

# Notes for Math 669

Yiwei Fu, Instructor: Alexander Barvinok

WN 2023

# Contents

<b>1</b>	<b>Introduction to Lattices</b>	<b>1</b>
1.1	Definition . . . . .	1
1.2	Lattice and Its Basis . . . . .	1
1.3	Sublattice . . . . .	4
1.4	Minkowski Theorem . . . . .	7
1.5	Applications of Minkowski's Theorem . . . . .	9
1.6	Sphere Packing . . . . .	13
1.7	Leech Lattice . . . . .	14
1.8	Lattice Packings . . . . .	16
1.9	Fourier Transform . . . . .	19

Office hours:

# Chapter 1

## Introduction to Lattices

### 1.1 Definition

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

1.  $\text{span}(\Lambda) = V$ .
2.  $\Lambda$  is an additive subgroup.
3.  $\Lambda$  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  $L = \text{span}(L \cap \Lambda)$

**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  $L \in \text{span}\{u_1, \dots, u_m\}$  linearly independent vectors,  $\Pi = \{\}$  There is  $u \in \Lambda \setminus L$  such that  $\text{dist}(u, \Pi) \leq \text{dist}(x, \Pi)$  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  $\Pi$ . ■

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

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

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

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  $\Lambda$ .

Then  $u$  is a basis of  $\Lambda$ . 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  $u_1, \dots, u_{n-1}$ . Pick  $u_n$  such that  $u_n \notin H$  and  $\text{dist}(u_n, H)$  is the smallest. We claim that  $u_1, \dots, u_{n-1}, u_n$  is a basis of  $\Lambda$ .

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  $\alpha_1, \dots, \alpha_{n-1} \in \mathbb{Z}$ . 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

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

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

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

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

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

EXERCISE Suppose  $u_1, \dots, u_n \in V$  is a basis of subspace. The integer combinations form a lattice.

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

EXERCISE If  $\Lambda$  is a lattice and  $L$  is a lattice subspace. The orthogonal projection  $\text{PR} : V \rightarrow L^\perp$ . Then  $\text{PR}(\Lambda) \subset L^\perp$  is a lattice.

**Definition 1.2.1.** Suppose  $u_1, \dots, u_n$  be a basis of  $\Lambda$ .

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

is the *fundamental parallelepiped* of a fundamental parallelepiped of  $\Lambda$ .

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

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

We start with a lemma:

**Lemma 1.2.1.** Let  $\Pi$  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:  $\Pi$  is the fundamental parallelepiped for  $u_1, \dots, u_n$ . 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  $y_2 - y_1 = \sum_{i=1}^n (\alpha_i - \beta_i) u_i$ . 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  $\text{vol } X_r = |B_r \cap \Lambda| \text{vol } \Pi$ .

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

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

This goes to 1 when  $r \rightarrow \infty$ . ■

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

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

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

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

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

EXERCISE  $(\det \Lambda)(\det \Lambda^*) = 1$

### 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.  $\Lambda_0$  is then called a sublattice of  $\Lambda$ .

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

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

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

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

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

*Proof.* 1. By Lemma 1.2.1, every coset has a unique representation in  $\Pi$ .

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

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

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

$$\lim_{r \rightarrow \infty} \frac{|B_r \cap (u + \Lambda_0)|}{\text{vol } B_r} = \frac{1}{\det \Lambda_0}. \implies \frac{1}{\det \Lambda} = |S| \frac{1}{\det \Lambda_0} \quad \blacksquare$$

EXERCISE

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  $a_1, \dots, a_n$  are coprime integers not all 0.

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

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

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

*then  $u_1, \dots, u_n$  is a basis.*

*Proof.* Look at

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

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

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

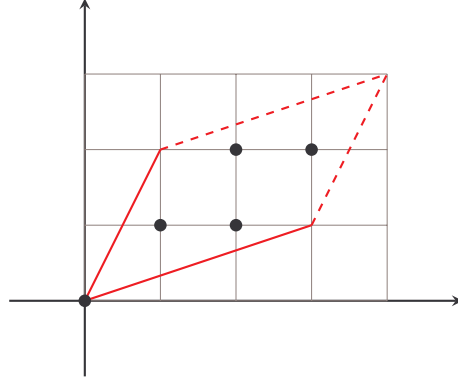
$$\Pi = \left\{ \sum_{i=1}^n \alpha_i u_i : 0 \leq \alpha_i < 1 \right\}.$$

Then

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

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

Suppose  $n = 2$ ,  $u_1 = (3, 1)$ ,  $u_2 = (1, 2)$ . Then  $\text{vol } \Pi = 5$ . 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. ■

EXERCISE 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.

