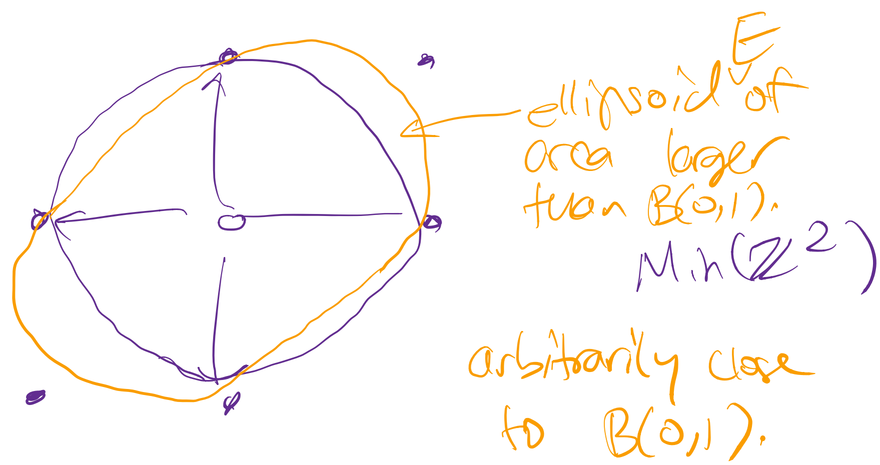
dim n	# critical	# perfect	# eutactic
2	1	1	2
3	1	1	5
4	2	2	16
5	3	3	118
6	6	7	?
7	30	33	
8	2408	10916	
9		$> 20{,}000{,}000$	
general	?	$e^{c_1 n} \leq \quad \leq e^{c_2 n^{2+\varepsilon}}$	

<u>Idea</u> (picture for $\mathbb{Z}^2$ lattice)



$\bar{\lambda}_1(L) = \dfrac{\lambda_1(L)}{\mathrm{covol}(L)^{\frac{1}{n}}}$. L_0 is <u>critical</u> if $L \mapsto \bar{\lambda}_1(L)$ has a local maximum at L_0.

Lattices Lecture 7

Some reminders from lecture 6:

Sym_n = symmetric $n\times n$ matrices

$GL_n(\mathbb{R}) \ni g \longmapsto A(g) = g^t g - \mathrm{Id}$.

A maps $\mathrm{Id} \mapsto 0$ and is <u>open</u> in a nbd of Id:

$\exists$ nbd $\mathcal{U}$ of Id in $GL_n(\mathbb{R})$ s.t. $\mathcal{V} = \{A(g) : g \in \mathcal{U}_0\}$ is a nbd of $\mathcal{O}$ in Sym_n, for any $\mathcal{U}_0 \subset \mathcal{U}$ nbd of Id.

$A(g_1) = A(g_2) \Leftrightarrow g_1^t g_1 = g_2^t g_2 \Leftrightarrow$

$\mathrm{Id} = g_2^t g_2 g_1^{-1} g_1^{-t} = g_2 g_1^{-1} g_1^{-t} g_2^t \Leftrightarrow g_2 g_1^{-1} \in O_n(\mathbb{R})$

$\Leftrightarrow \exists\, O \in O_n(\mathbb{R})$ s.t. $g_2 = O g_1$

For $x \in \mathbb{R}^n$, $\varphi_x : \mathrm{Sym}_n \to \mathbb{R}$, $\varphi_x(A) = \langle Ax, x\rangle$

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

$\mathrm{Min}(L) = \{v \in L : \|v\| = \lambda_1(L)\} = \{$shortest nonzero vectors of $L\}$

L is <u>perfect</u> if $\{\varphi_x : x \in \mathrm{Min}(L)\}$ spans $(\mathrm{Sym}_n)^*$.

Thm 0. (Korkine-Zolotarev 1857):

If L_0 is critical then L_0 is perfect.

Lemma 2 For any L, there are nbds $\mathcal{U}, \mathcal{V}$ of Id in $GL_n(\mathbb{R})$, and of 0 in Sym_n, s.t. for all $g \in \mathcal{U}$,

$$\lambda_1(gL)^2 = \lambda_1(L)^2 + \min_{v \in Min(L)} \varphi_v(A), \quad A = A(g),$$

$$\mathcal{V} = \{A(g) : g \in \mathcal{U}\}.$$

Lemma 3: There is a nbd $\mathcal{V}$ of 0 in Sym_n s.t. for any $A = A(g) \in \mathcal{V}$ with $tr(A) \leq 0$, either $g \in O_n$ or $\det g < 1$.

