Dynamics on the space of lattices and number theory

Elon Lindenstrauss

March 16, 2003
Introduction

• in dynamics we study actions of groups with complicated orbits

• a particularly appealing case: flows on locally homogeneous spaces, an example of which is space of unimodular lattices in $\mathbb{R}^n$ (for example $n = 3$).

• study of these are very specific dynamical systems involves deep issues and has many applications, e.g. Oppenheim conjecture (proved), Littlewood conjecture (open), diophantine approximation, and more!
The space of lattices

• If \( v_1, \ldots, v_n \) are \( n \) linearly independent vectors in \( \mathbb{R}^n \) then

\[
\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_n
\]

will be called a lattice (in \( \mathbb{R}^n \)).

• Many different \( v_1, \ldots, v_n \) generates the same \( \Lambda \).

\[
\text{covol } \Lambda := \det(v_1, \ldots, v_n) = \text{vol}(\mathbb{R}^n/\Lambda)
\]

does not depend on choice of generators.

• Space of (unimodal) lattices is

\[
X_n = \{ \text{lattices } \Lambda < \mathbb{R}^n : \text{covol } \Lambda = 1 \} \cong \text{SL}(n, \mathbb{Z}) \mathbin{\char'176} \text{SL}(n, \mathbb{R})
\]

isomorphism given by

\[
\mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_n \mapsto \text{SL}(n, \mathbb{Z})(v_1, \ldots, v_n)^T
\]

• Special case of \( \Gamma \mathbin{\char'176} G \) where \( G \) is Lie group and \( \Gamma \) discrete subgroup of \( G \).
Properties of the space lattices

- $\text{SL}(n, \mathbb{R})$ acts on $X_n$ by $\text{SL}(n, \mathbb{Z})h.g = \text{SL}(n, \mathbb{Z})(hg)$; in terms of lattices $\Lambda.g = \{g^Tv : v \in \Lambda\}$.

- Haar measure on $\text{SL}(n, \mathbb{R})$ projects to a $\text{SL}(n, \mathbb{R})$ invariant measure $\nu$ on $X_n$; unique up to a scalar. A nontrivial theorem says $\nu$ is finite.

- Even though $X_n$ as finite volume, it is not compact:

  **Mahler’s criterion:** $\Lambda_i \to \infty$ if and only if there are $v_i \in \Lambda_i$ with $\|v_i\| \to 0$.

  For every $\epsilon > 0$, $\{\Lambda \in X_n : \forall v \in \Lambda, \|v\| \geq \epsilon\}$ is compact.
Example: the case \( n = 2 \)

\( \text{SL}(2, \mathbb{R}) \) acts on \( \mathbb{H} = \{ z \in \mathbb{C} : \Im z > 0 \} \) by

\[
\begin{pmatrix}
  a & b \\
  c & d \\
\end{pmatrix} \cdot z = \frac{az + b}{cz + d}.
\]

\( i \in \mathbb{H} \) is fixed by \( \text{SO}(2, \mathbb{R}) \) so \( \mathbb{H} \cong \text{SL}(2, \mathbb{R})/\text{SO}(2, \mathbb{R}) \) and unit tangent bundle \( S\mathbb{H} \cong \text{SL}(2, \mathbb{R})/\{\pm I\} \).

In particular: \( X_2 \) can be identified with the unit tangent bundle of surface \( M = \text{SL}(2, \mathbb{Z}) \backslash \mathbb{H} \).
Two important 1-param subgroups acting on $X_2$:

$$a(t) = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \text{ and } u(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$  

$x \rightarrow x.a(t)$ gives geodesic flow on $SM$; $x \rightarrow a.u(t)$ gives horocyclic flow.
Geodesic flow and horocyclic flow are very different!

**Theorem 1 (Hedlund).** Any orbit of the horocyclic flow is either periodic or dense. In particular any bounded orbit is periodic.