EXERCISE 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.

EXERCISE Suppose  $u_1, \dots, u_k \in \mathbb{Z}^n$  are linearly independent vectors and  $\Lambda = \mathbb{Z}^n \cap \text{span}(u_1, \dots, u_k)$ . The  $\{u_1, \dots, u_k\}$  is a basis of  $\Lambda$  if and only if the great common divisor

of all  $k \times k$  minors of  $\begin{bmatrix} u_1^T \\ u_2^T \\ \vdots \\ u_k^T \end{bmatrix}$  is 1.

Linear algebra (Smith normal form, will not use)

If  $\Lambda_0 \subset \Lambda$  is a sublattice, then there is a basis  $u_1, \dots, u_n$  of  $\Lambda$  and a basis  $v_1, \dots, v_n$  of  $\Lambda_0$  such that  $v_i = m_i u_i$  for positive integer  $m_i$  and such that  $m_1$  divides  $m_2$  which divides  $m_3, \dots$



## 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  $\forall x, y \in A, [x, y] \subset A$  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  $\text{vol } A > 2^{\dim V} \det \Lambda$ . Then there is  $u \in \Lambda \setminus \{0\}$  such that  $u \in A$ .

2<sup>dim V</sup> IS SHARP: Pick  $\mathbb{Z}^n \subset \mathbb{R}^n, \det \mathbb{Z}^n = 1$ . Let  $A = \{-1 < x_i < 1, i = 1, \dots, n\}$  convex and symmetric. Then  $\text{vol } A = 2^n$  and  $A \cap \mathbb{Z}^n = \{0\}$ . 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  $X \subset V, \text{vol } X > \det \Lambda$ , 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  $\Pi$  of lattice  $\Lambda$ . Then  $\det \Lambda = \text{vol } \Pi$ . Then  $\{\Pi + u, u \in \Lambda\}$  cover  $V$  without overlap. In particular, they cover  $X$ .

Let  $X_u := ((\Pi + u) \cap X) - u$ .  $\sum_{u \in \Lambda} \text{vol } X_u = \text{vol } X > \text{vol } \Pi$ . 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  $X = \frac{1}{2}A = \{\frac{1}{2}x, x \in A\}$ . Then  $\text{vol } X = 2^{-\dim V} \text{vol } A > \det \Lambda$ . 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,  $\text{vol } A = 2^{\dim V} \det \Lambda$  and  $A \cap \Lambda = \{0\}$ .

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

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

**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  $u \in \Lambda \setminus \{0\}$  with  $\|u\| \leq \sqrt{\dim V} (\det \Lambda)^{\frac{1}{n}}$ .

EXERCISE If  $X \subset V$  is measurable and  $\text{vol } X > m \det \Lambda$  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  $\text{vol } A > m \cdot 2^{\dim V} \det \Lambda$ . 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  $f : V \rightarrow \mathbb{R}_+$  is integrable and  $\Lambda \subset V$  a lattice. Then there are  $z_1, z_2 \in V$  such that

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

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

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

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

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

We start with integral:

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

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

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

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

Then

$$\text{vol } B = \int_0^1 \kappa t^{n-1} dr = \frac{\kappa}{n} = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2} + 1)}.$$

## 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  $a = 0, 1, \dots, \frac{n-1}{2}$ . They are all distinct. Otherwise  $a_1^2 \equiv a_2^2 \pmod{n} \implies (a_1 - a_2)(a_1 + a_2) \pmod{n}$ .

Consider values  $-1 - b^2 \pmod{n}$  for  $b = 0, 1, \dots, \frac{n-1}{2}$ . 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  $a_1, \dots, a_k \in \mathbb{Z}^n$  and  $m_1, \dots, m_k$  positive integers and*

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

*Then  $\Lambda$  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

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

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  $\text{vol } B = 2n^2\pi^2 \geq 2^4 n^2 \geq 2^4 \det \Pi$ . 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  $8 \cdot \sum_{d|n, 4 \nmid d} d$ .

