

## THE WORK OF EINSIEDLER, KATOK AND LINDENSTRAUSS ON THE LITTLEWOOD CONJECTURE

AKSHAY VENKATESH

### CONTENTS

1. The Littlewood conjecture	118
1.1. Statement of the theorem	118
1.2. This document	119
1.3. Symmetry	119
2. The Oppenheim conjecture	120
2.1. Statement of the Oppenheim conjecture	120
2.2. Symmetry	121
2.3. Lattices	121
2.4. Background on the space of lattices	121
3. Unipotents acting on lattices	122
3.1. Unipotents from Margulis to Ratner	122
3.2. Ratner's theorems	122
3.3. An idea from the proof of Theorem 3.1: Measures not sets	123
4. The dynamics of coordinate dilations on lattices, I: Conjectures and analogies	123
4.1. Reduction to dynamics	123
4.2. An analogy with $\times 2 \times 3$ on $S^1$	124
4.3. A short detour on entropy	125
4.4. Conjectures and results for $\times 2 \times 3$ and for $A_n$	126
5. Coordinate dilations acting on lattices, II: The product lemma of Einsiedler-Katok	128
5.1. Some ideas in the general proof	128
5.2. Closed sets	128
5.3. What comes next	130
5.4. Conditional measures: the analogue of the $\sigma_x^{ij}$ for measures	130
5.5. From product lemma to unipotent invariance	130
5.6. Back to Theorem 1.1	132
5.7. Conditional measures and entropy	132

---

Received by the editors May 11, 2007, and, in revised form, May 28, 2007.

2000 *Mathematics Subject Classification*. Primary 11J13, 37A35, 33A45, 11H46.

This article is based on a lecture presented January 7, 2007, as part of the Current Events Bulletin at the Joint Mathematics Meetings in New Orleans, LA.

©2007 American Mathematical Society  
Reverts to public domain 28 years from publication

Acknowledgements	133
About the author	133
References	133

This document is intended as a (slightly expanded) writeup of my talk at the AMS Current Events Bulletin in New Orleans, January 2007. It is a brief report on the work of Einsiedler, Katok and Lindenstrauss on the Littlewood conjecture [5].

It is not intended in any sense for specialists and is, indeed, aimed at readers without any specific background in measure theory, dynamics or number theory. Any reader with any background in ergodic theory will be better served by consulting either the original paper or one of the surveys written by those authors: see [6] and [16].

My background is that of a number theorist, not a dynamicist. I apologize in advance for any errors; in particular, I am familiar with the pertinent dynamical ideas largely in a number-theoretic context and therefore may not properly represent their history or dynamical context. Nonetheless, I hope that this note serves as a useful introduction to the beautiful progress on an old arithmetic question.

## 1. THE LITTLEWOOD CONJECTURE

**1.1. Statement of the theorem.** For  $x \in \mathbb{R}$ , let  $\|x\|$  denote the distance from  $x$  to the nearest integer. It is not difficult to check that, for any  $\alpha \in \mathbb{R}$ , there exist integers  $p, q$  with  $1 \leq q \leq Q$  and  $|\alpha - \frac{p}{q}| \leq \frac{1}{qQ}$ . In other words,  $\|q\alpha\| \leq 1/Q$ . The behavior of  $\|q\alpha\|$ , as  $q$  varies through integers, thereby reflects *approximation of  $\alpha$  by rational numbers*.

The Littlewood conjecture concerns simultaneous approximation of *two* numbers  $\alpha, \beta$  by irrationals. It asserts that:

$$(1) \quad \liminf_{n \geq 1} n \cdot \|n\alpha\| \|n\beta\| = 0,$$

whatever be  $\alpha, \beta$ . In words, it asserts (in a somewhat peculiar-seeming way)

$$(2) \quad \alpha, \beta \text{ may be simultaneously approximated, moderately well,} \\ \text{by rationals with the same denominator.}$$

My goal is to discuss, and give some of the context around, the following theorem of M. Einsiedler, A. Katok and E. Lindenstrauss in [5]:

**Theorem 1.1.** *The set of  $\alpha, \beta$  for which (1) fails has Hausdorff dimension 0.*

This theorem is proved using ideas from dynamics: namely, by studying the action of coordinate dilations (e.g.  $(x, y, z) \mapsto (\frac{x}{2}, 2y, z)$ ) on the space of *lattices* in  $\mathbb{R}^3$ . These ideas build on the work of many: in addition to some of the work discussed in this paper, one should mention in particular the prior work of Katok-Spatzier [9, 10], Kalinin-Spatzier [8], Einsiedler-Katok [4] and Lindenstrauss [15].

