Lattices and Minkowsky's Theorem

Integer Lattices

A lattice point in the integer lattice $\mathbb{Z}^d$ is a point in $\mathbb{R}^d$ with integer coordinates.

Minkowski's Theorem

Let $C \subseteq \mathbb{R}^d$ be symetric around the origin (i.e., $C = -C$), convex, and bounded, and suppose that $\text{vol}(C) > 2^d$.
Then C contains at least one lattice point different from 0.

Claim

Let C' be $\frac{1}{2}C$, i.e., $C' = \{\frac{1}{2}x \mid x \in C\}$.
There exists a nonzero integer vector $v \in \mathbb{Z}^d \setminus \{0\}$ such that $C' \cap (C' + v) \neq \emptyset$; i.e., C' and a translate of C' by an intger vector intersect.
Sketch of proof

- By contradiction; suppose the claim is false.
- Let R be a large integer number.
- Consider the family $\mathcal{C}$ of translates of C' by the integer vectors in the cube $[-R, R]^d$ (See figure in the next page):

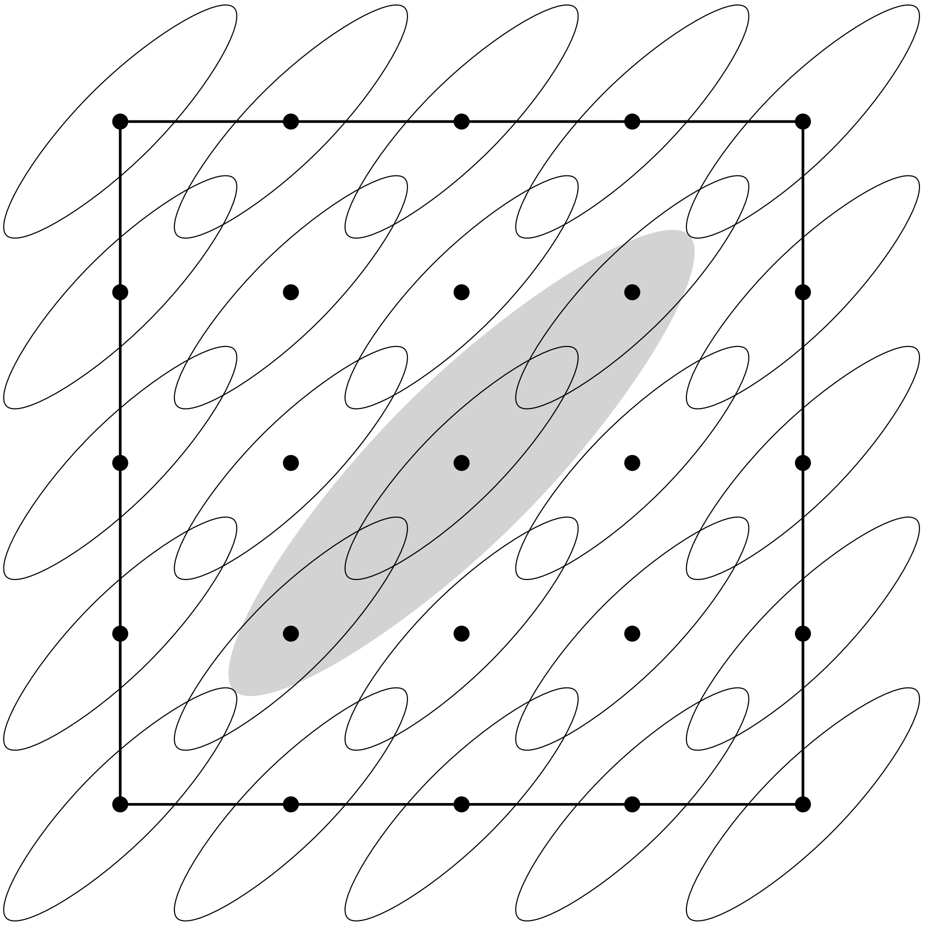
$$\mathcal{C} = \{C' + v \mid v \in [-R, R]^d \cap \mathbb{Z}^d\}$$

- By assumption, each such translate is disjoint from C', and every two of these translates are disjoint as well.
- All translates are contained in the enlarged cube $K = [-R - D, R + D]^d$, where D denotes the diameter of C':

$$\text{vol}(K) = (2R + 2D)^d \geq |\mathcal{C}|\text{vol}(C') = (2R+1)^d \text{vol}(C'), \text{ and}$$

$$\rightarrow \text{vol}(C') \leq \left(1 + \frac{2D - 1}{2R + 1}\right)^d.$$

- The right hand side is arbitrarily close to 1 for sufficiently large R
- Since $\text{vol}(C')2^{-d}\text{vol}(C) > 1$, the lefthand side, is a fixed number exceeding 1 by a certain amount independent of R.
- There exists a contradiction.



