1 Introduction

In this course, the first mathematical objects we will consider are known as *lattices*. What is a lattice? It is a set of points in n-dimensional space with a periodic structure, such as the one illustrated in Figure 1. Three-dimensional lattices occur naturally in crystals, as well as in stacks of oranges. Historically, lattices were investigated since the late 18th century by mathematicians such as Lagrange, Gauss, and later Minkowski.

One of the most elusive problem with lattices (of large dimension) is that of sphere packing: how to stack balls as densely as possible. This question can be found in a booklet of Johannes Kepler *Strena seu de Nive Sexangula* (1611), as a tentative explanation for the shape of snowflakes: the hexagonal structure would stem from optimal packing of spherical atoms. This first lecture will culminate with an upper bound on the density of lattice packing in arbitrary dimension (Minkowski's bound).

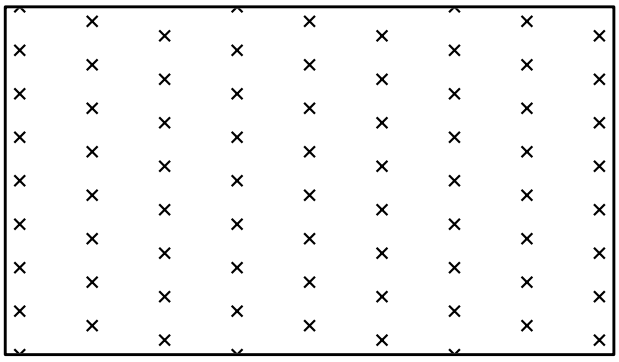

Figure 1: A lattice in $\mathbb{R}^2$

Lattices are a recurring tool in algebra and number theory, for example to prove finiteness of the class group of a number field, or to the efficiently factor rational polynomials.

More recently, lattices have become a topic of active research in computer science. Algorithmic problems based on lattices (e.g. Shortest and Closest Vector Problems, ...) have found a wide variety of applications; they are used within optimization algorithms, in the design of wireless communication protocols, and perhaps the most active research area, in the development of secure cryptographic primitives (cryptography) and in establishing the insecurity of certain cryptographic schemes (cryptanalysis). But lattices and their algorithm find applications in various branch of sciences, such as reconstructing molecule composition from mass spectrometry (chemistry), or detecting pulsars (astronomy).

2 Notation and Basic Concepts

We use $\mathbb{R}$ for the real numbers, $\mathbb{Z}$ for the integers and $\mathbb{N}$ for the natural numbers (positive integers). Correspondingly, we use $\mathbb{R}^n$ and $\mathbb{Z}^n$ to denote the n-dimensional versions for some

$n \in \mathbb{N}$. We write generally matrices as $\mathbf{B}$ in uppercase bold, vectors $\mathbf{x} \in \mathbb{R}^n$ in lowercase bold and scalars as $x \in \mathbb{R}$.

For a set $A \subseteq \mathbb{R}^n$, we use $\mathrm{span}(A)$ to denote its linear span of A, i.e. the smallest linear subspace containing A. We define the dimension $\dim(A)$ of A to be the dimension of the linear span, that is, $\dim(A) := \dim(\mathrm{span}(A))$. For two sets $A, B \subseteq \mathbb{R}^n$, $s, t \in \mathbb{R}$, we define their Minkowski sum $sA + tB := \{s\mathbf{a} + t\mathbf{b} : \mathbf{a} \in A, \mathbf{b} \in B\}$.

3 Definitions and Basic Concepts

The main goal of this lecture is to introduce the basic concept of a lattice, define one of its basic geometric parameters (the shortest non-zero vector), and present various equivalent definitions of a lattice. Our abstract definition of a lattice is given below:

Definition 1 (Lattice) *$\mathcal{L} \subseteq \mathbb{R}^n$ is a lattice if $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{R}^n$. $\mathcal{L}$ is a rank k lattice, or is k-dimensional, if $\dim_{\mathbb{R}}(\mathcal{L}) = k$. $\mathcal{L}$ is said to be full-rank if $\dim_{\mathbb{R}}(\mathcal{L}) = n$ (the dimension of the ambient space).*

Endowment of $\mathbb{R}^n$. For what is to come, $\mathbb{R}^n$ will be endowed with *some* norm denoted $\| \cdot \|$. A norm induces a metric on $\mathbb{R}^n$ which is non-trivial, and any non-trivial metric on $\mathbb{R}^n$ induces the same topology on $\mathbb{R}^n$. Note that a discrete group must be "uniformly discrete", a set S is uniformly discrete in a metric space X if there exists a $\delta > 0$ such that for all $s \in S$, the open ball of radius δ around s contains no other elements of S than s itself.