The theorem is not important solely as a result about simultaneous Diophantine approximation, but because of the techniques and results in dynamics that enter into its proof.

Several applications of this type of dynamics are surveyed in [6]. For now it is worth commenting on two rather different contexts in number theory where exactly the same dynamics arise:

- In the study of analytic behavior of automorphic forms (see [24] for discussion and historical context).
- In the study of the analytic behavior of ideal classes in number fields, see [7].

1.2. **This document.** I will try to stress:

- (1) Dynamics arises from a (not immediately visible) symmetry group; see §1.3. I will then discuss some historical context for this type of connection (§2, §3).
- (2) The dynamics that is needed is similar to the simultaneous action of  $x \mapsto 2x, x \mapsto 3x$  on  $\mathbb{R}/\mathbb{Z}$ ; see §4.4 for a description of these parallels.
- (3) A sketch of just one of the beautiful ideas that enters in proving Theorem 1.1 (see §5), which is to study the picture transverse to the acting group.

A massive defect of the exposition is that I will make almost no mention of *entropy*. This is an egregious omission, because the intuition which comes from the study of entropy underpins much of the recent progress in the subject. However, any serious discussion of entropy would require more space and time and competence than I have, and better references are available. So, instead, I have given a somewhat *ad hoc* discussion adapted to the cases under consideration. I will not come even close to sketching a proof of the main result.

Let us make two notes before starting any serious discussion:

- (1) The Littlewood conjecture, (1), is quite plausible. Here is a naive line of heuristic reasoning that supports it. A consequence of what we have said in §1.1 is that there exists a sequence  $q_k \rightarrow \infty$  of positive integers such that  $q_k \|q_k \alpha\| \leq 1$ . Barring some conspiracy to the contrary, one might expect that  $\|q_k \beta\|$  should be small *sometimes*. The problem in implementing this argument is that we have rather little control over the  $q_k$ .<sup>1</sup>
- (2) Despite all the progress that I shall report on, we do not know whether the statement (1) is true even for  $\alpha = \sqrt{2}, \beta = \sqrt{3}$ . The question of removing the exceptional set in Theorem 1.1 is related to celebrated conjectures (see Conjecture 4.1 and Conjecture 4.2) of Furstenberg and Margulis.

1.3. **Symmetry.** The next point is that the question (1) has a symmetry group that is not immediately apparent. This is responsible for our ability to apply dynamical techniques to it.

Pass to a general context for a moment. Let  $f(x_1, \dots, x_n)$  be an integral polynomial in several variables. An important concern of number theory has been to understand *Diophantine equalities*: solutions to  $f(\mathbf{x}) = 0$  in integers  $\mathbf{x} \in \mathbb{Z}^n$  (e.g. Does  $x^2 - y^2 - z^2 = 1$  have a solution in integers? Does  $x^3 + y^3 = z^3$  have a solution in integers?).

A variant of this type of question, somewhat less visible but nonetheless (in my opinion) difficult and fascinating, concerns *Diophantine inequalities*: if  $f$  does not

---

<sup>1</sup>Amusingly, it is not even clear this heuristic argument will work. It may be shown that given a sequence  $q_k$  such that  $\liminf q_{k+1}/q_k > 1$ , there exists  $\beta \in \mathbb{R}$  such that  $\|q_k \beta\|$  is bounded away from 0. See [11, 19] for this and more discussion.

have rational coefficients, one may ask about the solvability of an equation such as  $|f(\mathbf{x})| < \varepsilon$  for  $\mathbf{x} \in \mathbb{Z}^n$  (e.g. does  $|x^2 + y^2 - \sqrt{2}z^2| < 10^{-6}$  have a solution?).

In the most general context of an arbitrary  $f$ , our state of knowledge is somewhat limited. On the other hand, for special classes of  $f$  we know more: a typical class which is accessible to analytic methods is when the *degree of  $f$  is small compared to the number of variables*.

