

Mixing and Diophantine problems

QMW 11/5/04

Mixing: Let X be a shaker full of an incompressible fluid, containing $\frac{1}{5}$ G and $\frac{4}{5}$ T. If A is the region occupied at first by the liquid G, then after n shakes (applications of a map T) the proportion of G in any other region B is

$$\frac{\mu(T^n(A) \cap B)}{\mu(B)}$$

where μ denotes volume. Effective shaking means that the proportion of G in any region B will converge to $\frac{1}{5}$:

$$\frac{\mu(T^n(A) \cap B)}{\mu(B)} \longrightarrow \mu(A) = \frac{1}{5}.$$

More formally: let

$$T : (X, \mathcal{B}, \mu) \rightarrow (X, \mathcal{B}, \mu)$$

be an invertible μ -preserving transformation of a probability space. Then T is called *mixing* if

$$\mu(T^n(A) \cap B) \longrightarrow \mu(A)\mu(B)$$

for all $A, B \in \mathcal{B}$.

More generally, let α be an action of some group Γ by invertible μ -preserving transformations of (X, \mathcal{B}, μ) . That is, α is a representation $\Gamma \rightarrow MPT(X, \mathcal{B}, \mu)$. Call α *mixing* if

$$\lim_{\gamma \rightarrow \infty} \mu(\alpha_\gamma A \cap B) = \mu(A)\mu(B),$$

where $\gamma \rightarrow \infty$ means ‘leaving finite sets’.

Higher order mixing: Rokhlin introduced the following notion as a finer invariant of measure-preserving transformations. Say that α is *mixing on r sets* if

$$\mu(\alpha_{\gamma_1} A_1 \cap \cdots \cap \alpha_{\gamma_r} A_r) \longrightarrow \mu(A_1) \cdots \mu(A_r)$$

as $\gamma_i \gamma_j^{-1} \rightarrow \infty$.

[For $r \geq 3$ this is not a spectral property.]

Open problem: For $\Gamma = \mathbb{Z}$, does mixing imply mixing of order r for all r ?

[If there is a counter-example, then there is a zero entropy one.]

Sinai/Mozes: If Γ is a lattice in a Lie group of rank ≥ 2 , trivial centre, then mixing implies mixing of all orders.

Abelian groups of higher rank turn out to be different.

Ledrappier: There is a mixing \mathbb{Z}^2 action that is not mixing on 3 sets. Similar ideas show that for any k there is a \mathbb{Z}^2 -action that is mixing on k sets but not mixing on $(k + 1)$ sets.

Ledrappier's example: Let X be the set of points $x \in \{0, 1\}^{\mathbb{Z}^2}$ with

$$x_{n,m} + x_{n+1,m} + x_{n,m+1} = 0 \quad \forall n, m.$$

This carries a natural action of \mathbb{Z}^2 by shifting. The action is mixing (exercise).

Now let $A_1 = A_2 = \{x \in X \mid x_{0,0} = 0\}$ and $A_3 = \{x \in X \mid x_{0,0} = 1\}$. These sets each have (Haar) measure $\frac{1}{2}$. However

$$\alpha_{(0,0)}(A_1) \cap \alpha_{(0,-2^n)}(A_2) \cap \alpha_{(-2^n,0)}(A_3) = \emptyset.$$

Proof: Freshman's dream.

Infinity is large in \mathbb{Z}^d : there are many ways to make r points move apart in \mathbb{Z}^d . Schmidt introduced the following notion: a *shape*

$$S = \{\mathbf{n}_1, \dots, \mathbf{n}_r\}$$

is *mixing* if

$$\mu\left(\alpha_{-k\mathbf{n}_1}(A_1) \cap \dots \cap \alpha_{-k\mathbf{n}_r}(A_r)\right) \rightarrow \prod_{i=1}^r \mu(A_i).$$

as $k \rightarrow \infty$.

Notice that $\{(0, 0), (1, 0), (0, 1)\}$ is a non-mixing shape for Ledrappier's example.

Two orders of mixing: given a measure-preserving \mathbb{Z}^d -action α , let

$$m(\alpha) = \sup\{r \mid \alpha \text{ is mixing on } r \text{ sets}\}$$

and

$$s(\alpha) = \sup\{r \mid \text{all } r\text{-shapes are mixing shapes}\}.$$

Notice that $m(\alpha) \leq s(\alpha)$.

Example: For any $k \leq \infty$ there is a measure-preserving \mathbb{Z}^2 action α with $m(\alpha) = 1$ and $s(\alpha) = k$.

Theorem: If X is a compact abelian group and α is a \mathbb{Z}^d -action by automorphisms, then $m(\alpha) = s(\alpha)$.

1: Translate into commutative algebra

The character group \hat{X} of X is an abelian group carrying d commuting automorphisms. Call these multiplication by u_1, \dots, u_d and let

$$R_d = \mathbb{Z}[u_1^{\pm 1}, \dots, u_d^{\pm 1}].$$

Then $M_X = \hat{X}$ is an R_d -module. Conversely: any R_d module M defines such an action α_M on $X_M = \hat{M}$.

