Notes for Math 669

Yiwei Fu, Instructor: Alexander Barvinok

WN 2023

Contents

Office hours:

Chapter 1

Introduction to Lattices

1.1 Definition

Definition 1.1.1. A lattice $\Lambda \subset V$ has the following properties:

1. $\operatorname{span}(\Lambda) = V$.
2. Λ is an additive subgroup.
3. Λ is discrete: for any $r > 0$, let $B_r = \{x \in \mathbb{R}^n, \|x\| \leq r\}$, $\Lambda \cap B_r$ is finite.

1.2 Lattice and Its Basis

Last time: $L \in V$ is a subspace if $L = \operatorname{span}(L \cap \Lambda)$

Theorem 1.2.1. *If L is a lattice subspace, $L \neq V$, then $\exists u \in L \setminus \Lambda$ such that $d(u, L) \leq d(x, L)$ for all $x \in L \setminus \Lambda$.*

Say $L \in \operatorname{span}\{u_1, \ldots, u_m\}$ linearly independent vectors, $\Pi = \{\}$ There is $u \in \Lambda \setminus L$ such that $\operatorname{dist}(u, \Pi) \leq \operatorname{dist}(x, \Pi)$ for all $x \in \Lambda \setminus L$.

Proof. Take $\rho > 0$ large enough. Consider $\Pi_\rho = \{y, d(y, \Pi) \leq \rho\}$. It contains points from $\Lambda \setminus L$, choose the one in $\Pi_\rho \cap (\Lambda \setminus L)$ closet to Π. ■

<u>CLAIM</u> $u \in \Lambda \setminus L$ is what we need. Why? Pick any $x \in \Lambda \setminus L$. Let $y \in L$ be the closest to x.

$$\operatorname{dist}(x, L) = \|x - y\| = \|(x - w) - (y - w)\|\,.$$

$$y = \sum_{i=1}^{m} d_i u_i$$

Let $w = \sum_{i=1}^{m} \lfloor \alpha_i \rfloor u_i \in \Lambda \setminus L, y - w = \sum_{i=1}^{m} \{\alpha_i\} u_i \in \Pi$.

Theorem 1.2.2. *Every lattice has a basis.*

Proof. By induction on $n = \dim V$.

Base case: for $n = 1$, we have $V = \mathbb{R}$.

Let $u > 0$ be the lattice vector closet to 0, among all positive vectors in Λ.

Then u is a basis of Λ. Pick any $v \in \Lambda$. Assume $v > 0$ WLOG. Then $v = \alpha u$ for $\alpha > 0$. If $\alpha \in \mathbb{Z}$ then we are done. If not, consider $w = \alpha u - \lfloor \alpha \rfloor u = \{\alpha\} u$, this is closer to 0 than u, a contradiction.

Induction hypothesis: suppose any lattice of dimension $n - 1$ has a basis.

Induction step: pick a lattice hyperplane H (lattice subspace with $\dim = n - 1$). Then $\Lambda_1 = H \cap \Lambda$ has a basis $u_1, \ldots, u_{n-1}$. Pick u_n such that $u_n \notin H$ and $\operatorname{dist}(u_n, H)$ is the smallest. We claim that $u_1, \ldots, u_{n-1}, u_n$ is a basis of Λ.

Let $u \in \Lambda$, $u = \sum_{i=1}^{n} \alpha_i u_i$ with $\alpha_i \in \mathbb{R}$. If $\alpha_n = 0$ then $u \in \Lambda_1$, then $\alpha_1, \ldots, \alpha_{n-1} \in \mathbb{Z}$. Suppose $\alpha_n \neq 0$. Consider $w = u - \lfloor \alpha_n \rfloor u_n$. $w \in \Lambda$ and $w = \{\alpha_n\} u_n + \sum_{i=1}^{n-1} \alpha_i u_i$. So

$$\operatorname{dist}(w, H) = \operatorname{dist}(\{\alpha_n\} u_n, H) = \{\alpha_n\} \operatorname{dist}(u_n, H)$$

If $\{\alpha_n\} > 0$ then $0 < \operatorname{dist}(w, H) < \operatorname{dist}(u_n, H)$, a contradiction.

So $\{\alpha_n\} = 0 \implies \alpha_n \in \mathbb{Z}$. Then $w = \sum_{i=1}^{n-1} \alpha_i u_i \implies \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{Z}$.

So we have constructed a basis for lattice of dimension n, thus finishing the proof. ■

This is called A.N.Korkin(e)-Zolotarev(öff) basis.

<u>EXERCISE</u> Suppose $u_1, \ldots, u_n \in V$ is a basis of subspace. The integer combinations form a lattice.

<u>EXERCISE</u> Suppose a 2-dimensional lattice. Then there exists a lattice basis u, v such that the angle α between u, v satisfies $\frac{\pi}{3} \leq \alpha \leq \frac{\pi}{2}$.

<u>EXERCISE</u> If Λ is a lattice and L is a lattice subspace. The orthogonal projection $\mathrm{PR} : V \to L^{\perp}$. Then $\mathrm{PR}(\Lambda) \subset L^{\perp}$ is a lattice.

Definition 1.2.1. Suppose $u_1, \ldots, u_n$ be a basis of Λ.

$$\Pi = \left\{ \sum_{i=1}^{n} \alpha_i u_i : 0 \leq \alpha_i < 1, i = 1, \ldots, n \right\}$$

is the *fundamental parallelepiped* of a fundamental parallelepiped of Λ.

Theorem 1.2.3. *The volume of a fundamental parallelepiped Π doesn't depend on Π. The volume is called the determinant of Λ. Furthermore, if $B_r = \{x : \|x\| \leq r\}$, then*

$$\lim_{r\to\infty} = \frac{|B_r \cap \Lambda|}{\operatorname{vol} B_r} = \frac{1}{\det \Lambda}.$$

We start with a lemma:

Lemma 1.2.1. *Let Π be a fundamental parallelepiped of $\Lambda \subset V$. Then every vector $x \in V$ is uniquely written as $x = u + y$ where $u \in \Lambda, y \in \Pi$.*

Proof. Existence: Π is the fundamental parallelepiped for $u_1, \ldots, u_n$. If $x = \sum_{i=1}^n \alpha_i u_i$ then $u = \sum_{i=1}^n \lfloor \alpha_i \rfloor u_i$ and $y = \sum_{i=1}^n \{\alpha_i\} u_i$

Uniqueness: suppose $x = u_1 + y_1 = u_2 + y_2$ then $u_1 - u_2 = y_2 - y_1$. Since $u_1 - u_2 \in \Lambda$ we have $y_2 - y_1 = \sum_{i=1}^n (\alpha_i - \beta_i)\mathbf{u}_i$. We have $(\alpha_i - \beta_i) \in \mathbb{Z}$. Since $-1 < \alpha_i - \beta_i < 1$, it has to be 0. ■

A geometry interpretation is that we can cover the whole space with fundamental parallelepipeds without overlaps.

Proof of theorem. Let

$$X_r = \bigcup_{u \in B_r \cap \Lambda} (\Pi + u)$$

Then $\operatorname{vol} X_r = |B_r \cap \Lambda| \operatorname{vol} \Pi$.

Say, $\Pi \subset B_a$ for some $a > 0$. Then $X_r \subset B_{r+a}$. Look at B_{r-a}. It is covered by $\Pi + u : u \in \Lambda$. We should have $\|u\| \leq r$. Hence $B_{r-a} \subset X_r$.

So we have

$$\left(\frac{r-a}{a}\right)^n = \frac{\operatorname{vol} B_{r-a}}{\operatorname{vol} B_r} \leq \frac{\operatorname{vol} X_r}{\operatorname{vol} B_r} \leq \frac{\operatorname{vol} B_{r+a}}{B_r} = \left(\frac{r+a}{a}\right)^n$$

This goes to 1 when $r \to \infty$. ■

<u>REMARK/EXERCISE</u> The same holds for balls not centered in the origin:

$$B_r(x_0) = \{x : \|x - x_0\| \le r\}.$$

<u>EXERCISE</u> Suppose a lattice $\Lambda \subset V$ and $u \in \Lambda$. The Voronoi (G.F. Voronoi, 1868-1908) region is defined by

$$\Phi_u = \{x \in V : \|x - u\| \le \|x - v\|, \forall v \in \Lambda\}.$$

Show that Φ is convex (bounded by at most 2^n affine hyperplanes) and $\operatorname{vol}\Phi = \det\Lambda$.

<u>EXERCISE</u> $(\det\Lambda)(\det\Lambda^*) = 1$

1.3 Sublattice

Definition 1.3.1. Suppose $\Lambda \subset V$ is a lattice, and $\Lambda_0 \subset \Lambda, \Lambda_0 \subset V$ is also a lattice. Λ_0 is then called a sublattice of Λ.

Remark. We have $\operatorname{rank}\Lambda_0 = \operatorname{rank}\Lambda$.

Example 1.3.1. $D_n \subset \mathbb{Z}^n$.

Λ is an Abelian group and $\Lambda_0 \subset \Lambda$ is a subgroup. Look at the quotient Λ/Λ_0 and cosets $\{u + \Lambda_0\}$. The index of Λ_0 in $\Lambda|\Lambda/\Lambda_0| =$ the number of cosets.

Theorem 1.3.1. 1. *Let Π be a fundamental parallelepiped of Λ_0 Then $|\Lambda/\Lambda_0| = |\Pi \cap \Lambda|$.*

2. $|\Lambda/\Lambda_0| = \dfrac{\det\Lambda_0}{\det\Lambda}$.

Proof. 1. By Lemma 1.2.1, every coset has a unique representation in Π.

2. Let $B_r = \{x : \|x\| \le r\}$. Then

$$\lim_{r\to\infty} = \frac{|B_r \cap \Lambda|}{\operatorname{vol} B_r} = \frac{1}{\det\Lambda}.$$

Let $S \subset \Lambda$ be the set of coset representatives. Then $|S| = |\Lambda/\Lambda_0|$. Then $\Lambda = \bigcup_{u\in S}(u + \Lambda_0)$. Hence

$$\lim_{r\to\infty} \frac{|B_r \cap (u + \Lambda_0)|}{\operatorname{vol} B_r} = \frac{1}{\det\Lambda_0}. \implies \frac{1}{\det\Lambda} = |S|\frac{1}{\Lambda_0}$$ ∎

<u>EXERCISE</u>

1. $\det\mathbb{Z}^n = 1$

2. $\det D_n = 2$.
3. $\det D_n^+ = 1$. (n even)
4. $\det A_n = \sqrt{n+1}$. $\det E_8 = 1, \det E_7 = \sqrt{2}, \det E_6 = \sqrt{3}$.
5. If $a_1, \ldots, a_n$ are coprime integers not all 0.

$$\Lambda = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : a_1x_1 + \ldots + a_nx_n = 0\} \text{ has } \det \Lambda = \sqrt{a_1^2 + \ldots + a_n^2}.$$

Corollary 1.3.1. *If $u_1, \ldots, u_n \in \Lambda$ are linearly independent and*

$$\operatorname{vol}\left\{\sum_{i+1}^{n} \alpha_i u_i : 0 \le \alpha_i < 1\right\} = \det \Lambda$$

then $u_1, \ldots, u_n$ is a basis.

