W9 D2
22/12/14

Geometry of Numbers

<u>Main Goal</u>: Understand $\Delta_n = \min\{d(\Lambda) : \Lambda \subseteq \mathbb{R}^n \text{ lattice}, \Lambda \cap B(0,1) = \{0\}\} = \left[\max\{\lambda_1(\Lambda) \mid \Lambda \in \mathcal{L}_n\}\right]^{-n}$.

Showing upper bounds on Δ_n using "probabilistic techniques" to show that $\lambda_1(\Lambda)$ is "typically" large.

Recall $\mathcal{L}_n = SL_n(\mathbb{R}) / SL_n(\mathbb{Z})$, as sets but also as topological space.

We'd like to discuss measures on $SL_n(\mathbb{R}) / SL_n(\mathbb{Z})$, and get a measure on $\mathcal{L}_n$.

We will define an $SL_n(\mathbb{R})$-invariant measure coming from the Haar measure on $SL_n(\mathbb{R})$. $\exists$ unique such measure and it is <u>finite</u>.

Haar measure

Top. Group - group with top. such that the group actions $(g_1, g_2) \mapsto g_1 g_2$ and $g \mapsto g^{-1}$ are continous.

<u>Thm</u> On a locally compact top. group $\exists$ unique (up to scaling) left- (resp. right-) invariant measure (locally finite, Borel) - i.e. $\mu(A) = \mu(gA)$ (resp. $\mu(A) = \mu(Ag)$).

If left inv. = right inv., G is <u>unimodular</u>.

<u>Examples</u> Lesbague mesure on $\mathbb{R}^n$, $\mathbb{R}^n / \Lambda$ ($Leb_{\mathbb{R}^n}$) (both left- and right-invariant).

Any discrete group with the counting measure.

Proof of Uniqueness

Suppose μ_1, μ_2 loc. fin. left inv measures $\to$ so is $\nu = \mu_1 + \mu_2$. Then $\mu_1 \ll \nu$. Let $\varphi = \frac{d\mu_1}{d\nu}$ the R.N. derivative, i.e., $\forall A \subseteq G$ measurable, $\mu_1(A) = \int_A \varphi \, d\nu$. φ is unique up to a set of ν-zero measure. Then, $\mu_1(gA) = \mu_1(A) = \int_A \varphi \, d\nu = \int_A \varphi(g^{-1}A) \, d\nu = \int \varphi \, d\nu$ i.e., $x \mapsto \varphi(gx)$ is also G inv. $\Rightarrow \varphi$ is

ν-a.e. φ a const $\Rightarrow \mu_1 = \hat{c}\,\nu \Rightarrow \mu_1 = c\mu_2$

Existance for $SL_n(\mathbb{R})$

$M_n(\mathbb{R}) \cong \mathbb{R}^{n^2}$ so we can use $Leb_{\mathbb{R}^{n^2}}$. But there $SL_n(\mathbb{R})$ has measure zero. So, define $\mu(A) = Leb_{\mathbb{R}^{n^2}}(x \in M_n(\mathbb{R}) \mid \det x \in (0,1), \frac{x}{\det x^{1/n}} \in A\}$.

Check invariance: $\mu(gA) = Leb_{\mathbb{R}^{n^2}}\{gx \dots\} = \mu(A)$. Similarly for right-inv. ("price is $(\det g)^n = 1$).

Cor. $SL_n(\mathbb{R})$ is unimodular.

Prop. For a loc. comp. G, discrete $\Gamma \subseteq G$, $\exists$ measurable (Borel) fund. domain $\Omega \subseteq G$ for G/Γ such that $G = \dot{\bigcup}_{\gamma \in \Gamma} \gamma \Omega$.

A section $s: G/\Gamma \to G$ is a Borel map (Borel isomorphism onto its image) such that $G \underset{s}{\overset{\pi}{\rightleftarrows}} G/\Gamma$, $\pi \circ s = id_{G/\Gamma}$.

$\exists$ equivalence sections $\Leftrightarrow$ Borel fund. domains (bijection).

