Diophantine Approximation on Manifolds and Lie Groups

Emmanuel Breuillard

Université Paris-Sud and Universität Münster

Goa, February 2nd, 2016

Based on ongoing joint work with Menny Aka, Lior Rosenzweig and Nicolas de Saxcé.

Classical Diophantine Approximation

$\alpha \in \mathbb{R}$ a real number.

How well can α be approximated by rational numbers ?

Classical Diophantine Approximation

$\alpha \in \mathbb{R}$ a real number.

How well can α be approximated by rational numbers ?

Theorem (Dirichlet's theorem or box principle)

For every $N \in \mathbb{N}$ there is $p, q \in \mathbb{Z}$ with $0 < q \leqslant N$ such that

$$|q\alpha - p| \leqslant \frac{1}{N}.$$

Classical Diophantine Approximation

$\alpha \in \mathbb{R}$ a real number.

How well can α be approximated by rational numbers ?

Theorem (Dirichlet's theorem or box principle)

For every $N \in \mathbb{N}$ there is $p, q \in \mathbb{Z}$ with $0 < q \leqslant N$ such that

$$|q\alpha - p| \leqslant \frac{1}{N}.$$

in particular: there are infinitely many p, q's s.t.

$$|q\alpha - p| \leqslant \frac{1}{q}.$$

Classical Diophantine Approximation

This naturally leads to the following measure of approximation by rationals:

Definition (Diophantine exponent)

The *Diophantine Exponent* of $\alpha \in \mathbb{R}$ is the supremum $\beta(\alpha)$ of all $\beta > 0$ s.t. there are infinitely many integers p, q s.t.

$$|q\alpha - p| < \frac{1}{q^\beta}.$$

Classical Diophantine Approximation

This naturally leads to the following measure of approximation by rationals:

Definition (Diophantine exponent)

The *Diophantine Exponent* of $\alpha \in \mathbb{R}$ is the supremum $\beta(\alpha)$ of all $\beta > 0$ s.t. there are infinitely many integers p, q s.t.

$$|q\alpha - p| < \frac{1}{q^\beta}.$$

Well known fact: for Lebesgue almost every $\alpha \in \mathbb{R}$

$$\beta(\alpha) = 1.$$

Plan for this talk

In this talk we will discuss several generalizations:

Plan for this talk

In this talk we will discuss several generalizations:

1) approximating points on submanifolds of $X(\mathbb{R})$ by points in $X(\mathbb{Q})$; where X is an algebraic variety over $\mathbb{Q}$.

Plan for this talk

In this talk we will discuss several generalizations:

1) approximating points on submanifolds of $X(\mathbb{R})$ by points in $X(\mathbb{Q})$; where X is an algebraic variety over $\mathbb{Q}$.

2) approximating submanifolds $\{Y_\lambda(\mathbb{R})\}_\lambda$ of $X(\mathbb{R})$ varying in a family by points in $X(\mathbb{Q})$; (we will see that diophantine approximation on matrices is a special case of this, where $X = \mathbb{R}^{m+n}$, $\{Y_\lambda(\mathbb{R})\}_\lambda$ a family of n-planes).

Plan for this talk

In this talk we will discuss several generalizations:

1) approximating points on submanifolds of $X(\mathbb{R})$ by points in $X(\mathbb{Q})$; where X is an algebraic variety over $\mathbb{Q}$.

2) approximating submanifolds $\{Y_\lambda(\mathbb{R})\}_\lambda$ of $X(\mathbb{R})$ varying in a family by points in $X(\mathbb{Q})$; (we will see that diophantine approximation on matrices is a special case of this, where $X = \mathbb{R}^{m+n}$, $\{Y_\lambda(\mathbb{R})\}_\lambda$ a family of n-planes).

4) approximating the identity in a Lie group by words in some group elements;

Diophantine approximation on $\mathbb{R}^d$

For $\underline{\alpha} := (\alpha_1, \ldots, \alpha_d) \in \mathbb{R}^d$ we may define:

- The *linear form approximation*: i.e. how close $\alpha_1 q_1 + \ldots + \alpha_d q_d$ can be to an integer, for q_i's $\in \mathbb{Z}^d$,

Diophantine approximation on $\mathbb{R}^d$

For $\underline{\alpha} := (\alpha_1, \ldots, \alpha_d) \in \mathbb{R}^d$ we may define:

- The *linear form approximation*: i.e. how close $\alpha_1 q_1 + \ldots + \alpha_d q_d$ can be to an integer, for q_i's $\in \mathbb{Z}^d$,
- The *simultaneous approximation*: i.e. how close the vector $(q\alpha_1, \ldots, q\alpha_d)$, $q \in \mathbb{Z}$ can be to an integer vector in $\mathbb{Z}^d$?