Proof. Look at

$$\Lambda_0 = \left\{\sum_{i=1}^{n} m_i u_i : m_i \in \mathbb{Z}\right\}, |\Lambda/\Lambda_0| = 1 \implies \Lambda = \Lambda_0$$ ■

Counting integer points. Suppose $\Lambda = \mathbb{Z}^n$.

Pick n linearly independent vectors $u_1, \ldots, u_n \in \Lambda$. Consider

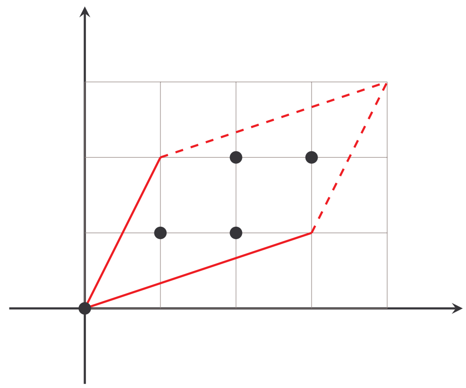
$$\Pi = \left\{\sum_{i=1}^{n} \alpha_i u_i : 0 \le \alpha_i < 1\right\}.$$

Then

$$|\Pi \cap \mathbb{Z}^n| = ?$$

Suppose $\Lambda_0 = \{\sum_{i=1}^n m_i u_i : m_i \in \mathbb{Z}\}$. Then $\det \Lambda_0 = \operatorname{vol} \Pi$.

Suppose $n = 2$, $u_1 = (3,1), u_2 = (1,2)$. Then $\operatorname{vol} \Pi = 5$. We can see that the parallelogram contains 5 integer points.



The case for $n = 2$ is special.

Theorem 1.3.2 (Pick Formula (G.A. Pick, 1859-1942))**.** *If $P \subset \mathbb{R}^2$ is a convex polygon with integer vertices and non-empty interior. Then*

$$|P \cap \mathbb{Z}^2| = \text{ area of } P + \frac{1}{2}|\partial P \cap \mathbb{Z}^2| + 1$$

Proof. Left as exercise. Hint: do it for parallelograms (in any dimension) first, then do it for triangles (special case for $n = 2$), and then all polygons with integer vertices. ■

<u>EXERCISE</u> For $n = 2$, linearly independent vectors of $u, v \in \mathbb{Z}^2$ form a basis $\iff$ the triangle with vertices $0, u, v$ has no other integer points.

<u>EXERCISE</u> For $n = 3$, construct an example of linearly independent $u, v, w \in \mathbb{Z}^3$ such that the tetrahedron with vertices $0, u, v, w$ has no other integer points but $\{u, v, w\}$ is not a basis of $\mathbb{Z}^3$. In fact, you can have $|\mathbb{Z}^n/\Lambda|$ arbitrarily large.

<u>EXERCISE</u> Suppose $u_1, \ldots, u_k \in \mathbb{Z}^n$ are linearly independent vectors and $\Lambda = \mathbb{Z}^n \cap \operatorname{span}(u_1, \ldots, u_k)$. The $\{u_1, \ldots, u_k\}$ is a basis of Λ if and only if the great common divisor of all $k \times k$ minors of $\begin{bmatrix} u_1^T \\ u_2^T \\ \cdots \\ u_k^T \end{bmatrix}$ is 1.

Proof. $\implies$: suppose $u_1, \ldots, u_k$ is a basis. Then we can extend $\{u_1, \ldots, u_k\}$ to get a basis $\{u_1, \ldots, u_k, \ldots, u_n\}$ of $\mathbb{Z}^n$. So $\det[u_1|u_2|\ldots|u_n] = 1$. Use Laplace expansion for the first k columns we have

$$\sum_{I \subset \{1,\ldots,n\}, |I|=k} \det A_I \cdot \det A_{\overline{I}} = \pm 1 \implies \gcd(\det A_I) = 1.$$

$\Longleftarrow$: suppose $\gcd = 1$. Pick any $x \in \Lambda$, then $x = \alpha_1 u_1 + \ldots + \alpha_k u_k$ for some $\alpha_i \in \mathbb{R}$. Pick any k rows of $U = \left[\begin{array}{c|c|c|c} u_1 & u_2 & \ldots & u_k \end{array}\right]$ where $\det A_I \neq 0$. By Kramer's dule, $\alpha_i = \frac{\det[\text{replace } u_i \text{ by } x \text{ in } U]}{\det A_I}$. $\det A_I$ are coprime $\implies \sum m_I \det A_I = 1$ for some $m_I \in \mathbb{Z}$. $\alpha_i \det A_I \in \mathbb{Z} \implies \sum_I \alpha_i m_I \det A_I \in \mathbb{Z}$. ■

Some linear algebra: (Smith Normal Form) If $\Lambda_0 \subset \Lambda$ is a sublattice, then there is a basis $u_1, \ldots, u_n$ of Λ and a basis $v_1, \ldots, v_n$ of Λ_0 such that $v_i = m_i u_i$ for positive integer m_i and such that m_1 divides m_2 which divides $m_3, \ldots$.

1.4 Minkowski Theorem

The goal today is to prove Minkowski Theorem (H. Minkowski, 1864-1909) for convex body.

Definition 1.4.1. Suppose V a Euclidean space, then a set $A \subset V$ is convex if $\forall x, y \in A, [x, y] \in A$ where $\{[x, y] = \alpha x + (1-\alpha) y : 0 \leq \alpha \leq 1\}$.

Definition 1.4.2. A set A is symmetric if $A = -A = \{-x : x \in A\}$.

Theorem 1.4.1. *Suppose $\Lambda \subset V$ a lattice and $A \subset V$ a convex symmetric set with $\operatorname{vol} A > 2^{\dim V} \det \Lambda$. Then there is $u \subset \Lambda \setminus \{0\}$ such that $u \in A.s$*

$2^{\dim V}$ IS SHARP: Pick $\mathbb{Z}^n \subset \mathbb{R}^n, \det \mathbb{Z}^n = 1$. Let $A = \{-1 < x_i < 1, i = 1, \ldots, n\}$ convex and symmetric. Then $\operatorname{vol} A = 2^n$ and $A \cap Z^n = \{0\}$. And from geometric intuition we see that convex and symmetric is needed.

It is a result from Blichfeldt's theorem.

Theorem 1.4.2 (H. F. Blichfeldt, 1873 - 1945)**.** *Let measurable $X \subset V$, $\operatorname{vol} X > \det \Lambda$, then there are $x, y \in X$ such that $x - y \in \Lambda \setminus \{0\}$.*

INTUITION $\det \Lambda$ describes the volume per lattice point. Consider $\{X + u\}$ the translations of X by lattice points. Some of them must overlap i.e. $(X + u_1) \cap (X + u_2) \neq \emptyset$. Then $x + u_1 = y + u_2 \implies x - y = u_2 - u_1 \in \Lambda \setminus \{0\}$.

Proof. Choose a fundamental parallelepiped Π of lattice Λ. Then $\det \Lambda = \operatorname{vol} \Pi$. Then $\{\Pi + u, u \in \Lambda\}$ cover V without overlap. In particular, they cover X.

Let $X_u := ((\Pi + u) \cap X) - u$. $\sum_{u \in \Lambda} \operatorname{vol} X_u = \operatorname{vol} X > \operatorname{vol} \Pi$. And $X_u \subset \Pi$. Then $\exists u_1 \neq u_2$ *s.t.* $X_{u_1} \cap X_{u_2} \neq \emptyset$. Then $\exists x, y \in X$ *s.t.* $x - u_1 = y - u_2 \implies x - y = u_1 - u_2 \in \Lambda \setminus \{0\}$. ■

Proof of Minkowski's Theorem. Let $X = \frac{1}{2} A = \left\{\frac{1}{2} x, x \in A\right\}$. Then $\operatorname{vol} X = 2^{-\dim v} \operatorname{vol} A >$

$\det \Lambda$. By Blichfeldt, there are $x, y \in X$ such that $x - y \in \Lambda \setminus \{0\}$. Write

$$u = x - y = \frac{1}{2}(2x) + \frac{1}{2}(-2y)$$

Since A is convex and symmetric, $2x, -2y \in A$ and $x - y \in A \implies u \in A$. ■

EXERCISE Suppose $\Lambda \subset V$ a lattice. Let $X = \{x \in V : \|x\| < \|x - u\|, \forall u \in \Lambda \setminus \{0\}\}$. Let $A = 2X$. Show that A is convex, symmetric, $A = 2^{\dim V} \det \Lambda$ and $A \cap \Lambda = \{0\}$.

Corollary 1.4.1. *If, in addition, A is compact, then it is enough to have* $\operatorname{vol} A \geq 2^{\dim V} \det \Lambda$.

We can apply the proof for $(1 + \varepsilon)A$ and let $\varepsilon \to 0$.

Corollary 1.4.2. *Let $V = \mathbb{R}^n$, and $\|x\|_\infty = \max_{i=1,\dots,n} |x_i|$. Then there is a $u \in \Lambda \setminus \{0\}$ with $\|u\|_\infty \leq (\det \Lambda)^{\frac{1}{n}}$.*

Consider $A = \left\{x, |x_i| \leq (\det \Lambda)^{\frac{1}{n}}\right\}$.

Corollary 1.4.3. *Suppose $\Lambda \subset V$. Then there is $u \subset \Lambda \setminus \{0\}$ with $\|u\| \leq \sqrt{\dim V}(\det \Lambda)^{\frac{1}{n}}$.*

EXERCISE If $X \subset V$ is measurable and $\operatorname{vol} X > m \det \Lambda$ with $m \in \mathbb{Z}^+$. Then there are $x_1, \dots, x_{m+1} \in X$ such that $x_i - x_j \in \Lambda$ for all pairs i, j.

If A is convex, symmetric, and $\operatorname{vol} A > m \cdot 2^{\dim V} \det \Lambda$. Then A contains m distinct pairs $\pm u_1, \dots, \pm u_m$ of nonzero lattice points.

EXERCISE (IMPORTANT) If $X \subset \Lambda$ is a set such that $|X| > 2^{\dim V}$ then there are distinct $x, y \in X$ such that $\frac{x+y}{2} \in \Lambda$.

EXERCISE Suppose $f : V \to \mathbb{R}_+$ is integrable and $\Lambda \subset V$ a lattice. Then there are $z_1, z_2 \in V$ such that

$$\sum_{u \in \Lambda} f(u + z_1) \geq \frac{1}{\det \Lambda} \int_V f(x) \, \mathrm{d}x \geq \sum_{u \in \Lambda} f(u + z_2).$$

We need the column of the unit ball in $\mathbb{R}^n$.

$$\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} \, \mathrm{d}t$$

$$\Gamma(x + 1) = x\Gamma(x)$$

$$B = \{x : \|x\| = 1\}, B \subset \mathbb{R}^n, \operatorname{vol} B = \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2} + 1\right)}$$

We start with integral:

$$\int_{-\infty}^{\infty} e^{-x^2}\,\mathrm{d}x = \sqrt{\pi}, \int_{\mathbb{R}^n} e^{-\|x\|^2}\,\mathrm{d}x = \left(\sqrt{\pi}\right)^n$$

Let $S(r) = \{x \in \mathbb{R}^n : \|x\| = r\}$ and κ be the surface area of $S(1)$.

$$\begin{aligned}
\left(\sqrt{\pi}\right)^n &= \int_0^{\infty} \left(\int_{S(r)} e^{-\|x\|^2}\,\mathrm{d}x \right) \mathrm{d}r \\
&= \int_0^{\infty} r^n \kappa e^{-r^2}\,\mathrm{d}r \\
&= \frac{1}{2} \int_0^{\infty} t^{\frac{n-2}{2}} \kappa e^{-t}\,\mathrm{d}t \\
&= \kappa \frac{1}{2} \int_0^{\infty} t^{\frac{n-2}{2}} \kappa e^{-t}\,\mathrm{d}t = \frac{1}{2}\kappa\gamma\left(\frac{n}{2}\right)
\end{aligned}$$

So we have $\kappa = \frac{2\left(\sqrt{\pi}\right)^n}{\Gamma\left(\frac{n}{2}\right)}$.

