3/11/14
W2D2

Geometry of Numbers

Minkowsky's First Theorem:
If A is conv. and centrally symm. with $Vol(A) > 2^n d(\Lambda)$ (for Λ a lattice in $\mathbb{R}^n$) then $A \cap \Lambda \neq \{0\}$. Same holds if $Vol(A) = 2^n d(\Lambda)$ and A is compact.

We've seen a usage in **Dirichlet's Theorem:** If $Q > 1$, $\forall \vec{x} \in \mathbb{R}^n$ $\exists \vec{p} \in \mathbb{Z}^n, q \in \mathbb{N}$ s.t. $q \leq Q$, $\|q\vec{x} - \vec{p}\|_\infty \leq \frac{1}{Q^{1/n}}$.

Cor. If $\vec{x} \in \mathbb{R}^n$ and $\forall q \in \mathbb{N}$, $q\vec{x} \notin \mathbb{Z}^n$, there are infinitely many $(\vec{p}_k, q_k) \in \mathbb{Z}^{n+1}$ s.t. $\|\vec{x} - \frac{\vec{p}}{q}\|_\infty \leq \frac{1}{q^{1+1/n}}$.

Ques. Is that tight? What about other norms?
Turns out, if we replace 1 with $\varepsilon < 1$ the set of $\vec{x}$ satisfying is of measure zero. The cor. can be slightly improved, but there exist badly approximable $x \in \mathbb{R}$ s.t. $\exists c = c(x)$ s.t. $\forall (q_k, \vec{p}_k) \in \mathbb{Z}^{n+1}$, $\|\vec{x} - \frac{\vec{p}}{q}\|_\infty \geq \frac{c}{q^{1+1/n}}$. So we can only (hope to?) improve the constant. The optimal c – open question, only $n=1$ is solved and is $\frac{1}{\sqrt{5}}$ (Hurwitz constant).

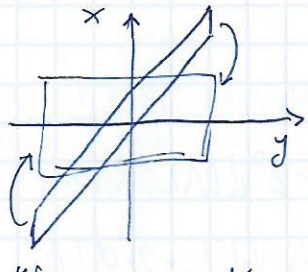
Thm. (Minkowski) $c = 1 - \frac{1}{n+1} = \frac{n}{n+1}$ also works. Not optimal for any n.

lemma. Let $t > 0$, $K_n = K_n(t) = \{(y, \vec{x}) \in \mathbb{R}^{n+1} \mid \frac{|y|}{t^n} + t\|x\|_\infty \leq 1\}$. Then K is compact, convex, centrally symm. and $Vol(K_n) = \frac{2^{n+1}}{n+1}$ (ind. of t).

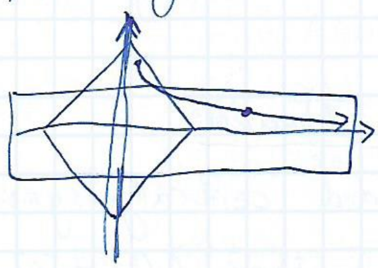
proof Compacticity, central symm. and convexity are easy to check.
$Vol(K_n) = Vol(K_1) = 2^{n+1} \int_0^1 (1-y)^n \, dy = \frac{2^{n+1}}{n+1}$.

proof of main thm. Define $\tilde{K}_n = \{(y, \vec{x}) \in \mathbb{R}^{n+1}$ s.t. $\frac{|y|}{t^n} + t\|y\vec{x}_0 - x\|_\infty \leq (n+1)^{\frac{1}{n+1}}\}$ and let $c = (n+1)^{\frac{1}{n+1}}$. $Vol(\tilde{K}_n) = c^{n+1} Vol(K_n) = 2^{n+1}$. Apply Minkowski's first thm. with $\mathbb{Z}^{n+1} = \Lambda$, so there's a non-zero $(\vec{p}, q)$ s.t. $\frac{|q|}{t^n} + t\|q\vec{x}_0 - \vec{p}\|_\infty \leq c$. If q was 0, $t\|\vec{p}\|_\infty \leq c$ which isn't possible for $t > c$. So $q \neq 0$ for large enough t. By ineq. of means, $\left(\frac{c}{n+1}\right)^{n+1} \geq |q| \cdot \|q\vec{x}_0 - \vec{p}\|_\infty^n / n^n$, so $|q| \cdot \|q\vec{x}_0 - \vec{p}\|_\infty^n \leq \left(\frac{n}{n+1}\right)^n$, so $\|q\vec{x}_0 - \vec{p}\|_\infty \leq \frac{n}{(n+1)q^{1/n}}$ as claimed (equiv. $\|\vec{x}_0 - \frac{\vec{p}}{q}\|_\infty \leq \frac{n}{(n+1)q^{1+1/n}}$).