Diophantine approximation on $\mathbb{R}^d$

For $\underline{\alpha} := (\alpha_1, \ldots, \alpha_d) \in \mathbb{R}^d$ we may define:

- The *linear form approximation*: i.e. how close $\alpha_1 q_1 + \ldots + \alpha_d q_d$ can be to an integer, for q_i's $\in \mathbb{Z}^d$,
- The *simultaneous approximation*: i.e. how close the vector $(q\alpha_1, \ldots, q\alpha_d)$, $q \in \mathbb{Z}$ can be to an integer vector in $\mathbb{Z}^d$?
- The *matrix diophantine approximation*: i.e. given a matrix $A \in M_{m,n}(\mathbb{R})$, $\mathfrak{q} \in \mathbb{Z}^n$, how close the vectors $M \cdot \mathfrak{q}$ be to an integer vector in $\mathbb{Z}^m$?

Diophantine approximation on $\mathbb{R}^d$

For $\underline{\alpha} := (\alpha_1, \ldots, \alpha_d) \in \mathbb{R}^d$ we may define:

- The *linear form approximation*: i.e. how close $\alpha_1 q_1 + \ldots + \alpha_d q_d$ can be to an integer, for q_i's $\in \mathbb{Z}^d$,
- The *simultaneous approximation*: i.e. how close the vector $(q\alpha_1, \ldots, q\alpha_d)$, $q \in \mathbb{Z}$ can be to an integer vector in $\mathbb{Z}^d$?
- The *matrix diophantine approximation*: i.e. given a matrix $A \in M_{m,n}(\mathbb{R})$, $\mathfrak{q} \in \mathbb{Z}^n$, how close the vectors $M \cdot \mathfrak{q}$ be to an integer vector in $\mathbb{Z}^m$?

case $m = 1 \longrightarrow$ linear form approximation,

case $n = 1 \longrightarrow$ simultaneous approximation.

Diophantine approximation on matrices

Definition (Diophantine exponent in $\mathbb{R}^d$)

For $M \in M_{m,n}(\mathbb{R})$ we can define the *Diophantine exponent* $\beta(M) > 0$ as the supremum of all $\beta > 0$ such that there are infinitely many $\mathfrak{q} \in \mathbb{Z}^n, \mathfrak{p} \in \mathbb{Z}^m$ such that

$$||M \cdot \mathfrak{q} + \mathfrak{p}|| < \frac{1}{||\mathfrak{q}||^{\beta}}.$$

Diophantine approximation on matrices

Definition (Diophantine exponent in $\mathbb{R}^d$)

For $M \in M_{m,n}(\mathbb{R})$ we can define the *Diophantine exponent* $\beta(M) > 0$ as the supremum of all $\beta > 0$ such that there are infinitely many $\mathfrak{q} \in \mathbb{Z}^n, \mathfrak{p} \in \mathbb{Z}^m$ such that

$$||M \cdot \mathfrak{q} + \mathfrak{p}|| < \frac{1}{||\mathfrak{q}||^{\beta}}.$$

Remarks:

- for Lebesgue almost every $M \in M_{m,n}(\mathbb{R})$ the exponent is $\beta(M) = \frac{n}{m}$ (= minimal possible value by Dirichlet's theorem),
- One says that $M \in M_{m,n}(\mathbb{R})$ is *extremal* if $\beta(M) = \frac{n}{m}$.

Diophantine approximation on manifolds

Consider first submanifolds of $\mathbb{R}^n$ (later we shall look at submanifolds of $M_{m,n}(\mathbb{R})$)

Diophantine approximation on manifolds

Consider first submanifolds of $\mathbb{R}^n$ (later we shall look at submanifolds of $M_{m,n}(\mathbb{R})$)

In the 1930's K. Mahler asked whether for Lebesgue almost every $x \in \mathbb{R}$, the point

$$(x, x^2, \dots, x^n)$$

is *extremal* in $\mathbb{R}^n$?

Diophantine approximation on manifolds

Consider first submanifolds of $\mathbb{R}^n$ (later we shall look at submanifolds of $M_{m,n}(\mathbb{R})$)

In the 1930's K. Mahler asked whether for Lebesgue almost every $x \in \mathbb{R}$, the point

$$(x, x^2, \dots, x^n)$$

is *extremal* in $\mathbb{R}^n$?

A submanifold is called extremal if the diophantine exponent of a random point in it is the same as that of a random point in the ambient space.

Diophantine approximation on manifolds

Mahler's question was answered affirmatively by Sprindzuk in 1964, i.e. *the Mahler curve is extremal.*

This led to the following more general questions:

- under what conditions on $\mathcal{M}$ is $\mathcal{M}$ extremal ?
- can one compute the exponent $\beta(x)$ of a random point $x \in \mathcal{M}$? of an algebraic point on $\mathcal{M}$?