Another endowment that we will use is its unique Lesbegue measure, denoted $\mathrm{vol}(\cdot)$; for a *measurable* set $S \subset \mathbb{R}^n$, the volume $\mathrm{vol}(S)$ is a non-negative real number or ∞. We recall that a measure is sub-additive under union and additive under disjoint union:

1. $\mathrm{vol}\left(\bigcup_i S_i\right) \leq \sum_i \mathrm{vol}\left(S_i\right)$
2. $\mathrm{vol}\left(\bigsqcup_i S_i\right) = \sum_i \mathrm{vol}\left(S_i\right)$

Being a Lesbegue measure on $\mathbb{R}^n$, it is also invariant by translation, is homogeneous, and is normalized on the canonical hypercube:

1. $\forall \mathbf{x} \in \mathbb{R}^n, \mathrm{vol}(S + \mathbf{x}) = \mathrm{vol}(S)$
2. $\forall \mathbf{T} \in \mathbb{R}^{n \times n}, \mathrm{vol}(\mathbf{T} \cdot S) = |\det(\mathbf{T})| \cdot \mathrm{vol}(S)$
3. $\mathrm{vol}([0,1]^n) = 1$

The second property implies invariance under rotations $\mathbf{T} \in \mathcal{O}_n(\mathbb{R})$. One can easily deduce that a bounded measurable set has finite measure, and that a set with non-empty interior has strictly positive measure.

Issues of measurability shall not arise in this course and will be ignored; most bodies $S \subset R^n$ we will encounter are convex or are a finite combination of convex bodies.

Remark 2 The term lattice is quite overloaded in the literature, and can also refer to an order, or to subgroup of other groups than $\mathbb{R}^n$. The lattices as defined above are sometimes referred to as "point lattices". The term "Euclidean lattices" is also used when the considered metric is Euclidean.

PROPOSITION 3 *A non-trivial subgroup $L \subset \mathbb{R}^n$ is discrete if and only if it admits a strictly positive minimal distance, that is if $\min_{\mathbf{x}\neq\mathbf{y}\in L} \|\mathbf{x}-\mathbf{y}\|$ is well defined and strictly positive.*

Because a lattice L is a group, its minimum distance can be rewritten as $\min_{\mathbf{x}\in L\setminus\{\mathbf{0}\}} \|\mathbf{x}\|$. It will be denoted $\lambda_1(L)$.

PROOF: Having a minimal distance immediately implies discreteness: around each element of the subgroup L, we can take the open ball of radius $\lambda_1/2$, which does not include any other point in L.

For the other direction, we will show that the minimal distance is attained and is strictly positive. By discreteness and non-triviality of L, the greatest lower bound

$$\lambda_1 \;=\; \inf\,\{\|\mathbf{x}\| : \mathbf{x} \in L \setminus \{\mathbf{0}\}\}$$

exists and is strictly positive. Consider the open ball B of radius 2λ about the point 0. By definition of λ, the ball B will include at least one non-zero element $\mathbf{x} \in L$. This ball is bounded and thus has finite volume $V := \mathrm{vol}(B)$. Moreover, an open ball C of radius $\lambda/2$ has a strictly positive volume. For any two $\mathbf{x}, \mathbf{y} \in L \cap B$, the intersection $\mathbf{x} + C \cap \mathbf{y} + C$ is empty, by definition of λ. Thus the union

$$U = \bigsqcup_{\mathbf{x}\in B\cap L} \mathbf{x} + C$$

is disjoint, and therefore has volume

$$\mathrm{vol}(U) = \sum_{\mathbf{x}\in B\cap L} \mathrm{vol}(\mathbf{x}+C) = \sum_{\mathbf{x}\in B\cap L} \mathrm{vol}(C) = |B \cap L|\mathrm{vol}(C).$$

Note that U is also bounded (it is a subset of the open ball D of radius $5\lambda/2$) and therefore has finite volume. Therefore, $|B \cap L|$ is finite. This finite set has an element with minimal norm, which by construction is λ. Thus the infimum is attained and is thus a minimum. □