Then

$$\operatorname{vol} B = \int_0^1 \kappa t^{n-1}\,\mathrm{d}r = \frac{\kappa}{n} = \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}.$$

1.5 Applications of Minkowski's Theorem

First application:

Theorem 1.5.1 (Lagrange's four squares theorem (J-L Lagrange, 1736-1813))**.** *If $n \geq 0$ is a non-negative integer, then $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ for some integer x_1, x_2, x_3, x_4.*

Proof. Start as Lagrange did: first, prove assuming that n is prime, then there are $a, b \in \mathbb{Z}$ such that $a^2 + b^2 + 1 \equiv 0 \pmod{n}$.

$n = 2$ is clear. Consider values of $a^2 \pmod{n}$ for $n > 2$ and $a = 0, 1, \ldots, \frac{n-1}{2}$. They are all distinct. Otherwise $a_1^2 \equiv a_2^2 \equiv \pmod{n} \implies (a_1 - a_2)(a_1 + a_2) \pmod{n}$.

Consider values $-1 - b^2 \pmod{n}$ for $b = 0, 1, \ldots, \frac{n-1}{2}$. They are all different values.

There are a total of $n + 1$ values, so there exists $a^2 \equiv -1 - b^2 \pmod{n}$ by pigeonhole principle.

We introduce one generally useful lemma:

Lemma 1.5.1. *Suppose $a_1, \ldots, a_k \in \mathbb{Z}^n$ and $m_1, \ldots, m_k$ positive integers and*

$$\Lambda = \{x \in \mathbb{Z}^n : \langle x, a_i \rangle \equiv 0 \pmod{m_i}\}.$$

Then Λ *is a lattice and* $\det \Lambda \leq m_1 \cdots m_k$.

Consider their cosets: pick $0 \leq b_i \leq m_i$, and the coset is

$$\{x \in \mathbb{Z}^n : \langle x, a_i \rangle \equiv b_i \pmod{m_i}\}$$

if the set is non-empty. Then $|\mathbb{Z}^n/\Lambda| = \frac{\det \Lambda}{\det \mathbb{Z}^n}$.

The rest is from Davenport: Suppose a lattice

$$\Lambda = \left\{ x \in \mathbb{Z}^4 : \begin{array}{l} x_1 \equiv ax_3 + bx_4 \\ x_2 \equiv ax_4 - bx_3 \end{array} \pmod{n} \right\}.$$

If $(x_1, x_2, x_3, x_4) \in \Lambda$ then

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &\equiv (ax_3 + bx_4)^2 + (ax_4 - bx_3)^2 + x_3^2 + x_4^2 \pmod{n} \\ &a^2x_3^2 + b^2x_4^2 + 2abx_3x_4 + \\ a^2x_4^2 + b^2x_3^2 - 2abx_3x_4 + x_3^2 + x_4^2 &\equiv (a^2 + b^2 + 1)x_3^2 + (b^2 + a^2 + 1)x_4^2 \equiv 0 \pmod{n} \end{aligned}$$

So we have $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{n}$ for all $(x_1, x_2, x_3, x_4) \in \Lambda$. So $\det \Lambda \leq n^2$. Consider the ball B with radius $\sqrt{2n}$. The volume of the ball $\operatorname{vol} B = 2n^2\pi^2 \geq 2^4 n^2 \geq 2^4 \det \Pi$. So there exists $(x_1, x_2, x_3, x_4) \in \Lambda \setminus \{0\}$ such that $x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{n}$.

So we conclude that such $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$.

Now suppose n is not prime, write $n = \prod p_i$ where p_i's are prime numbers.

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

where

$$\begin{cases} z_1 = x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 \\ z_2 = x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 = x_1y_3 + x_2y_4 + x_3y_1 + x_4y_2 \\ z_4 = x_1y_4 - x_2y_3 - x_3y_3 + x_4y_1 \end{cases}$$

Remember through quaternions. $x_1 + ix_2 + jx_3 + kx_4$. ■

Jacobi's Formula (C.G.J Jacobi, 1804-1851) The number of integer solutions (not necessarily positive) of the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$$

is $8 \cdot \sum_{d|n, 4\nmid d} d$.

<u>EXERCISE</u> Deduce the Jacobi's Formula from the identity

$$\left(\sum_{k=-\infty}^{\infty} q^k \right)^4 = 1 + 8 \sum_{k=1}^{\infty} \frac{q^k}{(1+(-q)^k)^2}, \text{ for } |q| < 1.$$

Gauss Circle Problem (C.-F Gauss, 1777, 1855) $B_r = \left\{ x \in \mathbb{R}^2 : \|x\| \le r \right\}$. As $r \to \infty$, $|B(r) \cap \mathbb{Z}^2| \approx \pi r^2 + O(r^{1/2+\varepsilon})$ for any $\varepsilon > 0$? Best known is $O(r^{0.63})$ for $\varepsilon = 0.13$.

<u>EXERCISE</u> If n is prime, $n \equiv 1 \pmod 4$. Then $n = x_1^2 + x_2^2$ for some $x_1, x_2 \in \mathbb{Z}$.

How well can we approximate a real number for rational numbers?

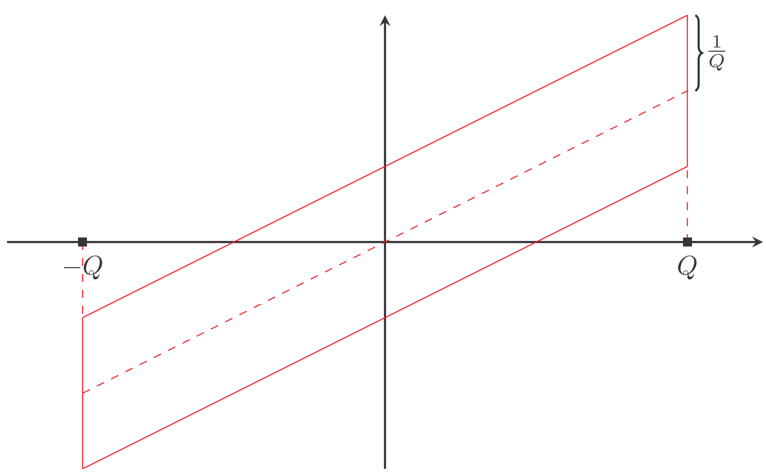
If $\alpha \in \mathbb{R}$ and $q \ge 1$ is an integer, then for some integer p we have $\left| \alpha - \frac{p}{q} \right| \le \frac{1}{2q}$.

Theorem 1.5.2. *For any $\alpha \in \mathbb{R}$ and $M > 0$, there exists $q \ge M$ and an integer p such that $\left| \alpha - \frac{p}{q} \right| \le \frac{1}{q^2}$.*

In fact, we can have $\left| \alpha - \frac{p}{q} \right| \le \frac{1}{q^2 \sqrt{5}}$, which is optimal.

It shows that this holds for infinitely many q.

Proof. Assume WLOG that α is irrational. Pick $Q \ge 1$ an integer. Consider the parallelogram in $\mathbb{R}^2 : \left\{ |x| \le Q, |\alpha x - y| \le \frac{1}{Q} \right\}$.



Π is convex, symmetric, compact, with area $\Pi = 4 = 2^2$.

By Minkowski, there exists $(q, p) \in \mathbb{Z}^2 \setminus \{0\}, (q, p) \in \Pi$ such that $|\alpha q - p| \leq \frac{1}{Q}, |p| \leq \frac{1}{Q} \implies p = 0$. Assume that $q > 0$.

We have $q \leq Q$, and

$$|\alpha q - p| \leq \frac{1}{Q} \implies \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{Qq} \leq \frac{1}{q^2}$$

It remains to show that for any M we can choose $q \geq M$.

Why? α is irrational. Choose Q so large that we cannot have $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{Q}$ for $q \leq M$. ■

<u>EXERCISE</u> For any $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ and any M, there are integers $p_1, \ldots, p_n$ and $q \geq M$ such that $\left|\alpha_k - \frac{p_k}{q}\right| \leq \frac{1}{q^{\frac{n+1}{n}}}$ for $k = 1, \ldots, n$.

Continued fractions: given α, we produce a possibly infinite expression:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\vdots}}}$$

and denote $\alpha = [a_0; a_1, a_2, \ldots]$ How: introduce variables $\beta_0, \beta_1 \ldots$ where $\beta_0 = \alpha$. Write $\beta_0 = \lfloor \beta_0 \rfloor + \{\beta_0\}$.

Let $a_0 = \lfloor \beta_0 \rfloor$, if $\{\beta_0\} = 0$ then stop. Otherwise let $\beta_1 = \frac{1}{\{\beta_0\}}$. Let $\alpha_1 = \lfloor \beta_1 \rfloor$, continue.

Example 1.5.1. Let $\alpha = \sqrt{2}$. $\beta_0 = \sqrt{2}$ and $a_0 = 1$.

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\frac{1}{\sqrt{2}-1}} = 1 + \frac{1}{\sqrt{2} + 1}$$

$$= 1 + \frac{1}{2 + (\sqrt{2} - 1)} = 1 + \frac{1}{2 + \frac{1}{\frac{1}{\sqrt{2}-1}}}$$

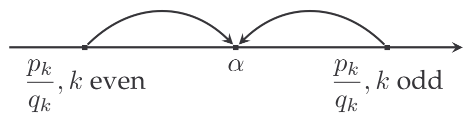
Convergents: k-th convergent:

$$[a_0; a_1, \ldots, a_k] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + \frac{1}{a_k}}}} = \frac{p_k}{q_k}$$

<u>EXERCISES</u> Suppose p_k, q_k are coprime. Prove that $p_k = a_k p_{k-1} + p_{k-2}, q_k = a_k q_{k-1} + q_{k-2}$ for $k \geq 2$. Hint: Induction $[a_0; a_1, \ldots, a_k] \to [a_1; a_2, \ldots, a_k]$.

Prove that $p_{k-1} q_k - p_k q_{k-1} = (-1)^k$ for $k \geq 1$.

Prove that $q_k q_{k-2} - p_k q_{k-2} = (-1)^{k-1} a_k$ for $k \geq 2$.



Prove that $\left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k q_{k+1}}, k \geq 0$.

(Hard, easy if replace 5 by 2) Prove that at least one of the three holds:

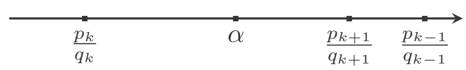
$$\left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k^2\sqrt{5}}, \left|\alpha - \frac{p_{k-1}}{q_{k-1}}\right| \leq \frac{1}{q_{k-1}^2\sqrt{5}}, \text{ or } \left|\alpha - \frac{p_{k-2}}{q_{k-2}}\right| \leq \frac{1}{q_{k-2}^2\sqrt{5}}.$$

Convergents are the best rational approximation in the following sense:

Given α and integer $Q > 1$, we want to find $\frac{a}{b}$ such that $|b| \leq Q$ and $|\alpha b - a|$ is the smallest possible.