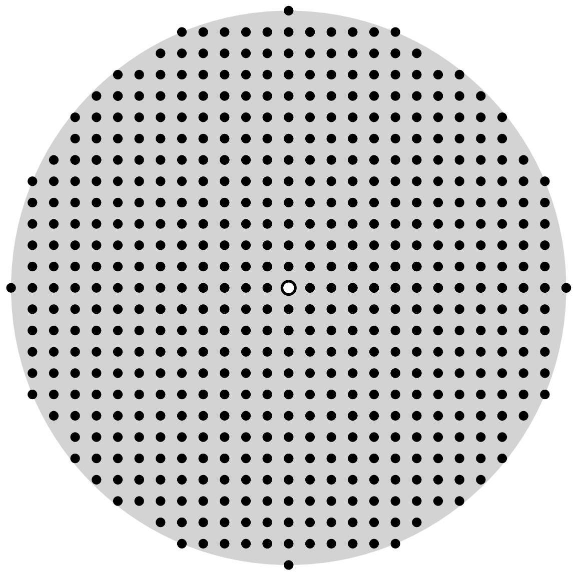
Proof of Minkowski Theorem

- Fix a vector $v \in \mathbb{Z}^d$ as in the Claim, and choose a point $x \in C' \cap (C' + v)$.
- $x - v \in C'$.
- Since C' is symetric, $v - x \in C'$.
- Since C' is convex, the midpoint of the segment between x and $v - x$ lies in C', i.e.,

$$\frac{1}{2}x + \frac{1}{2}(v - x) = \frac{1}{2}v \in C'$$

- To conclude,

$$v \in C.$$



Example (A regular forest)
Let K be a circle of diamter 26 centered at the origin. Threes of diameter 0.16 grow at each lattice point within K except for the origin. You stand at the origin. Prove that you cannot see outside this miniforest.