Exercise 1 Provide two counterexamples when the either assumption of the above proposition is not met:

- A finitely generated subgroup of $\mathbb{R}$ that is not discrete, and doesn't admit a minimal distance
- A discrete subset (but not uniformly) of $\mathbb{R}$ that is not a group, and doesn't admit a minimal distance

3.1 Bases

DEFINITION 4 (BASIS OF A LATTICE) *A matrix $\mathbf{B} = [\mathbf{b}_1 \dots \mathbf{b}_k] \in \mathbb{R}^{n\times k}$ is a basis of a lattice $L \subset \mathbb{R}^n$ if its column vectors are linearly independent over $\mathbb{R}$ and the $\mathbb{Z}$-span of its columns is exactly L, i.e.*

$$\mathcal{L}(\mathbf{B}) := \mathbf{B} \cdot \mathbb{Z}^k = L.$$

The goal of this section is to prove that all lattices admit a basis. By definition, one can find a set of linearly independent vectors in L. We will show that such a set generates a sublattice of L of finite index. From there, we will reconstruct a basis. For the first step, we resort to the *fundamental parallelepiped*: if $\mathbf{B} \in \mathbb{R}^{m\times k}$ has linearly independent columns we denote $\mathcal{P}(\mathbf{B}) := \mathbf{B} \cdot [-1/2, 1/2)^n$ the parallelepiped spanned by $\mathbf{B}$.

PROPOSITION 5 *For any basis* $\mathbf{B}$ *of* L, $\mathcal{P}(\mathbf{B})$ *is a fundamental domain of* L, *that is any* $\mathbf{t} \in \mathrm{Span}_{\mathbb{R}}(L)$ *can be uniquely written as* $\mathbf{t} = \mathbf{x} + \mathbf{e}$ *where* $\mathbf{x} \in L$ *and* $\mathbf{e} \in \mathcal{P}(\mathbf{B})$.

PROOF: If $L = \{0\}$, then $\mathbf{t} = 0$, so we take $\mathbf{x} = 0$ and $\mathbf{e} = 0$ and we are done. Otherwise, let $\mathbf{t} \in \mathrm{Span}_{\mathbb{R}}(L)$. As an element of the $\mathbb{R}$-span, $\mathbf{t}$ can be written as a linear combination

$$\mathbf{t} = c_1\mathbf{b}_1 + \ldots + c_k\mathbf{b}_k,$$

where $k > 0$ is the dimension of the lattice and each $c_i \in \mathbb{R}$. Now define the rounding function $\lfloor \cdot \rceil : \mathbb{R} \to \mathbb{Z}$ that rounds a real number x to the largest integer not greater than $x + 0.5$ (that is, the familiar rounding function where half-integers are rounded up to the next integer). Consider now $\mathbf{x} := \lfloor c_1 \rceil \mathbf{b}_1 + \ldots + \lfloor c_k \rceil \mathbf{b}_k$. This is a $\mathbb{Z}$-linear combination of the basis vectors in $\mathbf{B}$, so $\mathbf{x} \in L$. Define

$$\mathbf{e} := \mathbf{t} - \mathbf{x} = (c_1 - \lfloor c_1 \rceil)\mathbf{b}_1 + \ldots + (c_k - \lfloor c_k \rceil)\mathbf{b}_k.$$

Each $c_i - \lfloor c_i \rceil \in [-1/2, 1/2)$, so $\mathbf{e} \in \mathcal{P}(\mathbf{B})$.

It remains to show uniqueness. Suppose we have two different such representations $\mathbf{t} = \mathbf{x} + \mathbf{e} = \mathbf{x}' + \mathbf{e}'$, where $\mathbf{x} \neq \mathbf{x}'$ and $\mathbf{e} \neq \mathbf{e}'$. Then $0 = \mathbf{x} - \mathbf{x}' + \mathbf{e} - \mathbf{e}'$. Since $\mathbf{x} - \mathbf{x}' \in L$, we also require that $\mathbf{e} - \mathbf{e}' \in L$. But $\mathbf{e}, \mathbf{e}' \in \mathcal{P}(\mathbf{B})$, so $\mathbf{e} - \mathbf{e}' \in \mathbf{B} \cdot (-1, 1)^k \cap L = \{0\}$. Thus $\mathbf{e} = \mathbf{e}'$ and $\mathbf{x} = \mathbf{x}'$ follows. □

