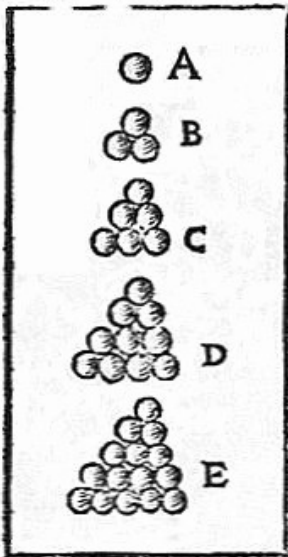


(d)
Figure 1.3 (cont.)

$$V_n = V_{vol}(B(0,1))$$

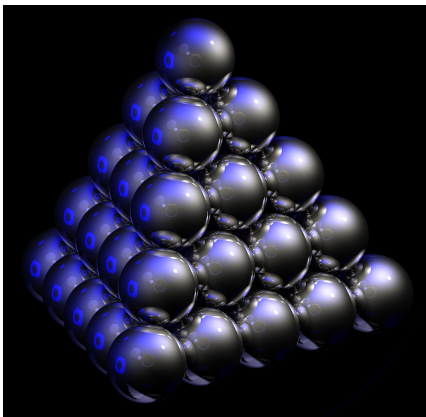
$$= \frac{\text{volume of one sphere}}{\text{volume of fundamental region}} = \frac{\left(\frac{D_1(L)}{2}\right)^n \cdot V_n}{\text{covol}(L)}$$

num pro apice, esto & alia copi



alia
ore
Est
sup
tan
inti
rior
è su
qua
bus
pe c
sup
tion
gul
Pat

necessitate concurrente cum r a



From "the six-cornered snowflake",
Kepler 1611 (based on correspondence
with Harriot).

dim n	lattice	proved optimal by (year)	optimal among all packings?
2	A2 Hexagonal (lattice)	Lagrange 1773	yes Fejes-Tóth 1943
3	A3=D3	Gauss 1831	yes Hale <u>1998</u> , <u>2015</u>
4	D4	Korkine- Zolotarev 1877	?
5	D5		?
6	E6	Blichfeldt 1934	?
7	E7	(following Voronoi 1908)	?
8	E8	Blichfeldt 1934	yes Viazovska 2016
24	Leech lattice	Cohn-Kumar <u>2004</u>	yes Cohn-Kumar-Miller- Radchenko-Viazovska 2017

Lattices Lecture 6

Reminders from Lecture 5

On $C(\mathbb{R}^n)$, define the Choquet-Fell metric by $D(X, Y) = \inf \left\{ \epsilon > 0 \mid \begin{array}{l} \forall x \in B(x, \frac{\epsilon}{2}) \cap X, \exists y \in Y \\ \text{with } \|x - y\| < \epsilon \\ \forall y \in B(y, \frac{\epsilon}{2}) \cap Y, \exists x \in X \\ \text{with } \|x - y\| < \epsilon \end{array} \right\}$

Prop Let L_1, L_2, L_3, \dots be lattices in \mathbb{R}^n .

The following are equivalent:

(a) $L_j \xrightarrow{j \rightarrow \infty} L$ (w.r.t. D)

(b) (i) $\forall l \in L \exists l_j \in L_j$ s.t. $l_j \xrightarrow{j \rightarrow \infty} l$

(ii) If $j_k \rightarrow \infty$, $l_{j_k} \in L_{j_k}$ s.t. $l_\infty = \lim_{k \rightarrow \infty} l_{j_k}$ exists,

then $l_\infty \in L$.

(c) For any basis v_1, \dots, v_n of L \exists bases

$v_1^{(j)}, \dots, v_n^{(j)}$ of L_j s.t. for $i=1, \dots, n$,

$$V_i^{(j)} \xrightarrow{j \rightarrow \infty} V_i.$$

(d) Writing $L_j = g_j \mathbb{Z}^n$ $g_j \in GL_n(\mathbb{R})$

$$L = g \mathbb{Z}^n \quad g \in GL_n(\mathbb{R})$$

$\exists \delta_j \in GL_n(\mathbb{Z})$ st. $g_j \delta_j \xrightarrow{j \rightarrow \infty} g$.
(convergence in $GL_n(\mathbb{R}) \subset \mathbb{R}^{n^2}$).