Pf: Suppose $tr(A) \leq 0$, $A \neq 0$, $A = A(g)$, $g \in \mathcal{U}$.

Consider the function $h : [0,1] \longrightarrow \mathbb{R}$

$$h(s) = \log \det (Id + sA).$$

Let $\lambda_1, \dots, \lambda_n$ be the eigenvalues of A (real since A is symmetric).

$$h(s) = \log\left(\prod_{i=1}^{n}(s\lambda_i+1)\right)$$

$$h'(s) = \sum_{i=1}^{n} \frac{\lambda_i}{1+s\lambda_i} \qquad h'(0) = \sum_{i=1}^{n}\lambda_i = tr(A) \le 0$$

$$h''(s) = -\sum_{i=1}^{n} \frac{\lambda_i^2}{(1+s\lambda_i)^2} \qquad h''(0) = -\sum \lambda_i^2 < 0.$$

So for $s \in (0, R_A)$ (for some $R_A > 0$)

$h(s) < 0 \Rightarrow \det(Id + sA) < 1$

$A(g_s) = sA$. $\qquad \det(g_s^t g_s) = (\det g_s)^2$

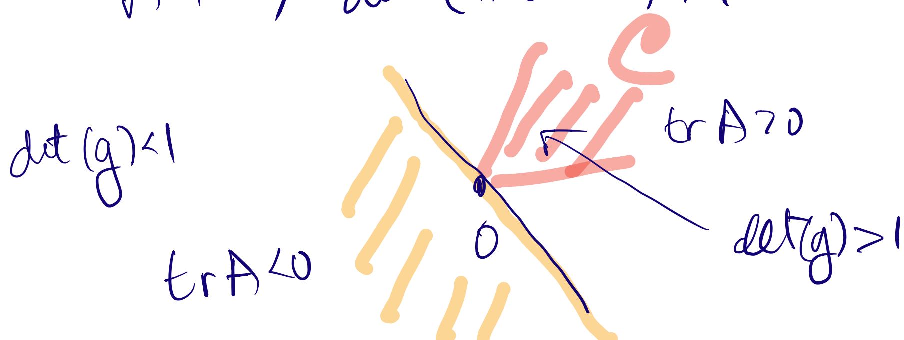
By a compactness argument (ex.) we can choose R_A independent of A, to get a nbd $\mathcal{V}$ of 0 in Sym_n s.t. $\det(Id + A) < 1$ for $A \in \mathcal{V}$, $A \neq 0$, $tr(A) \le 0$.

A <u>cone</u> in $\mathbb{R}^N$ is a set $\mathcal{C}$ satisfying

$\forall x, y \in \mathcal{C}$, $\forall \alpha, \beta \geq 0$, $\alpha x + \beta y \in \mathcal{C}$

(in particular C is convex and closed under multiplication by non-negative scalars).

<u>Lemma 4</u> Let $C \subset Sym_n$ be a closed cone s.t. $tr(A)>0$ for all $A \in C \setminus \{0\}$.
Then $\exists$ nbd V of 0 in Sym_n s.t. $\forall A \in V \cap C$, $A \neq 0$, $\det(Id + A) > 1$.



<u>Pf</u> Let $Sym_n^{(1)} = \{A \in Sym_n : \|A\| = 1\}$

(the unit sphere for some norm on Sym_n).

Let $A \in C \cap Sym_n^{(1)}$, $h(s) = \log\det(Id + sA)$

(as in Lemma 3).

Since $tr(A) > 0$, $h'(0) > 0$.

Therefore $\exists\, R_A > 0$ such that for $s \in (0, R_A)$, $h(s) > 0$. By a compactness argument, can take $0 < R \le R_A$ independent of $A \in C \cap \mathrm{Sym}_n^{(1)}$.

Using this, $\quad \mathcal{V} = \left\{ sA : \begin{array}{l} s \in [0,R] \\ A \in \mathrm{Sym}_n^{(1)} \cap C \end{array} \right\}$.

satisfies the conclusion.

<u>Def</u> L, L' are <u>similar</u> if $\exists\, t \in \mathbb{R} \setminus \{0\}$ and $O \in \mathcal{O}_n$ s.t. $L' = tOL$.