CLAIM Must have $\frac{a}{b} = \frac{p_k}{q_k}$. (With possible exception of $k = 0, 1$.)

WHY/EXERCISES Suppose not: pick the largest k such that $\frac{a}{b}$ is between $\frac{p_{k-1}}{q_{k-1}}$ and $\frac{p_k}{q_k}$.



Then $\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| \geq \frac{1}{bq_{k-1}}$, easy. Then $\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| \leq \left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_k q_{k-1}}$ from last exercise.

On the other hand $\left|\alpha - \frac{a}{b}\right| \geq \left|\frac{p_{k+1}}{q_{k+1}} - \frac{a}{b}\right| \geq \frac{1}{bq_{k+1}}$. So $|\alpha b - a| \geq \frac{1}{q_{k+1}}$ but $|\alpha q_k - p_k| \leq \frac{1}{q_{k+1}}$.

So $b > q_k$.

Theorem 1.5.3 (Liouville's theorem (Joseph Liouville, 1809-1882))**.** *If α is an algebraic irrational of degree $n \geq 2$. Then $\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}$ with $c(\alpha) > 0$.*

Corollary: $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental. (the rough idea is that if an irrational number is approximated too well then it is transcendental)

1.6 Sphere Packing

Denote balls: $B_r(x_0) := \{x : \|x - x_0\| \leq r\}$.

Definition 1.6.1. *A sphere packing* is a (usually infinite) collection of balls $B_r(x_i)$ with the same radius with pairwise non-intersecting interiors.

The *density* of a sphere packing σ is defined as

$$\sigma = \limsup_{R\to\infty} \frac{\mathrm{vol}\,(B_R(0) \cap \bigcup_i B_r(x_i))}{\mathrm{vol}\, B_R(0)}$$

Generally we want to find the largest density of a sphere packing in $\mathbb{R}^n$. We know $n = 1, 2, 3, 8, 24$.

If centers x_i forms a lattice, then it is called a lattice (sphere) packing. For densest lattice packings, we know $n = 1, 2, 3, 4, 5, 6, 7, 8$, and 24.

<u>REMARK/EASY EXERCISE</u> If $\{x_i\}$ forms a lattice $\Lambda \subset \mathbb{R}^n$, $\sigma(\Lambda) = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)} \frac{\rho^n}{\det \Lambda}$ where ρ is called the packing radius, which is defined by $\rho(\Lambda) = \frac{1}{2} \min_{x\in\Lambda\setminus\{0\}} \|x\|$. If $\Lambda_1 \sim \Lambda_2$ then $\sigma(\Lambda_1) = \sigma(\Lambda_2)$.

For $n = 1, \sigma(\Lambda) = 1$.

For $n = 2, \rho(\mathbb{Z}^2) = \frac{1}{2}, \det \mathbb{Z}^2 = 1, \sigma(\mathbb{Z}^2) = \frac{\pi}{4}$. $\rho(A_2) = \frac{\sqrt{2}}{2}, \det A_2 = \sqrt{3}, \sigma(A_3) = \pi \frac{1}{2\sqrt{3}}$. (locally denest) (Best lattice packing by Gauss, best packing overall by Laselo Fejes Toth (1915-2005))

For $n = 3, \Lambda = A_3 = D_3, \rho(\Lambda) = \frac{\sqrt{2}}{2}, \det \Lambda = 2, \sigma(\Lambda) = \frac{4\pi}{3} \frac{1}{4\sqrt{2}} = \frac{\pi}{3\sqrt{2}}$. (not locally denest) (Best lattice packing by Gauss, best packing overall by T.Hales (1958-))

There is a continuum of non-equivalent non-lattice densest packings.

12 balls touching the ball of the same radius.

For $n = 4$ compare A_4, D_4.

$\rho(A_4) = \rho(D_4) = \frac{\sqrt{2}}{2}$. $\det A_4 = \sqrt{5}$. And $\det D_4 = 2 < \sqrt{5}$.

$\sigma(D_4) = \frac{\pi^2}{2} \frac{1}{8} = \frac{\pi^2}{16} \approx 0.617$.

Densest lattice packing (Korkin Zolotaren) 24 vectors of length $\sqrt{2} = (\pm 1, 0, \pm 1, 0)$, 24 balls touching central ball (cannot have more by musin, 2008)

For $n = 5$, consider D_5

$\rho(D_5) = \frac{\sqrt{2}}{2}, \det D_5 = 2$. $\sigma(D_5) = \frac{\pi^2}{15\sqrt{2}} \approx 0.465$.

Densest lattice packing (Korkin Zolotaren), 40 balls touching central ball.

For $n = 8$, consider E_8.

$\rho(E_8) = \frac{\sqrt{2}}{2}, \det E_8 = 1, \sigma(E_8) = \frac{\pi^4}{24} \frac{1}{16} = \frac{\pi^4}{384} \approx 0.254$. Densest lattice packing(Blichfeldt), densest overall(M. Vyazovska, 1984-)

240 vectors of length $\sqrt{2}$: $(\pm 1, 0, \pm 1, 0, \dots)\left(-\frac{1}{2}, -\frac{1}{2}, \dots\right)$ with an even number of $-\frac{1}{2}$ turned into positive ones.

240 balls touching the central ball, cannot fir more (Odlyzko and sloane, 1979) (it is rigid)

For $n = 7$, $\rho(D_7) = \frac{\sqrt{2}}{2}, \det D_7 = 2$. $\rho(E_7) = \frac{\sqrt{2}}{2}, \det E_7 = \sqrt{2}$.

$\sigma(E_7) = \frac{\pi^3}{105} \approx 0.292$. Densest lattice (Blichfeldt), not rigid.

For $n = 6$, $\rho(D_7) = \frac{\sqrt{2}}{2}, \det D_7 = 2$. $\rho(E_7) = \frac{\sqrt{2}}{2}, \det E_7 = \sqrt{3}$.

$\sigma(E_7) = \frac{\pi^3}{48\sqrt{3}} \approx 0.373$. Densest lattice (Blichfeldt)

1.7 Leech Lattice

John Leech, 1926-1992

Consider $\mathbb{R}^{26}$, number coordinates, $D_{26} \subset \mathbb{Z}^{26} : \sum_{k=0}^{2} 5 \equiv 0 \pmod 2$

$u = \left(\frac{1}{2}, \dots, \frac{1}{2}\right)$.

$D_{26}^{+} = D_{26} \cup (D_{26} + u)$

$$\sum_{k=0}^{24} = k^2 = 4900 = 70^2.$$

(No other integer satisfies this afterwards)

$w_+ = (0, 1, \dots, 24, 70), w_- = (0, 1, \dots, 24, -70), W_+, W_- \in D_{26}$. $\sum_{k=0}^{24} \pm 70 = \frac{25 \cdot 24}{2} \pm 60 \equiv 0 \pmod 2$.

Look at the hyperplane $H \subset \mathbb{R}^{26} = \{x : \langle x, w_- \rangle = 0\}$.

$\Lambda_{25} = D_{25}^{+} \cap H$ is a lattice of rank 25. We see that w_+ lies in the lattice. Take $L = w_+^{\perp} \subset H, \dim L = 24$. Define Λ_{24} to be the orthogonal projection of Λ_{25} onto L.

Λ_{24} is discrete because $\operatorname{span}(w_+) \subset H$ is a lattice subspace.

Λ_{24} is the Leech lattice.

Useful formula for the length.

Pick $(x_0, x_1, \dots, x_{25})$ in Λ_{25}, what is the length of projection in Λ_{24}?

Let $\widehat{x} \in \Lambda_{24}$ be the projection: $\widehat{X} = x - \alpha w_+$ so that $\langle \widehat{x}, w_+ \rangle = 0$. So $\langle x, w_+ \rangle - \alpha \langle w_+, w_+ \rangle = 0 \implies \frac{\langle x, w_+ \rangle}{\langle w_+, w_+ \rangle}$.

$\|\widehat{x}\|^2 = \|x\|^2 - \|\alpha w_+\|^2 = \|x\|^2 - \frac{\langle x, w_+ \rangle^2}{\langle w_+, w_+ \rangle}$

$x \in \Lambda_{25} \subset H \implies \langle x, w_- \rangle = 0$. $w_+ = w_- + 140 \implies \langle x, w_+ \rangle = \langle x, w_- \rangle + 140 x_{25} =$

$140x_{25}$.

$\|\widehat{x}\|^2 = \sum_{k=0}^{25} x_k^2 - \frac{140^2 x_{25}^2}{\sum_{k=0}^{24} k^2+70^2} = \sum_{k=0}^{25} x_k^2 - 2\cdot x_{25}^2 = \sum_{k=0}^{24} x_k^2 - x_{25}^2$.

Some shortest non-zero vectors in Λ_{24}. $x = (0,1,-1,-1,1,0,\dots,0) \in D_{25} \subset D_{26}^+$. $\langle x, w_-\rangle = 0+1-2-3+4 = 0 \implies x \in \Lambda_{25}$, also $\langle x, w_+\rangle = 0+1-2-3+4 = 0 \implies x \in \Lambda_{24}, \|x\| = 2$.

Pick $y = \left(\frac{1}{2}, \underbrace{-\frac{1}{2},\dots,-\frac{1}{2}}_{\text{9 times}}, \underbrace{\frac{1}{2},\dots,\frac{1}{2}}_{\text{15 times}}, \frac{3}{2}\right)$. $y - u \in D_{26} \implies y \in D_{26}^+$.

$\langle y, w_-\rangle = 0, \|\widehat{y}\|^2 = \sum_{k=0}^{24} \frac{1}{4} - \frac{9}{4} = \frac{25-9}{4} = 4$.

There are 196560 vectors of length 2. (<- many balls touching the central ball) cannot put more (Odlyzko & Sloane, 1979) and this configuration is rigid.

Rigid phenomenon in dim 2, 8, and 24.

EXERCISES

1. $\det D_{26} = 2, \det D_{26}^+ = 1, \det \Lambda_{25} = 70\sqrt{2}, \det \Lambda_{24} = 1$.
2. For any $x \in \Lambda_{24}$, $\|x\|^2$ is an even integer.
3. $\min_{x\in\Lambda_{24}\setminus 0} \|x\| = 2$.
4. $\Lambda_{24}^* \cong \Lambda_{24}$.

What happens if $n = \dim V$ is large?

Gilbert-Varshamov Bound (E.N. Gilbert, 1923-2013, R.R Varshamov, 1927-1999)

Theorem 1.7.1. *THere is a sphere packing in $\mathbb{R}^n$ of density $\geq 2^{-n}$.*

Proof. Consider a saturated packing (young cannot add another ball to the poacking) of balls of radius 1.

Claim: its density $\geq 2^{-n}$.

Why? If $\bigcup_{i\in I} B(x,1)$ is saturated then $\bigcup_{i\in I} B(x_i,2) = \mathbb{R}^n$.