Diophantine approximation on manifolds

Mahler's question was answered affirmatively by Sprindzuk in 1964, i.e. *the Mahler curve is extremal.*

This led to the following more general questions:

- under what conditions on $\mathcal{M}$ is $\mathcal{M}$ extremal ?
- can one compute the exponent $\beta(x)$ of a random point $x \in \mathcal{M}$? of an algebraic point on $\mathcal{M}$?

Theorem (Kleinbock-Margulis 1998)

If $\mathcal{M} \subset \mathbb{R}^n$ is a real analytic submanifold not contained in a proper affine subspace, then it is extremal.

Diophantine approximation on manifolds

This was for submanifolds of $\mathbb{R}^n$. What about submanifolds of $M_{m,n}(\mathbb{R})$?

Beresnevich, Kleinbock, Margulis and Wang:

- thorny question because the right condition on $\mathcal{M}$ seems hard to pin down.
- they gave examples showing the condition if it exists cannot be linear in the matrix entries.
- they also gave some sufficient (yet slightly too strong) conditions for extremality in terms of non planarity of certain minors of the matrix.

Diophantine approximation in the Grassmannian

It turns out that diophantine approximation on matrices *is a special case* of the following diophantine problem about submanifolds of the Grassmannian:

Consider the Grassmannian $\mathcal{G}(n, m+n)$ of n-planes in $\mathbb{R}^{m+n}$. For $x \in \mathcal{G}(n, m+n)$, define its diophantine exponent $\beta(x)$ to be the supremum of all $\beta > 0$ such that there are infinitely many $\mathfrak{q} \in \mathbb{Z}^{m+n}$ s.t.

$$d(x, \mathfrak{q}) < \frac{1}{\|\mathfrak{q}\|^{\beta}}.$$

Note that Dirichlet says that $\beta(x) \geqslant \frac{n}{m} = \frac{n+m}{m} - 1$. For a random n-plane x in $\mathcal{G}(n, m+n)$ this is an equality.

A family of obstructions to extremality

Given a subspace $W \leqslant \mathbb{R}^{n+m}$ and an integer $r \in [0, m]$, consider the pencil $\mathcal{P}_{W,r}$

$$\mathcal{P}_{W,r} := \{x \in \mathcal{G}(n, m+n); \dim(x \cap W) \geqslant \dim W - r\}$$

A family of obstructions to extremality

Given a subspace $W \leqslant \mathbb{R}^{n+m}$ and an integer $r \in [0, m]$, consider the pencil $\mathcal{P}_{W,r}$

$$\mathcal{P}_{W,r} := \{x \in \mathcal{G}(n, m+n); \dim(x \cap W) \geqslant \dim W - r\}$$

Observe: if W is rational, then just by Dirichlet's box principle any $x \in \mathcal{P}_{W,r}$ will have an exponent

$$\beta(x) \geqslant \frac{\dim W}{r} - 1$$

A family of obstructions to extremality

Given a subspace $W \leqslant \mathbb{R}^{n+m}$ and an integer $r \in [0, m]$, consider the pencil $\mathcal{P}_{W,r}$

$$\mathcal{P}_{W,r} := \{x \in \mathcal{G}(n, m+n); \dim(x \cap W) \geqslant \dim W - r\}$$

Observe: if W is rational, then just by Dirichlet's box principle any $x \in \mathcal{P}_{W,r}$ will have an exponent

$$\beta(x) \geqslant \frac{\dim W}{r} - 1$$

So if $\frac{\dim W}{r} - 1 > \frac{n}{m}$, any x in the pencil will not be extremal. Call such a pencil *constraining*.

Criterion for extremality in $M_{m,n}(\mathbb{R})$

Theorem 1 (ABRS 2014)

If $\mathcal{M} \subset \mathcal{G}(n, m+n)(\mathbb{R})$ (or $\mathcal{M} \subset M_{m,n}(\mathbb{R})$) is an analytic submanifold, which is not contained in any constraining pencil, then $\mathcal{M}$ is extremal, i.e. Lebesgue almost every x has $\beta(x) = \frac{n}{m}$.

Remark: Beresnevich-Kleinbock-Wang's non-planarity condition is slightly (but strictly) stronger...

A converse statement

As usual in metric diophantine approximation the converse does not hold *unless further rationality assumptions are made.*

Theorem 2 (converse)

Assume that the Zariski-closure of $\mathcal{M} \subset \mathcal{G}(n, m+n)(\mathbb{R})$ *(or* $\mathcal{M} \subset M_{m,n}(\mathbb{R})$*) is defined over* $\mathbb{Q}$*. Then* $\mathcal{M}$ *is extremal if and only if it is not contained in any constraining pencil.*

Computation of the exponent

Theorem (Kleinbock, 2008)

If $\mathcal{M} \subset \mathbb{R}^n$ (i.e. $m = 1$) is a connected analytic submanifold, then $\beta(\mathcal{M})$ is well-defined and

$$\beta(\mathcal{M}) = \beta(\mathit{AffineSpan}(\mathcal{M})).$$

$\beta(\mathcal{M})$ well-defined means that a.e. $\beta(x) = \beta(\mathcal{M})$.