EXERCISE 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)  $B_r = \{x \in \mathbb{R}^2 : \|x\| \leq r\}$ . As  $r \rightarrow \infty$ ,  $|B(r) \cap \mathbb{Z}^2| \approx \pi r^2 + O(r^{1/2+\varepsilon})$  for any  $\varepsilon > 0$ ? Best known is  $O(r^{0.63})$  for  $\varepsilon = 0.13$ .

EXERCISE 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?

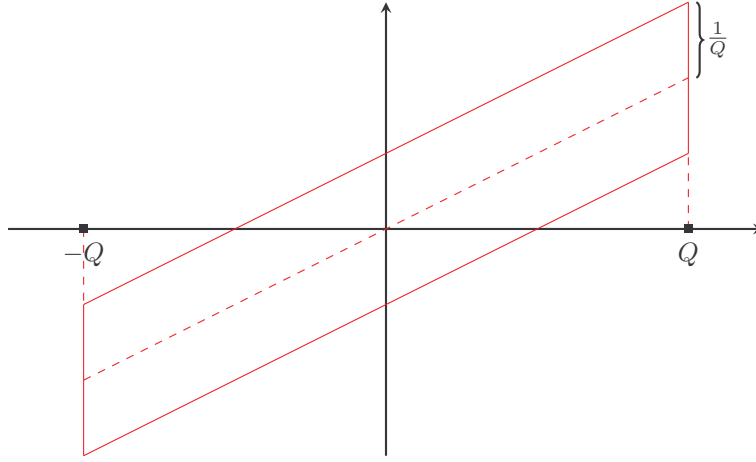
If  $\alpha \in \mathbb{R}$  and  $q \geq 1$  is an integer, then for some integer  $p$  we have  $\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{2q}$ .

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

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

It shows that this holds for infinitely many  $q$ .

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



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

EXERCISE For any  $\alpha_1, \dots, \alpha_n \in \mathbb{R}$  and any  $M$ , there are integers  $p_1, \dots, p_n$  and  $q \geq M$

such that  $\left| \alpha_k - \frac{p_k}{q} \right| \leq \frac{1}{q^{\frac{n+1}{n}}}$  for  $k = 1, \dots, n$ .

Continued fractions: given  $\alpha$ , we produce a possibly infinite expression:

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots}}}$$

and denote  $\alpha = [a_0; a_1, a_2, \dots]$  How: introduce variables  $\beta_0, \beta_1 \dots$  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  $a_0 = 1$ .

$$\begin{aligned} \sqrt{2} &= 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\frac{1}{\sqrt{2}-1}} = 1 + \frac{1}{\sqrt{2}+1} \\ &= 1 + \frac{1}{2 + (\sqrt{2} - 1)} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2}-1}} \end{aligned}$$

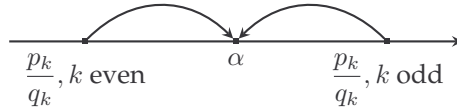
Convergents:  $k$ -th convergent:

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

EXERCISES 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  $[a_0; a_1, \dots, a_k] \rightarrow [a_1; a_2, \dots, a_k]$ .

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:

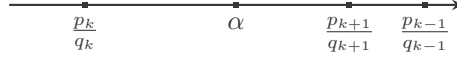
$$\left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k^2 \sqrt{5}}, \left| \alpha - \frac{p_{k-1}}{q_{k-1}} \right| \leq \frac{1}{q_{k-1}^2 \sqrt{5}}, \text{ or } \left| \alpha - \frac{p_{k-2}}{q_{k-2}} \right| \leq \frac{1}{q_{k-2}^2 \sqrt{5}}.$$

Convergents are the best rational approximation in the following sense:

Given  $\alpha$  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  $\left| \frac{a}{b} - \frac{p_k}{q_k} \right| \leq \left| \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} \right| = \frac{1}{q_k q_{k-1}}$  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  $\alpha$  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  $\sigma$  is defined as

$$\sigma = \limsup_{R \rightarrow \infty} \frac{\text{vol}(B_R(0) \cap \bigcup_i B_r(x_i))}{\text{vol } B_R(0)}$$

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.

REMARK/EASY EXERCISE 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  $\rho$  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  $A_4, D_4$ .