If it does not cover, say point $y \in \mathbb{R}^n$. We can add a ball $B(y)$ to the packing. If $x_i \in B_{R-1}(0)$ then $B_1(x_i) \subset B_R(0)$. If $B_2(x_i) \cap B_{R-3}(0) \neq \emptyset$ then $x_i \in B_{R-1}$.

$$\sum_{x_i\in B_{R-1}(0)} \operatorname{vol} B_2(x_i) \geq \operatorname{vol} B_{R-3}(0) \implies \sum_{x_i\in B_{R-1}} 2^n \operatorname{vol} B_1(x_i) \geq \operatorname{vol} B_{R-3}(0).$$

Hence

$$\operatorname{vol}\left(B_R(0)\cap\bigcup_i B_1(x_i)\right)\geq\sum_{x_i\in B_{R-1}\operatorname{vol}B_1(x_i)\geq 2^{-n}\operatorname{vol}B_{R-3}}\quad(0)$$

Take $R\to\infty$. ■

1.8 Lattice Packings

We will prove "today" for any $0<\alpha<2^{-n}$ there is a lattice $\Lambda\subset\mathbb{R}^n$ with $\sigma(\Lambda)\geq a$. Later in this course $\sigma(\Lambda)\geq 2^{-n}$.

Real Minkowski-Hlawka theorem is $\sigma(\Lambda)\geq 2\cdot\zeta(n)2^{-n}$ (assuming $n>1$) where $\zeta(n)=\sum_{k=1}^{\infty}\frac{1}{k^n}$.

What's known: There is a lattice $\Lambda\subset\mathbb{R}^n\sigma(\Lambda)\geq 1.68n2^{-n}$ (Davenport-Rogers, 1947)

$\sigma(\Lambda)\geq 2(n-1)\zeta(n)2^{-n}$ (K. Ball, 1992)

$\sigma(\Lambda)\geq\frac{1}{2}(n\ln\ln n)2^{-n}$ for infinitely many n. (Venkatesh, 2013)

What's going on with packing radius? Say we scale to $\det\Lambda=1$.

$$\sigma(\Lambda)=\frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)\frac{\rho^n(\Lambda)}{\det\Lambda}}\geq 2^{-n}$$

$$\implies\rho(\Lambda)\geq\frac{1}{2}\frac{\left(\Gamma\left(\frac{n}{2}+1\right)\right)^{1/n}}{\sqrt{\pi}}\approx\frac{\sqrt{\pi}}{2\sqrt{2\pi e}}$$

$\min_{x\in\Lambda\setminus\{0\}}\|x\|\geq\sqrt{\frac{n}{2\pi e}}$. Try to construct explicitly a lattice in $\mathbb{R}^n$ of $\det\Lambda=1$ with $\min_{x\in\Lambda\setminus\{0\}}\|x\|\geq 10^{-9}\sqrt{n}$.

So the lower bound is not that trivial.

Now we go back to our theorems.

Theorem 1.8.1. *For any $0<\alpha<2^{-n}$ there is a lattice $\Lambda\subset\mathbb{R}^n$ with $\sigma(\Lambda)\geq a$. Later in this course $\sigma(\Lambda)\geq a$.*

This theorem can be deduced from the following theorem:

Theorem 1.8.2. *If $M\subset\mathbb{R}^n$ is a bounded Jordan-measurable set of $\operatorname{vol}M<1$. Then there is a lattice $\Lambda\subset\mathbb{R}^n$ such that $\det\Lambda=1$ and $M\cap(\Lambda\setminus\{0\})=\emptyset$.*

Proof. Pick $\alpha>0$ so small that

1. $M\cap\{x_n=0\}$ It is entirely contained in the cube $|x_i|<\alpha^{-\frac{1}{\alpha-1}}, i=1,\ldots,n-1$.

2. Let $H_k = \{x_n = k\alpha, k \in \mathbb{Z}\}$.

$$\alpha \sum_{k=-\infty}^{\infty} \operatorname{vol}_{n-1}(M \cap H_k) < 1.$$

Define the lattice Λ as follows: pick the first $n-1$ basis vectors $u_i = \alpha^{-\frac{1}{n-1}} e_i$ for $i = 1, \ldots, i-1$. Let Π be the fundamental parallelepiped of $u_1, \ldots, u_{n-1}$ for $x \in \Pi$, let $u_n(x) = \alpha e_n + x$ and let Λ_x be the lattice with basis $u_1, \ldots, u_{n-1}, u_n(x)$.

$$\det \Lambda(x) = \operatorname{vol} \Pi \cdot \alpha = \left(\alpha^{-\frac{1}{n-1}}\right)^{n-1} \alpha = 1.$$

Claim: for some x, $|(\Lambda \setminus \{0\}) \cap M| = \emptyset$.

$$|(\Lambda \setminus \{0\}) \cap M| = \sum_{k \in \mathbb{Z} \setminus \{0\}} |M \cap (\Lambda_0 + kx)|$$

$$\begin{aligned} \frac{1}{\operatorname{vol} \Pi} \int_{x \in \Pi} |M \cap (\Lambda(x) \setminus \{0\})| \, \mathrm{d}x &= \alpha \sum_{k \in \mathbb{Z} \setminus \{0\}} \int_{\Pi} |M \cap (\Lambda_0 + kx)| \, \mathrm{d}x \\ &= \alpha \sum_{k=-\infty}^{\infty} \operatorname{vol}_{n-1}(M \cap H_k) < 1. \end{aligned}$$

So for some x we have $(\Lambda(x) \setminus \{0\}) \cap M = \emptyset$. ■

Choose $M = B_r(0)$ such that $\operatorname{vol} B_r(0) = 2^n \cdot a < 1$. Construct a lattice $\Lambda \cap B_r(0) = 0$ and $\det \Lambda = 1$. The $\min_{x \in \Lambda \setminus \{0\}} \|x\| \geq r \implies \rho(\Lambda) \geq \frac{r}{2}$. Then

$$\sigma(\Lambda) \geq \left(\frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)} r^n\right) 2^{-n} = a$$

Lemma 1.8.1. *Let $M \subset V$ be a Lebesgue measurable. Let $\Lambda \subset V$ be a lattice. Let Π be a fundamental parallelepiped of Λ. Define $f : V \to \mathbb{R}$ by $f(x) = |M \cap (x + \Lambda)|$. Then*

$$\int_{\Pi} f(x) \, \mathrm{d}x = \operatorname{vol} M$$

Proof. For $u \in \Lambda$. Let $f_a(x) = \mathbf{1}_M(x+u)$, $f(x) = \sum_{u \in \Lambda} f_u(x)$. So

$$\int_{\Pi} f(x) \, \mathrm{d}x = \sum_{u \in \Lambda} \int_{\Pi} f_u(x) \, \mathrm{d}x = \sum_{u \in \lambda} \operatorname{vol}((\Pi + u) \cap M)$$

$\Pi + u$ covers V without holes $\implies \sum_{u\in\lambda} \text{vol}((\Pi + u) \cap M) = \text{vol}\, M$. ■

Lemma 1.8.2.

$$\int_\Pi |M \cap (x + \Lambda)| \,\mathrm{d}x = \text{vol}\, M$$

Corollary 1.8.1. *For $k \in \mathbb{Z} \setminus \{0\}$, $\int_\Pi |M \cap (kx + \Lambda)| \,\mathrm{d}x = \text{vol}\, M$*

If $k > 0$, let $y = kx, x = k^{-1}y$.

$$\int_\Pi |M \cap (x + \Lambda)| \,\mathrm{d}x = \text{vol}\, M = k^{-n} \int_{k\Pi} |M \cap (y + \Lambda)| \,\mathrm{d}y$$

($k\Pi$ is the disjoint union of k^n lattice shifts of Π.)

For $k < 0$, make $y = -x$ and reduce to $k > 0$.

Some sharpening:

1. There exists $\Lambda \subset \mathbb{R}^n, \sigma(\Lambda) \geq 2^{-n}$ through compactness in the space of lattices
2. If M is symmetric, we can require instead that $\text{vol}\, M < 2$. (non-zero vectors come in pairs) $\implies \exists \Lambda, \sigma(\Lambda) \geq 2^{-n+1}$.
3. (Hlawka) If M is star shaped (for all $x \in M, [0, x] \subset M$) about 0 and $M = -M$. We can require $\text{vol}\, M < 2\zeta(n)$.

A lattice vector $u \in \Lambda \setminus \{0\}$ is primitive if you cannot write $u = mv$ for $v \in \Lambda, |m| \geq 2$.

1. If M is star shaped and contains a non-zero lattice point, then it contains a primitive lattice point.
2. The density of primitive points is $\frac{1}{\zeta(n)}$.

1.9 Fourier Transform

(J. Fourier, 1786-1830) Given $f : \mathbb{R}^n \to \mathbb{C}$ such that $\int_{\mathbb{R}^n} |f(x)| \,\mathrm{d}x, \int_{\mathbb{R}^n} |f(x)|^2 \,\mathrm{d}x < \infty$. We define

$$\widehat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi i\langle x,y\rangle} f(x) \,\mathrm{d}x \iff f(x) = \int_{\mathbb{R}^n} e^{2\pi i\langle x,y\rangle} \widehat{f}(y) \,\mathrm{d}y.$$

$\widehat{f} : \mathbb{R}^n \to \mathbb{C}$.

$f(x) = e^{-\pi\|x\|^2} \iff \widehat{f}(y) = e^{-\pi\|y\|^2}$.

Poisson summation formula: if $|f(x)| + \left|\widehat{f}(x)\right| \leq \frac{C}{(1+\|\cdot\|+\|\cdot\|)^{n+\delta}}$ with $c, \delta > 0$ (admissible). Then $\sum_{u\in\mathbb{Z}^n} f(u) = \sum_{u\in\mathbb{Z}^n} \widehat{f}(u)$.

Lemma 1.9.1. *If $f, \widehat{f} : \mathbb{R}^n \to \mathbb{C}$ are admissible and $\Lambda \subset \mathbb{R}^n$ is a lattice. Then*

$$\sum_{u \in \Lambda} f(u) = \det \Lambda \sum_{\ell \in \lambda^*}$$

Proof. Let $u_1, \dots, u_n$ be a basis of Λ and let $T : \mathbb{R}^n \to \mathbb{R}^n$ be linear such that $T(e_j) = u_j for j = 1, \dots, n$

SO $\Lambda = T(\mathbb{Z}^n)$. So $\sum i \in \Lambda f(u) = \sum_{u \in \Lambda} f(u) = f(u) = \sum_{u \in \Lambda} f(Tu)$.

Define

$$g(x) = f(Tx), \implies \sum_{u \in \Lambda} \sum_{u \in \Lambda} f(u) = \sum_{u \in \Lambda} = g(u) = \sum_{u \in \mathbb{Z}^n} \widehat{g}(u).$$

$$\widehat{g}(y) = \int_{R^n} e^{-2\pi i \langle y, x \rangle} g(x) \, \mathrm{d}x = \int_{\mathbb{R}^n} e^{-2\pi i \langle y, x \rangle} f(Tx) \, \mathrm{d}x.$$

Let $z = Tx$, then $\mathrm{d}x = \det T^{-1}$.