PROPOSITION 6 *Let* L' *be a lattice admitting a basis* $\mathbf{B}$, *and* L *a superlattice of* L' *of the same dimension. The index of the quotient group* $|L/L'| < \infty$ *is finite.*

PROOF: Given $L' \subseteq L$ have the same rank, we know their $\mathbb{R}$-spans are the same. Thus for every coset in L/L', we can lift to an element in $\mathbf{s} \in L \subseteq \mathrm{Span}_{\mathbb{R}}(L)$. Let S be a set consisting of a lifted element for every coset in L/L'. Then $|S| = |L/L'|$. Now, by Proposition 5 $\mathbf{s} = \mathbf{t}_s + \mathbf{e}_s$ for some $\mathbf{t}_s \in L'$ and $\mathbf{e}_s \in \mathcal{P}(\mathbf{B})$. Let E be the set of all $\mathbf{e}$ resulting from this decomposition. Since no two lifts $\mathbf{s}$ differ by an element of L', we know that each $\mathbf{e}$ is unique to each $\mathbf{s} \in S$, and so $|S| = |E|$. Furthermore, E is discrete since L is discrete. Following the same argument as in the proof of Proposition 3, we know that only finitely many elements of the uniformly discrete set E can be contained in the bounded set $\mathcal{P}(\mathbf{B})$. But since $E \subseteq \mathcal{P}(\mathbf{B})$, E is finite, and therefore so is $|L/L'|$. □

THEOREM 7 *Any lattice admits a basis.*

PROOF: Let $L \subset \mathbb{R}^n$ be a lattice of rank k. Let $\mathbf{B} \subset \mathbb{R}^{n \times k}$ be matrix whose column vectors are linearly independent vectors of L. By Proposition 6, the quotient $G = L/\mathcal{L}(\mathbf{B})$ is finite.

If the quotient is trivial then $L = \mathcal{L}(\mathbf{B})$, and $\mathbf{B}$ is a basis of L, we are done. Otherwise, choose some $\mathbf{x} \in L \setminus \mathcal{L}(\mathbf{B})$ of prime order p in G. Because $p\mathbf{x} \in \mathcal{L}(\mathbf{B})$, it can be written as $\mathbf{x} = \mathbf{B}\mathbf{y}$ where $\mathbf{y} \in \frac{1}{p}\mathbb{Z}^k$. Without loss of generality (by permutation of the basis vectors of $\mathbf{B}$), we can assume that its first coordinate is not integral: $\mathbf{y} = (\frac{a}{p}, \mathbf{y}')$ where $a \neq 0 \bmod p$. We can further assume that $a = 1$, by replacing $\mathbf{x}$ by $c\mathbf{x} - \frac{ac-1}{p}\mathbf{b}_1$ where $ac = 1 \bmod p$.

The claim is that $\mathbf{B}' := (\mathbf{x}, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ generates a sublattice of L that is a strict superlattice of $\mathcal{L}(\mathbf{B})$, namely $\mathcal{L}(\mathbf{B}) + \mathbf{x}\mathbb{Z}$. That it is a sublattice of L is trivial: by construction $\mathbf{x} \in L$ and for all i, $\mathbf{b}_i \in L$. To show that it is a superlattice of $\mathcal{L}(\mathbf{B})$, it suffices to prove that $\mathbf{b}_1 \in \mathcal{L}(\mathbf{B}')$. Recall that

$\mathbf{x} = \mathbf{B} \cdot (\frac{1}{p}, \mathbf{y}')$ for some $\mathbf{y}'$ in $\frac{1}{p} \cdot \mathbb{Z}^{k-1}$. Simply note that $\mathbf{b}_1 = p\mathbf{x} - \mathbf{B}' \cdot (0, p\mathbf{y}')$. Finally, because $\mathbf{x} \notin \mathcal{L}(\mathbf{B})$, the inclusion $\mathcal{L}(\mathbf{B}) \subset \mathcal{L}(\mathbf{B}')$ is indeed strict.

