6.5 Discreteness of Lattices

Back to a general lattice Λ in $\mathbb{R}^n$, considered with the standard basis $e_1, \dots, e_n$ and standard scalar product $\langle \cdot, \cdot \rangle$.

Let $v_1, \dots, v_n$ be a basis of Λ, $Q := Gr_\Lambda(v_1, \dots, v_n) = (\langle v_i, v_j \rangle)$, and

$v_i = \sum_j A_{ij} e_j$, so $Q = AA^t$.

Let $x \in \Lambda$, so $x = \sum_i x_i v_i$. Then

$$\|x\|^2 = \langle x, x \rangle = \sum_{i,j} x_i x_j \langle v_i, v_j \rangle = \sum_{i,j} x_i x_j Q_{ij} = xQx^t =: Q(x)$$

For a constant $C > 0$ we are interested in

$$\{ x \in \mathbb{Z}^n \mid \|x\|^2 \leq C \}.$$

So, we need to find lattice point inside the ellipsoid

$$\{ x \in \mathbb{R}^n \mid Q(x) \leq C \}$$

Let $\tilde{Q}$ be the quadratic supplement of Q, so

$$Q(x) = \sum_{i=1}^n \tilde{Q}_{ii} \left(x_i + \sum_{j=i+1}^n \tilde{Q}_{ij} x_j \right)^2$$

Then

$$Q(x) \leq C \Leftrightarrow \tilde{Q}_{ii} \left(x_i + \sum_{j=i+1}^n \tilde{Q}_{ij} x_j \right)^2 \leq C - \sum_{p=i+1}^n \tilde{Q}_{pp} \left(x_p + \sum_{j=p+1}^n \tilde{Q}_{pj} x_j \right)^2 =: T_i \in \mathbb{R}^n$$

for $i = n, n-1, \dots, 1$.

Now, do a backtrack search:

1. Find the $x_n \in \mathbb{Z}$ with $|x_n| \leq \sqrt{T_n / \tilde{Q}_{nn}} = \sqrt{C / \tilde{Q}_{nn}}$
2. For fixed $x_{i+1}, \dots, x_n \in \mathbb{Z}$ satisfying

$$\sum_{p=i+1}^n \tilde{Q}_{pp} \left(x_p + \sum_{j=p+1}^n \tilde{Q}_{pj} x_j \right)^2 \leq T_{i+1}$$

determine all possibilities for x_i as follows:

$$U_i := \sum_{j=i+1}^{n} \tilde{Q}_{ij} x_j \quad \text{for } n-1 \geq i \geq 1$$

and then find the x_i with

$$-\sqrt{T_i/\tilde{Q}_{ii}} - U_i \leq x_i \leq \sqrt{T_i/\tilde{Q}_{ii}} - U_i$$

This is a constructive algorithm and it is clear that:

<u>Corollary 6.17</u>

a) For each $C > 0$ there are only finitely many $x \in \Lambda$ with $\|x\| \leq C$.

b) Λ is a discrete subset of $\mathbb{R}^n$.

c) If $(x_n)_{n\in\mathbb{N}}$ is a sequence in Λ which converges to $x \in \mathbb{R}^n$, then $x \in \Lambda$. $\square$

6.6 Shortest vectors and lattice density

Cor 6.17 a) implies that Λ contains a <u>shortest non-zero vector</u>. By §6.4 we have an algorithm to find one. Let $\lambda_1(\Lambda)$ be the length of the shortest vectors.

This quantity is related to the density of Λ.

For $x \in \mathbb{R}^n$ and $r \in \mathbb{R}_{>0}$ let $B^n(x,r) = \{y \in \mathbb{R}^n \mid \|x-y\| \leq r\}$ be the ball of radius r centered at x. A <u>sphere packing</u> is a collection

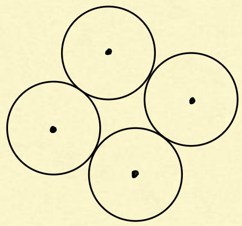
$$P = \bigcup_{x \in X} B^n(x,r)$$

for some set $X \subset \mathbb{R}^n$ such that the balls have pairwise disjoint interior.

The <u>density</u> $\rho(P)$ of P quantifies how much of the volume of $\mathbb{R}^n$ is made up of P, precisely:

$$\rho(P) = \lim_{t \to \infty} \frac{\mathrm{vol}(P \cap B^n(t))}{\mathrm{vol}(\underbrace{B^n(t)}_{\text{ball of rad. } t \text{ centered in } 0})}$$

If $X = \Lambda$ is a lattice, then P is called a <u>lattice sphere packing</u>, e.g.