■

Theorem 1.9.1 (Cohn, Elkies, 2003)**.** *Suppose that there is an admissible function $f : \mathbb{R}^n \to \mathbb{R}$ such that $\widehat{f} : \mathbb{R}^n \to \mathbb{R}$ is also admissible and*

1. *$f(x) \leq 0$ for every $x \in \mathbb{R}^n$ such that $\|x\| > 1$.*
2. *$\widehat{f}(y) \geq 9$ for all $y \in \mathbb{R}^n$*

Then the density of a sphere packing in $\mathbb{R}^n \leq \frac{\pi^{11/2}}{\Gamma\left(\frac{n}{n+2}\right)} \frac{f(0)}{2^n} \widehat{f}0$

Proof. Let m = . ■

Proof. Sketch, for any, not necessarily lattice, packing

First, prove for periodic packings. (the centers written as $v_i + \Lambda$, $v_i, i = 1, \dots, N$ are distinct cosets $\mathbb{R}^n / \Lambda$ representatives) Scale the radius to $\frac{1}{2}$.

Consider the sum

$$S = \sum_{i,j=1}^{N} \sum_{u \in \Lambda} f(v_i - v_j + u).$$

If $i \neq j$ $v_i + u$ and v_j are different centers.

If $i = j$, $u \neq 0$, then $v_i + u$ and $v_j = v_i$ are different centers.

We have

$$\|v_i - v_j + u\| \geq 1 \text{ if } i \neq j \text{ or } i = j, u \neq 0$$

So $f(v_i - v_j + u) \geq 0$.

By Poisson, $\sum_{u\in\Lambda} f(v_i - v_j + u) = \frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*} e^{2\pi i\langle v_i - v_j, \ell\rangle}\widehat{f}(\ell)$.

$$\begin{aligned}
S &= \frac{1}{\det\Lambda}\sum_{i,j=1}^{N}\sum_{\ell\in\Lambda^*} e^{2\pi i\langle v_i - v_j,\ell\rangle}\widehat{f}(\ell)\\
&= \frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*}\widehat{f}(\ell)\sum_{i,j=1}^{N} e^{2\pi i\langle v_i - v_j,\ell\rangle}\\
&= \frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*}\widehat{f}(\ell)\sum_{i=1}^{N}\left|e^{2\pi i\langle v_i - v_j,\ell\rangle}\right|^2\\
&\geq \frac{1}{\det\Lambda}\widehat{f}(0)\cdot N^2.
\end{aligned}$$

Hence we have

$$\begin{gathered}
\frac{1}{\det\Lambda}N^2\widehat{f}(0) \leq S \leq Nf(0)\\
\implies Nf(0) \geq \frac{1}{\det\Lambda} \implies \frac{N}{\det\Lambda} \leq \frac{f(0)}{\widehat{f}(0)}
\end{gathered}$$

Take a large ball of volumn V, each coset $v_i + \Lambda$ contains roughly $\frac{V}{\det\Lambda}$. number of centers inside $\frac{NV}{\det\Lambda}$, each contributes volume $\frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}\frac{1}{2^n}$.

So the density

$$\frac{NV}{\det\Lambda}\frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}\frac{1}{2^n}\frac{1}{V} = \frac{N}{\det\Lambda}\frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}\frac{1}{2^n} \leq \frac{f(0)}{\widehat{f}(0)}\frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}\frac{1}{2^n}$$

For arbitrary packing: Claim: then density of an "arbitrary" packing can be approximated arbitrarily close by a periodic packing.

Why? Pick any dense packing with density $d > 0$. Consider a really large cube such that all balls inside that cube approximate the volume of the cube with density $\geq \sigma - \varepsilon$.

Now, tile $\mathbb{R}^n$ with lattice translates of the cube and balls inside. You get a periodic packing with density $\geq \sigma - \varepsilon$. ■

A bunch of useful results and methods by W Banaszczyk (1993).

Goal:

Theorem 1.9.2. *Pick any $\gamma > \frac{1}{2\pi}$, then for all sufficiently large $n \geq n_0(\gamma)$, for any lattice $\Lambda \subset \mathbb{R}^n$ such that* $\det\Lambda = 1$ *there is $u \in \Lambda \setminus \{0\}$ such that $\|u\| \leq \sqrt{\gamma n}$.*

Proof. Poisson:

$$\sum_{u\in\Lambda} f(u) = \frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*}\widehat{f}(\ell), \sum_{u\in\Lambda} e^{-\pi\|u\|^2} = \frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*} e^{-\pi\|\ell\|^2}$$

Lemma 1.9.2. *For* $0<\tau<1$,

$$\sum_{u\in\Lambda} e^{-\pi\tau\|u\|^2} \le \tau^{-n/2}\sum_{u\in\Lambda} e^{-\pi\|u\|^2}$$

Proof.

$$\begin{aligned}
\sum_{u\in\Lambda} e^{-\pi\tau\|u\|^2} &= \sum_{u\in\sqrt{\tau}\Lambda} e^{-\pi\|u\|^2} \\
&= \frac{1}{\det(\sqrt{n}\Lambda)}\sum_{\ell\in(\sqrt{\tau}\lambda)^*} e^{-\pi\|\ell\|^2} = \tau^{-n/2}\frac{1}{\det\Lambda}\sum_{\ell\in(\sqrt{\tau}\Lambda)^*} e^{-\pi\|\ell\|^2} \\
&= \tau^{-n/2}\frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*} e^{-\pi\|\ell\|^2/\tau} \\
&\le \tau^{-n/2}\frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*} e^{-\pi\|\ell\|^2} = \tau^{-n/2}\frac{1}{\det\Lambda}\sum_{u\in\Lambda} e^{-\pi\|u\|^2}
\end{aligned}$$

■

Lemma 1.9.3. *For any* $\gamma > \frac{1}{2\pi}$,

$$\sum_{u\in\Lambda, \|u\|\ge\sqrt{\gamma n}} e^{-\pi\|u\|^2} \le \left(e^{-\pi\gamma+\frac{1}{2}}\sqrt{2\pi\gamma}\right)^n \sum_{u\in\Lambda} e^{-\pi\|u\|^2}$$

Proof. Choose $0<\tau<1$. (to be adjusted later)

$$\begin{aligned}
\sum_{u\in\Lambda, \|u\|\ge\sqrt{\gamma n}} e^{-\pi\|u\|^2} &\le e^{-\pi\tau\gamma n}\sum_{u\in\Lambda, \|u\|\ge\sqrt{\gamma n}} \sqrt{\gamma n} e^{-\pi\|u\|^2} e^{\pi\tau\|u\|^2} \\
&\le e^{-\pi\tau\gamma n}\sum_{u\in\Lambda} \sqrt{\gamma n} e^{-\pi\|u\|^2} e^{-\pi(1-\tau)\|u\|^2} \\
&\le e^{-\pi\tau\gamma n}(1-\tau)^{\frac{n}{2}}\sum_{u\in\Lambda} \sqrt{\gamma n} e^{-\pi\|u\|^2} e^{-\pi\|u\|^2}
\end{aligned}$$

Choose $\tau = 1-\frac{1}{2\pi\gamma}$. Then RHS $= \left(e^{-\pi\gamma+\frac{1}{2}}\sqrt{2\pi\gamma}\right)^n \sum_{u\in\Lambda}\sqrt{\gamma n} e^{-\pi\|u\|^2} e^{-\pi\|u\|^2}$ ■

Now, pick some $\frac{1}{2\pi} < \gamma' < \gamma$. Let $\alpha = \sqrt{\frac{\gamma'}{\gamma}} < 1$.

Consider lattice $\alpha\Lambda$. Apply lemma:

$$\sum_{\substack{u\in\alpha\Lambda\\ \|u\|=\sqrt{\gamma n}}} e^{-\pi\|u\|^2} \le \left(e^{-\pi\gamma'+\frac{1}{2}\sqrt{2\pi\gamma'}}\right)\sum_{u\in\alpha\Lambda} e^{-\pi\|u\|^2}$$

$$\sum_{\substack{u\in\alpha\Lambda\\ \|u\|=\sqrt{\gamma n}}} e^{-\pi\|u\|^2} \ge \left(1-e^{-\pi\gamma'+\frac{1}{2}\sqrt{2\pi\gamma'}}\right)\sum_{u\in\alpha\Lambda} e^{-\pi\|u\|^2}$$

From Poisson,

$$\begin{aligned}\sum_{u\in\alpha\Lambda} &= \frac{1}{\det(\alpha\Lambda)}\sum_{\ell\in(\alpha\Lambda)^*} e^{-\pi\|\ell\|^2} > \frac{1}{\det(\alpha\Lambda)}\\ &= \frac{1}{\alpha^n\det\Lambda} = \frac{1}{\alpha^n} > 1\end{aligned}$$

If n is large, there is $u\in\alpha\Lambda\setminus\{0\}$ with $\|u\|<\sqrt{\gamma' n} \implies$ there is $u\in\Lambda\setminus\{0\}$ with $\|u\|<\frac{\sqrt{\gamma' n}}{\alpha}=\sqrt{\gamma n}$. ■

Density of lattice packing:

$$\rho(\Lambda)\le\frac{1}{2}\sqrt{\gamma n}\approx\frac{1}{2}\sqrt{\frac{n}{2\pi}}$$

$$\begin{aligned}\sigma(\Lambda) &= \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}\frac{\rho(\Lambda)}{\det\Lambda} \approx \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}\frac{1}{2^n}\left(\frac{n}{2\pi}\right)^{\frac{n}{2}}\\ &\approx \frac{\pi^{n/2}}{\left(\frac{n}{2}\right)^{n/2}e^{-n/2}2^n}\left(\frac{n}{2\pi}\right)^{\frac{n}{2}} = \frac{e^{n/2}}{2^n}\approx(0.82)^n\to 0.\end{aligned}$$

<u>EXERCISE</u> We proved that $\sigma(\Lambda)\le(0.82)^n\approx\left(\frac{\sqrt{e}}{2}\right)^n$. Prove the same bound for any packing.

Prove for periodic packings first, then consider the sum $\sum_{i,j=1}^N e^{-\pi\|v_i-v_j+u\|}$.

1.10 Covering Radius

Definition 1.10.1. Suppose $\Lambda\subset V$ a lattice.

$$\mu(\Lambda)=\max_{x\in V}\operatorname{dist}(x,\Lambda)=\max_{x\in\Pi}\operatorname{dist}(x,\Lambda).$$

This is the smallest radius such that the Balls $B_r(u), u\in\Lambda$ cover V.

Thickness:

$$\liminf_{\text{vol of space} \to \infty} = \frac{\text{total volume of balls}}{\text{total volume of space}} \geq 1$$

We are generally interested in the thinnest lattices.

<u>EXERCISES</u> Find the covering radius of Z^n $\left(\frac{\sqrt{n}}{2}\right)$, A_n^* $\left(\frac{1}{2}\sqrt{\frac{n(n+2)}{3(n+1)}}\right)$, D_n $\left(\frac{\sqrt{n}}{2}\right)$ for $n \geq 4$, 1 for D_3, $E_8(1)$, Leech lattice (hard) $\sqrt{2}$.

If $u_1, \ldots, u_n$ are linearly independent then $\mu(\Lambda) \leq \frac{1}{3}\sum_{i=1}^n \|u_i\|$.

Definition 1.10.2. The global maximum of $x \to \operatorname{dist}(x, \Lambda)$ is called a deep hold of Λ, the local maximum is called a shallow hole.

<u>EXERCISE</u> Show that $(1,0,0)$ "octahedral hole" is a deep hole for D_3 and $\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$ "tetrahedral hole" is a shallow hole.

