W5D2
24/11/14

Geometry of Numbers

Minkowski I - $K \subseteq \mathbb{R}^n$ convex & centrally symm. and Λ a lattice with $Vol(K) \geq 2^n d(\Lambda)$ then $K \cap \Lambda$ contains a non-zero point.

Minkowski Successive Minima let K be convex, centrally-symm bounded that contains a ball around 0 - so we can define a norm $\|x\|_K = \inf\{r>0 : x \in rK\}$. Furthermore, any norm on $\mathbb{R}^n$ is $\|\cdot\|_K$ for some such K.

Given K as above and $\Lambda \subseteq \mathbb{R}^n$ a lattice $i=1,\dots,n$ define $\lambda_i = \inf\{r>0 \ \ rK \cap \Lambda \text{ contains } i \text{ lin. ind. vectors}\}$.

Since K is bounded & Λ discrete, $\lambda_i = \|v_i\|_K$ for some $v_i \in \Lambda$. Clearly $\lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n$.

Claim $\lambda_1^n \leq \frac{2^n d(\Lambda)}{Vol(K)}$

pf If $r < \lambda_1$ then $rK \cap \Lambda = \{0\}$ so $r^n Vol(K) < 2^n d(\Lambda)$, so $r^n \leq \frac{2^n d(\Lambda)}{Vol(K)}$, so this is also true for λ_1.

both sharp - $K = [-1,1]^n$, $\Lambda = \mathbb{Z}^n$ achives the upper bound

Minkowski II $\frac{2^n d(\Lambda)}{Vol(K) \cdot n!} \leq \lambda_1 \cdot \lambda_2 \cdot \dots \cdot \lambda_n \leq \frac{2^n d(\Lambda)}{Vol(K)}$.

We'll only prove lower bound + upper for $K = B(0,1)$ only.

Recall The crit. det. $\Delta(K) = \inf\{d(\Lambda) \mid K \cap \Lambda = \{0\}\}$.

Minkowski I $\Rightarrow$ $\frac{1}{\Delta(K)} \leq \frac{2^n}{Vol(K)}$ [if not $2^n \Delta(K) < Vol(K) \Rightarrow \exists \Lambda$ s.t. $2^n d(\Lambda) < Vol(K)$ and $\Lambda \cap K = \{0\}$.]

For Euclidean norm we'll actually prove the stronger upper bound $\lambda_1 \dots \lambda_n \leq \frac{d(\Lambda)}{\Delta(K)}$ (*). Davenport conj. - (*) holds for any K as above. Best known - $\lambda_1 \dots \lambda_n \leq \frac{2^{\frac{n-1}{2}} d(\Lambda)}{\Delta(K)}$.

Pf. of LHS Replacing K by AK, Λ by $A\Lambda$ for some invertible A, we can assume $\Lambda = \mathbb{Z}^n$. Let $v_1, \dots, v_n$

be the vectors associated with $\lambda_1, \dots, \lambda_n$.

Let $B = \begin{pmatrix} | & | & & | \\ v_1 & v_2 & \dots & v_n \\ | & | & & | \end{pmatrix}$ and $I = |\det(B)| > 0$ (since $v_1, \dots v_n$ are lin. ind.). In fact $I = [\Lambda : \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n]$. the points $\frac{\pm v_i}{\lambda_i} \in \partial K$. We can assume WLG $\bar{K} = K$ so they're in K. Let $P = \operatorname{conv}(\pm \frac{v_i}{\lambda_i}, i = 1, \dots n) \subseteq K$. So,

$$Vol(K) \geq Vol(P) = \frac{2^n}{n!} \frac{I}{\lambda_1 \cdot \dots \cdot \lambda_n} \geq \frac{2^n}{n! \lambda_1 \cdots \lambda_n}, \text{ so } \lambda_1 \cdots \lambda_n \geq \frac{2^n}{n!} \frac{1}{Vol(K)}.$$

<u>Pf. of RHS for $K = B(0,1)$</u> $v_1, \dots v_n$ like last pf. $\|v_i\| = \lambda_i$.

Preform Gram-Schmidt to get $u_1, \dots u_n$ orth., with span $v_1, \dots v_i$ = span $u_1, \dots u_i$.