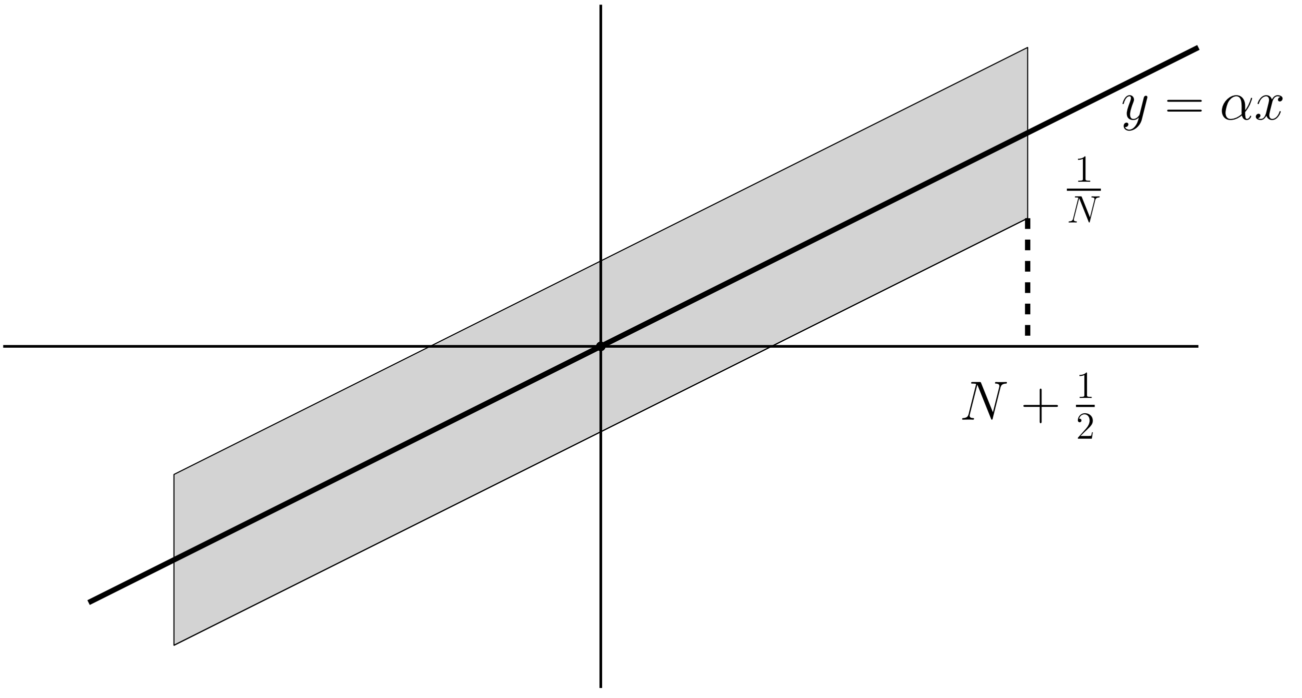
Sktech of Proof

- Assume the contrary that one could see outside along some line l passing through the origin.
- The strip S of width 0.16 with l as the middle line contains no lattice point in K except for the origin.
- In other words, the sysmetric convex set $C = K \cap S$ contains no lattice points bu the origin.
- Since $\text{vol}(C) > 4$, it contradicts Minkowski's theorem.

Proposition (Approximating an irrational number by a fraction)
Let $\alpha \in (0, 1)$ be a real number and N be a natural number. Then there exists a pair of natural numbers m, n such that $n \leq N$ and

$$|\alpha - \frac{m}{n}| < \frac{1}{nN}.$$

This proposition implies that there are infinitely many pairs m, n such that $\alpha - \frac{m}{n} < \frac{1}{n^2}$, which is a basic and well-known result in elemantary numner theory.



Proof of the Proposition

- Consider the set

$$C = \{(x, y) \in \mathbb{R}^2 \mid -N - \frac{1}{2} \leq x \leq N + \frac{1}{2},\ |\alpha x - y| < \frac{1}{N}\}$$

- C is symmetric.
- $\mathrm{vol}(C) = (2N + 1)\frac{2}{N} > 4$.
- Therefore, C contains some nonzero integer lattice point $(n,\ m)$.
- By symmetry, assume $n > 0$.
- By the definition of C, $n \leq N$, and $|\alpha n - m| < \frac{1}{N}$. In other words,

$$|\alpha - \frac{m}{n}| < \frac{1}{nN}.$$

General Lattices

Let $z_1, z_2, \ldots, z_d$ be a d-tuple of linearly independent vectors in $\mathbb{R}^d$.
The **lattice with basis** $\boldsymbol{\{z_1,\ z_2, \ldots,\ z_d\}}$ is the set of all linear combinations of the z_i with integer coefficients:

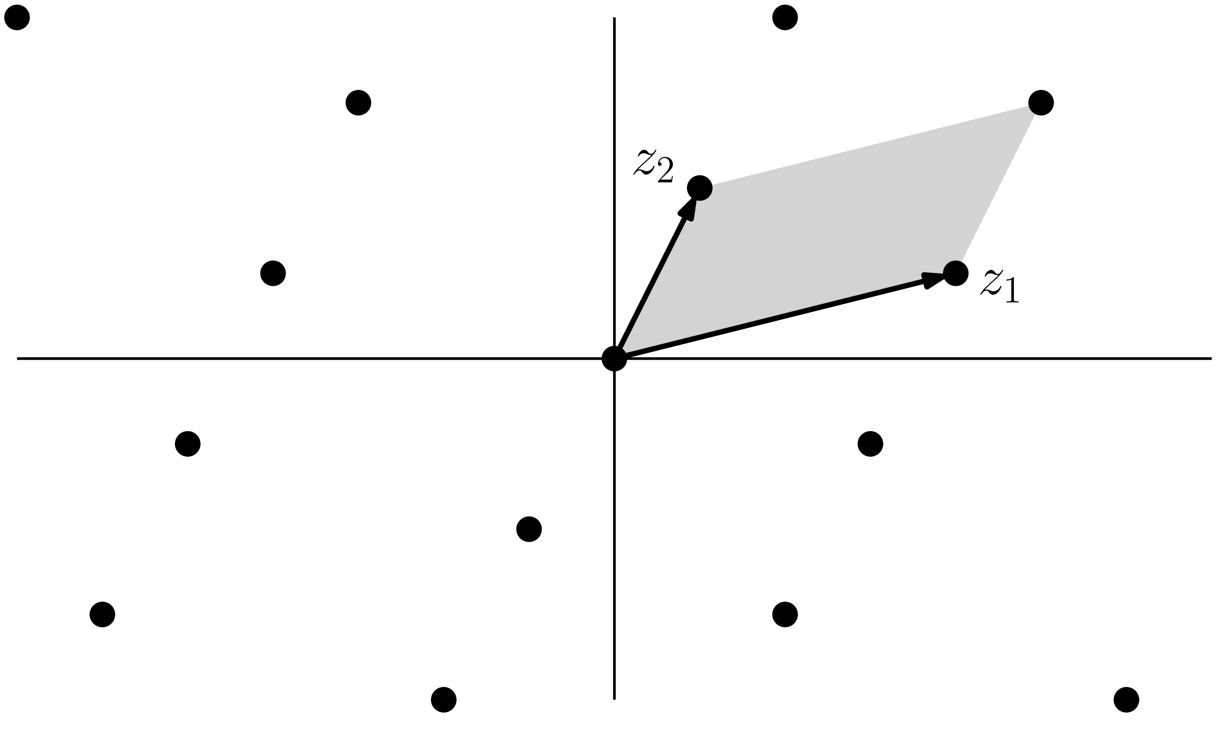
$$\Lambda = \Lambda(z_1,\ z_2, \ldots,\ z_d) = \{i_1 z_1 + i_2 z_2 + \cdots + i_d z_d \mid\ (i_1,\ i_2, \ldots,\ i_d) \in \mathbb{Z}^d\}$$

Remark

A general lattice has in general many different bases.
For example, the sets $\{(1,0),\ (0,1)\}$ and $\{(1,0),\ (3,1)\}$ are both bases of the "standard" lattice $\mathbb{Z}^2$.

Determinant of a lattice

Form a $d \times d$ matrix Z with the vector $z_1, \ldots, z_d$ as columns.
The **determinant of the lattice** $\Lambda = \Lambda(z_1,\ z_2, \ldots,\ z_d)$, denoted by $\det \Lambda$ is $|\det\ Z|$.
Geometrically, $\det \Lambda$ is the volume of the parallelepiped $\{\alpha_1 z_1 + \alpha_2 z_2 + \cdots + \alpha_d z_d \mid \alpha_1, \ldots, \alpha_d \in [0,\ 1]\}$.



Remark

- $\det \Lambda$ is a property of Λ, and it does not depend on the choice of basis of Λ.
- If Z is the matrix of some basis of Λ, the matrix of every basis of Λ has the form BU, where U is an integer matrix with determinant ± 1

Minkowski's theorem for general lattices
Let Λ be a lattice in $\mathbb{R}^d$, and let $C \subseteq \mathbb{R}^d$ be a symmetric convex set with $\mathrm{vol}(C) > 2^d \det \Lambda$. Then C contains a point of Λ different from 0.

Sketch of Proof

- Let $\{z_1, \ldots, z_d\}$ be a basis of Λ.
- Define a linear mapping $f : \mathbb{R}^d \to \mathbb{R}^d$ by $f(x_1,\ x_2, \ldots,\ x_d) = x_1 z_1 + x_2 z_2 + \cdots + x_d z_d$.
- f is a bijection and $\Lambda = f(\mathbb{Z}^d)$.
- For any convex set X,

$$\mathrm{vol}(f(X)) = \det(\Lambda)\mathrm{vol}(X).$$

  - If X is a cube, this trivially holds.
  - A convex set can be approximated by a disjoint union of sufficiently small cubes with arbitrary precision.
- Let C' be $f^{-1}(C)$.
- C' is a symmetric convex set with $\mathrm{vol}(C') = \mathrm{vol}(C)/\det \Lambda > 2^d$.
- By Minkowski's theorem, C' contains a integer lattice v in $\mathbb{Z}^d$.
- C contains $f(v)$, and $f(v)$ is a lattice point of Λ.