Main Goal: ("transference" theorem)

Theorem 1.10.1. *If $\Lambda \subset \mathbb{R}^n$ is a lattice then*

$$\frac{1}{4} \leq \mu(\Lambda)\rho(\Lambda^*) \leq \operatorname{const}(n)$$

We will eventually show that $\operatorname{const}(n) = \frac{n}{2}$. Elementary: $\operatorname{const}(n) = \frac{n^{3/2}}{4}$. (Lagarias)

First result: $\operatorname{const}(n) \approx (n!)^2$ (Khinchin)

Lower Bound:

Construct $u_1, \ldots, u_n \in \Lambda$ as follows: ("successive minima")

$$\|u_1\| = \min_{u \in \Lambda \setminus \{0\}} \|u\|$$
$$\|u_2\| = \min_{\substack{u \in \Lambda \\ u, u_1 \text{ linearly independent}}} \|u\|$$
$$\vdots$$

So $\|u_1\| \leq \|u_2\|, \ldots$.

Pick $x = \frac{1}{2}u_n$.

<u>CLAIM</u> $\operatorname{dist}(x, \Lambda) = \frac{1}{2}\|u_n\|$.

Suppose not. There is a $u \in \Lambda$ such that

$$\left\|\frac{1}{2}u_n - u\right\| < \frac{1}{2}\|u_n\| \implies \|u\| < \|u_n\| \implies u \in \operatorname{span}\{u_1, \ldots, u_{n-1}\}.$$

Then for $v = 2u - u_n$ we have

$$v \notin \operatorname{span}\{u_1, \dots, u_{n-1}\}, \|v\| = 2\left\|u - \frac{1}{2}u_n\right\| < \|u_n\|,$$

contradiction.

Now, pick $w \in \Lambda^*$ such that $\|w\| = 2\rho(\Lambda^+)$. We have for some $k = 1, \dots, n$, $\langle w_1, U_K \rangle \in \mathbb{Z}$ and $\neq 0 \implies |\langle w_1, U_K \rangle| = 1$.

$\implies \|w\| \|u_k\| \geq 1 \implies \|w\| \|u_n\| \geq 1$. So

$$2\rho(\Lambda^*) \cdot 2\mu(\Lambda) \geq 1 \implies \rho(\Lambda^*) \cdot \mu(\Lambda) \geq \frac{1}{4}$$

Upper bound (elementary) J.C. Lagarias, H.W. Lenstra Jr, C.-P. Schnorr (1990)

$$\sigma(\Lambda)\rho(\Lambda^*) \leq \frac{n^{3/2}}{4}.$$

Lemma 1.10.1. *Suppose $\Lambda \subset \mathbb{R}^n$ is a lattice then $\rho(\Lambda)\rho(\Lambda^*) \leq \frac{n}{4}$.*

Proof. Minkowski convex body (long time ago)

$$\rho(\Lambda) \leq \frac{1}{2}\sqrt{n}(\det\Lambda)^{\frac{1}{n}},\ \rho(\Lambda^*) \leq \frac{1}{2}\sqrt{n}(\det\Lambda^*)^{\frac{1}{n}}$$

$(\det\Lambda)(\det\Lambda^*) = 1$. Suppose $u_1, \dots, u_n$ is a basis of Λ, $u_1^*, \dots, u_n^*$ a basis of Λ^*. $\langle u_i^*, u_j \rangle = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$. ■

Proof. By induction on n.

Base case: $n = 1$, $\Lambda = \alpha\mathbb{Z}, \Lambda^* = \alpha^{-1}\mathbb{Z}$. $\mu(\Lambda) = \frac{1}{2}\alpha$ and $\rho(\Lambda^*) = \frac{1}{2\alpha}$. $\mu(\lambda)\rho(\Lambda^*) = \frac{1}{4}$.

Induction hypothesis

Induction step Pick $u \in \Lambda \setminus \{0\}$ so that $\|u\| = 2\rho(\Lambda)$. Let $\mathrm{pr} : \mathbb{R}^n \to H$ be the orthogonal projection. Let $\Lambda_1 = \mathrm{pr}(\Lambda)$.

<u>CLAIM</u> $\Lambda_1^* \subset \Lambda \implies \rho(\Lambda^*) \geq \rho(A^*)$ must check if $x \in H$ is such that $\langle x, \mathrm{pr}(v) \rangle \in \mathbb{Z}$ for all $v \in \Lambda$. Then $\langle x, v \rangle \in \mathbb{Z}$ for all $v \leq \Lambda$.

Pick any $x \in V$, need to bound $\operatorname{dist}(x, \Lambda)$. Let $y = \mathrm{pr}(x)$ choose $y_1 \in \Lambda_1$ closest to y so that $\|y_1 - y\| = \mu(\Lambda_1)$.

Look at the line through y_1 parallel to y. It contains points from Λ distance $\|u\| = 2\rho(\Lambda)$

apart.

Pick $w \in \Lambda$ so that $\|w - (x + y_1 - y)\| \leq \rho(\Lambda)$.

Use Pythagoras theorem, $\|w - x\|^2 \leq \rho^2(\Lambda) + \mu^2(\Lambda_1) \implies \mu^2(\Lambda) \leq \rho^2(\Lambda) + \mu^2(\Lambda_1)$.

So

$$\begin{aligned}\rho^2(\Lambda^*)\mu^2(\Lambda) &\leq \rho^2(\Lambda^*)\rho^2(\Lambda) + \mu^2(\Lambda_1)\rho^2(\Lambda^*)\\ &\leq \left(\frac{n}{4}\right)^2 + \mu^2(\Lambda_1)\rho^2(\Lambda_1^*)\end{aligned}$$

■

We can use Fourier to prove an optimal bound $\mathrm{const}(n) = \frac{n}{2}$.

Let's start with a lemma.

Lemma 1.10.2. *Suppose $\Lambda \subset V$ a lattice and $x \in V$. Then*

$$\sum_{u\in\Lambda} e^{-\pi\|x-u\|^2} \leq \sum_{u\in\Lambda} e^{-\pi\|u\|^2}.$$

Proof. Using Poisson summation,

$$\sum_{u\in\Lambda} f(u) = \frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*}\widehat{f}(\ell).$$

Choose $f(x) = e^{-\pi\|x\|^2}$ then $\widehat{f}(y) = e^{-\pi\|y\|^2}$. Choose $f(x) = e^{-\pi\|x-a\|^2}$ then $\widehat{f}(y) = e^{-2\pi i\langle y,a\rangle\|y\|^2}$. So

$$\begin{aligned}\sum_{u\in\Lambda} e^{-\pi\|x-u\|^2} &= \frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*} e^{-2\pi i\langle x,\ell\rangle\|\ell\|^2}\\ &\leq \frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*} e^{-\pi\|\ell\|^2} = \sum_{u\in\Lambda} e^{-\pi\|u\|^2}\end{aligned}$$

■

<u>EXERCISE</u>

1. See if you can find an elementary proof
2. $\sum_{u\in\Lambda} e^{-\pi\|x-u\|^2} \geq e^{-\|x\|^2}\sum_{u\in\Lambda} e^{-\pi\|u\|^2}$.

Lemma 1.10.3. *For $0 < \tau < 1, x \in V$.*

$$\sum_{u\in\Lambda} e^{-\pi\tau\|x-u\|^2} \leq \tau^{-n/2} \sum_{u\in\Lambda} e^{-\pi\|u\|^2}.$$

We had it with $x = 0$, with

$$\sum_{u\in\Lambda} e^{-\pi\tau\|x-u\|^2} \leq \sum_{u\in\Lambda} e^{-\pi\tau\|u\|^2}.$$

Rescale $\Lambda = \sqrt{\tau}\Lambda$ to get

$$\sum_{u\in\Lambda e^{-\pi}\|x-u\|^2} \leq \sum_{u\in\Lambda} e^{-\pi\|u\|^2}$$

Lemma 1.10.4. *If $\Lambda \subset \mathbb{R}^n$ is a lattice, $x \in \mathbb{R}^n$ is a point. For any $\gamma > \frac{1}{2\pi}$,*

$$\sum_{\substack{u\in\Lambda \\ \|u-x\|\geq\sqrt{\gamma n}}} e^{-\pi\|x-u\|^2} \leq \left(e^{-\pi\gamma+\frac{1}{2}}\sqrt{2\pi\gamma}\right)^n \sum_{u\in\Lambda} e^{-\pi\|u\|^2}.$$

Proof. Choose $0 < \tau < 1$ to be specified.

$$\begin{aligned}
\sum_{\substack{u\in\Lambda \\ \|u-x\|\geq\sqrt{\gamma n}}} e^{-\pi\|x-u\|^2} &\leq e^{-\pi\gamma n\tau} \sum_{\substack{u\in\Lambda \\ \|u-x\|\geq\sqrt{\gamma n}}} e^{-\pi\|x-u\|^2} e^{\pi\tau\|x-u\|^2} \\
&\leq e^{-\pi\gamma n\tau} \sum_{\substack{u\in\Lambda \\ \|u-x\|\geq\sqrt{\gamma n}}} e^{-\pi(1-\tau)\|x-u\|^2} \\
&\leq e^{-\pi\gamma n\tau}(1-\tau)^{-\frac{n}{2}} \sum_{u\in\Lambda} e^{-\pi\|u\|^2}.
\end{aligned}$$

Take $\tau = 1 - \frac{1}{2\pi\gamma}$. ∎

Corollary 1.10.1. *Take $\gamma = 1$,*

$$\sum_{\substack{u\in\Lambda \\ \|u-x\|\geq\sqrt{\gamma n}}} e^{-\pi\|x-u\|^2} \leq 5^{-n} \sum_{u\in\Lambda} e^{-\pi\|u\|^2}.$$

Now we have

Theorem 1.10.2.

$$\mu(\Lambda)\rho(\Lambda^*) \leq \frac{n}{2}$$

Proof. Suppose not. Then $\mu(\Lambda)\rho(\Lambda^*) > \frac{n}{2}$. If we scale $\Lambda := \alpha\Lambda, \alpha > 0$, $\mu(\alpha\Lambda) =$

$\alpha\mu(\Lambda), (\alpha\Lambda)^* = \frac{1}{\alpha}\Lambda^*, \rho((\alpha\Lambda)^*) = \frac{1}{\alpha}\rho(\Lambda^*)$.

Let's scale so that $\mu(\Lambda) > \sqrt{n}, \rho(\Lambda^*) > \frac{\sqrt{n}}{2} \implies$ there is $x \in V$ such that $\operatorname{dist}(x, \Lambda) > \sqrt{n}$.

Let $L = \sum_{u\in\Lambda} e^{-\pi\|u\|^2}, L^* = \sum_{\ell\in\Lambda^*} e^{-\pi\|\ell\|^2}$.

$$\sum_{u\in\Lambda} e^{-\pi\|x-u\|^2} = \sum_{\substack{u\in\Lambda \\ \|u-x\|\geq\sqrt{n}}} e^{-\pi\|x-u\|^2} \leq 5^{-n}L.$$

$$L^* = 1 + \sum_{\ell\in\Lambda^*\setminus\{0\}} e^{-\pi\|\ell\|^2} = 1 + \sum_{\ell\in\Lambda^*\|\ell\|\geq\sqrt{n}} e^{-\pi\|ell\|^2} \leq 1 + 5^{-n}L^*$$

This $\implies (1-5^{-n})L^* \leq 1 \implies L^* \leq \frac{1}{1-5^{-n}} = \frac{5^n}{5^n-1}$.