The functions $L \mapsto \mathcal{D}_1(L)$

$$L \mapsto \text{covol}(L)$$

are both continuous w.r.t. D .

$$\mathcal{X}_n \stackrel{\text{def}}{=} \{ \text{lattices in } \mathbb{R}^n \} \xleftrightarrow{\text{bijection}} GL_n(\mathbb{R}) / GL_n(\mathbb{Z})$$

$$\mathcal{X}_n \stackrel{\text{def}}{=} \{ \text{lattices in } \mathbb{R}^n \text{ of volume one} \} \xleftrightarrow{\quad} SL_n(\mathbb{R}) / SL_n(\mathbb{Z})$$

$$g\mathbb{Z}^n \xleftrightarrow{\quad} gP \quad (P = SL_n(\mathbb{Z}) \text{ or } GL_n(\mathbb{Z}))$$

Def: We say that $L_j \rightarrow \infty$ (L_j diverges
in \bar{X}_n) if the sequence $\{L_j\}$ has no
convergent subsequence (w.r.t. D).

Example: If $\inf(L_j) \rightarrow 0$ or
 $\sup(L_j) \rightarrow \infty$ or
 $\sup(L_j) \rightarrow 0$

Then $L_j \rightarrow \infty$.

Prop $L_j \rightarrow \infty$ (in \bar{X}_n) if and only if
one of $\inf(L_j) \rightarrow 0$, $\sup(L_j) \rightarrow \infty$, $\sup(L_j) \rightarrow 0$.
($\inf(L_j) \rightarrow \infty$)

Pf We saw \uparrow .

\Downarrow : Suppose by $\inf(L_j) \rightarrow 0$, $\sup(L_j) \rightarrow \infty$
 $\sup(L_j) \rightarrow 0$.

Passing to a subsequence, $\inf(L_j)$ is
bounded below, and $\sup(L_j)$ bounded
above and below. Want to $L_j \rightarrow L$

(possibly passing to a further subsequence).

$\alpha_i(L)$ = length of i^{th} vector in Korkin-Zolotarev reduction procedure.

(ex. 7) $\alpha_i \asymp \alpha_i$

where $A \asymp B$ means A, B are functions on \mathbb{Z}^n

and there is a constant $C \geq 1$ s.t. $\forall L \in \mathbb{Z}^n$,

$$\frac{1}{C} A(L) \leq B(L) \leq C A(L).$$

(C may depend on n).

By Minkowski's second theorem

$$\alpha_1(L_j) \cdots \alpha_n(L_j) \asymp \text{covol}(L_j)$$

$$0 \leq \alpha_1(L_j) \leq \cdots \leq \alpha_n(L_j)$$

\uparrow ind. of j .

\uparrow bounded above and below ind. j .

$$\alpha_n(L_j) \leq C \frac{\text{covol}(L_j)}{\alpha_1(L_j) \cdots \alpha_{n-1}(L_j)} \leq C \frac{\text{covol}(L_j)}{\alpha_1(L_j)^{n-1}}$$

\uparrow bounded above

$\Rightarrow \forall i$ $\alpha_i(L_j)$ bounded above

$\Rightarrow \forall i \ \mathcal{K}_i(L_j)$ bounded above.

If $\|v_i^{(j)}\| = \mathcal{K}_i(L_j)$, $L_j = \text{span}_{\mathbb{Z}}(v_1^{(j)}, \dots, v_n^{(j)})$

Then (passing to a subsequence)

$$v_i^{(j)} \rightarrow v_i$$

$\Rightarrow L_j$ is a convergent subseq.
by ③ of the prop.

Cor (Mahler's compactness criterion
a.k.a. Mahler's selection principle).

Let $\pi: \text{SL}_n(\mathbb{R}) \rightarrow \mathcal{X}_n = \text{SL}_n(\mathbb{R}) / \text{SL}_n(\mathbb{Z})$

$$g \mapsto g\mathbb{Z}^n$$

Then for $S \subset \text{SL}_n(\mathbb{R})$, $\overline{\pi(S)}$ is compact

$\Leftrightarrow \exists \varepsilon > 0 \ \forall x \in S, \ \mathcal{N}_1(\pi(x)) \geq \varepsilon.$

Equivalently: let $K_\varepsilon \subset \mathcal{X}_n$

$$K_\varepsilon = \{ L \in \mathcal{X}_n : \lambda_1(L) \geq \varepsilon \}$$

Then K_ε is compact for all $\varepsilon > 0$

and any $K \subset \mathcal{X}_n$ compact is contained
in K_ε for some $\varepsilon > 0$.