$\mathcal{O}_n$: orthogonal $n \times n$ matrices

<u>Thm 1</u>: The following are equivalent:

(a) L is critical

(b) If $A \in \mathrm{Sym}_n$, $\mathrm{tr}(A) \le 0$, and $\min_{x \in \mathrm{Min}(L)} \varphi_x(A) \ge 0$ then $A = 0$.

(c) There is a nbd $\mathcal{U}$ of Id in $GL_n(\mathbb{R})$ s.t. $\forall g \in \mathcal{U}$, either $g = tO$ for $t \in \mathbb{R}$, $O \in O_n$ (so that gL and L are similar) or $\bar{\lambda}_1(gL) < \bar{\lambda}_1(L)$.

Pf: (c) $\Rightarrow$ (a) obvious.

(a) $\Rightarrow$ (b) By contradiction. Suppose $A \neq 0$ $A \in Sym_n$, with $\min_{x \in Min(L)} \varphi_x(A) \geq 0$, $tr(A) \leq 0$.

Multiplying A by $s > 0$, can make sA close to 0, so can assume that the conclusions of Lemmas 2 and 3 apply to A. Since L is a local max for $\bar{\lambda}_1$, $\bar{\lambda}_1(gL) \leq \bar{\lambda}_1(L)$, for g s.t. $A(g) = A$.

By Lemma 2, $\lambda_1(gL) \geq \lambda_1(L)$

By Lemma 3, $\det(g) < 1$ so

$$\bar{\lambda}_1(gL) = \frac{\lambda_1(gL)}{\operatorname{covol}(gL)^{\frac{1}{n}}} \geq \frac{\lambda_1(L)}{\operatorname{covol}(L)} \cdot \frac{1}{\det(g)^{\frac{1}{n}}} > \bar{\lambda}_1(L)$$

(b) $\Rightarrow$ (c) Let $\mathcal{C} = \{A \in \mathrm{Sym}_n : \min_{x \in \mathrm{Min}(L)} \varphi_x(A) \geq 0\}$.

$\mathcal{C}$ is a closed cone. By (b), $\operatorname{tr}(A) > 0$ for $A \in \mathcal{C} \setminus \{0\}$, so can apply Lemma 4.

Suppose $\mathcal{U}$ as in Lemma 4, let $g \in \mathcal{U}$, suppose $\det g = 1$, $g \notin O_n$.

Then by Lemma 4, $A(g) \notin \mathcal{C}$, so $\bar{\lambda}_1(gL)^2 =$

$$= \frac{\lambda_1(gL)^2}{\operatorname{covol}(gL)^{2/n}} = \frac{\lambda_1(L)^2 + \min_{x \in \mathrm{Min}(L)} \varphi_x(A(g))}{\operatorname{covol}(gL)^{2/n}}$$

$$\overset{\det g = 1}{=} \frac{\lambda_1(L)^2 + \min_{x \in \mathrm{Min}(L)} \varphi_x(A(g))}{\operatorname{covol}(L)^{2/n}} \overset{A(g) \notin \mathcal{C}}{<} \frac{\lambda_1(L)^2}{\operatorname{covol}(L)^{2/n}} = \bar{\lambda}_1(L).$$

If $\det g \neq 1$, then can rescale g by multiplying by a scalar. This does not affect $\lambda_1(gL)$ or the conclusion.

<u>Def</u> $F \subset \mathbb{R}^n$ finite is called <u>eutactic</u> if there are <u>positive</u> coefficients $\{\lambda_x : x \in F\}$ s.t. for each $A \in \mathrm{Sym}_n$, $\mathrm{tr}(A) = \sum_{x \in F} \lambda_x \varphi_x(A)$.

<u>Remark</u> Since $\mathrm{tr} \in \mathrm{Sym}_n^*$, so if F is perfect then $\exists \{\lambda_x : x \in F\}$ s.t. $\mathrm{tr}(A) = \sum_{x \in F} \lambda_x \varphi_x(A)$

For eutactic, we need the λ_x to be positive.

<u>Def</u> L is called eutactic if $\mathrm{Min}(L)$ is eutactic.

<u>Example:</u> $n=2$, $L = \mathbb{Z}^2$, $\min(L) = \{\pm e_1, \pm e_2\}$

We computed $\varphi_{e_1}\begin{pmatrix} a & b \\ b & c \end{pmatrix} = \varphi_{-e_1}\begin{pmatrix} a & b \\ b & c \end{pmatrix} = a$

and $\quad \varphi_{e_2}\begin{pmatrix} a & b \\ b & c \end{pmatrix} = \varphi_{-e_2}\begin{pmatrix} a & b \\ b & c \end{pmatrix} = c$

$tr(A) = a+c = \frac{1}{2}(\varphi_{e_1} + \varphi_{-e_1} + \varphi_{e_2} + \varphi_{-e_2})(A).$

So $\mathbb{Z}^2$ is eutactic.

