Last time reduced bases

Defn $G = Gl_n(\mathbb{R}) \longleftrightarrow \{\text{ordered bases } v_1, \dots, v_n \text{ of } \mathbb{R}^n\}$

$g \longleftrightarrow e_i g$, $g = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$

OR $G = Sl_n(\mathbb{R})$

$G = NAK$ (Iwasawa decomposition)

$N = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, $A = \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix}$ (>0 entries), $K = O(n)$, $SO(n)$

A **Siegel domain** for G is a subset of the form

$\mathfrak{S} = \omega A_t K$, $\omega \subseteq N$ is compact

$A_t := \{a : a_i / a_{i+1} \geq t\}$

ex $\omega = \omega_B := \{u \in N : |u_{ij}| \leq B \ \forall i<j\}$

Example $\mathfrak{S} = \omega_B A_t K$ with $B = 1/2$, $t = \sqrt{3}/2$

$\updownarrow$

{reduced bases}

Theorem Let $G = Gl_n\mathbb{R}$ OR $Sl_n\mathbb{R}$

$\Gamma = Gl_n\mathbb{Z}$ OR $Sl_n\mathbb{Z}$

(i) $\exists$ Siegel domain $\mathfrak{S}$ s.t. $\Gamma \cdot \mathfrak{S} = G$

($\Leftrightarrow \mathfrak{S} \longrightarrow \Gamma \backslash G$ is surjective)

(ii) $\#\{\gamma \in \Gamma : \gamma \mathfrak{S} \cap \mathfrak{S} \neq \emptyset\} < \infty$ $\forall$ Siegel domains $\mathfrak{S}$

Proof (i) $\Leftrightarrow$ every lattice has some reduced basis (for $\mathfrak{S}$ as in Example).

Indeed, for $g \in G$ (any $G = Gl_n(\mathbb{R})$), $\rightsquigarrow$ lattice $\mathbb{Z}^n g$

$\rightsquigarrow$ reduced basis $v_1, \dots, v_n$ for $\mathbb{Z}^n g$

$\Rightarrow$ (check) $g \in Gl_n(\mathbb{Z}) v$, $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathfrak{S}$.

$\Rightarrow G = \Gamma \mathfrak{S}$, as desired.

(ii) See notes. $\square$

Background on Haar measure

G: locally compact group

$\Rightarrow \exists$ unique (up to scaling) Radon measures $d^L g$, $d^R g$ on G that are left (resp. right) inv. under G: $\forall x \in G$,

$$\int f(xg)\, d^L g = \int f(g)\, d^L g \qquad d^L g : \text{"left Haar measure"}$$

$$\int f(gx)\, d^R g = \int f(g)\, d^R g \qquad d^R g : \text{"right Haar measure"}$$

$\exists$ continuous homomorphism $\delta = \delta_G : G \to \mathbb{R}_+^\times$ s.t. $d^R g = \delta(g) d^L g$.

cf. G: Lie group, then $\delta(g) = |\det \mathrm{Ad}(g)|$,

where $\mathrm{Ad}: G \to GL(\mathfrak{g})$, $\mathfrak{g} = \mathrm{Lie}(G)$.

Call G unimodular if $\delta = 1$.

$\Rightarrow d^L g = d^R g =: dg$: "Haar measure"

Examples { abelian groups; nilpotent/unipotent groups; $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$; compact groups; reductive groups } are unimodular

Calculation for $G = GL_n(\mathbb{R})$, $g = a \in A$ (≤ $\mathrm{diag}(a_1, \dots, a_n)$):

$\mathfrak{g} = M_n(\mathbb{R}) \ni x = (x_{ij})_{i,j}$

$$\mathrm{Ad}(a)\, x = \left(\frac{a_i}{a_j} x_{ij}\right)_{i,j}$$

$$\Rightarrow \det \mathrm{Ad}(a) = \prod_{i,j} \frac{a_i}{a_j} = 1 \Rightarrow \delta_G(a) = 1$$

(By an analyticity / density argument, $\Rightarrow \delta = 1$.)