I.e. $\{K_\varepsilon : \varepsilon > 0\}$ are an exhaustion of \mathcal{X}_n .

Application

$$\text{Cor } \alpha_r(L) = \inf \left\{ \text{covol}(L_0) : \begin{array}{l} L_0 \subset L \text{ primitive} \\ \text{rank}(L_0) = r \end{array} \right\}$$

Then α_r is actually a minimum, i.e.

$$\exists L_0 \subset L \text{ primitive of rank } r, \text{ s.t.} \\ \text{covol}(L_0) = \alpha_r(L).$$

Pf: Let $L_j \subset L$ be primitive subgroups
of rank r s.t. $\text{covol}(L_j) \rightarrow \alpha_r(L)$.

By ex. 7 \exists a basis $u_1^{(j)}, \dots, u_r^{(j)}$ of
 L_j s.t. $\|u_i^{(j)}\| = \lambda_i(L_j) \asymp \lambda_i(L_j)$

$$\alpha_1(L) \leq \alpha_1(L_j) \leq \dots \leq \alpha_r(L_j) \leq \frac{\text{covol}(L_j)}{\alpha_1(L_j)^{r-1}} \quad \text{for some } c$$

using Mink. 2nd thm, as in previous pf.

So passing to subsequences, $u_i^{(j)} \rightarrow u_i$
for all i

$u_i \in L$ because $u_i^{(j)} \in L$, L is closed.

Define $L_\infty = \text{span}_{\mathbb{Z}}(u_1, \dots, u_r)$

$$\text{covol}(L_\infty) = \|u_1, \dots, u_r\| = \lim_{j \rightarrow \infty} \|u_1^{(j)}, \dots, u_r^{(j)}\|$$

$$= \lim_{j \rightarrow \infty} \text{covol}(L_j) \rightarrow \alpha_r(L)$$

So min is attained.

A Hermitian proof: $L = g\mathbb{Z}^n$

$$L_i = \text{span}_{\mathbb{Z}}(u_1^{(j)}, \dots, u_r^{(j)})$$

$$u_i^{(j)} = g v_i^{(j)} \quad v_i^{(j)} \in \mathbb{Z}^n.$$

$v_1^{(j)} \wedge \dots \wedge v_r^{(j)}$ is an element of $\wedge^r \mathbb{R}^n = \mathbb{R}^{\binom{n}{r}}$
 (the space of r -vectors in the Grassman algebra)
 and with integer coefficients with respect
 to the standard basis $\{e_\sigma : \sigma = (i_1 < \dots < i_r \leq n)\}$

Since $\|u_1^{(j)} \wedge \dots \wedge u_r^{(j)}\|$ converges,

so does $\|v_1^{(j)} \wedge \dots \wedge v_r^{(j)}\|$.

Since \mathbb{Z} -span of $\{e_\sigma\}$ is discrete,

$\|v_1^{(j)} \wedge \dots \wedge v_r^{(j)}\|$ is eventually constant.

So $\|u_1^{(j)} \wedge \dots \wedge u_r^{(j)}\|$ is eventually constant.

Reminder $\delta(L) =$ packing density of L

$$= \frac{\text{Vol}(B(0, \frac{\lambda_1(L)}{2}))}{\text{covol}(L)} = \frac{V_n}{2^n} \frac{\lambda_1(L)^n}{\text{covol}(L)}$$

^{max}
 $=$ proportion of space filled by
 non-overlapping balls centered at pts of L .

$$\delta_n = \sup \{ \delta(L) : L \in \mathcal{X}_n \},$$

Cor: sup is a max, i.e. in each dimension n there is L s.t. $\delta(L) = \delta_n$.

Pf: Looking for L_0 s.t.

$$\frac{\lambda_1(L_0)}{\text{covol}(L_0)^{\frac{1}{n}}} \geq \frac{\lambda_1(L)}{\text{covol}(L)^{\frac{1}{n}}} \text{ for all } L \in \mathcal{X}_n.$$

equivalently, $\mu(L_0) \stackrel{\text{def}}{=} \frac{\lambda_1(L_0)^2}{\text{covol}(L_0)^{\frac{2}{n}}}$ is maximal.

this is the Hermite constant.