We conclude by repeating the above process, replacing $\mathbf{B}$ by the newly constructed $\mathbf{B}'$, until $\mathbf{B}$ is indeed a basis of L. Note that since $\mathcal{L}(\mathbf{B}) \subsetneq \mathcal{L}(\mathbf{B}')$, the size of the quotient group $|L/\mathcal{L}(\mathbf{B})|$ is finite and stricly decreases at each step. Therefore it must terminate after some finite number of steps, at which point $|L/\mathcal{L}(\mathbf{B})| = 1$, and $\mathcal{L}(\mathbf{B}) = L$. □

PROPOSITION 8 *For any two bases $\mathbf{B}, \mathbf{B}' \in \mathbb{R}^{n \times k}$ of the same lattice L of rank k, there exists $\mathbf{U} \in \mathrm{GL}_k(\mathbb{Z})$ such that $\mathbf{B}' = \mathbf{BU}$. Conversely, if $\mathbf{B}$ is a basis of L, so is $\mathbf{BU}$ for any unimodular matrix $\mathbf{U} \in \mathrm{GL}_k(\mathbb{Z})$.*

PROOF: The lattices $\mathcal{L}(\mathbf{B}), \mathcal{L}(\mathbf{B}')$ are equal and therefore sublattices of one another. Since $\mathcal{L}(\mathbf{B}) \subseteq \mathcal{L}(\mathbf{B}')$, each basis vector in $\mathbf{B}'$ is an integer linear combination of basis vectors in $\mathbf{B}$. This can be written as $\mathbf{B}' = \mathbf{BM}$ for some $\mathbf{M} \in \mathbb{Z}^{k \times k}$. The matrix M has non-zero determinant, since both $\mathbf{B}$ and $\mathbf{B}'$ have rank k. The same is true for the other direction of the inclusion, i.e. $\mathbf{B} = \mathbf{B}'\mathbf{M}'$ for some $\mathbf{M}' \in \mathbb{Z}^{k \times k}$ with rank k. Combining these two facts tells us

$$\mathbf{B} = \mathbf{BMM}'.$$

The matrix $\mathbf{B}$ is non-singular, so the above holds if and only if $\mathbf{MM}' = \mathbf{I}_k$. Since both of $\mathbf{M}$ and $\mathbf{M}'$ are integer valued, their determinants are also integers, and thus $\mathbf{M}, \mathbf{M}' \in \mathrm{GL}_n(\mathbb{Z})$.

For the converse, we argue as above that for any basis $\mathbf{B}$, the lattice generated by $\mathbf{BU}$ for any $\mathbf{U} \in \mathbb{Z}^{k \times k}$ is a sublattice of $\mathcal{L}(\mathbf{B})$, and so $\mathcal{L}(\mathbf{BU}) \subseteq \mathcal{L}(\mathbf{B})$. Now if $\mathbf{U}$ is unimodular, then $\mathbf{U}^{-1} \in \mathbb{Z}^{k \times k}$ and so by the same argument, $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{BUU}^{-1}) \subseteq \mathcal{L}(\mathbf{BU})$. Therefore $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{BU})$. □

3.2 Covering, Packing, Tiling

Subsets of $\mathbb{R}^n$ are called coverings, packings or tilings based on how well they "fill up" the space between lattice points. A set S is covering if the repeated pattern of S at every lattice point will cover all of $\mathrm{Span}_{\mathbb{R}}(L)$. Similarly, a set S is packing if no repeated instance of S will intersect with another instance of S. Tiling is when both of these are true: every point of $\mathrm{Span}_{\mathbb{R}}(L)$ can be found in exactly one instance of S, when S is repeated at every lattice point. Formally,

DEFINITION 9 (COVERING, PACKING, TILING) *Let $S \subseteq \mathrm{Span}_{\mathbb{R}}(L)$.*

1. *The set S is said to be L-covering if $L + S = \mathrm{Span}_{\mathbb{R}}(L)$.*
2. *S is L-packing if for any pair $\mathbf{t}, \mathbf{u} \in L$, $\mathbf{t} + S \cap \mathbf{u} + S = \emptyset$.*
3. *S is L-tiling if it is both packing and covering.*

All these properties can be though as in term of the union underlying the notation $L + S := \bigcup_{\mathbf{x} \in L} S + \mathbf{x}$: covering means this union is the whole space, and packing means this union is disjoint. Tiling is a synonym of being a fundamental domain for L.

The fundamental parallelepiped $\mathcal{P}(\mathbf{B})$ is a tiling with respect to L, as a corollary of Proposition 5. Since the concept of covering, packing and tiling are so closely linked, we often use an abbreviation of notation that hopefully doesn't lead to any confusion.