We also have

$$\sum_{\ell\in\Lambda^*\setminus\{0\}} e^{-\pi\|\ell\|^2} = L^* - 1 \leq \frac{1}{5^n-1}.$$

By Poisson, $L = \frac{1}{\det\Lambda}L^*$.

Finally, getting a contradiction

$$\sum_{u\in\Lambda} e^{-\pi\|x-u\|^2} \leq 5^{-n}L = \frac{L^*}{5^n\det\Lambda} \leq \frac{1}{\det\Lambda}\frac{1}{5^n-1}.$$

On the other hand, by Poisson summation:

$$\sum_{u\in\Lambda} e^{-\pi\|x-u\|^2} = \frac{1}{\det\Lambda}\sum_{\ell\in\Lambda^*} e^{2\pi i\langle\ell,x\rangle}e^{-\pi\|\ell\|^2}$$

$$\sum_{\ell\in\Lambda^*} e^{2\pi i\langle\ell,x\rangle}e^{-\pi\|\ell\|^2} = 1 + \sum_{\ell\in\Lambda^*\setminus\{0\}} e^{2\pi i\langle\ell,x\rangle}e^{-\pi\|\ell\|^2} \geq 1 - \sum_{\ell\in\Lambda^*\setminus\{0\}} e^{-\pi\|ell\|^2} \geq 1 - \frac{1}{5^n-1}$$

So we have

$$\begin{aligned}\frac{1}{\det\Lambda}\frac{1}{5^n-1} &\geq \frac{1}{\det\Lambda}\frac{5^n-2}{5^n-1} \\ \iff \frac{1}{5^n-1} &\leq \frac{5^n-2}{5^n-1} \\ \iff 5^N &\leq 3\end{aligned}$$

a contradiction. So we have proved the argument. ■

Later:

Corollary 1.10.2 (Flatness theorem)**.** *If $A \subset \mathbb{R}^n$ is convex, $A \cap Z^n = \emptyset$. Then there is*

$a \in \mathbb{Z}^n \setminus \{0\}$ *such that* $\max_{x \in A} \langle a, x \rangle - \min_{x \in A} \langle a, x \rangle \leq c(n)$.

General case exercises:

1. Fill in gaps on ellipsoidal approximations
2. if $K = -K$, $E \subset K$ the maximum volumn ellipsoid then $E \subset K \subset \sqrt{n}E$.
3. (Easy) If $P \subset \mathbb{R}^2$ is a convex polygon with interger vertices and no other integer points other than vertices. Then there is a $u \in \mathbb{Z}^2$ such that $\max_{x \in P} \langle u, x \rangle - \min_{x \in P} \langle u, x \rangle = 1$.
4. (Hard) If $P \subset \mathbb{R}^3$ is a convex polytope with integer vertices and no other integer points then there is $u \in \mathbb{Z}^3$ such that $\max_{x \in P} \langle x, u \rangle - \min_{x \in P} \langle x, u \rangle \leq 1$.

1.11 Existence of a Good Basis

Existence of a good ("nearly orthogonal") basis

$u_1, u_2, \ldots, u_n$ is a basis of Λ then $\|u_1\| \cdot \ldots \cdot \|u_n\| \leq \mathrm{const}(n) \det \Lambda$. For $n = 2, c(2) = \frac{2}{\sqrt{3}} \approx 1.15$. We will prove roughly $c(n) \approx n^n$.

Constuct such a basis efficiently (LLL) $c(n) \approx 2^{n^2}$.

Theorem 1.11.1 (2nd Minkowski convex body theorem)**.** *Let K be a convex body, $K \subset \mathbb{R}^n$ convex compact with non empty interior. Suppose that $K = -K$. Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Define successive minima: for $i = 1, \ldots, n, \Lambda_i = \lambda_i(K) = \min \{\lambda > 0 : \dim \mathrm{span}(\lambda K \cap \Lambda) \geq i\}$ min $\lambda > 0$ such that λK contains (at least) i linearly independent lattice vectors.*

$$\lambda_1(K) \leq \lambda_2(K) \leq \ldots \leq \lambda_n(K)$$

Then

$$(\mathrm{vol}\, K) \prod_{i=1}^{n} \lambda_i(K) \leq 2^n \det \Lambda$$

Plan:

We reduce it to the case $\Lambda = \mathbb{Z}^n$

Pick the fundamental parallelepiped $\Pi = \{x = (x_1, \ldots, x_n) : 0 \leq x_i < 1\}$ and stare ar the projection $\mathbb{R}^n / \mathbb{Z}^n \to \Pi$.

$P : (x_1, \ldots, x_n) \mapsto (\{x_1\}, \ldots, \{x_n\})$ and prove various things about it.

some notes missing

Last time: If $\Lambda \subset \mathbb{R}^n$ is a lattice then there is a basis $u_1, \ldots, u_n$ such that $\|u_1\| \ldots \|u_n\| \leq$

$c(n)\det\Lambda$,

$$c(n)=\frac{(n+1)!\Gamma\left(\frac{n}{2}+1\right)}{\pi^{n/2}}$$

Convergence: If $\{\Lambda_k\subset\mathbb{R}^n\}, k=1,\ldots$ are lattices and $\Lambda\subset\mathbb{R}^n$ is a lattice. We say that $\lim_{k\to\infty}\Lambda_k=\Lambda$ is we can find a basis $u_{k_1},\ldots,u_{kn}$ of Λ_k and a basis $u_1,\ldots,u_n$ of Λ so that $\lim_{k\to\infty}u_{ki}=u_i$ for $i=1,\ldots,n$.

Mahler Compactness Criterion: (K. Mahler, 1903 - 1988) If $\Lambda_i\subset\mathbb{R}^n, i\in I$ is an infinite family of lattices, and for some $c>0, C>0$ we have $\det\Lambda_i\le C$ abd $\rho(\Lambda_i)\ge c$ for all $i\in I$. Then there is a sequence Λ_{i_k} such that $\lim_{k\to\infty}\Lambda_k=\Lambda$.

<u>EXERCISE</u>: If $\lim_{n\to\infty}\Lambda_n=\Lambda$ then $\lim_{n\to\infty}\rho(\Lambda_n)=\rho(\Lambda)$.

In Minkowski-Hlawka, we showed that for every $0<\alpha<2^{-n}$ there is $\Lambda_a\subset\mathbb{R}^n$ such that $\sigma(\Lambda_a)\ge a$. We can choose $\det\Lambda_a=1$ and Mahler compactness so there is a limit lattice Λ as $a\to2^{-n}$ with $\sigma(\Lambda)\ge2^{-n}$.

(Weakly) reduced basis

Say, $u_1,\ldots,u_n$ is a basis of Λ. Let $L_0=\backslash 0$. $L_k=\operatorname{span}\{u_1,\ldots,u_k\}, k=1,\ldots,n$. Let w_k be the orthogonal projection of u_k onto $L_{k-1}^{\perp}$. $w_1,\ldots,w_k,w_n$ is the Gram-Schmidt orthogonalization (without normalization) of $u_1,\ldots,u_n$. Then $u_k=w_k+\sum_{i=1}^{k-1}\alpha_{ki}w_i, k=1,\ldots,n$.

We say that $u_1,\ldots,u_n$ is (weakly) reduced, provided $|\alpha_{ki}|\le\frac{1}{2}$ for all k and i.

How to reduce a basis quickly. If all $|\alpha_{ki}|\le\frac{1}{2}$ already reduced. If not, choose the largest I such that $|\alpha_{ki}|>\frac{1}{2}$. Let m_i be the integer closet to α_{ki} then $|\alpha_{ki}-m_i|\le\frac{1}{2}$. Update $u_k:=u_k-m_iu_i$. What happens? $L_0,\ldots,L_n$ do not change. $\alpha_{ki}\mapsto\alpha_{ki}-m_i$. Now $|\alpha_{ki}|\le\frac{1}{2}$ may messup α_{ki} with $j<i$.

Repeat. In at most $\binom{n}{2}$ steps, we'll have it reduced.

Theorem 1.11.2 (Lagarias, Lenstra, Schnorr, 1990). *If $\Lambda\subset\mathbb{R}^n$, and $u_1,\ldots,u_n$ is a (weakly) reduced Korkin-Zolotarev basis. Then $\|u_k\|\le\frac{\sqrt{k+3}}{2}\lambda_k, k=1,\ldots,n$, where λ_k is the k-th successive minimum w.r.t unit ball.*

Remark.

1. Korkin-Zorotarev basis. Choose u_1 to be the shortest non-zero, u_2 to be closest to $L_1=\operatorname{span}\{u_1\}$ and not in L_1 ...Choose u_k closest to L_{k-1} but not in L_{k-1}.
2. The reduction procedure does not change $w_1,\ldots,w_k,\ldots,w_n$ and does not change $\operatorname{dist}(u_k,L_{k-1})=\|w_k\|$. Starting with K-Z basis we still get K-Z basis.
3. $\lambda=\min\{\lambda>0,\dim\operatorname{span}\{\lambda\cap\{x,\|x\|\le\lambda\}\}\ge K\}$.

Compared to the basis we constructed last time

1. last time we had $\|u_k\| \le \frac{k+1}{2}\lambda_k$ for $k = 1, \dots, n$. which gave $c(n) = \frac{(n+1)!\Gamma\left(\frac{n}{2}+1\right)}{\pi^{n/2}}$. Now we have $c(n) = \frac{\sqrt{(n+3)!}\Gamma\left(\frac{n}{2}+1\right)}{\sqrt{6}\pi^{n/2}}$, which is better.

Proof. <u>CLAIM</u> $\|w_k\| \le \lambda_k$ for $k = 1, \dots, n$. Why? $\|w_k\| \leftarrow$ smallest distance from a point in Λ which is not in L_{k-1} to L_{k-1}. (Krokin-Zolotarev) Let Λ_k' be the orthogonal projection of Λ onto $L_{k-1}^{\perp}$, then $\|w_k\| = \min_{v \in \Lambda_k' \setminus \{0\}} \|v\|$. Pick linearly independent $v_1, \dots, v_k$ such that $\|v_i\| \le \lambda_k$ for $i = 1, \dots, k$, so $\|w_k\| \le \|v\| \le \lambda_k$. The projection v of at least one of them onto $L_{k-1}^{\perp}$ will be non-zero.

<u>REDUCED</u> $\|u_k\|^2 = \|w_k\|^2 + \sum_{i=1}^{k-1} |\alpha_{ki}|^2 \|w_i\|^2 \le \lambda_k^2 + \sum_{i=1}^{k-1} \frac{1}{4}\lambda_i^2 \le \lambda_k^2 \left(1 + \frac{k-1}{4}\right) = \lambda_k^2 \frac{k+3}{4} \implies \|u_k\| \le \frac{\sqrt{k+3}}{4}$. ■

Certifying packing radius Given a Λ and $u_1, \dots, u_n$ a basis. Then $2\rho(\Lambda) \ge \min_{k=1,\dots,n} \mathrm{dist}_{u_k, L_{k-1}}$.

We will construct a basis such that $2\rho(\Lambda) \le n \min_{k=1,\dots,n} \mathrm{dist}(n_k, L_{k-1})$.