A seemingly more general definition of a lattice
What if we consider integer linear combinations of more than d vectors in $\mathbb{R}^d$?
If we take $d = 1$ and the vectors $v_1 = (1)$ and $v_2 = \sqrt{2}$, then the integer linear combination $i_1 v_1 + i_2 v_2$ are dense in the real line.
But it is not called a lattice.

Definition
A **discrete subgroup** of $\mathbb{R}^d$ is a set Λ of $\mathbb{R}^d$ such that whenever $x, y \in \Lambda$, then also $x - y \in \Lambda$ and such that the distance of any two distinct points of Λ is at least δ, for some fixed positive real number $\delta > 0$.

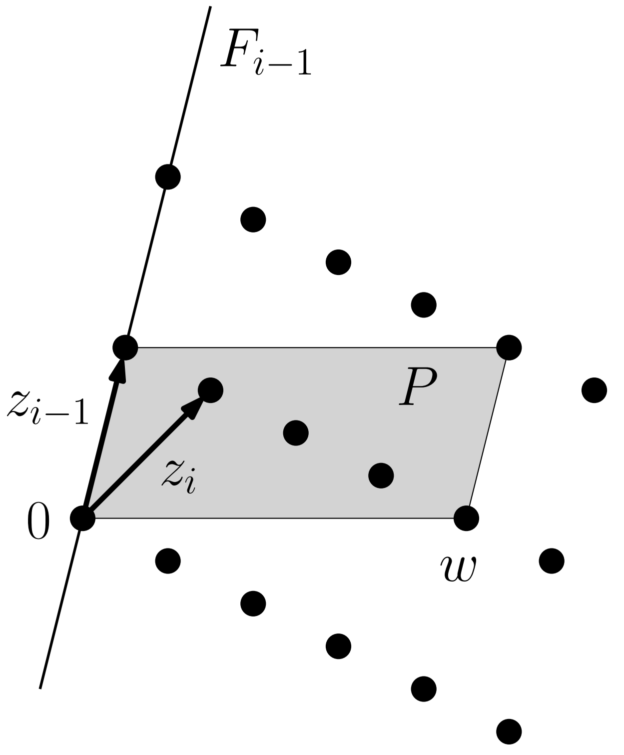
Remark

- If $v_1,\ v_2, \dots,\ v_n \in \mathbb{R}^d$ are vectors with *rational* coordinates, the set Λ of all their integer linear combinations is a discrete subgroup of $\mathbb{R}^d$.
- Any discrete subgroup of $\mathbb{R}^d$ whose linear span is all of $\mathbb{R}^d$ is a general lattice. (The following theorem)

Lattice Basis Theorem
Let $\Lambda \subset \mathbb{R}^d$ be a discrete group of $\mathbb{R}^d$ whose linear span is $\mathbb{R}^d$.
Then Λ has a basis: there exists d linearly independent vectors $z_1,\ z_2, \dots,\ z_d \in \mathbb{R}^d$ such that $\Lambda = \Lambda(z_1,\ z_2, \dots,\ z_d)$.

- Prove by induction
- Consider i, $1 \le i \le d+1$, and assume linearly independent vectors $z_1,\ z_2, \dots,\ z_{i-1}$ have already constructed:
  - Let F_{i-1} denoetes the $(i-1)$-dimensional subspace spanned by $z_1,\ z_2, \dots,\ z_{i-1}$.
  - All points of Λ lying in F_{i-1} can be written as integer linear combinations of $z_1,\ z_2, \dots,\ z_{i-1}$.
- If $i = d+1$, the statement of the theorem holds.
- So consider $i \le d$ and construct z_i
- Since Λ generates $\mathbb{R}^d$, there exists a vector $w \in \Lambda$ not lying in the subspace F_{i-1}.
- Let P be i-dimensional parallelepiped determined by $z_1,\ z_2, \dots,\ z_{i-1}$ and by w:

$$P = \{\alpha_1 z_1 + \alpha_2 z_2 + \cdots + \alpha_{i-1} z_{i-1} + \alpha_i w \mid \alpha_1, \dots,\ \alpha_i \in [0,1]\}$$