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

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

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

For  $n = 8$ , consider  $E_8$ .

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

240 vectors of length  $\sqrt{2}$ :  $(\pm 1, 0, \pm 1, 0, \dots) (-\frac{1}{2}, -\frac{1}{2}, \dots)$  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)

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

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

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

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

## 1.7 Leech Lattice

John Leech, 1926-1992



Consider  $\mathbb{R}^{26}$ , number coordinates,  $D_{26} \subset \mathbb{Z}^{26} : \sum_{k=0}^{25} 5 \equiv 0 \pmod{2}$

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

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

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

(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  $\Lambda_{24}$  to be the orthogonal projection of  $\Lambda_{25}$  onto  $L$ .

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

$\Lambda_{24}$  is the Leech lattice.

Useful formula for the length.

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

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

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

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

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

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

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

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

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 (you cannot add another ball to the packing) of balls of radius 1.

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

Why? If  $\bigcup_{i \in I} B(x_i, 1)$  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  $x_i \in B_{R-1}$ .

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

Hence

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

Take  $R \rightarrow \infty$ . ■

## 1.8 Lattice Packings

We will prove "today" for any  $0 < \alpha < 2^{-n}$  there is a lattice  $\Lambda \subset \mathbb{R}^n$  with  $\sigma(\Lambda) \geq \alpha$ . 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  $\Lambda \subset \mathbb{R}^n$   $\sigma(\Lambda) \geq 1.68n 2^{-n}$  (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  $\det \Lambda = 1$ .

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

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

$\min_{x \in \Lambda \setminus \{0\}} \|x\| \geq \sqrt{\frac{n}{2\pi e}}$ . 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  $\sigma(\Lambda) \geq \alpha$ . Later in this course  $\sigma(\Lambda) \geq \alpha$ .*

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  $\text{vol } M < 1$ . 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  $|x_i| < \alpha^{-\frac{1}{\alpha-1}}, i = 1, \dots, n-1$ .
2. Let  $H_k = \{x_n = k\alpha, k \in \mathbb{Z}\}$ .

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

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

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

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

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

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

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

Choose  $M = B_r(0)$  such that  $\text{vol } B_r(0) = 2^n \cdot a < 1$ . Construct a lattice  $\Lambda \cap B_r(0) = \emptyset$  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  $\Pi$  be a fundamental parallelepiped of  $\Lambda$ . Define  $f : V \rightarrow \mathbb{R}$  by  $f(x) = |M \cap (x + \Lambda)|$ . Then*

$$\int_{\Pi} f(x) \, dx = \text{vol } M$$

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

$$\int_{\Pi} f(x) \, dx = \sum_{u \in \Lambda} \int_{\Pi} f_u(x) \, dx = \sum_{u \in \Lambda} \text{vol}((\Pi + u) \cap M)$$

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

**Lemma 1.8.2.**

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

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

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

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

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

*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  $f : \mathbb{R}^n \rightarrow \mathbb{C}$  such that  $\int_{\mathbb{R}^n} |f(x)| dx, \int_{\mathbb{R}^n} |f(x)|^2 dx < \infty$ . We define

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

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

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

Poisson summation formula; if  $|f(x)| + |\widehat{f}(x)| \leq \frac{C}{(1+\|\cdot\|+\|\cdot\|)^{n+\delta}}$  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  $f, \widehat{f} : \mathbb{R}^n \rightarrow \mathbb{C}$  are admissible and  $\Lambda \subset \mathbb{R}^n$  is a lattice. Then

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

*Proof.* Let  $u_1, \dots, u_n$  be a basis of  $\Lambda$  and let  $T : \mathbb{R}^n \rightarrow \mathbb{R}^n$  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

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

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

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

■

**Theorem 1.9.1** (Cohn, Elkies, 2003). *Suppose that there is an admissible function  $f : \mathbb{R}^n \rightarrow \mathbb{R}$  such that  $\widehat{f} : \mathbb{R}^n \rightarrow \mathbb{R}$  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  $\mathbb{R}^n \leq \frac{\pi^{11/2}}{\Gamma(\frac{n}{n+2})} \frac{f(0)}{2^n} \widehat{f}(0)$*

*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

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

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

So the density

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

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:

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

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

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

*Proof.*

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

■

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

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

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

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

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

■

■

Density of lattice packing:

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

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