(could also write $tr = \varphi_{e_1} + \varphi_{e_2}$, but this would not show L is eutactic).

<u>Thm 2</u> (Voronoi) L is critical if and only if L is perfect and eutactic.

<u>Pf of direction $\Uparrow$</u>: We assume L is perfect and eutactic, and check condition (b) of Thm 1.

Let $\{\lambda_x : x \in Min(L)\}$ s.t. $\lambda_x > 0 \ \forall x$

and $\sum \lambda_x \varphi_x = tr.$

Let $A \in Sym_n$, $\min\limits_{x \in Min(L)} \varphi_x(A) \geq 0$, $tr(A) \leq 0$.

Need to show $A = 0$.

$0 \geq tr(A) = \sum \lambda_x \varphi_x(A) \geq 0$

and $\varphi_x(A)=0$ for all $x \in \mathrm{Min}(L)$.

But L is perfect, $\varphi(A)=0$ for all $\varphi \in \mathrm{Sym}_n^*$,

so $A=0$.

For the converse, need a lemma (from linear programming).

<u>Lemma 5</u> Let V be a vector space over $\mathbb{R}$, and let V^* be its dual. Let $\varphi_1, \dots, \varphi_r \in V^*$. Then TFAE: (i) $\varphi_i(x) \geq 0$, $i=1,\dots,r$

$$\Downarrow$$

$$\varphi_i(x) = 0, \quad i=1,\dots,r$$

(for any $x \in V$).

(ii) $\exists\, \lambda_1, \dots, \lambda_r$ positive s.t. $\sum_{i=1}^{r} \lambda_i \varphi_i = 0$.

(ii) $\Rightarrow$ (i) is easy (ex.) and we will not need it.

(i) $\Rightarrow$ (ii). Let $W = \bigcap_{i=1}^{r} \ker \varphi_i$.

φ_i induces a linear functional on V/W for any i. The validity of both (i) and (ii) only depends on whether they are valid on V/W, so we can replace V by V/W.

In other words, we can assume $\bigcap_{i=1}^{r} \ker \varphi_i = \{0\}$, and V is finite dimensional.

We will prove (i) $\Rightarrow$ (ii) by induction on r and on $\dim V$. Trivial if $r=0$ or $r \geq 1$ and $\dim(V)=0$.

Let $m \leq r$ to be the largest possible, for which there are $\varphi_{i_1}, \ldots, \varphi_{i_m} \subset \{\varphi_1, \ldots, \varphi_r\}$, distinct, s.t. (i) fails for this m-tuple, i.e. $\exists x \in V$, with $\varphi_{i_j}(x) \geq 0$ $j=1, \ldots, m$ and not all zero. Since we assumed (i) for $\varphi_1, \ldots, \varphi_r$, we have $m < r$.

By re-indexing, assume $\varphi_{i_1},\dots,\varphi_{i_m} = \varphi_1,\dots,\varphi_m$.

Claim: $V^* = \operatorname{span}(\varphi_1,\dots,\varphi_m)$.

Otherwise, $\exists y \in \bigcap_{i=1}^{m} \ker \varphi_i$, $y \neq 0$.

Since $\bigcap_{i=1}^{r} \ker \varphi_i = \{0\}$, $\exists k > m$, s.t.

$\varphi_k(y) \neq 0$. Replacing y with $-y$ if necessary, can assume $\varphi_k(y) > 0$.

This contradicts the maximality in def of m, and $(\varphi_1,\dots,\varphi_m,\varphi_k)$ does not satisfy (i).

This proves the claim.

We continue with two cases.

Case 1. $r > m+1$. Replacing $\varphi_1,\dots,\varphi_r$ with $\varphi_1,\dots,\varphi_{r-1}$. Using the fact that m is chosen as large as possible, (i) holds for $\varphi_1, \dots, \varphi_{r-1}$. By induction hypothesis, (ii) holds for $\varphi_1, \dots, \varphi_{r-1}$.