Example: Ledrappier's example corresponds to the module $R_2/\langle 2, 1 + u_1 + u_2 \rangle$.

Approximate the indicator functions of the sets by trigonometric polynomials, apply orthogonality relations of characters, write $\mathbf{u}^{\mathbf{n}} = u_1^{n_1} \dots u_d^{n_d}$ to get the following.

A sequence $\left(\mathbf{n}_1^{(j)}, \dots, \mathbf{n}_r^{(j)} \right)$ is mixing for α_M if and only if for any a_1, \dots, a_r in $M \setminus \{0\}$,

$$\mathbf{u}^{\mathbf{n}_1^{(j)}} a_1 + \dots + \mathbf{u}^{\mathbf{n}_r^{(j)}} a_r = 0 \quad (1)$$

implies j is finite.

2: Exploit the algebra

A simple argument using (1) shows that a given sequence is mixing for α_M if and only if it is mixing for $\alpha_{R_d/\mathfrak{p}}$ for every prime ideal \mathfrak{p} associated to the module M .

Hence: without loss of generality, we can assume the module is R_d/\mathfrak{p} .

Example: Let $\mathfrak{p} = \langle u_1 - 2, u_2 - 3 \rangle$. Then the problem we need to understand is the following. Given a_1, \dots, a_r non-zero, if

$$\mathbf{n}_s^{(j)} - \mathbf{n}_t^{(j)} \rightarrow \infty \text{ as } j \rightarrow \infty \text{ for } s \neq t,$$

can

$$a_1 2^{n_{1,1}^{(j)}} 3^{n_{1,2}^{(j)}} + \dots + a_r 2^{n_{r,1}^{(j)}} 3^{n_{r,2}^{(j)}} = 0$$

for infinitely many j ?

3. Realise this is a Diophantine problem

This looks like the following problem: fix a field or integral domain k , and let G be a finitely-generated multiplicative subgroup of k^* . Then solve

$$a_1x_1 + \cdots + a_rx_r = 0$$

for $x_i \in G$.

You can get many solutions:

Example: For Ledrappier, the relevant integral domain is

$$k = R_2 / \langle 2, 1 + u_1 + u_2 \rangle,$$

and $G = \langle\langle u_1, u_2 \rangle\rangle$. Notice that

$$1 + u_1^{2^n} + u_2^{2^n} = (1 + u_1 + u_2)^{2^n} = 0$$

for all n .

Example: That was Frobenius. Now take $k = \mathbb{F}_3(t)$; then

$$1 + u + u^2 - (u - 1)^2 = 0$$

for any $u \in \mathbb{F}_3[[t]]$ with $u \not\equiv 1 \pmod{t}$.

4. Deus ex machina

We need to classify the solutions to such linear equations in finitely-generated multiplicative subgroups.

Theorem: Let k be an algebraic number field of degree D over \mathbb{Q} , let S be a finite set of places of k including all the infinite places. Then

$$ax_1 + \cdots + a_n x_n = 1$$

has no more than

$$(4|S|D!)^{2^{36nD!}|S|^6}$$

solutions in S -units such that no proper subsums vanish.

(Schlickewei)

Corollary: In a field of characteristic zero, for G finitely generated

$$a_1 x_1 + \cdots + a_n x_n = 1$$

has only finitely many solutions with $x_i \in G$ and no vanishing subsums.

5. The connected case

Assume that X is a connected group. Then the resulting modules R_d/\mathfrak{p} have no additive torsion, so embed in fields of characteristic zero.

The S -unit theorem says that if a sequence $(\mathbf{n}_1^{(j)}, \dots, \mathbf{n}_r^{(j)})$ is NOT mixing (infinitely many solutions), rearrange to get a 1 on the right-hand side, then some subsum vanishes, giving a NOT mixing sequence of lower order.

So $m(\alpha) > 1 \Rightarrow m(\alpha) = \infty \Rightarrow s(\alpha) = m(\alpha)$.

QED

Schmidt (1989): $s(\alpha) > 1 \Rightarrow s(\alpha) = \infty$;

Schmidt and Ward (1993): $m(\alpha) > 1 \Rightarrow m(\alpha) = \infty$.

6. The disconnected case

If X is not connected, then there are associated prime ideals \mathfrak{p} with $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime p . The resulting modules can be embedded in function fields of characteristic p , so all one needs is a version of the S -unit theorem in positive characteristic (where is it not on the face of it true).

Einsiedler and Ward proved that $m(\alpha) = s(\alpha)$ if $d = 2$ and $m(\alpha) \leq 3$ (!).

In 2003 Masser proved the following.

Theorem: If X is not connected, then

$$m(\alpha) \leq R \Rightarrow s(\alpha) \leq R.$$

That is, a non-mixing *sequence* of order R implies there is a non-mixing *shape* of order R . It follows that

$$s(\alpha) \leq m(\alpha).$$

His proof amounts to a special kind of S -unit theorem in positive characteristic.

Hence:

Theorem: If X is a compact abelian group and α is a \mathbb{Z}^d -action by automorphisms, then $m(\alpha) = s(\alpha)$.