$B = NA = \begin{pmatrix} * & * \\ & \ddots \\ & & * \end{pmatrix} \leq GL_n(\mathbb{R})$ is not unimodular:

$$\underset{B}{\delta}(ua) = \prod_{i<j} \frac{a_i}{a_j} = a_1^{n-1} a_2^{n-3} \cdots a_n^{1-n}$$

$\delta_B(ua) = \delta(a)$

$$d^R(ua) = du \cdot da, \quad du = \prod_{i<j} du_{ij}$$ (Lebesgue)

$$d^L(ua) = \frac{du\, da}{\delta(a)} \qquad da = \prod_{i=1}^{n} \frac{da_i}{a_i}$$ (Haar measure on $\mathbb{R}_+^\times$; da_i: Lebesgue on $\mathbb{R}$)

$B = NA \leq SL_n(\mathbb{R})$: similar, but $da = \prod_{i=1}^{n-1} \frac{da_i}{a_i}$, $a_n := \frac{1}{a_1 \cdots a_{n-1}}$

$G = GL_n(\mathbb{R})$ or $SL_n(\mathbb{R})$:

$g = uak$ $\qquad dg = d^L(ua)\, dk$ (see notes)

Quotient Haar measure: for $\Gamma <$ (closed subgroup) G, both unimodular,

dg: Haar on G, $d\gamma$: Haar on Γ $\rightarrow$ (unique) quotient Haar $d\bar{g}$ on $\Gamma \backslash G$ (G-invariant)

characterized by: $\forall f \in C_c(G)$,

$$\int_G f(g)\, dg = \int_{\Gamma\backslash G} \left(\sum_{\Gamma} f(\gamma \bar{g})\, d\gamma \right) d\bar{g}.$$

$\rightarrow$ Haar measure on $SL_n\mathbb{Z} \backslash SL_n\mathbb{R}$, $GL_n\mathbb{Z} \backslash GL_n\mathbb{R}$

(counting measure on $SL_n\mathbb{Z}$, $GL_n\mathbb{Z}$)

Thm $\mathrm{vol}(\mathrm{SL}_n\mathbb{Z}\backslash \mathrm{SL}_n\mathbb{R}) < \infty$ (with respect to any Haar)

Proof It suffices to show $\mathrm{vol}(\mathfrak{S}) < \infty$
$\forall$ Siegel domains $\mathfrak{S} \subseteq \mathrm{SL}_n(\mathbb{R})$. (check!)
Let $dg = d^L(na)\,dk$, $g = nak$.

$$\mathrm{vol}_{\mathrm{SL}_n\mathbb{R}}(\mathfrak{S}) = \int_{\mathrm{SL}_n(\mathbb{R})} \underbrace{1_{\mathfrak{S}}(nak)}_{\text{detects } n \in \omega:\ \text{compact}}\, d^L(na)\,dk = \underbrace{\mathrm{vol}_N(\omega)\,\mathrm{vol}_K(K)}_{<\infty}\, I,$$

$\mathfrak{S} = \omega A_t K$ $\qquad a_i/a_{i+1} \geq t$

$$I = \int_{a_1,\dots,a_n \in \mathbb{R}^\times_+,\ a_1\cdots a_n = 1,\ a_i/a_{i+1} \geq t} \frac{1}{\delta(a)} \frac{da_1}{a_1} \cdots \frac{da_{n-1}}{a_{n-1}}.$$

$$= (\text{constant}) \cdot \int_{\substack{y_i = t \\ \forall i = 1..n-1}}^{\infty} \frac{1}{\delta(a/y))} \frac{dy_1}{y_1} \cdots \frac{dy_{n-1}}{y_{n-1}}$$

φ

$y_i = a_i/a_{i+1}$ $(i = 1,\dots,n-1)$ $\qquad \delta(a/y)) = y_1^{\beta_1} \cdots y_{n-1}^{\beta_{n-1}}$

$\Rightarrow y_n = (\dots)$,

$a_1 = y_1 \cdots y_n$

$a_2 = y_2 \cdots y_n$

$(\dots)$

Key each $\beta_i > 0$. (Exercise.)

Conclude using that $\int_t^\infty z^{-\beta} \frac{dz}{z} < \infty$ $\forall\, \beta > 0$. $\square$

How many vectors does a random lattice put in a nice region?

Let $\Omega \subseteq \mathbb{R}^n$ bounded, open subset, $0 \notin \Omega$. ($\mathrm{vol} = 1$)

$\mathbb{E}_{L \in X_n^{(1)}}$ ← integral with respect to a probability Haar measure

Theorem (Siegel) $\mathbb{E}_{L \in X_n^{(1)}} |L \cap \Omega| = \mathrm{vol}(\Omega)$. ← Lebesgue

Proof sketch For $f : \mathbb{R}^n \to \mathbb{C}$, define

$$E_f : X_n^{(1)} \longrightarrow \mathbb{C}$$
$$L \longmapsto \sum_{0 \neq v \in L} f(v) \quad \text{(if convergent)}.$$

(Thus if $f = 1_\Omega$, then $E_f(L) = |L \cap \Omega|$.)

Set $B_R := \{x \in \mathbb{R}^n : |x| < R\}$.