That is, there are $\rho_1, \dots, \rho_{r-1}$ positive, with $0 = \sum_{i=1}^{r-1} \rho_i \varphi_i$. Since $\mathrm{span}(\varphi_1, \dots, \varphi_{r-1}) = V^*$

(from Claim and $m \le r-1$)

$\exists c_1, \dots, c_{r-1}$ s.t. $\varphi_r = \sum_{i=1}^{r-1} c_i \varphi_i$.

Choose $\lambda_r > 0$ small enough, so that if we define $\lambda_i = \rho_i - \lambda_r c_i$ we have $\lambda_i > 0$ for $i = 1, \dots, r-1$.

Then $\sum_{i=1}^{r} \lambda_i \varphi_i = \sum_{i=1}^{r-1} (\rho_i - \lambda_r c_i) \varphi_i + \lambda_r \varphi_r$

$= 0 - \lambda_r \sum_{i=1}^{r-1} c_i \varphi_i + \lambda_r \varphi_r = 0$.

<u>Case 2</u> $r = m+1$. Let $H = \ker \varphi_r$.

Apply induction to H. For any $x \in H$, if $\varphi_i(x) \geq 0$ for $i=1,\dots,r-1$, then $\varphi_i(x)=0$ for $i=1,\dots,r$.

So (i) holds for $(H, \varphi_1,\dots,\varphi_{r-1})$

so $\exists \lambda_1,\dots,\lambda_{r-1}$ positive, s.t.

$$\sum_{i=1}^{r-1} \lambda_i \varphi_i \text{ vanishes on } H.$$

By (i) and the definition of $m=r-1$

there is $v \in V$ s.t. $\varphi_r(v) < 0$ and $\varphi_i(v) \geq 0$ for $i=1,\dots,r-1$, and $\varphi_i(v) > 0$ for at least one index i.

Then $\sum_{i=1}^{r-1} \lambda_i \varphi_i(v) > 0$, $\varphi_r(v) < 0$,

so there is $\lambda_r > 0$ s.t.

$$\sum_{i=1}^{r} \lambda_i \varphi_i(v) = 0.$$

This means that $\sum_{i=1}^{r} \lambda_i \varphi_i$ vanishes both on H and on v. Since

$\mathrm{span}(\{v\} \cup H) = V$, $\sum_{i=1}^{r} \lambda_i \varphi_i = 0$ on V.

Pf of $\Downarrow$ in Thm 2. We already showed (Thm 0) that L is perfect. To show L is eutactic, apply Lemma 5, to the linear forms $\{-tr\} \cup \{\varphi_x : x \in Min(L)\}$

(ii) of Lemma 5 implies L is eutactic, need to check (i) of Lemma 5.

Need to show that if $tr(A) \leq 0$, and $\varphi_x(A) \geq 0$ for all $x \in Min(L)$, then $\varphi_x(A) = 0$ $\forall x \in Min(L)$ and $tr(A) = 0$.

Let $k \in \mathbb{R}$ be a parameter, and $A' = A - k \cdot Id$

Then $tr(A') = tr(A) - nk$, and for $x \in Min(L)$,
$\varphi_x(A') = \varphi_x(A) - k\lambda_1^2(L)$

So $\min_{x \in Min(L)} \varphi_x(A') = \min_{x \in Min(L)} \varphi_x(A) - k\lambda_1^2(L)$.

Choose k to make this minimum equal to
0. So $k \geq 0$ and hence $tr(A') \leq tr(A) \leq 0$

By Thm 1, statement (5), $A' = 0$.
So $A = k \cdot Id$
Since $\varphi_x(A) = -k^2 \lambda_1(L) \leq 0$ and
$tr(A) = kn \geq 0$, we find $k = 0$
and hence $A = 0$. So
$tr(A) = 0 = \varphi_x(A)$ for all $x \in Min(L)$
verifying (i).

Thm 3 (Voronoi) For each n, there are finitely many perfect lattices in $\mathcal{X}_n$ (up to similarity). In particular, finitely many critical lattices (up to similarity).

Remark In 1977, Ash proved that there are only finitely many eutactic lattices in $\tilde{\mathcal{X}}_n$ (up to similarity).

Pf of thm 3 Let $L_1, L_2, \ldots \in \tilde{\mathcal{X}}_n$ be pairwise non-similar perfect lattices (by contradiction). By rescaling we can assume $\lambda_1(L_j) = 1$ for each j.

As we saw, for each perfect lattice,

$\mathrm{Min}(L)$ span $\mathbb{R}^n$, and hence

$$\lambda_1(L_j) = \lambda_2(L_j) = \cdots = \lambda_n(L_j).$$

Since $1 = \lambda_1(L) \cdots \lambda_n(L) \asymp \mathrm{covol}(L)$

(by Minkowski's 2nd thm).

