(\mathcal{L})$. On the other hand, we have $\det(c\mathcal{L}) = c^n \det(\mathcal{L})$, so the right hand side also scales by a factor of $c$, as we expect. So we could equivalently state Minkowski's first theorem as saying that any rank-$n$ lattice with determinant 1 contains a nonzero vector of length at most $\sqrt{n}$.

How tight is this bound? It is easy to see that there are cases in which it is very far from being tight. Consider for example the lattice generated by $(\varepsilon, 0)^T$ and $(0, 1/\varepsilon)^T$ for some small $\varepsilon > 0$. Its determinant is 1 yet its shortest nonzero vector is of length $\varepsilon$. On the other hand, consider the lattice $\mathbb{Z}^n$. Its determinant is 1 whereas $\lambda_1(\mathbb{Z}^n) = 1$, so the bound is closer to being tight, but still not tight. In fact, it is known that for any $n$ there exists a rank $n$ lattice of determinant 1 whose shortest nonzero vector is of length at least $c\sqrt{n}$ for some constant $c$. So up to a constant, Minkowski's bound is tight. In fact, by a slightly more careful analysis, one can improve the $\sqrt{n}$ bound to $c\sqrt{n}$ for some constant $c < 1$.

Finally, we mention that in the discussion above we considered the $\ell_2$ norm. It is easy to extend Minkowski's theorem to other norms. All that is required is to compute the volume of a ball under the given norm.

Minkowski's first theorem considers the shortest nonzero vector, i.e., the first successive minimum $\lambda_1$. A strengthening of the bound is given by what is known as Minkowski's second theorem. Instead of considering just $\lambda_1$, this bound considers the geometric mean of all $\lambda_i$ (which is clearly at least $\lambda_1$).

Theorem 21 (Minkowski's second theorem) *For any full-rank lattice $\mathcal{L}$ of rank $n$,*

$$\Big(\prod_{i=1}^{n} \lambda_i(\mathcal{L})\Big)^{1/n} \le 2\frac{\det(\mathcal{L})^{\frac{1}{n}}}{\mathrm{vol}_n(\mathcal{B}_2^n)^{\frac{1}{n}}} \le \sqrt{n}\det(\mathcal{L})^{1/n}.$$

Proof: For $i \in [n]$, let $\lambda_i = \lambda_i(\mathcal{L})$. Let $\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathcal{L}$ be linearly independent vectors achieving the successive minima, i.e. $\|\mathbf{x}_i\| = \lambda_i$ for $i \in [n]$. Let $\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_n$ be their Gram-Schmidt orthogonalization. Consider the open ellipsoid with axes $\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_n$ and lengths $\lambda_1, \ldots, \lambda_n$,

$$E = \Big\{ \mathbf{y} \in \mathbb{R}^n \;\Big|\; \sum_{i=1}^{n} \Big( \frac{\langle \mathbf{y}, \tilde{\mathbf{x}}_i \rangle}{\|\tilde{\mathbf{x}}_i\| \cdot \lambda_i} \Big)^2 < 1 \Big\}.$$

See Figure 3. We compute the volume of $E$. Let $\mathbf{Q} = (\frac{\tilde{\mathbf{x}}_1}{\|\tilde{\mathbf{x}}_1\|}, \ldots, \frac{\tilde{\mathbf{x}}_n}{\|\tilde{\mathbf{x}}_n\|})^{\mathsf{T}} \in \mathbb{R}^{n\times n}$, the matrix with rows corresponding to the normalized Gram-Schmidt vectors of $\mathbf{x}_1, \ldots, \mathbf{x}_n$, and $\mathbf{D} = (\frac{1}{\lambda_1}\mathbf{e}_1, \ldots, \frac{1}{\lambda_n}\mathbf{e}_n) \in \mathbb{R}^{n\times n}$, the diagonal matrix with diagonal $\frac{1}{\lambda_1}, \ldots, \frac{1}{\lambda_n}$. From here, we see that