We can write each v_i as $\sum_{j=1}^{I} t_{ij} u_j$ with $t_{ii} \neq 0$. Let $a_1, \dots a_n$ be integers, not all zero. $\sum_{j=1}^{n} a_j v_j = \sum_{i=1}^{n} \left(\sum_{j \geq i} a_j t_{ji} \right) u_i$ so it's norm is

(**) $\sum_{i=1}^{n} \left(\sum_{j \geq i} a_j t_{ji} \right)^2 \left[= \|\sum_{i=1}^{n} a_j v_j\|^2 \right]$. <u>Claim</u> $\sum_{i=1}^{n} \frac{1}{\lambda_i^2} \left(\sum_{j \geq i} a_j t_{ji} \right)^2 \geq 1$. <u>pf of the claim</u> Let

J be the last index with $a_J = 0$, so $a_j = 0$ for $j > J$. Then $\sum_{j=1}^{n} a_j v_j \notin \operatorname{span}(v_1, \dots v_{J-1})$ so $\|\sum a_j v_j\|^2$. Theefore $\|\sum_{j=1}^{n} a_j v_j\| \geq \lambda_J^2$, by the def. of λ_J. All summands in (**) with $i > J$ are 0. Since $\lambda_j \leq \lambda_J$ for $j \leq J$, we get $\sum_{i=1}^{n} \frac{1}{\lambda_i^2} \left(\sum_{j \geq i} a_j t_{ji} \right)^2 = \sum_{i \leq J} \frac{1}{\lambda_i^2} \left(\sum_{j \geq i} a_j t_{ji} \right)^2 \geq$

$$\sum_{i \leq J} \frac{1}{\lambda_J^2} \left(\sum_{j \geq i} a_j t_{ji} \right)^2 = \frac{1}{\lambda_J^2} \sum_{i \leq J} \left(\sum_{j \geq i} a_j t_{ji} \right)^2 = \frac{1}{\lambda_J^2} \|\sum_{j=1}^{n} a_j v_j\|^2 \geq 1.$$

Now, let Λ' be the lattice generated by $v_j' = \frac{v_{j1}}{\lambda_1} u_1 + \dots + \frac{v_{ji} u_i}{\lambda_J}$.

By claim, $\|v'\| \geq 1$ for every $v' \in \Lambda' \setminus \{0\}$, so $B(0,1) \cap \Lambda' = \{0\}$ so $\Delta_n \leq d(\Lambda') = \frac{1}{\lambda_1 \cdots \lambda_n} \cdot d(\Lambda)$, so $\lambda_1 \cdots \lambda_n \leq \frac{d(\Lambda)}{\Delta_n}$ which gives the upper bound ⊛ $\to$ RHS of Minkowski II

<u>Lattice Reduction Algorithms</u>

Goal of lattice reduction - find an efficiet basis - short $v_1, \dots, v_n$ which span a lattice. How can we do it practically.

<u>Naive approach</u> Take some K conv. and $v_1, \dots v_n$ with $\|v_i\|_K = \lambda_i$. Recall,

however, they may not generate Λ: $\mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_n \oplus \frac{1}{2}\mathbb{Z}(1,1,\dots,1)$ for $n \geq 5$ is an example (WRT Euclidean norm).

to remedy this, define $\mu_i = \inf\{r \geq 0 \mid rK \text{ contains } i \text{ lin. ind } \underline{\text{primitive}} \text{ vectors}\}$.

Minkowski II - $\lambda_1 \cdots \lambda_n \leq C(n,k)$ for $\Lambda \in \mathcal{L}_n$. We wish to similarly bound μ_i.

<u>prop.</u> $\mu_i \leq \left(\frac{3}{2}\right)^{i-1} \lambda_i$.

A basis $v_1, \dots v_n$ with $\|v_i\|_K = \mu_i$ is said to be <u>Minkowski reduced</u>.