If Ω is a fund. dom. $x \in G/\Gamma$, $\exists!\, w \in \Omega$ such that $\pi(w) = x$, define $s(x) = w$. If s is a setion $\operatorname{Im} s = \Omega$ is fund. dom.

~~Prop.~~

Prop If μ is a right inv. Haar measure, $\mu_1\ \mu_2$ fund. doms., then $\mu(\Omega_1) = \mu(\Omega_2)$.

Pf. $\forall w \in W_2\ \exists \gamma = \gamma(w)$ s.t. $w\gamma \in \Omega_1$. So $\Omega_2 = \bigcup_{\gamma \in \Gamma} \Omega_2(\gamma) = \{w \in \Omega_2 \mid \gamma_w = \gamma\}$.

Then $\mu(\Omega_2) = \sum_{\gamma \in \Gamma} \mu(\Omega_2(\gamma)) = \sum_{\gamma \in \Gamma} \mu(\Omega_2(\gamma)\gamma) \leq \mu(\Omega_1)$. By symm. they're equal.

$\exists$ measurable fund. dom. for $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. Given $\Lambda \subseteq \mathbb{R}^n$ $\exists$ basis obtained by Mink. reduction - v_1 shortest, v_2 shortest s.t. $\{v_1, v_2\}$ lin. ind. & prim... (Resolve ties measurably - say, by lex. order). This is a map $SL_n(\mathbb{R})/SL_n(\mathbb{Z}) \longrightarrow SL_n(\mathbb{R})$ and one can verify that it is a section.

Prop Let G, Γ as above, G unimodular. Ω fund. dom, S the corresponding section. Then let μ be the Haar measure of G. Define a measure on G/Γ by $\nu(A) = \mu(s(A))$. Then μ is ind. of choice of S/Ω and is left-invariant.

Pf. Ind. of S since the projection $\Omega_1 \to \Omega_2$ is 1-1... Decompose $\Omega_1 \cap \pi^{-1}(A)$, $\Omega_2 \cap \pi^{-1}(A)$ into countably many pieces $\Omega_1(\gamma)$ such that $\Omega_2(0)\Gamma \subseteq \Omega_1$ and repeat prev. proof.

left-invariance: s section defining ν. Define $S_1(x) = g^{-1}s(gx)$.

This is also a section since $\pi(S_1(x)) = \pi(g^{-1}(s(gx))) = g^{-1}(\pi(s(gx))) = g^{-1}gx = x$. Therefore $\nu(g(A)) = \mu(s(g(A))) = \mu(g S_1(A)) = \mu(S_1(A)) = \mu(s(A))$.

<u>Summary</u>: $\exists\ SL_n(\mathbb{R})$ inv. measure on $\mathcal{L}_n$, coming from the Haar measure on $SL_n(\mathbb{R})$.

G, Γ as before. Γ is called a <u>lattice</u> if the measure on G/Γ is finite. We'll show $SL_n(\mathbb{Z})$ is a lattice in $SL_n(\mathbb{R})$.

<u>Thm.</u> Let $G = SL_n(\mathbb{R})$, $\Gamma = SL_n(\mathbb{Z})$, μ as above, Ω fund. dom. for G/Γ. Then:

(1) $\mu(\Omega) = \dfrac{\zeta(2)\cdots\zeta(n)}{n}$

(2) If $f: \mathbb{R}^n \to \mathbb{R}$ is Riemann measurable, define $\hat{f}(\Lambda) = \sum_{u \in \Lambda\setminus\{0\}} f(u)$. Then $\mu(\Omega)\int_{\mathbb{R}^n} f \, dLeb_{\mathbb{R}^n} = \int_{\mathcal{L}_n} \hat{f}\, d\nu$ (ν obtained from μ as before). In particular $\bar{\nu} = \nu/\mu(\Omega)$ is the unique G-inv. prob. measure on $\mathcal{L}_n$.