This is an example of an important geometric idea:



gives $c=1$,



we "fly around" the point with a hyperbolic trajectory s.t. for some point in it we reach an integer point in , and this makes it possible to take a larger  (or smaller ).

Charactarization of Lattices

We defined a lattice as $\mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$ with $v_1, \dots, v_n$ lin. ind in $\mathbb{R}^n$. We with to characterize without finding a basis.

Thm. The following are equivalent:

1. Λ is a lattice.
2. Λ is a discrete subgroup of $\mathbb{R}^n$ containing n lin. ind. vectors over $\mathbb{R}$.
3. like 2 but over $\mathbb{Q}$.

Proof We're seen $1 \to 2$ and obviously $2 \to 3$.

$3 \to 2$: In a disc. subgroup of $\mathbb{R}^n$, lin. dep. over $\mathbb{R}^n$ $\to$ lin. dep. over $\mathbb{Q}$. Suppose $a_1, \dots a_n \in \mathbb{R}^n$ ($\vec{a}$) s.t. $\sum_{i=1}^{n} a_i v_i = 0$.

Let $M = \left\{ \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \;\middle|\; \left\| \sum_{i=1}^{n} b_i v_i \right\| < \eta \right\}$ where η is chosen s.t. the only element of $M \cap \Lambda$ is 0 (exists since Λ is discreet).

If $\vec{b} \in M$, so does $\vec{b} + t\vec{a}$. M contains a small ball B around 0, so M contains $M \supseteq \bigcup_{t \in \mathbb{R}} (B + t\vec{a})$, so $Vol(M) = \infty$.

Moreover, M is convex and cent. symm. by Minkovski $\exists \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{Z}^n \cap M$, so $\sum_{i=1}^{n} b_i v_i = 0$ a lin. dep. over $\mathbb{Q}$.

$2 \to 1$: $v_1 \dots v_n \in \Lambda$ are lin. ind. over $\mathbb{R}$, we seek n generators.

By prev. argument Λ doesn't contain $n+1$ lin. ind. vectors over $\mathbb{Q}$. We need the following

lemma if $\Lambda_1 \subseteq \Lambda_2$ lattices, $r = [\Lambda_2 : \Lambda_1]$, then $d(\Lambda_1) = r\, d(\Lambda_2)$.

proof: Let $a_1, \dots, a_r$ be coset members in $\Lambda_1 \subset \Lambda_2$. so, $\forall \lambda_2 \in \Lambda_2 \; \exists i, \lambda_1 \in \Lambda_1$ s.t. $\lambda_2 = a_i + \lambda_1$. So, if Ω is a fund. dom. for Λ_2. We claim $\tilde{\Omega} = \dot{\bigcup_{i=1}^{r}} \Omega - a_i$ is a fund dom - easy to see. So $d(\Lambda_1) = r d(\Lambda_2)$.

Now, let $\Lambda_0 = \mathbb{Z} v_1 \oplus \dots \mathbb{Z} v_n$. If $\Lambda_0 = \Lambda$ we're done, o/w $\exists u \in \Lambda \setminus \Lambda_0$ and $u, v_1, \dots v_n$ aren't ind. over $\mathbb{Q}$, therefore $\exists b_1, \dots b_n, b \in \mathbb{Z}$ s.t. not all are 0 and $bu = \sum_{i=1}^{n} b v_i$ (so $b \neq 0$), and $b \neq \pm 1$ since $u \notin \Lambda_0$. Choose u that minimizes $|b|$. Suppose $p | b$, then $\exists i$ $p \nmid b_i$. Assume it's b_1 WLG. So, $\exists m, l \in \mathbb{Z}$ s.t. $lp - mb_1 = 1$. Define $u_1 = l v_1 - \frac{mb}{p} u$, $u_2 = v_2, \dots, u_n = v_n$. Let's show $v_1 \in \mathbb{Z} u_1 \oplus \dots \mathbb{Z} u_n$ - $\left(\frac{n}{\mathbb{Z}}\right)$

$p u_1 + m(b_2 u_2 + \dots + b_n u_n) = lp v_1 - mbu + m(b_2 u_2 + \dots b_n u_n) =$
$v_1(lp - m b_1) + m(b_2 u_2 + \dots + b_n u_n + b_1 v_1 - bu) = v_1 + 0 = v_1$.