Clearly $\exists$ such basis & $\mu_1 \leq \dots \leq \mu_n$

<u>pf of prop.</u> Clearly $\mu_1 = \lambda_1$. Write $\|\cdot\| = \|\cdot\|_K$. Let $v_1, \dots v_n$ with $\|v_i\| = \lambda_i$ and $u_1, \dots, u_n$ a basis with $\|u_i\| = \mu_i$. WLG assume $v_1 = u_1$. Consider $u_1, \dots u_{k-1}$ and $v_1, \dots v_k$. Each is lin. ind. so $\exists j \neq 1$ s.t. v_j isn't a lin. comb. of $u_1, \dots, u_k$. $\|v_j\| = \lambda_j \leq \lambda_k$. $u_1, \dots, u_{k-1}$ are primitive so $\exists u \in \Lambda$ s.t. $u = a_1 u_1 + \dots + a_{k-1} u_{k-1} + \rho v$ with $u_1, \dots u_{k-1}, u$ primitime, with $\rho \in \mathbb{R}$, $\rho \neq 0$.

v_j is an integral lin. comb. of $u_1, \dots u_{k-1}, u$ - so by lin. ind. there is a <u>unique</u> such representation, so $\frac{1}{\rho} \in \mathbb{Z}$, $|\rho| \leq 1$. By replacing u_i with $u_i - k_i u$ if necessary $(k_i \in \mathbb{Z})$ we may assume $|a_i| \leq \frac{1}{2}$. $\mu_k \overset{\text{choice of } u_k}{\leq} \|u\| \leq |a_1| \cdot \|u_1\| + \dots + |a_{k-1}| \|u_{k-1}\| + |\rho| \|v_j\| \leq \frac{\|u_1\| + \dots + \|u_{k-1}\|}{2} + \lambda_k \leq \frac{\mu_1 + \dots + \mu_{k-1}}{2} + \lambda_k$. The bound follows by induction - seen for $k=1$, by induction $\mu_k \leq \frac{1}{2}\left(\lambda_1 + \frac{3}{2}\lambda_2 + \dots + \left(\frac{3}{2}\right)^{k-2} \lambda_{k-1}\right) + \lambda_k \leq$

$\leq \frac{1}{2}\lambda_k \left(1 + \frac{3}{2} + \dots + \left(\frac{3}{2}\right)^{k-2}\right) + \lambda_k = \frac{1}{2}\lambda_k \left(\frac{\left(\frac{3}{2}\right)^{k-1} - 1}{\frac{3}{2} - 1}\right) + \lambda_k = \left(\frac{3}{2}\right)^{k-1} \lambda_k$.

<u>Ques.</u> Is prop optimal? no - optimal estimate unknown. For Euc. norm, $\mu_i = \lambda_i$ $(i = 1, \dots 4)$, $\mu_i \leq \left(\frac{5}{4}\right)^{i-4} \lambda_i$ for $i > 4$.

<u>conj.</u> $\mu_i \leq \frac{i}{4} \lambda_i$ for $i \geq 5$. If true it must be optimal.

<u>Cor.</u> $\mu_1 \cdots \mu_n = \left(\frac{3}{2}\right)^{\frac{n(n-1)}{2}} \lambda_1 \cdots \lambda_n$.

<u>Correction</u> we have to choose u_k s.t. $u_1, \dots u_{k-1}, u_k$ is primitive - not clear how/why we can...

Korkine - Zolotarev Reduction

Let Λ be a lattice, $\|\cdot\| = \|\cdot\|_2$. Choose $v_1 \in \Lambda \setminus \{0\}$ as shortest as possible. suppose $v_1, \ldots, v_{i-1}$ where chosen. Choose v_i with min. projection (non zero) onto $(v_1 \ldots v_{i-1})^{\perp}$.

Claim $v_1, \ldots, v_n$ form a basis of Λ. (ex.).

Thm. $\frac{4}{i+3} \lambda_i \leq \|v_i\| \leq \frac{i+3}{4} \lambda_i$

LLL Algorithm - given d lin. ind. $v_1, \ldots v_d \in \mathbb{R}^n$, produce $u_1, \ldots u_d$ a basis of $\bigoplus_{i=1}^{d} \mathbb{Z} v_i$ with $\|u_i\| \leq c_i(d,n) \lambda_i$ using $O(d^5 n (\log \max \|v_i\|)^3)$.

Thm Finding the shortest vector in Λ is NP-hard & "generically NP-hard".