Compare with folklore theorem:

**Theorem 2.** For any $d \in [0, 2)$ there is nonperiodic bounded orbit $\{x.g(t)\}$ of the geodesic flow so that $\dim_H \{x.g(t)\} = d$.

Note: geodesic flow is ergodic, so for a.e. $x$ we have that $\{x.g(t)\}$ is dense. However, unlike case of horocyclic flow, this gives nothing for specific $x$ ...
Unipotent flows

$g \in \text{SL}(n, \mathbb{R})$ is \textbf{unipotent} if $(g-I)^n = 0$. Example: $u(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$.

A lot is known about actions of unipotent one parameter groups, for instance

**Theorem 3 (Ratner).** $G$ Lie group, $\Gamma$ discrete subgroup with finite covolume, $X = \Gamma \backslash G$ (for example $X_n$), $u(t)$ unipotent one parameter group. For every $x \in X$ there is a connected subgroup $L < G$ so that $xL$ is closed and $\{xu(t)\}$ is equidistributed (in particular, dense) in $xL$.

This is only special case of Ratner’s theorems, which also covers actions of groups generated by one parameter unipotent subgroups (such as $\text{SL}(k, \mathbb{R})$ but not, e.g., group of $n \times n$ diagonal matrices).
Oppenheim’s conjecture = Margulis’ theorem

Let $Q(x) = \sum_{i,j} a_{i,j} x_i x_j$ be an indefinite quadratic form in $n \geq 3$ variables (interesting case: 3 vars). If $a_{i,j} \in \mathbb{Z}$ for all $i, j$ then $Q(\mathbb{Z}^n) \subset \mathbb{Z}$.

**Conjecture 4 (Oppenheim).** Suppose $Q$ is not a scalar multiple of a quadratic form with integer coefficients. for every $\epsilon > 0$ there is a $z \in \mathbb{Z}^n$ so that $|Q(z)| < \epsilon$ (stronger form: $0 < |Q(z)| < \epsilon$).

Margulis proved this using the following: Set $Q_0(x) = 2x_1x_3 - x_2^2$, $H = \{h \in \text{SL}(3, \mathbb{R}) : Q_0 \circ h = Q_0\}$ ($H \cong \text{SL}(2, \mathbb{R})$ & generated by unipotents).

**Theorem 5 (Margulis).** Any $H$ orbit in $X_3$ is either closed or dense.

Key observation: write $Q(\mathbb{Z}^3) = cQ_0(\Lambda)$ with $\Lambda \in X_3$. If $\Lambda$ contains small vectors, $Q_0(\Lambda)$ has small values.
**Littlewood’s conjecture**

For \( a \in \mathbb{R} \), let \( ||a|| = \min_{n \in \mathbb{Z}} |a - n| \).

**Conjecture 6 (Littlewood).** For any real \( \alpha, \beta \),

\[
\lim_{n \rightarrow \infty} n ||n\alpha|| ||n\beta|| = 0.
\]

Will follow from dynamical statement:

**Conjecture 7 (Margulis).** Let \( A < SL(3, \mathbb{R}) \) be group of \( 3 \times 3 \) diagonal matrices. Then any bounded \( A \) orbit in \( X_3 \) is actually closed.

One reason this is difficult: false for any 1-param subgroup of \( A \) (which behave similarly to geodesic flow).