Since Λ is additive, we have

$$\lambda_1(\Lambda) = \min_{0 \neq x \in \Lambda} \|x\| = \min_{\substack{x,y \in \Lambda \\ x \neq y}} \|x-y\|$$

Hence, the maximal radius for the balls of a lattice sphere packing with $X = \Lambda$ is $\frac{1}{2}\lambda_1(\Lambda)$. The corresponding density $\rho(\Lambda)$ is the <u>density</u> of Λ.

This can be computed relative to the volume of the fundamental region.

Recall from §6.2 that

$$d(\Lambda) = \sqrt{\mathrm{Gr}_\Lambda(b_1, \dots, b_n)} = \mathrm{vol}\, \overset{\{\sum a_i b_i \,|\, 0 \le a_i \le 1\}}{\Phi}$$

is independent of the chosen basis.

By symmetry you can see that

$$\rho(\Lambda) = \frac{\mathrm{vol}\left(B^n\left(\tfrac{1}{2}\lambda_1(\Lambda)\right)\right)}{\mathrm{vol}(\Phi)}$$

We have

$$\mathrm{vol}\left(B^n(r)\right) = \frac{\pi^{n/2}}{\underset{\uparrow \text{ Euler Gamma}}{\Gamma(n/2+1)}}\, r^n = \underbrace{\mathrm{vol}\left(B^n(1)\right)}_{=:\varkappa_n} \cdot r^n$$

$$\Rightarrow \rho(\Lambda) = \frac{\lambda_1(\Lambda)^n}{d(\Lambda)} \cdot 2^{-n} \varkappa_n$$ is the density of Λ.

For fixed n, what is the maximal density one can achieve with a lattice sphere packing? This amounts to finding

$$\rho_n := \sup_{\substack{\Lambda\subset\mathbb{R}^n \\ \text{lattice}}} \rho(\Lambda) \iff \sqrt{\gamma_n} := \sup_{\substack{\Lambda\subset\mathbb{R}^n \\ \text{lattice}}} \frac{\lambda_1(\Lambda)}{d(\Lambda)^{1/n}}$$

γ_n is called <u>Hermite constant</u>

So, $\rho_n = \sqrt{\gamma_n^n}\cdot 2^{-n}\varkappa_n$

This is only known in a few cases:

n	1	2	3	4	5	6	7	8	$9\le n\le 23$	24	$n\ge 25$
γ_n^n	1	4/3	2	4	8	64/3	64	256	?	4^{24}	2
$\approx\rho_n$	1	0.907	0.74	0.617	0.465	0.373	0.295	0.254	?	0.002	?

↑ Kepler conjecture (general packings)

↑ Leech lattice

<u>FACT</u>: γ_n^n is a rational number.

The sphere packing interpretation immediately gives us an upper bound for $\lambda_1(\Lambda)$:

$$\rho_n \le 1$$

$$\Rightarrow \frac{\lambda_1(\Lambda)^n}{d(\Lambda)}\cdot 2^{-n}\varkappa_n \le 1$$

$$\Rightarrow \lambda_1(\Lambda)^n \le 2^n\varkappa_n^{-1} d(\Lambda) = \Gamma(n/2+1)\cdot\frac{2^n}{\pi^{n/2}}\cdot d(\Lambda)$$

$$\overset{\sqrt[n]{\ }}{\Rightarrow} \underline{\lambda_1(\Lambda) \le 2\,\varkappa_n^{-1/n}\, d(\Lambda)^{1/n}}$$

$(\lambda_1^2)^n \le \Gamma(n/2+1)^2\left(\frac{4}{\pi}\right)^n d(\Lambda)^2$

$\Uparrow$ <u>Blichfeldt</u>: $(\lambda_1^2)^n \le \Gamma(n/2+2)^2\left(\frac{2}{\pi}\right)^n d(\Lambda)^2$

(Much better than Hermite's $\left(\frac{4}{3}\right)^{\frac{n-1}{2}}$ for $n\ge 8$)

In other words, the ball

$$B := \{\|x\| \le 2\varkappa_n^{-1/n} d(\Lambda)^{1/n}\} \subset \mathbb{R}^n$$

contains a non-zero lattice point.

We have

$$\mathrm{vol}(B) = \varkappa_n\cdot\left(2\varkappa_n^{-1/n} d(\Lambda)^{1/n}\right)^n = 2^n d(\Lambda)$$

There's a generalization of this observation called <u>Minkowski's first theorem</u> (or convex body theorem).