Suppose $L_j \in \mathcal{X}_n$ s.t. $L_j \rightarrow \sup_{j \rightarrow \infty} \{ \lambda_1(L) : L \in \mathcal{X}_n \}$

So $\lambda_1(L_j) \geq c > 0$. By Minkowski's compactness criterion,

$L_j \rightarrow L_\infty$ along a subsequence

$$\Rightarrow \lambda_1(L_j) \xrightarrow{j \rightarrow \infty} \lambda_1(L_\infty) = \max\{\lambda_1(L) : L \in \mathcal{L}_n\}$$

(λ_1 is σ_1).

History of lattice packing problem

Hilbert's 18th problem, part 3

What is the densest sphere packing in \mathbb{R}^3 ?

What about other shapes?



Solved by Hales 1998.

Def. L_0 is called critical if

$L \mapsto \frac{\lambda_1(L)}{\text{covol}(L)^{1/n}}$ achieves a local max

at L_0 . Extreme if L_0 achieves the global max. (Extreme \Rightarrow critical).

Strategy followed for finding optimal lattices

in dimensions $n=2, \dots, 8$ is roughly the

following:

(KZ)
Step 1 If L_0 is critical then L_0
is perfect (will be defined later).

Step 2, # of perfect lattices in any
fixed dimension n is finite (up to dilations
and orthogonal transformations). (Voronoi)

Step 3 Enumerate all perfect lattices and
find the one for which $\frac{\Delta(L)}{\text{covol}(L)^{1/n}}$ is maximal.
(KZ - $n=4,5$ Blichfeldts $n=6,7,8$)

Step 4 Show L is critical

$\Leftrightarrow L$ is perfect and eutactic (will be
defined later)
(Voronoi)

of eutactic lattices in any dim is finite
(again up to dilations and orth. trans.).
(Voronoi)

Symmetric matrices

$$\text{Sym}_n = \{A \in M_n(\mathbb{R}) : A^t = A\}.$$

$$= \{ A \in M_n(\mathbb{R}) : \forall x, y \in \mathbb{R}^n, \langle Ax, y \rangle = \langle x, Ay \rangle \}$$

Sym_n is a real vector space of dim $\frac{n(n+1)}{2}$.

Facts: • Any $A \in \text{Sym}_n$ can be diagonalized

over \mathbb{R} , by an orthonormal transformation.

i.e. $\exists O \in O_n(\mathbb{R})$ s.t. $O^t A O$ is diagonal.

↑
orthonormal matrices, $O_n(\mathbb{R}) = \{ g \in GL_n(\mathbb{R}) : g^t = g^{-1} \}$

• $A \in \text{Sym}_n$ called positive definite if the eigenvalues are positive

$$\Leftrightarrow \forall x \in \mathbb{R}^n, \langle Ax, x \rangle \geq 0, \langle Ax, x \rangle = 0 \Leftrightarrow x = 0$$

$$\Leftrightarrow \exists B \in GL_n(\mathbb{R}) \text{ s.t. } A = B^t B.$$

Pf of last equivalence.

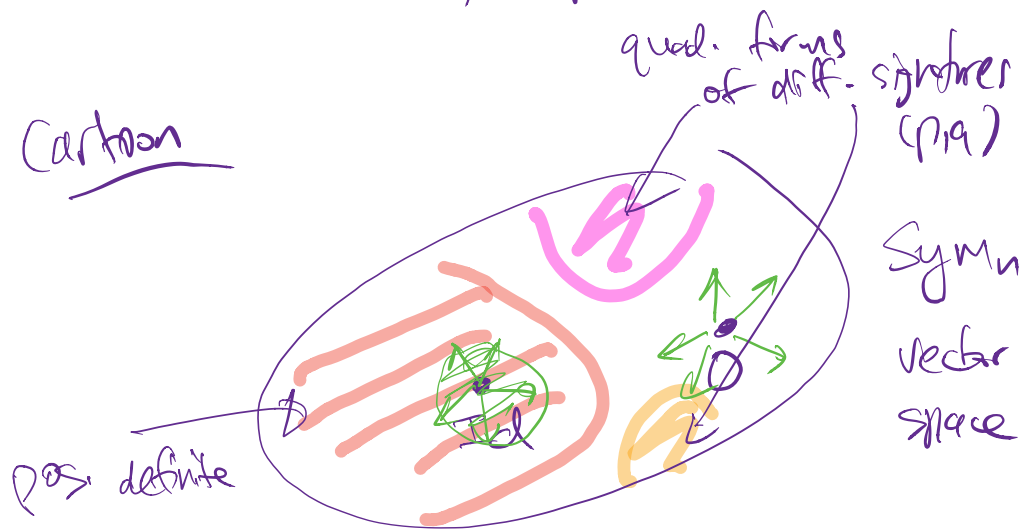
$$\uparrow A = B^t B, \text{ then } \forall x \in \mathbb{R}^n \quad \forall x \in \mathbb{R}^n - \{0\}$$