Computation of the exponent

Theorem 3 (exponent)

If $\mathcal{M} \subset \mathcal{G}(n, m+n)(\mathbb{R})$ (or $\mathcal{M} \subset M_{m,n}(\mathbb{R})$) is a connected analytic submanifold, then

1. $$\beta(\mathcal{M}) = \beta(PluckerSpan(\mathcal{M})),$$

2. $$\max_{\mathcal{P}_{W,r} \supset \mathcal{M}, W \, rational} \frac{\dim W}{r} \leqslant \beta(\mathcal{M}) + 1 \leqslant \max_{\mathcal{P}_{W,r} \supset \mathcal{M}} \frac{\dim W}{r},$$

3. *equality holds on the LHS if $\mathcal{M}$ is defined over $\mathbb{Q}$, or even $\overline{\mathbb{Q}}$. In particular, then, $\beta(\mathcal{M}) \in \mathbb{Q}$.*

Computation of the exponent

Theorem 3 (exponent)

If $\mathcal{M} \subset \mathcal{G}(n, m+n)(\mathbb{R})$ (or $\mathcal{M} \subset M_{m,n}(\mathbb{R})$) is a connected analytic submanifold, then

1. $$\beta(\mathcal{M}) = \beta(PluckerSpan(\mathcal{M})),$$

2. $$\max_{\mathcal{P}_{W,r} \supset \mathcal{M}, W\, rational} \frac{\dim W}{r} \leqslant \beta(\mathcal{M}) + 1 \leqslant \max_{\mathcal{P}_{W,r} \supset \mathcal{M}} \frac{\dim W}{r},$$

3. *equality holds on the LHS if $\mathcal{M}$ is defined over $\mathbb{Q}$, or even $\overline{\mathbb{Q}}$. In particular, then, $\beta(\mathcal{M}) \in \mathbb{Q}$.*

Rk: Point 1. has been obtained independently by Das-Fishman-Simmons-Urbański.

Speculations

Schubert varieties are certain nice algebraic varieties of the Grassmannian $\mathcal{G}(n, m+n)$.

$$\textit{pencils} = \text{“special Schubert varieties”}$$

$$\textit{SchubertSpan}(\mathcal{M}) := \bigcap_{\mathcal{M} \subset S \subset \mathcal{G}(n,m+n)} S = \bigcap_{\mathcal{M} \subset \mathcal{P}_{W,r}} \mathcal{P}_{W,r}$$

Speculations

Schubert varieties are certain nice algebraic varieties of the Grassmannian $\mathcal{G}(n, m+n)$.

$$pencils = \text{“special Schubert varieties”}$$

$$SchubertSpan(\mathcal{M}) := \bigcap_{\mathcal{M} \subset S \subset \mathcal{G}(n,m+n)} S = \bigcap_{\mathcal{M} \subset \mathcal{P}_{W,r}} \mathcal{P}_{W,r}$$

Conjecture: $\beta(\mathcal{M}) = \beta(SchubertSpan(\mathcal{M}))$

Speculations

Schubert varieties are certain nice algebraic varieties of the Grassmannian $\mathcal{G}(n, m+n)$.

$$\textit{pencils} = \text{“special Schubert varieties”}$$

$$SchubertSpan(\mathcal{M}) := \bigcap_{\mathcal{M} \subset S \subset \mathcal{G}(n,m+n)} S = \bigcap_{\mathcal{M} \subset \mathcal{P}_{W,r}} \mathcal{P}_{W,r}$$

Conjecture: $\beta(\mathcal{M}) = \beta(SchubertSpan(\mathcal{M}))$

Further speculations/problems:

- perhaps even $\exists$ one pencil $\mathcal{P}_{W,r} \supset \mathcal{M}$ such that $\beta(\mathcal{M}) = \beta(\mathcal{P}_{W,r})$.
- then can one compute $\beta(\mathcal{P})$ only in terms of *deterministic exponents* of W ?

... so far only partial answers.