- Among all the points of Λ lying in P but not in F_{i-1}, choose one nearest to F_{i-1} and call it z_i.
- If the points of $\Lambda \cap P$ are written in the from $\alpha_1 z_1 + \alpha_2 z_2 + \cdots + \alpha_{i-1} z_{i-1} + \alpha_i w$, z_i is the w with smallest α_i.
- Let F_i be the linear space of $z_1, \ldots, z_i$. Then, if a point $v \in \Lambda$ lies in F_i, v can be written as $\beta_1 z_1 + \beta_2 z_2 + \cdots + \beta_i z_i$ for some real numbers $\beta_1, \ldots, \beta_i$.
- We will prove that all β_j, for $1 \leq j \leq i$, are all integers, leading to the theorem
- Let γ_j be the fractional part of β_j, for $1 \leq j \leq i$, i.e., $\gamma_j = \beta_j - \lfloor \beta_j \rfloor$.
- Let v' be $\gamma_1 z_1 + \gamma_2 z_2 + \cdots + \gamma_i z_i$.
- v' must belong to Λ since v and v' differ by an integer linear combination of vectors of Λ.
- Since $0 \leq \gamma_j < 1$, v' lies in the parallelepiped P.
- We must have $\gamma_i = 0$; otherwise, v' would be nearer to F_{i-1} than z_i.
- Hence $v' \in \Lambda \cap F_{i-1}$, and by the inductive hypothesis, we also get that all the other γ_j are 0.
- So all the β_j are integers.

Remark
A general lattice can also be defined as a full-dimensional discrete subgroup of $\mathbb{R}^d$.

Applications

Two-Square Theorem
Each pime $p \equiv 1 (\mod 4)$ can be wriited as a sum of two squares:

$$p = a^2 + b^2, a, b \in \mathbb{Z}.$$

Definition
An integer a is called a **quadratic residue** modulo p if there exists an integer x such that

$$x^2 \equiv a \pmod p.$$

Otherwise, q is a **quadratic nonresidue** modulo p.

Lemma
If p is a prime with $p \equiv 1 \pmod 4$, then -1 is a quadratic residue modulo p.

- Let F be the field of residue classes modulo p, and let F^* be $F \setminus \{0\}$.
- $i^2 = 1$ has two solutions in F, namely, $i = 1$ and $i = -1$.
- For any $i \neq \pm 1$, there exists exactly one $j \neq i$ with $ij = 1$, namely, $j = i^{-1}$ is the inverse element in F.
- Therefore, all the elements of $F^* \setminus \{-1, 1\}$ can be divided into pairs such that product of elements in each pair is 1.
- $(p-1)! = 1 \cdot 2 \cdots (p-1) \equiv -1 \pmod p$.
- Suppose that contradiction that the equation $i^2 = -1$ has no solution in F.
- All the elements in F^* can be divided into pairs such that the product of the elements in each pair is -1.
- There are $(p-1)/2$ pairs, which is an even number.
- Hence $(p-1)! \equiv (-1)^{(p-1)/2} = 1$, a contradiction.

Proof of Two-square theorem

- Choose a number q such that $q^2 \equiv -1 (\mod p)$.
- Consider the lattice $\Lambda = \Lambda(z_1,\ z_2)$, where $z_1 = (1,\ q)$ and $z_2 = (0,\ p)$.
- $\det \Lambda = p$.
- Consider a disk $C = \{(x,\ y) \in \mathbb{R}^2 \mid x^2 + y^2 < 2p\}$.
- The area of C is $2\pi p > 4p = 2^2 \det \Lambda$.
- By Minkowski's theorem for general lattices, C contains a point $(a, b) \in \Lambda \setminus \{0\}$.
- We have $0 < a^2 + b^2 < 2p$.
- At the same time, $(a, b) = iz_1 + jz_2$ for some $i,\ j \in \mathbb{Z}^2$, i.e., $a = i$, $b = iq + jp$.
- $a^2+b^2 = i^2+(iq+jp)^2 = i^2+i^2q^2+2iqjp+j^2p^2 \equiv i^2(1+q^2) \equiv 0 (\mod p)$.
- Therefore $a^2 + b^2 = p$.