$$\langle Ax, x \rangle = \langle B^t B x, x \rangle = \langle x, B^t B x \rangle = \langle Bx, Bx \rangle \downarrow > 0$$

↓ If $A = O^t D O$, $D = \text{diag}(\beta_1, \dots, \beta_n)$ $\beta_i > 0$

⊗ Define $\sqrt{D} = \text{diag}(\sqrt{\beta_1}, \dots, \sqrt{\beta_n})$

Define $B = O^t \sqrt{D} O$, compute $B^t B = A$.



For vs, Sym_n will play the role of n tangent space at Id of pos. def. matrices.

For $x \in \mathbb{R}^n$, define $\varphi_x: \text{Sym}_n \rightarrow \mathbb{R}$

$$\varphi_x(A) = \langle Ax, x \rangle$$

$$\varphi_x \in (\text{Sym}_n)^*$$

Def Let $F = \mathbb{R}^n$. F is called perfect if

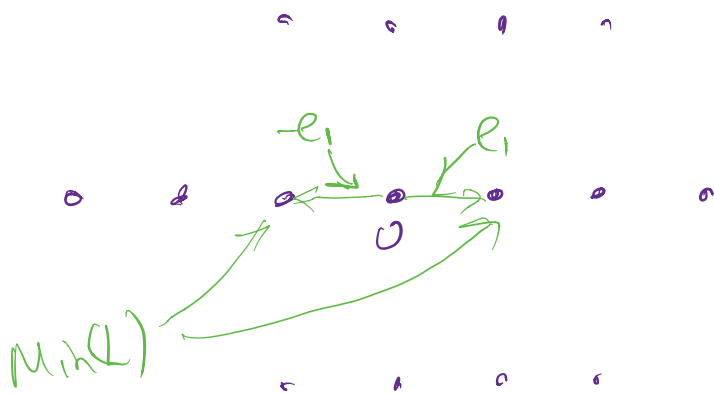
$$(\text{Sym}_n)^* = \text{span}(\{\varphi_x : x \in F\}).$$

The vectors $\{v \in L : \gamma_v(L) = \|v\|\}$ are

the minimizers for L , notation: $\text{Min}(L)$.

L is perfect if $\text{Min}(L)$ is perfect.

Examples (a) $L = \mathbb{Z}(b) \oplus \mathbb{Z}(\begin{pmatrix} 0 \\ 2 \end{pmatrix})$.



$$\text{Sym}_2 = \left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

$$\varphi_{e_1}(A) = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} a \\ b \end{pmatrix} \right\rangle = a$$

$(a, b, c) \mapsto a$.

not perfect.

(b) $L = \mathbb{Z}^2$ $\text{Min}(L) = \{\pm e_1, \pm e_2\}$.

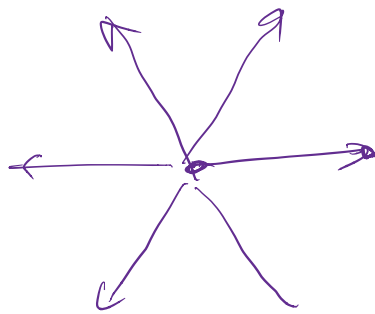
$$\psi_{e_2}(A) = \langle \begin{pmatrix} 0 & a & b \\ 1 & b & c \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rangle = c.$$

not perfect.

(two functionals can't span a

3-dim space).

(c)



$L = \text{hex. lattice}$

$$|\text{Min}(L)| = 6.$$

ex. L is perfect.

Prop: If $F \in \mathbb{R}^n$ is perfect then $\mathbb{R}^n = \text{span}(F)$.

(not iff as example (b) shows).