$$E = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{DQx}\|^2 < 1\} = (\mathbf{DQ})^{-1}\{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\|^2 < 1\} = \mathbf{Q}^{\mathsf{T}}(\lambda_1\mathbf{e}_1, \ldots \lambda_n\mathbf{e}_n)\mathrm{int}(\mathcal{B}_2^n),$$

since $\mathbf{Q}$ is an orthogonal matrix and $\mathbf{D}$ is diagonal. Therefore

$$\mathrm{vol}_n(E) = |\det(\mathbf{Q}^{\mathsf{T}}(\lambda_1\mathbf{e}_1, \ldots \lambda_n\mathbf{e}_n))|\mathrm{vol}_n(\mathrm{int}(\mathcal{B}_2^n)) = (\prod_{i=1}^{n}\lambda_i)\mathrm{vol}_n(\mathcal{B}_2^n)$$

We claim that $E$ does not contain any non-zero lattice points. Indeed, take any nonzero $\mathbf{y} \in \mathcal{L}$ and let $1 \le k \le n$ be the largest index such that $\|\mathbf{y}\| \ge \lambda_k(\Lambda)$. It must be that $\mathbf{y} \in \mathrm{span}(\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_k) = \mathrm{span}(\mathbf{x}_1, \ldots, \mathbf{x}_k)$, since otherwise $\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}$ are $k+1$ linearly independent lattice vectors of length less than $\lambda_{k+1}(\mathcal{L})$. Now,

$$\sum_{i=1}^{n} \Big( \frac{\langle \mathbf{y}, \tilde{\mathbf{x}}_i \rangle}{\|\tilde{\mathbf{x}}_i\| \cdot \lambda_i} \Big)^2 = \sum_{i=1}^{k} \Big( \frac{\langle \mathbf{y}, \tilde{\mathbf{x}}_i \rangle}{\|\tilde{\mathbf{x}}_i\| \cdot \lambda_i} \Big)^2 \ge \frac{1}{\lambda_k^2} \sum_{i=1}^{k} \Big( \frac{\langle \mathbf{y}, \tilde{\mathbf{x}}_i \rangle}{\|\tilde{\mathbf{x}}_i\|} \Big)^2 = \frac{\|\mathbf{y}\|^2}{\lambda_k^2} \ge 1$$

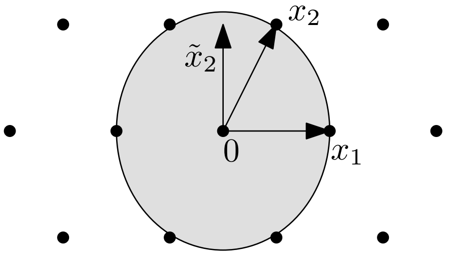


Figure 3: The ellipsoid $E$. The vector $\mathbf{x}_1$ is on the boundary of $E$, and $\mathbf{x}_2$ is strictly outside.

and therefore, $\mathbf{y} \notin E$.

By Minkowski's convex body theorem, $\mathrm{vol}(E) \leq 2^n \det(\mathcal{L})$. But on the other hand,

$$\mathrm{vol}_n(E) = \Big(\prod_{i=1}^{n} \lambda_i\Big) \mathrm{vol}_n(\mathcal{B}_2^n) \geq \Big(\prod_{i=1}^{n} \lambda_i\Big) \Big(\frac{2}{\sqrt{n}}\Big)^n .$$

Combining the two bounds, we obtain that

$$\Big(\prod_{i=1}^{n} \lambda_i\Big)^{1/n} \leq 2 \frac{\det(\mathcal{L})^{\frac{1}{n}}}{\mathrm{vol}_n(\mathcal{B}_2^n)^{\frac{1}{n}}} \leq \sqrt{n} \det(\mathcal{L})^{1/n} .$$

□