Homogeneous dynamics and the Dani correspondence

... a view on the proofs: they are based on homogeneous dynamics and *quantitative non-divergence estimates* for one-parameter flows in the space of unimodular lattices in $\mathbb{R}^{m+n}$:

$$\Omega_{m+n} := \mathrm{SL}_{m+n}(\mathbb{R}) / \mathrm{SL}_{m+n}(\mathbb{Z})$$

Homogeneous dynamics and the Dani correspondence

... a view on the proofs: they are based on homogeneous dynamics and *quantitative non-divergence estimates* for one-parameter flows in the space of unimodular lattices in $\mathbb{R}^{m+n}$:

$$\Omega_{m+n} := \mathrm{SL}_{m+n}(\mathbb{R}) / \mathrm{SL}_{m+n}(\mathbb{Z})$$

For $\Delta \in \Omega_{m+n}$, let

$$\alpha_1(\Delta) := \inf\{||v||; v \in \Delta \setminus \{0\}\}$$

Dani's correspondence in an example:

As above let $x \in \mathbb{R}$, and consider the flow $\{g_t\}_{t\in\mathbb{R}}$ and the unimodular lattice Δ_x in the plane

$$g_t := \left(\begin{array}{cc} e^t & 0 \\ 0 & e^{-t} \end{array} \right), \qquad \Delta_x := \left(\begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right) \cdot \mathbb{Z}^2.$$

Dani's correspondence in an example:

As above let $x \in \mathbb{R}$, and consider the flow $\{g_t\}_{t\in\mathbb{R}}$ and the unimodular lattice Δ_x in the plane

$$g_t := \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix}, \qquad \Delta_x := \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \mathbb{Z}^2.$$

For $\beta \geqslant 1$ set

$$\gamma := \frac{\beta - 1}{\beta + 1} \in [0, 1).$$

Then the following are equivalent (exercise):

$$(i) \qquad \liminf_{q\to+\infty} q^{\beta} \cdot d(qx, \mathbb{Z}) = 0,$$

Dani's correspondence in an example:

As above let $x \in \mathbb{R}$, and consider the flow $\{g_t\}_{t\in\mathbb{R}}$ and the unimodular lattice Δ_x in the plane

$$g_t := \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix}, \qquad \Delta_x := \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \mathbb{Z}^2.$$

For $\beta \geqslant 1$ set

$$\gamma := \frac{\beta - 1}{\beta + 1} \in [0,1).$$

Then the following are equivalent (exercise):

$$(i) \qquad \liminf_{q\to+\infty} q^{\beta} \cdot d(qx, \mathbb{Z}) = 0,$$

$$(ii) \qquad \liminf_{t\to+\infty} e^{\gamma t} \cdot \alpha_1(g_t \Delta_x) = 0$$

The Dani correspondence for the Grassmannian

For us if $x \in \mathcal{G}(n, m+n)$ is an n-plane, we consider the diagonal flow $\{g_t^x\}_{t>0} \subset SL_{m+n}(\mathbb{R})$, where g_t^x

- contracts vectors in x by a factor $e^{-t/n}$ and,
- dilates vectors in $x^{\perp}$ (say) by a factor $e^{t/m}$.

The Dani correspondence for the Grassmannian

For us if $x \in \mathcal{G}(n, m+n)$ is an n-plane, we consider the diagonal flow $\{g_t^x\}_{t>0} \subset SL_{m+n}(\mathbb{R})$, where g_t^x

- contracts vectors in x by a factor $e^{-t/n}$ and,
- dilates vectors in $x^\perp$ (say) by a factor $e^{t/m}$.

Let $\gamma(x)$ be the supremum of all $\gamma > 0$ s.t. the forward $\{g_t^x\}$-orbit of $\Delta = \mathbb{Z}^{m+n}$ ventures infinitely often in the cusp of Ω_{m+n} at linear speed γt measured w.r.t α_1.

Then

$$\beta(x) = \frac{\frac{1}{m} + \gamma(x)}{\frac{1}{n} - \gamma(x)}.$$

Diophantine approximation on Lie groups

We move to another, related, problem. Here is the setting:

Diophantine approximation on Lie groups

We move to another, related, problem. Here is the setting:

G is a connected Lie group.

$S = \{1, s_1^{\pm 1}, \dots, s_k^{\pm 1}\} \subset G$ is a finite symmetric set and $\Gamma := \langle S \rangle$ is the subgroup of G generated by S.

Diophantine approximation on Lie groups

We move to another, related, problem. Here is the setting:

G is a connected Lie group.

$S = \{1, s_1^{\pm 1}, \ldots, s_k^{\pm 1}\} \subset G$ is a finite symmetric set and $\Gamma := \langle S \rangle$ is the subgroup of G generated by S.

We are interested in words w in k letters and of length n, and how close to the identity in G they can be when evaluated on S.

e.g.

$$k = 2, n = 14, \qquad w = s_1 s_2^3 s_1^{-2} s_2^7 s_1.$$

Diophantine approximation on Lie groups

How does this relate to classical diophantine approximation ?

Diophantine approximation on Lie groups

How does this relate to classical diophantine approximation ?

e.g. take $G = (\mathbb{R}, +)$, and $S = \{0, \pm 1, \pm \alpha\}$, $\alpha \in \mathbb{R}$.

The subgroup $\Gamma = \langle S \rangle$ is just $\mathbb{Z} + \alpha\mathbb{Z}$.