PF: Suppose by contradiction $V = \text{span}(F) \neq \mathbb{R}^n$

Let $A \neq 0$ $V \subset \ker A$. Can take A

symmetric (ex.).

Then $\forall x \in F$, $\varphi_x(A) = \langle Ax, x \rangle = \langle 0, x \rangle = 0$

Contradiction to $\{\varphi_x : x \in F\}$ spans $(\text{Sym}_n)^*$.

Prop: If L is perfect then

$$|\text{Min}(L)| \geq n(\text{ut}).$$

PF: Let $\text{Min}(L) = \{\pm v_1, \dots, \pm v_t\}$

$$|\text{Min}(L)| = 2t. \quad \varphi_{v_i} = \varphi_{-v_i} \quad \forall i$$

$$\text{span}(\{\varphi_x : x \in \text{Min}(L)\}) = \text{span}(\{\varphi_{v_i} : i=1, \dots, t\})$$

$$\text{has dim } \frac{n(\text{ut})}{2} \Rightarrow t \geq \frac{n(\text{ut})}{2} \Rightarrow |\text{Min}(L)| \geq 2t \geq n(\text{ut}).$$

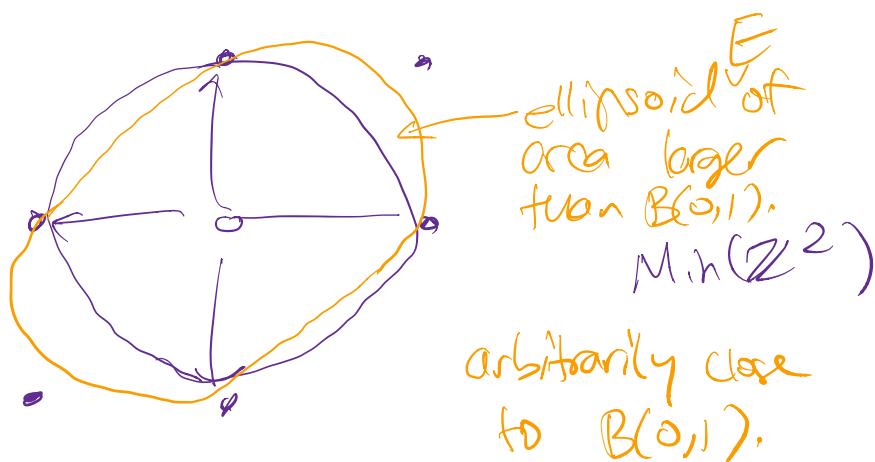
From this, easy to show (ex.) that hexagonal

lattice is the unique (up to dilation and rotation) perfect lattice in \mathbb{R}^2 .

Thm (Korkine-Zolotarev)

If L is critical then L is perfect.

Idea (picture for \mathbb{Z}^2 lattice)



Apply a lin. trans. g that maps E to

$$B(0,r) \quad r > 1, \det g = 1.$$

$g\mathbb{Z}^2$ is close to \mathbb{Z}^2 because E is

close to $B(0,1)$, and $\lambda_1(g\mathbb{Z}^2) > 1$.

$$\begin{aligned}
 \text{Ellipsoid } g(B(0,1)) &= \{g \in GL_n(\mathbb{R})\} \\
 &= g \{x \in \mathbb{R}^n : \langle x, x \rangle \leq 1\} \\
 &= \{y \in \mathbb{R}^n : \langle g^{-1}x, g^{-1}x \rangle \leq 1\} = \{y \in \mathbb{R}^n : \langle Ay, y \rangle \leq 1\}
 \end{aligned}$$

$$A = (g^{-1})^t g^{-1}.$$

Prop: Define $GL_n(\mathbb{R}) \rightarrow \text{Sym}_n$
 $g \mapsto A(g) = g^t g - \text{Id}.$

There is a nbd \mathcal{U} of Id in $GL_n(\mathbb{R})$
 s.t. $\mathcal{V} = \{A(g) : g \in \mathcal{U}\}$ is a nbd of 0

in Sym_n , and $g \mapsto A(g)$ restricted
 to \mathcal{U} is an open surjective $\mathcal{U} \rightarrow \mathcal{V}$.

$$(g \in \mathcal{U}, A(g) = 0) \iff g \in O_n,$$

\uparrow
 orthogonal matrices.

PF: Open mapping theorem. (ex.)

( is an inverse of $g \mapsto Ag$,

as long as $\text{Id} + A$ is pos. definite).