That is, $\exists\, C > 0\ \forall j$

$$\frac{1}{C} \leq \mathrm{covol}(L_j) \leq C.$$

By a proposition from previous lecture, $L_j \underset{j\to\infty}{\not\to} \infty$, i.e. has a convergent subsequence.

Passing to a subsequence, assume $L_j \underset{j\to\infty}{\longrightarrow} L_\infty$. Claim: $\#(\mathrm{Min}(L_j))$ is bounded above (ind. of j).

Indeed, for each j, the balls $\{B(x,\frac{1}{2}) : x \in \mathrm{Min}(L_j)\}$ are disjoint, and contained in $B(0,\frac{3}{2})$. So $\#(\mathrm{Min}(L_j)) \leq 3^n$.

Passing to a subsequence, can assume $\#\mathrm{Min}(L_j) = M$ (ind. of j).

Write $L_j = g_j\mathbb{Z}^n$, where $g_j \underset{j\to\infty}{\longrightarrow} g_\infty$

$L_\infty = g_\infty \mathbb{Z}^n$. $\mathrm{Min}_j = g_j^{-1}(\mathrm{Min}(L_j)) \subset \mathbb{Z}^n$

For large enough j, vectors in Min_j

have length at most $2\|g_\infty^{-1}\|_{op}$

So passing to a subsequence, can

assume $\mathrm{Min}_j = \mathrm{Min}$ is the same

for all j.

To get a contradiction, enough to show

that if $L_1 = g_1\mathbb{Z}^n$, $L_2 = g_2\mathbb{Z}^n$

with $\lambda_1(L_1) = \lambda_1(L_2) = 1$

L_1, L_2 perfect, $\mathrm{Min}(L_i) = g_i \mathrm{Min}$, $i=1,2$

then L_1 and L_2 are similar.

To see this, let $x \in \mathrm{Min}$, $x = g_1^{-1}y$, $y \in \mathrm{Min}(L_1)$

$$1 = \|y\|^2 = \|g_1 x\|^2 = \langle g_1 x, g_1 x\rangle = \langle g_1^t g_1 x, x\rangle$$

$= \langle A_1 x, x \rangle$, where $A_1 = g_1^t g_1$

Similarly, $1 = \langle A_2 x, x \rangle$ where $A_2 = g_2^t g_2$.

So $\forall x \in \mathrm{Min}$, $\langle (A_1 - A_2) x, x \rangle = 0$

$$\|$$

$\langle (A_1 - A_2) g_1^{-1} y, g_1^{-1} y \rangle$ for all $y \in \mathrm{Min}(L_1)$.

$$\|$$

$\langle g_1^{-t} (A_1 - A_2) g_1^{-1} y, y \rangle$.

Since L_1 is perfect,

$$0 = g_1^{-t} (A_1 - A_2) g_1^{-1} \Longrightarrow A_1 - A_2 = 0$$

$$\Longrightarrow g_1^t g_1 = g_2^t g_2 \Longrightarrow g_2^t g_2 g_1^{-1} g_1^{-t} = Id$$

$$\Longrightarrow g_2 g_1^{-1} g_1^{-t} g_2^t = Id \Longrightarrow g_2 g_1^{-1} \in O_n$$

$\Longrightarrow \exists\, O \in O_n$ s.t. $g_2 = O g_1$

$\Longrightarrow L_2$ and L_1 are similar.

Connection ellipsoids and symmetric matrices

$$B = \{ x : \langle x, x \rangle \le 1 \}$$

$$gB = \{ y : \langle g^{-1}y, g^{-1}y \rangle \le 1 \} = \{ y : \langle Ay, y \rangle \le 1 \}$$

ellipsoid

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

symm. matrix

$\left\{ \begin{matrix} \text{norms associated} \\ \text{with pos. def.} \\ \text{quad. forms} \\ \text{on } \mathbb{R}^n \end{matrix} \right\} \longleftrightarrow \{ \text{ellipsoids} \}$

$\longleftrightarrow S_n^+ \longleftrightarrow O_n(\mathbb{R}) \backslash GL_n(\mathbb{R})$

$g^t g \longleftarrow g$

The space of interest for us will be

similarity classes of $\to O_n(\mathbb{R}) \backslash SL_n(\mathbb{R}) / SL_n(\mathbb{Z})$

lattices of
covolume one