Lemma (Generalized Blichfeldt Theorem)

$S \subseteq \mathbb{R}^d$, $m \in \mathbb{Z}_{\geq 1}$, $\operatorname{vol} S > m \det \Lambda$

Then there are pairwise distinct $p_1, \dots, p_{m+1} \in S$ s.th.

$$p_i - p_j \in \Lambda \quad \forall i,j$$

proof: we may assume that S is bounded

Λ basis with fundamental parallelepiped Π

Let $P = \overline{\Pi}$. Then

$$\operatorname{vol} P = \operatorname{vol} \Pi = \det \Lambda$$

For $u \in \Lambda$: $S_u := \{y \in P \mid u + y \in S\} = P \cap (S - u)$

and

$$i_u : \mathbb{R}^d \longrightarrow \{0,1\}$$

$$x \longmapsto \begin{cases} 1 & x \in S_u \\ 0 & \text{else} \end{cases}$$

$$i_u \not\equiv 0 \iff u \in (P - S) \cap \Lambda$$

$\{p - s \mid p \in P, s \in S\}$

$P - S$ is bounded, so $i_u \not\equiv 0$ only for finitely many u

$\Rightarrow f := \sum_{\Lambda} i_u$ is well-defined.

$$\Rightarrow \int_P f \, dx = \sum_{\Lambda} \int_P i_u \, dx = \sum_{\Lambda} \operatorname{vol} S_u$$

$$= \sum_{\Lambda} \operatorname{vol}(P \cap (S - u)) = \sum_{\Lambda} \operatorname{vol}(S \cap (u + P)) = \operatorname{vol} S$$

$$> m \det \Lambda = m \operatorname{vol} P$$

$\Rightarrow$ there is $v \in P : f(v) > m$

$$\Rightarrow f(v) \geq m+1$$

$\Rightarrow$ there are $u_1, \dots, u_{m+1} \in \Lambda : v \in \bigcap_{i=1}^{m+1} S_{u_i}$

Let $p_i := u_i + v$ $\square$

We use this for a proof of van der Corput's Theorem:

Assume $\operatorname{vol} K > 2^d m \det \Lambda$

Let $T = \frac{1}{2} K \Rightarrow \operatorname{vol} T = \frac{1}{2^d} \operatorname{vol} K > m \det \Lambda$

So there are $p_1, \dots, p_{m+1} \in T$ with $p_i - p_j \in \Lambda \setminus \{0\}$

Let
$$x_i := p_i - p_{m+1}$$
$$= p_i + (-p_{m+1}) \in T + T = K$$

$$\Rightarrow 0, \pm x_1, \dots, \pm x_m \in K \Rightarrow |K \cap \Lambda| \geq 2m+1$$

The strict inequality for compact K follows by approximation:

$(2K \setminus K) \cap \Lambda$ is finite, so there is $\varepsilon > 0$ with

$$|K \cap \Lambda| = |(1+\varepsilon)K \cap \Lambda|$$

and $\operatorname{vol}((1+\varepsilon)K) > \operatorname{vol} K \geq 2^d m \det \Lambda$ $\square$

We can use Minkowski's Thm to bound the length of a shortest vector:

Let B be the unit ball in our norm

If $\operatorname{vol}(\alpha B) \geq 2^d \det \Lambda$, then there is a nonzero $a \in \Lambda$ with $\|a\| \leq \alpha$

so $$\|a\| \leq \left(\frac{2^d \det \Lambda}{\operatorname{vol} B}\right)^{1/d}$$

For Euclidean norm

$$\operatorname{vol} B = \frac{\pi^{\lfloor d/2 \rfloor} \, 2^{\lceil d/2 \rceil}}{\prod_{0 \leq i \leq d/2} (d-2i)}$$

using $k! \approx \sqrt{2\pi k}\left(\frac{k}{e}\right)^k$ we get

$$\operatorname{vol} B \geq \left(\frac{2\pi e}{d}\right)^{d/2} \geq \left(\frac{4}{d}\right)^{d/2}$$

$$\Rightarrow \quad a \leq \sqrt{d}\,(\det \Lambda)^{1/d}$$

<u>Thm:</u> A lattice $\Lambda \subseteq \mathbb{R}^d$ has a non-zero lattice vector a with

$$\|a\| \leq \sqrt{d}\,(\det \Lambda)^{1/d}$$ ∎

<u>Def</u> $K \subseteq \mathbb{R}^d$ closed, convex, cs. The k-th <u>successive min</u> is

$$\lambda_k := \lambda_k(K) := \inf(\dim \operatorname{lin}(\lambda K \cap \Lambda) \geq k)$$

Note: • $\lambda_d \geq \lambda_{d-1} \geq \dots \geq \lambda_1 > 0$

• Minkowski's Thm $\iff \lambda_1^d \operatorname{vol} K \leq 2^d \det \Lambda$

Norm $\|\cdot\|_K$ in $\mathbb{R}^d$ $\longleftrightarrow$ compact convex cs sets K

Prop: There is a vector space basis $v_1, \dots, v_d \in \Lambda$ s.th.

$$\|v_j\|_K = \lambda_j$$

proof: Let $1 \leq j \leq d$. There is a sequence

$$(w_i)_{i \geq 1} \subseteq \Lambda \quad \text{s.th.} \quad \lim_{i \to \infty} \|w_i\| = \lambda_j$$

K compact $\Rightarrow$ converging subsequence

$$(w_{i_k})_{k \geq 1} \quad \text{with} \quad \lim_{k \to \infty} w_{i_k} = w \in \mathbb{R}^d$$

$\to$ need to check $w \in \Lambda$:

$$\|w - w_{i_k}\| \leq \frac{\lambda_1}{2} \quad \text{for large } k$$

so $\|w_{i_k} - w_{i_\ell}\| \leq \|w_{i_k} - w\| + \|w_{i_\ell} - w\| < \lambda_1$

$\Rightarrow w_{i_k} = w_{i_\ell} = w$ for k, ℓ large $\boxtimes$

Minkowski's Second Thm

K convex, bounded, cs. Then

$$\frac{1}{d!} 2^d \det \Lambda \leq \lambda_1 \lambda_2 \cdots \lambda_d \operatorname{vol} K \leq 2^d \det \Lambda \quad \boxtimes$$

11. Packings and Coverings

here: $B_r(z) := \{ x \in \mathbb{R}^d \mid \| x - z \| < r \}$ open ball

Def: $\rho(\Lambda) := \sup_{r \geq 0} (B_r(x) \cap B_r(y) = \emptyset \ \forall x, y \in \Lambda)$

packing radius

$$\mu(\Lambda) = \max_{x \in \mathbb{R}^d} \operatorname{dist}(x, \Lambda)$$

covering radius

Prop: Λ lattice, a shortest non-zero vector. Then

$$\tfrac{1}{2} \| a \| = \rho(\Lambda)$$ ☒

Recall: Dual lattice $\Lambda^* := \{ \alpha : \mathbb{R}^d \to \mathbb{R} \mid \alpha(x) \in \mathbb{Z} \ \forall x \in \Lambda \}$

$\longrightarrow$ lattice in $(\mathbb{R}^d)^*$

Prop:

$$\rho(\Lambda) \rho(\Lambda^*) \leq d/4$$

proof: $\rho(\Lambda) \leq \frac{1}{2} \sqrt{d} \, (\det \Lambda)^{1/d}$ $\quad \rho(\Lambda^*) \leq \frac{1}{2} \sqrt{d} \, (\det \Lambda^*)^{1/d}$

and $\det \Lambda \cdot \det \Lambda^* = 1$ ☒