Diophantine approximation on Lie groups

How does this relate to classical diophantine approximation ?

e.g. take $G = (\mathbb{R}, +)$, and $S = \{0, \pm 1, \pm \alpha\}$, $\alpha \in \mathbb{R}$.

The subgroup $\Gamma = \langle S \rangle$ is just $\mathbb{Z} + \alpha\mathbb{Z}$.

And a word w of length n in two letters x, y becomes a linear form

$$w(x, y) = px + qy,$$

with $|p| + |q| = n$.

So asking how close $w(1, \alpha)$ can be to 0 *is the same as* asking for the diophantine properties of α.

Diophantine approximation on Lie groups

Consider the smallest distance to 1 of a word of length n, namely

$$\delta_n(S) := \inf\{d(\gamma, 1); \gamma \in S^n \setminus \{1\}\}$$

where $d(x, y)$ is a left-invariant Riemannian metric on the Lie group G and $S^n := S \cdot \ldots \cdot S$ is the n-fold product set.

We will say that Γ *is Diophantine* if there is $\beta > 0$ such that for all large enough n.

$$\delta_n(S) > \frac{1}{|S^n|^\beta},$$

Remarks:

This definition does not depend on the choice of generating set S in Γ, nor on the choice of metric $d(x, y)$.

Diophantine approximation on Lie groups

Consider the smallest distance to 1 of a word of length n, namely

$$\delta_n(S) := \inf\{d(\gamma, 1); \gamma \in S^n \setminus \{1\}\}$$

where $d(x, y)$ is a left-invariant Riemannian metric on the Lie group G and $S^n := S \cdot \ldots \cdot S$ is the n-fold product set.

We will say that Γ *is Diophantine* if there is $\beta > 0$ such that for all large enough n.

$$\delta_n(S) > \frac{1}{|S^n|^\beta},$$

Remarks:

$\mathbb{Z} + \alpha\mathbb{Z}$ is diophantine in $\mathbb{R}$ iff α is a diophantine number.

Diophantine approximation on Lie groups

Consider the smallest distance to 1 of a word of length n, namely

$$\delta_n(S) := \inf\{d(\gamma, 1); \gamma \in S^n \setminus \{1\}\}$$

where $d(x, y)$ is a left-invariant Riemannian metric on the Lie group G and $S^n := S \cdot \ldots \cdot S$ is the n-fold product set.

We will say that *Γ is Diophantine* if there is $\beta > 0$ such that for all large enough n.

$$\delta_n(S) > \frac{1}{|S^n|^\beta},$$

Remarks:

$|S^n|$ grows either polynomially or exponentially in n.

Metric diophantine approximation on Lie groups

Definition (Diophantine Lie group)

The Lie group G is said to be Diophantine on k letters if for almost every choice (w.r.t Haar measure) of k elements $s_1, \ldots, s_k$ in G, the subgroup $\langle s_1, \ldots, s_k \rangle$ is diophantine.

We also say that G is Diophantine if it is diophantine on k letters for all k.

Metric diophantine approximation on Lie groups

Definition (Diophantine Lie group)

The Lie group G is said to be Diophantine on k letters if for almost every choice (w.r.t Haar measure) of k elements $s_1, \ldots, s_k$ in G, the subgroup $\langle s_1, \ldots, s_k \rangle$ is diophantine.

We also say that G is Diophantine if it is diophantine on k letters for all k.

Sarnak's conjecture: $G = \mathrm{SU}(2)$ is diophantine.

see related work of Gamburd-Jakobson-Sarnak and Bourgain-Gamburd in relation with uniform distribution and spectral gaps.

Metric diophantine approximation on Lie groups

Definition (Diophantine Lie group)

The Lie group G is said to be Diophantine on k letters if for almost every choice (w.r.t Haar measure) of k elements $s_1, \ldots, s_k$ in G, the subgroup $\langle s_1, \ldots, s_k \rangle$ is diophantine.

We also say that G is Diophantine if it is diophantine on k letters for all k.

Sarnak's conjecture: $G = \mathrm{SU}(2)$ is diophantine.

conjecturally every semisimple Lie group is diophantine

Metric diophantine approximation on Lie groups

Definition (Diophantine Lie group)

The Lie group G is said to be Diophantine on k letters if for almost every choice (w.r.t Haar measure) of k elements $s_1, \dots, s_k$ in G, the subgroup $\langle s_1, \dots, s_k \rangle$ is diophantine.

We also say that G is Diophantine if it is diophantine on k letters for all k.

Sarnak's conjecture: $G = \mathrm{SU}(2)$ is diophantine.

Kaloshin-Rodniansky 2001: for a.e. S, $\delta_n(S) > \exp(-O(n^2))$.

Metric diophantine approximation on Lie groups

Is every Lie group diophantine ?

Metric diophantine approximation on Lie groups

Is every Lie group diophantine ?