<u>Remarks</u> (2) is called Siegel integral formular (summation formula). Developed by Siegel for the application we are discussing ("mean value theorem in geometry of numbers"). Map $f \mapsto \hat{f}$ is sometimes called the Siegel transform (Siegel-Veech). For $f \in L^1(\mathbb{R}^n, Leb_{\mathbb{R}^n})$ and the definition of $\hat{f}$ can be shown to converge a.e.

<u>Notation</u> $G_n = SL_n(\mathbb{R})$, $\Gamma_n = SL_n(\mathbb{Z})$, Ω_n fund. dom. for G_n/Γ_n, μ, τ Haar measures on G_n, G_{n-1}. $C_n = [0,1)^n$.

<u>pf.</u> Both sides depend linearly on f. Suffices to show for 1_M, $M \subseteq \mathbb{R}^n$ bounded & Riemman measurable, $\forall x \in M, x_1 \neq 0$.

Define $M_1^* = \{g \in G_n \mid ge_1 \in M$, eq. 1^{st} col. in $M\}$.

<u>claim</u> each $g \in M_1^*$ can be written uniquely as $\begin{pmatrix} x_1 & 0\ 0 \cdots 0 \\ \vdots & \tilde{X} \\ x_n & \end{pmatrix}\begin{pmatrix} 1 & y_2 \cdots y_n \\ 0 & \\ \vdots & B \\ 0 & \end{pmatrix}$

where $B \in G_{n-1}$, $x=(x_1,\dots,x_n)\in M$, $\tilde{X} = \mathrm{diag}\left(\frac{1}{|x_1|^{n-1}}, \frac{1}{|x_1|^{n-1}}, \dots, \frac{\pm 1}{|x_1|^{n-1}}\right)$.

pf check $\begin{pmatrix} x_1 & 0 \cdots 0 \\ \vdots & \tilde{X} \\ x_n & \end{pmatrix}^{-1} g$ has required form.

Now set $M^* = \{g \in M^* \mid y \in C_{n-1},\ B \in \Omega_{n-1}\}$. Let $\chi = 1_M$, $\chi^* = 1_{M^*}$, $I = \mathrm{Leb}_{\mathbb{R}^n}(M) = \int_{\mathbb{R}^n} \chi \, d\mathrm{Leb}_{\mathbb{R}^n}$.

Claim $\mu(M^*) = \frac{n-1}{n} \tau(\Omega_{n-1}) I$. (Skip proof.) Idea - change of variables and explicit calculation.

Let $u \in \mathbb{Z}^n$ primitive, $\Gamma(u) = \{\gamma \in \Gamma_n \mid 1^{st}$ col. of γ is $u\}$. Then $\Gamma_n = \dot{\bigcup}_{u \text{ primitive}} \Gamma(u)$. $\Gamma(u) = \gamma_0(\{\gamma \in \Gamma_n \mid \gamma e_1 = e_1\})$, for any $\gamma_0 \in \Gamma(u)$.

Claim For any u, $g \in G_n$, $\#\{\gamma \in \Gamma(u) \mid g\gamma \in M^*\} = \begin{cases} 1 & gu \in M \\ 0 & gu \notin M \end{cases} = \chi(gu)$.

pf. If $gu \notin M$ then $g\gamma e_1 = gu \notin M$ so for any $\gamma \in \Gamma(u)$, $g\gamma \notin M^*$.

If $gu \in M$ then fix $\gamma_0 \in \Gamma(u)$. $g\gamma_0 e_1 \overset{\in M}{\Longrightarrow} g\gamma_0 \in M_1^*$. Write $g\gamma_0 = \begin{pmatrix} x_1 & 0 \cdots 0 \\ \vdots & \tilde{X} \\ x_n & \end{pmatrix}\begin{pmatrix} 1 & y_2 \cdots y_n \\ 0 & \\ \vdots & B \\ 0 & \end{pmatrix}$. $g\gamma_0\gamma = \begin{pmatrix} x_1 & 0 \cdots 0 \\ \vdots & \tilde{X} \\ x_n & \end{pmatrix}\begin{pmatrix} 1 & y_2 \cdots y_n \\ 0 & \\ \vdots & B \\ 0 & \end{pmatrix}\gamma =$