Let $\Lambda_1 = \mathbb{Z} u_1 \oplus \dots \oplus \mathbb{Z} u_n$, so $\Lambda_0 \subseteq \Lambda_1$ and $u_1, 2u_1, \dots (p-1) u_1 \notin \Lambda_0$, so $[\Lambda_1 : \Lambda_0] \geq p \geq 2$, so $d(\Lambda_1) \leq \frac{1}{2} d(\Lambda_0)$. Continue as $d(\Lambda_k) \searrow 0$, so any small ball $B_0(\varepsilon)$ will contain $x \in \Lambda_k$, $x \neq 0$ for large enough k (assuming the process won't stop), contradicting discreetness of Λ.

Other Applications: Diophantine Equations

Thm (Legandre) Any prime $p \equiv 1 \; (4)$ is the sum of ($p = x^2 + y^2$) two squares.

Remark No solution for $p \equiv 3 \; (4)$ even mod 4.

proof: Let j satisfy $j^2 \equiv -1 \; (p)$. Define $\Lambda = \{(x,y) \in \mathbb{Z}^2 \mid y = jx \pmod{p}\}$. Λ is a lattice, $[\mathbb{Z}^2 : \Lambda] = p$ so $d(\Lambda) = p$. Let $S = B_{\sqrt{2p}}(0)$, $Vol(S) = 2\pi p > 4p$ so $S \cap \Lambda \neq \{0\}$, $\exists x, y$ s.t. $0 < x^2 + y^2 < 2p$ and $x^2 + y^2 \equiv x^2 + (jx)^2 \equiv x^2 - x^2 \equiv 0 \; (p)$, so $x^2 + y^2 = p$.

Thm. (Lagrange) $\forall m \in \mathbb{N} \; \exists x_1, \dots x_4 \in \mathbb{Z}$ s.t. $x_1^2 + x_2^2 + x_3^2 + x_4^2 = m$.

Proof Enough to prove for square-free m. $m = p_1 \dots p_g$ different (since m is square free). Claim - for each p $\exists a, b$ s.t. $a^2 + b^2 + 1 \equiv 0 \; (p)$. If $p = 2$ take $a = 1, b = 0$. If $p = 2k+1$ then $\{a^2 \mid 0 \leq a \leq k\}$ and $\{-1 - b^2 \mid 0 \leq b \leq k\}$. Together they contain $2k+2$ elements, so they mustn't be disjoint mod p and $a^2 \equiv -1-b^2$ (p).

Now, let Λ be $\left\{(u_1,\dots,u_4)\in\mathbb{Z}^4 \;\middle|\; \begin{matrix} u_1 \equiv a_p u_3 + b_p u_4 \\ u_2 \equiv b_p u_3 - a_p u_4 \end{matrix} \begin{pmatrix} \text{mod } p, \text{ for} \\ \text{any } p=p_i \end{pmatrix} \right\}$.

This is a lattice with $d(\Lambda) \leq m^2$. As before take $B_{\sqrt{2m}}(0)$ with $Vol = \frac{1}{2}\pi^2 4m^2 = 2(\pi m)^2 > 16m^2 \geq 2^4 d(\Lambda)$. So $\exists (u_1,\dots,u_4)\in\mathbb{Z}^4$ s.t. $u_1^2+u_2^2+u_3^2+u_4^2 < 2m$ – it's enough to show it's 0 mod m, or mod each $p=p_i$. But $u_1^2+u_2^2+u_3^2+u_4^2 \equiv$
$(a_pu_3+b_pu_4)^2+(b_pu_3-a_pu_4)^2+u_3^2+u_4^2 \equiv (1+a_p^2+b_p^2)u_3^2+(1+a_p^2+b_p^2)u_4^2+$
$2a_pu_3b_pu_4-2b_pu_3a_pu_4 \equiv 0$ (p) as required.