Connection: via the lattice \( \Lambda_{\alpha, \beta} \) generated by

\[
\begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}
\]
Diophantine approximations

• $y \in \mathbb{R}^n$ is said to be **very well approximable (VWA)** if $\exists \delta > 0$ and $\infty$ many $p \in \mathbb{Z}^n, q \in \mathbb{Z}_+$ to

$$\|qy - p\| < q^{-\frac{1+\delta}{n}}.$$ 

• slightly less restrictive notion: $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$ is **very well multiplicatively approximable (VWMA)** if $\infty$ many solutions to

$$\prod_{i=1}^n |qy_i - p_i| < q^{-(1+\delta)}.$$ 

• set of very well multiplicatively approximable $y$ has measure zero, $\dim_H = n.$
The Diophantine properties of \( y \in \mathbb{R}^n \) correspond to properties of orbit of lattice \( \Lambda_y \in X_{n+1} \) generated by

\[
\begin{pmatrix}
1 \\
y_1 \\
\vdots \\
y_n
\end{pmatrix}, \begin{pmatrix}
0 \\
1 \\
\vdots \\
0
\end{pmatrix}, \ldots, \begin{pmatrix}
0 \\
0 \\
\vdots \\
1
\end{pmatrix}
\]

For \( t = (t_1, \ldots, t_n) \in \mathbb{R}^n_+ \) let \( g_t = \text{diag}(e^{-t}, e^{t_1}, \ldots, e^{t_n}) \), \( t = \sum_{i=1}^n t_i \).

Action of \( g_t \) on a lattice \( \Lambda \) contracts first component of every vector of \( \Lambda \) and expand the remaining components.

**Proposition 8.** For \( y \in \mathbb{R}^n \), TFAE:

1. \( y \) is not very well multiplicatively approximable;
2. \( \forall \gamma > 0, \min_{v \in g_t \Lambda_y} \|v\| > e^{-\gamma t} \) for \( t \in \mathbb{R}^n_+ \) large.
Diophantine approximations on manifolds and fractal sets

- Mahler conjectured, and Sprindžuk proved (30 years later): for a.e. \( x \in \mathbb{R} \), the point \( (x, x^2, \ldots, x^n) \) is not VWA.

- A submanifold \( M \subset \mathbb{R}^n \) is extremal (strongly extremal) if almost every point on \( M \) is not VWA (VWMA), nonplanar if \( \not\subset \) any affine hyperplane. Sprindžuk proved any nonplanar algebraic variety is extremal.

- Compare with: for every \( x \in \mathbb{R} \), the point \( (x, x, \ldots, x) \) is VWA.

- Kleinbock-Margulis: nonplanar real analytic manifold \( \subset \mathbb{R}^n \) are strongly extremal (conjectured by Sprindžuk). Proof via transition to space of lattices and using ideas developed to prove non-divergence of unipotent (!) flows.
• More generally: can consider measures. \( \mu \) on \( \mathbb{R}^n \) is strongly extremal if \( \mu \)-a.e. pt. is not VWMA.

• Volume (or area etc.) on non planar real analytic manifolds is strongly extremal

• natural measure on Sierpinski Gasket, Cantor set, and many other fractals, and their images under real analytic maps (as long as it’s not planar!)

All these measures \( \mu \) satisfy three natural conditions (non planar, Federer, decaying) that can be shown to imply strong extremality (Kleinbock-L-Weiss).
A key fact used in Kleinbock-Margulis proof

Question: How can you prove a lattice $\Lambda$ has no short vectors?

A flag is a chain of linear subspaces $0 < V_1 < \cdots < V_{n-1} < \mathbb{R}^n$ with $\dim V_i = i$. It is $\Lambda$ rational if $\Lambda \cap V_i$ a lattice in $V_i$ for all $i$.

**Proposition 9.** If $\exists$ a $\Lambda$-rational flag $0 < V_1 < \cdots < V_{n-1} < \mathbb{R}^n$ with
\[
\theta < \text{covol}(\Lambda \cap V_i) < \Theta \quad \text{with} \quad \theta < 1 < \Theta
\]
then the size of every vector in $\Lambda$ is at least $\|v\| < \frac{\Theta}{\theta}$.

Finding one such flag shows all vectors aren’t too short.
Conclusion

• Many problems in number theory translates naturally to questions about orbits in the space of lattices.

• There are powerful methods from dynamical systems and ergodic theory to deal with these questions.

• There are also a lot of deep open questions.