$\begin{pmatrix} 1 & 0 \\ x & \tilde{X} \end{pmatrix}\begin{pmatrix} 1 & \tilde{y} \\ 0 & \tilde{B} \end{pmatrix}\begin{pmatrix} 1 & \overbrace{a_2 \dots a_n}^{\text{integers}} \\ 0 & \\ \vdots & \Gamma_{n-1} \\ 0 & \end{pmatrix}$. Since Ω_{n-1} is a fund. dom, $\exists$ unique $\tilde{B}$ s.t. $B\tilde{B} \in \Omega_{n-1}$. Having chosen it, $\exists$ unique $a_2, \dots, a_n$ s.t. $(a_2, \dots, a_n) + y\tilde{B} \in C_{n-1}$.

Therefore $\sum_{\gamma \in \Gamma_n} \chi^*(g\gamma) = \sum_{u \text{ prim.}} \sum_{\gamma \in \Gamma(u)} \chi^*(g\gamma) = \sum_{\substack{u' \text{ prim.} \\ \text{in } g\mathbb{Z}^n}} \chi(u')$. Since Ω_{n-1} is a fund. dom. $\mu(M^*) = \int_{G_n} \chi^* d\mu = \sum_{\gamma \in \Gamma_n} \int_{\Omega_n} \chi^*(g\gamma) d\mu = \int_{\Omega_n} \sum_{\gamma \in \Gamma_n} \chi^*(g\gamma) d\mu =$

$\int_{\Omega_n} \sum_{\substack{u' \in g\mathbb{Z}^n \\ \text{prim.}}} \chi(u') d\mu$. So, $\frac{n-1}{n} \tau(\Omega_{n-1}) I = \int_{\Omega_n} \sum_{\substack{u \in \mathbb{Z}^n \\ \text{prim.}}} \chi(gu) d\mu$. $P(\mathbb{Z}^n)$ = prim. vectors in $\mathbb{Z}^n$, then $\mathbb{Z}^n \setminus \{0\} = P(\mathbb{Z}^n) \cup 2P(\mathbb{Z}^n) \cup 3 \dots$ so this gives (a) $\int_{\Omega_n} \sum_{u \in \mathbb{Z}^n \setminus \{0\}} \chi(gu) = \frac{n-1}{n} I \left(1 + \left(\tfrac{1}{2}\right)^n + \left(\tfrac{1}{3}\right)^n \dots\right) \tau(\Omega_n) = \frac{n-1}{n} \zeta(n) \tau(\Omega_n) I$.

By replacing $\chi(x)$ with $\chi(\varepsilon x)$ $(\varepsilon > 0)$ (b) $\int_{\Omega_n} \overbrace{\varepsilon^n \sum_{u \in \mathbb{Z}^n \setminus \{0\}} \chi(\varepsilon g u)}^{\xrightarrow[\varepsilon \searrow 0]{} I \text{ pointwise}} d\mu = \frac{n-1}{n} \zeta(n) \tau(\Omega_n) I$.

We can now prove inductively. $\mu(\Omega_1) = 1$. $\underbrace{\varepsilon^n \sum_{u \in \mathbb{Z}^n \setminus \{0\}} \chi(\varepsilon g u)}_{\text{integrable by (a)}} = O\left(\sum_{u \in \mathbb{Z}^n \setminus \{0\}} 1_W(gu)\right)$ with $W = [-1,1]^n$ and const. dep. only on M_n. ← pf. next week. For $\varepsilon \searrow 0$, (b) shows (by Lebesgue dom. conv.) $\int_\Omega I = I \cdot \mu(\Omega_n) = \frac{n-1}{n} \zeta(n) \tau(\Omega_{n-1}) I$, and by induction $\mu(\Omega) = \frac{\zeta(1)\zeta(2) \dots \zeta(n)}{n}$

This proves (1) while (a) implies (2).