PROPOSITION 10 *Let $L \subseteq \mathbb{R}^n$ be a k-dimensional lattice and let $S \subseteq \mathrm{Span}_{\mathbb{R}}(L)$ be a measurable set. If S is L-(covering, packing, tiling), then* $\mathrm{vol}(S) \quad (\geq, \leq, =) \quad \mathrm{vol}(\mathcal{P}(\mathbf{B}))$. *In particular, every tiling has the same volume.*

PROOF: The proof proceeds with a collage. Let us simplify the notation $P = \mathcal{P}(\mathbf{B})$. Cut S into the disjoint union $S = \bigsqcup_{\mathbf{x}\in L} S \cap (P + \mathbf{x})$. Move each piece back to P by translating it by $-\mathbf{x}$, and glue them back as $T := \bigcup_{\mathbf{x}\in L} ((S - \mathbf{x}) \cap P)$. In particular $T \subseteq P$. By the properties of the Lebesgue measure, $\mathrm{vol}(T) \leq \mathrm{vol}(P)$ and $\mathrm{vol}(T) \leq \mathrm{vol}(S)$.

If S is packing, then the union defining $T = \bigcup_{\mathbf{x}\in L} ((S - \mathbf{x}) \cap P)$ is disjoint because the $(S - \mathbf{x})$ are disjoint. So $\mathrm{vol}(T) = \sum_{\mathbf{x}} \mathrm{vol}((S - \mathbf{x}) \cap P) = \sum_{\mathbf{x}} \mathrm{vol}(S \cap (P + \mathbf{x})) = \mathrm{vol}(S)$ and we conclude that $\mathrm{vol}(S) \leq \mathrm{vol}(P)$.

If S is now covering, we claim that $T = P$, and we conclude that $\mathrm{vol}(S) \geq \mathrm{vol}(P)$. Indeed, $T = \bigcup_{\mathbf{x}\in L} ((S - \mathbf{x}) \cap P) = (\bigcup_{\mathbf{x}\in L}(S - \mathbf{x})) \cap P = \mathrm{Span}_{\mathbb{R}}(L) \cap P = P$. □

3.3 Determinant, Volume and Density

The above leads us to define the determinant of a lattice (sometimes called the volume, or less frequently but more accurately the co-volume).

DEFINITION 11 *The determinant* $\det(L)$ *is defined as* $\sqrt{|\det(\mathbf{B}^t\mathbf{B})|}$ *for any basis* $\mathbf{B}$ *of L.*

It follows from Proposition 8 that this value does not depend on the choice of basis. In that sense it is an *invariant* of the lattice. Note that if L is full rank, then its determinant can be computed more simply as $|\det(\mathbf{B})|$. The determinant can be thought as the inverse of the density of the lattice: tiling the space as $\bigcup_{\mathbf{x}\in L} \mathcal{P}(\mathbf{B}) + \mathbf{x}$, each tile has volume $\mathrm{vol}(\mathcal{P}(\mathbf{B})) = \det(L)$, and contains one lattice point.

This density intuition can be formalized as the following statement, (which applies to any choice of norm).

THEOREM 12 *Let $L \subset \mathbb{R}^n$ be a full-rank lattice, and let $\mathcal{B}$ denote the closed ball of radius* 1, $\mathcal{B} := \{\mathbf{x} \in \mathbb{R}^n \mid \|\mathbf{x}\| \leq 1\}$. *Then,*

$$\lim_{r\to\infty} \frac{|r\mathcal{B} \cap L|}{r^n \mathrm{vol}(\mathcal{B})} = \frac{1}{\det(L)}.$$

We will prove Theorem 12 using a packing and covering argument.

PROPOSITION 13 *Let T be a bounded tiling for a lattice L, and $\mu = \sup_{\mathbf{x}\in T} \|x\|$. Then, for any radius $r > \mu$ it holds that* $\frac{(r-\mu)^n}{\det(L)} \leq \frac{|L\cap r\mathcal{B}|}{\mathrm{vol}(\mathcal{B})} \leq \frac{(r+\mu)^n}{\det(L)}$.