Claim 1 $\forall R > 0$, $\mathbb{E}_L |L \cap B_R| \ll 1 + R^n$ ← constant(n)

Assuming the claim, we see that $\forall f \in C_c(\mathbb{R}^n)$, E_f : abs. conv., $\mathbb{E}_L E_f(L)$ is bounded by some continuous function of f.

Thus $C_c(\mathbb{R}^n) \ni f \longmapsto \mathbb{E}_L E_f(L)$ defines a measure μ on $\mathbb{R}^n$. **Note** μ is $\mathrm{SL}_n(\mathbb{R})$-invariant: ($\forall g \in \mathrm{SL}_n(\mathbb{R})$, $E_{f(\cdot g)}(L) = E_f(Lg)$.)

Fact (related to uniqueness of Haar measure): every $\mathrm{SL}_n(\mathbb{R})$-inv. measure μ on $\mathbb{R}^n$ is of the form $\mu = c_0 \delta_0 + c_1 \cdot \text{Lebesgue}$.

Claim 2 $c_0 = 0$, $c_1 = 1$.

Theorem follows from Claim 2.

Proof sketch of Claim 2 Take $f := \frac{1_{B_R}}{\mathrm{vol}(B_R)}$

$\Rightarrow \mu(f) = \frac{c_0}{\mathrm{vol}(B_R)} + c_1$

For each L, $E_f(L) \longrightarrow 1$ as $R \to \infty$. (Riemann summation in $\mathbb{R}^n$)

By claim 1 and dominated convergence, $\mathop{\mathbb{E}}_{L} E_f(L) \to 1$ as $R \to \infty$

$\mu(f) \to c_1$ as $R \to \infty$, so $c_1 = 1$.

(Check, similarly, that $c_0 = 0$ by considering $R \to 0$.)

Proof of claim 1

$$\mathop{\mathbb{E}}_{L} |L \cap B_R| \overset{?}{\ll} 1 + R^n$$

Suppose L: any lattice w/ reduced basis $v_1, \dots, v_n$

Iwasawa coordinates $a_1 \gg \cdots \gg a_n$

$a_j = |v_j^*|$

Recall that $\forall x \in \mathbb{Z}^n$,

$$\Big| \underbrace{\sum_{j=1}^{n} x_j v_j}_{=: v} \Big| \asymp \max_{1 \le j \le n} a_j |x_j|.$$

Thus $v \in B_R \Longrightarrow$ each $a_j |x_j| \ll R$, $x_j \in \mathbb{Z}$

$$\#(\text{possibilities for } x_j) \ll 1 + \frac{R}{a_j}$$

$$\Rightarrow \quad |L \cap B_R| \ll \prod_{j=1}^{n} \left(1 + \frac{R}{a_j}\right)$$

$$\asymp 1 + \frac{R}{a_n} + \frac{R^2}{a_n a_{n-1}} + \frac{R^3}{a_n a_{n-1} a_{n-2}}$$

$a_1 \gg \cdots \gg a_n$

$$+ (\cdots) + \frac{R^n}{a_n \cdots a_1}$$

$$\asymp \max_{0 \le m \le n} R^{n-m} a_1 \cdots a_m \overset{(?)}{\ll} 1 + R^n.$$

L: unimodular,

$\Leftrightarrow$ $a_1 \cdots a_n = 1$;

multiply through by $a_1 \cdots a_n$

Thus it suffices to show $\mathop{\mathbb{E}}_{L} a_1 \cdots a_m \overset{(?)}{<} \infty$.

By integrating over a Siegel domain, reduce to showing

$$\int_{\substack{a_1, \ldots, a_n \in \mathbb{R}_+^\times \\ a_1 \cdots a_n = 1 \\ a_i / a_{i+1} \ge \sqrt{3}/2}} (a_1 \cdots a_m) \frac{1}{\delta(a)_B} \, da$$

$x+iy \leftrightarrow \langle (y^{1/2}, xy^{-1/2}), (0, y^{-1/2}) \rangle$

For SL_2: $\int_{y \ge \sqrt{3}/2} y^{1/2} \frac{dx\,dy}{y^2} < \infty$

To see this, change to coordinates $v_1, \ldots, v_{n-1}$ as before and explicitly calculate (Exercise.)

Exercise $\mathop{\mathbb{E}}_{L} |L \cap \mathcal{R}|^2$ diverges in general.

$$\text{e.g. } \int_{y \ge \frac{\sqrt{3}}{2}} y \frac{dx\,dy}{y^2} = \infty$$

Plan for next few weeks

- definition of automorphic forms
- approximations by constant terms
- cusp forms
- finiteness theorems for autom. forms.
- Eisenstein series
- series defn, properties
- Proofs + applications