Obvious remark: every Lie group is diophantine on 1 letter.

Metric diophantine approximation on Lie groups

Is every Lie group diophantine ?

Obvious remark: every Lie group is diophantine on 1 letter.

Answer: NO!

Theorem 4 (Existence of non diophantine Lie groups)

For every $k \geqslant 1$ there is a connected Lie group, which is diophantine on k letters, but not on $k+1$ letters.

Nilpotent Lie groups

The case of G nilpotent is particularly interesting.

Nilpotent Lie groups

The case of G nilpotent is particularly interesting.

Recall: G nilpotent $\Leftrightarrow$ G embeds as a closed subgroup of *unipotent upper triangular matrices*.

$$\begin{pmatrix} 1 & * & * & * \\ 0 & . & * & * \\ 0 & 0 & . & * \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Basic facts:

- for every finite subset $S \subset G$, $|S^n|$ grows polynomially fast in n.

Nilpotent Lie groups

The case of G nilpotent is particularly interesting.

Recall: G nilpotent $\Leftrightarrow$ G embeds as a closed subgroup of *unipotent upper triangular matrices*.

$$\begin{pmatrix} 1 & * & * & * \\ 0 & . & * & * \\ 0 & 0 & . & * \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Basic facts:

- G is diffeomorphic to $\mathbb{R}^d$ via the exponential map

$$\exp : Lie(G) \to G,$$

which is a diffeo.

Nilpotent Lie groups

The case of G nilpotent is particularly interesting.

Recall: G nilpotent $\Leftrightarrow$ G embeds as a closed subgroup of *unipotent upper triangular matrices*.

$$\begin{pmatrix} 1 & * & * & * \\ 0 & . & * & * \\ 0 & 0 & . & * \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Basic facts:

• the Lie product is a *polynomial map* when pulled back on $Lie(G)$.

Nilpotent Lie groups

Let G be a nilpotent Lie group. Every word w on k letters induces

a word map

$$w : G^k \to G.$$

Nilpotent Lie groups

Let G be a nilpotent Lie group. Every word w on k letters induces

a word map
$$w : G^k \to G.$$

Fact 1: the word map is a polynomial map, when viewed on $Lie(G)$ via exp.

Nilpotent Lie groups

Let G be a nilpotent Lie group. Every word w on k letters induces

a word map

$$w : G^k \to G.$$

Fact 1: the word map is a polynomial map, when viewed on $Lie(G)$ via exp.

Fact 2: the family $F_{k,G}$ of all word maps on G on k letters forms a group: the relatively-free group on k generators "in the variety of G".

Nilpotent Lie groups

Let G be a nilpotent Lie group. Every word w on k letters induces

a word map

$$w : G^k \to G.$$

Fact 1: the word map is a polynomial map, when viewed on $Lie(G)$ via exp.

Fact 2: the family $F_{k,G}$ of all word maps on G on k letters forms a group: the relatively-free group on k generators "in the variety of G".

Actually $F_{k,G}$ is a nilpotent group and is the group of *integer points* of a nilpotent Lie group $F_{k,G}(\mathbb{R})$ (the Malcev closure).

Nilpotent Lie groups

Using exp one pulls back everything to $Lie(G)$ and word maps just become linear combinations with *integer* coefficients of basic Lie bracket maps such as:

$$\begin{aligned} Lie(G)^5 &\rightarrow Lie(G), \\ (X_1, \ldots, X_k) &\mapsto [X_1, [[X_2, X_3], [X_4, X_5]]] \end{aligned}$$

Nilpotent Lie groups

Using exp one pulls back everything to $Lie(G)$ and word maps just become linear combinations with *integer* coefficients of basic Lie bracket maps such as:

$$\begin{aligned} Lie(G)^5 &\rightarrow Lie(G), \\ (X_1, \ldots, X_k) &\mapsto [X_1, [[X_2, X_3], [X_4, X_5]]] \end{aligned}$$

And the question becomes for a random choice of

$$X_1, \ldots, X_k \in Lie(G)$$

how well integer linear combinations of these brackets approximate 0 in $Lie(G)$.

Nilpotent Lie groups

Using exp one pulls back everything to $Lie(G)$ and word maps just become linear combinations with *integer* coefficients of basic Lie bracket maps such as:

$$\begin{aligned} Lie(G)^5 &\to Lie(G), \\ (X_1, \ldots, X_k) &\mapsto [X_1, [[X_2, X_3], [X_4, X_5]]] \end{aligned}$$

These brackets form a basis of the Lie algebra $\mathcal{F}_{k,G}$ of $F_{k,G}$ and each choice of $X_1, \ldots, X_k$ gives rise to a

$$\dim(G) \times \dim \mathcal{F}_{k,G} \text{ matrix}$$

varying analytically (in fact polynomially) in the X_i's.