PROOF: We first show the right-hand bound. Let T be a tiling set of L that is contained in $\mu\mathcal{B}$. This is a covering set by definition, so $\mathbb{R}^n = L + T$. Furthermore, $(L \cap r\mathcal{B}) + T \subseteq (r + \mu)\mathcal{B}$ by the triangle inequality. This gives

$$\mathrm{vol}((L \cap r\mathcal{B}) + T) \leq \mathrm{vol}((r + \mu)\mathcal{B}) = (r + \mu)^n \mathrm{vol}(\mathcal{B}).$$

But since T is tiling, and any tiling set has volume $\det(L)$, the left hand side can be written as $\sum_{\mathbf{x}\in L\cap r\mathcal{B}} \mathrm{vol}(T) = |L \cap r\mathcal{B}|\det(L)$. Thus $|L \cap r\mathcal{B}|\det(L) \leq (r + \mu)^n \mathrm{vol}(\mathcal{B})$ and the right hand side follows.

For the left-hand bound, note first that $(r-\mu)\mathcal{B} \subseteq (L \cap r\mathcal{B}) + T$. Then, for the same reasoning as before, we see

$$(r-\mu)^n \mathrm{vol}(\mathcal{B}) \leq |L \cap r\mathcal{B}| \det(L),$$

and the bound follows. □

Proof of Theorem 12: This is an immediate corollary of Proposition 13, by choosing $T = \mathcal{P}(\mathbf{B})$ for any basis $\mathbf{B}$ of L, noting that $\mu \leq \frac{1}{2}\sum \|\mathbf{b}_i\|$ is finite. Divide across by r^n and take the limit. □

4 Minkowski's First Theorem

With all the above prequisite, there is not much left to do to reach Minkowski's first theorem and Minkowski's bound. It is often demonstrated via the so-called Blichfeldt lemma, which at this point is merely the contrapositive of the volume bound for packing (Proposition 10).

Lemma 14 (Blichfeldt) *For any lattice L and any measurable set $S \subset \mathrm{Span}_{\mathbb{R}}(L)$ such that $\mathrm{vol}(S) > \det(L)$, there exist distinct $\mathbf{x}, \mathbf{y} \in S$ such that $\mathbf{x} - \mathbf{y} \in L$.*

Theorem 15 (Minkowski Convex Body Theorem) *For any lattice L of rank n and any symmetric ($S = -S$) convex set $S \subset \mathrm{Span}_{\mathbb{R}}(L)$ such that $\mathrm{vol}(S) > 2^n \cdot \det(L)$, there exists a non-zero lattice vector in S: $|S \cap L| > 1$.*

Proof: Apply Blichfeldt lemma to the lattice $L' = 2L$, of determinant $\det(L') = 2^n \cdot \det(L)$, and obtain distinct $\mathbf{x}, \mathbf{y} \in S$ such that $\mathbf{x} - \mathbf{y} \in L'$. Note that $\mathbf{z} := \frac{\mathbf{x}-\mathbf{y}}{2} \in L$, and because S is symmetric and convex, $\mathbf{z}$ also belongs to S. Note finally that $\mathbf{z}$ is non-zero since $\mathbf{x}$ and $\mathbf{y}$ are distinct. □

Theorem 16 (Minkowski Bound) *The minimal distance of any full rank lattice $L \subset \mathbb{R}^n$ is bounded by below: $\lambda_1(L) \leq 2 \cdot (\frac{\det(L)}{\mathrm{vol}(\mathfrak{B})})^{\frac{1}{n}}$, where $\mathfrak{B}$ is the ball of radius 1: $\mathfrak{B} = \{\mathbf{x} \in \mathbb{R}^n \mid \|\mathbf{x}\| \leq 1\}$.*

In particular, for the Euclidean norm $\|\mathbf{x}\| := \sqrt{\sum x_i^2}$ (a.k.a. the ℓ_2 norm) the unit ball $\mathfrak{B}$ has volume $\mathrm{vol}(\mathfrak{B}) = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}$ where $\Gamma(x+1) \sim \sqrt{2\pi x}(x/e)^x$ (Stirling's approximation). Hence, n-dimensional lattice of rank n have a normalized minimal distance of at most:

$$\frac{\lambda_1^{(2)}(L)}{\det(L)^{1/n}} \leq \sqrt{\frac{2n}{\pi e}} + o(\sqrt{n}).$$

Note that because the restriction of an ℓ_2-ball to any subspace of $\mathbb{R}^n$ is still an ℓ_2-ball, this bound is not limited to full-rank lattices.