Lemma 1 For any lattice L , there is
a hbd \mathcal{U} of Id in $\text{GL}_n(\mathbb{R})$ s.t.

$\forall g \in \mathcal{U}, \text{Min}(gL) \subset g \text{Min}(L)$.

PF: Since L is discrete, there is $\eta > 0$
s.t. if $v \in L, v \neq 0, v \in \text{Min}(L)$

then $\|v\| > (1 + \eta) \lambda_1(L)$.

Define $\mathcal{U} = \left\{ g \in \text{GL}_n(\mathbb{R}) : \|g - \text{Id}\|_{\text{op}} < \frac{\eta}{2(1+\eta)} \right\}$

Then $\forall v \in \text{Min}(L), \forall g \in \mathcal{U}, \|v\| = \lambda_1(L)$

$\|gv\| \leq \|v\| + \|(g - \text{Id})v\| < \left(1 + \frac{\eta}{2(1+\eta)}\right) \|v\|$
 $< (1 + \frac{\eta}{2}) \lambda_1(L)$.

$\forall v \in L, v \neq 0, v \notin \text{Min}(L) \forall g \in \mathcal{U},$

$$\begin{aligned} \|gv\| &\geq \|v\| - \|(g - \text{Id})v\| \geq \|v\| - \frac{\eta}{2(1+\eta)} \|v\| \\ &= \|v\| \left[\frac{2+\eta}{2(1+\eta)} \right] \geq \lambda_1(L)(1+\eta) \left(\frac{1+\eta/2}{1+\eta} \right) = \left(1 + \frac{\eta}{2}\right) \lambda_1(L) \end{aligned}$$

So the shortest vector of gL is of the form gv for some $v \in \text{Min}(L)$.

Lemma 2 For any L , there is a word

\mathcal{N} of 0 in Sym_n s.t. for $A = A(g) \in \mathcal{N}$

$$\lambda_1(gL)^2 = \lambda_1(L)^2 + \min_{v \in \text{Min}(L)} \langle v, Av \rangle.$$

PF: By Lemma 1, in order to compute

$\lambda_1(gL)$ (where $g \in \mathcal{U}$), suffices

to consider vectors $gv, v \in \text{Min}(L)$.

For such v ,

$$\|gv\|^2 = \langle gv, gv \rangle = \langle v, g^t g v \rangle = \langle v, (\text{Id} + A)v \rangle$$

$$= \|v\|^2 + \langle v, Av \rangle = \|v\|^2 + \psi_v(A).$$

We are trying to maximize $\frac{\mathcal{D}_1(L)}{\text{covol}(L)^{\frac{1}{n}}}$.

To understand denominator, need to understand $\det(g)$ for g close to Id .

Lemma 3: There is a nbd \mathcal{U} of 0 in Sym_n such that for any $A = A(g) \in \mathcal{U}$, with $\text{Tr}(A) \leq 0$, either $g \in O_n$, or $\det g < 1$.

Rk If $A(g_1) = A(g_2)$ then $g_1 = O g_2$ where $O \in O_n$ and $|\det(g_1)| = |\det(g_2)|$.

Let's postpone the proof.

Proof of KZ thm (assuming Lemma 3).

Suppose L is critical, and suppose
(by contradiction) that $\exists A \in \text{Sym}_n$, $A \neq 0$

s.t. $\forall x \in \text{Min}(L)$, $\ell_x(A) = 0$.

By replacing (if necessary) A with
 $-A$, we can $\text{tr}(A) \leq 0$. By replacing A

with sA for $s > 0$ small, can find
such A arbitrarily close to 0.

For each small s , let $g_s \in \text{GL}_n(\mathbb{R})$

s.t. $A(g_s) = sA$. Since $sA \neq 0$,

$g_s \notin O_n$. By Lemma 3, $\det(g_s) < 1$.

By Lemma 2,

$$\pi_1(gL) = \pi_1(L).$$

$$\text{So } \frac{\chi_1(gL)}{\text{covol}(gL)^{\frac{1}{n}}} = \frac{\chi_1(L)}{\text{covol}(L)^{\frac{1}{n}}} \cdot \frac{1}{\det(g_S)^{\frac{1}{n}}}$$

$$> \frac{\chi_1(L)}{\text{covol}(L)^{\frac{1}{n}}} \quad \cdot L \text{ is not critical.}$$