Nilpotent Lie groups

Using exp one pulls back everything to $Lie(G)$ and word maps just become linear combinations with *integer* coefficients of basic Lie bracket maps such as:

$$\begin{aligned} Lie(G)^5 &\rightarrow Lie(G), \\ (X_1, \ldots, X_k) &\mapsto [X_1, [[X_2, X_3], [X_4, X_5]]] \end{aligned}$$

So we are precisely in the setting of diophantine approximation on analytic submanifolds of matrices!

Nilpotent Lie groups

Using exp one pulls back everything to $Lie(G)$ and word maps just become linear combinations with *integer* coefficients of basic Lie bracket maps such as:

$$\begin{aligned} Lie(G)^5 &\rightarrow Lie(G), \\ (X_1, \ldots, X_k) &\mapsto [X_1, [[X_2, X_3], [X_4, X_5]]] \end{aligned}$$

So we are precisely in the setting of diophantine approximation on analytic submanifolds of matrices!

Hence we may apply our main theorem.

Nilpotent Lie groups

The right exponent depends on a subtle way on the structure constants of the Lie algebra $\mathcal{F}_{k,G}$.

Nilpotent Lie groups

The right exponent depends on a subtle way on the structure constants of the Lie algebra $\mathcal{F}_{k,G}$.

There is a natural $\mathbb{Q}$-structure on the free Lie algebra $\mathcal{F}_k$ on k generators, but not always on $\mathcal{F}_{k,G}$. This depends on the way the ideal of laws of G, $\mathcal{L}_{k,G}$ sits in $\mathcal{F}_k$.

$$\mathcal{F}_{k,G} = \mathcal{F}_k / \mathcal{L}_{k,G}$$

Nilpotent Lie groups

The right exponent depends on a subtle way on the structure constants of the Lie algebra $\mathcal{F}_{k,G}$.

There is a natural $\mathbb{Q}$-structure on the free Lie algebra $\mathcal{F}_k$ on k generators, but not always on $\mathcal{F}_{k,G}$. This depends on the way the ideal of laws of G, $\mathcal{L}_{k,G}$ sits in $\mathcal{F}_k$.

$$\mathcal{F}_{k,G} = \mathcal{F}_k / \mathcal{L}_{k,G}$$

If $\mathcal{L}_{k,G}$ is defined over $\mathbb{Q}$, then G will be diophantine on k letters and one can compute the exponent.

Nilpotent Lie groups

Theorem 5 (Diophantine exponent for rational groups)

If G is a nilpotent group with structure constants in $\mathbb{Q}$, then it is diophantine on k letters for all k and there is a rational fraction $f \in \mathbb{Q}(X)$ such that the diophantine exponent β_k is

$$\beta_k = f(k)$$

for all large k.

Nilpotent Lie groups

Theorem 5 (Diophantine exponent for rational groups)

If G is a nilpotent group with structure constants in $\mathbb{Q}$, then it is diophantine on k letters for all k and there is a rational fraction $f \in \mathbb{Q}(X)$ such that the diophantine exponent β_k is

$$\beta_k = f(k)$$

for all large k.

e.g. for the group $G = U_s(\mathbb{R})$ of $(s+1) \times (s+1)$ upper triangular unipotent matrices,

$$f(X) = \frac{\sum_{d|s} \mu(d) X^{s/d} - s}{\sum_{i=1}^{s} \mu(i)(X + \ldots + X^{[s/i]})}$$

Non diophantine Lie groups

They don't exist in nilpotency class 5 or lower. Examples arise in class 6 and higher.

Main point: in nilpotency class $s \leqslant 5$, the free Lie algebra on k generators $\mathcal{F}_k$ is multiplicity-free as a GL_k-module.

Non diophantine Lie groups

They don't exist in nilpotency class 5 or lower. Examples arise in class 6 and higher.

Main point: in nilpotency class $s \leqslant 5$, the free Lie algebra on k generators $\mathcal{F}_k$ is multiplicity-free as a GL_k-module.

Consequently: every GL_k-submodule, and in particular every ideal of laws, must be defined over $\mathbb{Q}$.

Multiplicity arises starting from class 6 and on (work of Thrall, Klyachko, Kraskiewicz-Weyman).

Non diophantine Lie groups

Multiplicity arises starting from class 6 and on (work of Thrall, Klyachko, Kraskiewicz-Weyman).

Then taking a GL_k-submodule $E^\lambda \leqslant \mathcal{F}_k$ appearing with multiplicity at least 2, one builds an bad ideal

$$\mathcal{L} := \{(x, \alpha x) \in E^\lambda \oplus E^\lambda\},$$

where $\alpha \in \mathbb{R}$ is a Liouville number. Then

$$Lie(G) := \mathcal{F}_k / \mathcal{L}$$

will be non-diophantine.

THANK YOU