Another important class about which we have been able to make progress consists of those  $f$  possessing symmetry groups. Both the examples  $x^2 - y^2 - z^2 = 1$  and  $x^2 + y^2 - \sqrt{2}z^2$  admit orthogonal groups in three variables as automorphisms.<sup>2</sup> The homogeneous equation  $x^3 + y^3 = z^3$  has symmetry but not by a linear algebraic group (it defines an elliptic curve inside  $\mathbb{P}^2$ ).

The Littlewood conjecture also has symmetry, although not immediately apparent. To see it, we note that  $\|x\| = \inf_{m \in \mathbb{Z}} |x - m|$ ; consequently, we may rewrite (1) as the statement:

$$(3) \quad |n(n\alpha - m)(n\beta - \ell)| < \varepsilon \text{ is solvable, with } (n, m, \ell) \in \mathbb{Z}^3, n \neq 0, \text{ for all } \varepsilon > 0.$$

But the function  $L(n, m, \ell) = n(n\alpha - m)(n\beta - \ell)$  is a product of three linear forms and admits a two-dimensional torus as a group of automorphisms.<sup>3</sup>

## 2. THE OPPENHEIM CONJECTURE

Here we pause to put the developments that follow into their historical context.

**2.1. Statement of the Oppenheim conjecture.** We briefly discussed above the form  $x^2 + y^2 - \sqrt{2}z^2$ . This is a particular case of a problem considered in 1929: A. Oppenheim conjectured that if  $Q(x_1, \dots, x_n) = \sum_{i,j} a_{ij}x_i x_j$  is an *indefinite* quadratic form in  $n \geq 3$  variables which is not a multiple of a rational form, then  $Q$  takes values which are arbitrarily small, in absolute value.

In other words – note the analogy with (3) –

$$(4) \quad |Q(\mathbf{x})| < \varepsilon \text{ is solvable, with } \mathbf{x} \in \mathbb{Z}^n, \text{ for all } \varepsilon > 0.$$

When  $n$  is sufficiently large his conjecture was solved by Davenport (in 1956) by analytic methods. His paper required  $n \geq 74$ . This is an example of the fact, noted in §1.3, that purely analytic methods can often handle cases when the number of variables is sufficiently large relative to the degree.

On the other hand, the complete resolution of the conjecture<sup>4</sup> had to wait until G. Margulis, in the early 1980s, gave a complete proof using dynamical methods that made critical use of the group of automorphisms of  $Q$ .

<sup>2</sup>Although unimportant in the context of this paper, there is an important difference: while  $x^2 + y^2 - \sqrt{2}z^2$  admits an action of the real Lie group  $O(2, 1)$ , the analysis of the form  $x^2 + y^2 + z^2$  involves studying the action of the much larger *adelic* Lie group of automorphisms. In particular, this adelic group is noncompact even though the real group  $O(3)$  is compact, and this is a point that can be fruitfully exploited; see [2].

<sup>3</sup>The  $n$ -dimensional version of the Littlewood conjecture takes  $n$  linear forms  $\ell_1, \dots, \ell_n$  and asks: is the equation  $0 < |\ell_1(\mathbf{x}) \dots \ell_n(\mathbf{x})| < \varepsilon$  solvable with  $\mathbf{x}$  integral? Conjecturally, this is so if  $n \geq 3$  and  $\ell_1 \dots \ell_n$  is not a real multiple of an integral polynomial. It is false for  $n = 2$ ; see footnote 4.

<sup>4</sup>The analogous statement is false for  $n = 2$ : take e.g.  $Q(x, y) = (x - \sqrt{2}y)y$ . To see that, write  $Q(x, y) = \frac{(x^2 - 2y^2)y}{(x + \sqrt{2}y)}$ .

**2.2. Symmetry.** Let  $H = \text{SO}(Q)$ , the group of orientation-preserving linear transformations of  $\mathbb{R}^n$  preserving  $Q$ . By definition  $Q(\mathbf{x}) = Q(h.\mathbf{x})$ . We wish to exploit<sup>5</sup> the fact that  $H$  is large.

In particular, in order to show (4), it suffices to show that  $Q$  takes values in  $(-\varepsilon, \varepsilon)$  at a point of the form  $h.\mathbf{x}$  ( $h \in H, \mathbf{x} \in \mathbb{Z}^n$ ). *A priori*, this set might be much larger than  $\mathbb{Z}^n$ ; certainly, if it were dense in  $\mathbb{R}^n$ , this would be enough to show (4).

For instance, if we could prove that

$$(5) \quad \text{The set } h.\mathbf{x} : h \in H, \mathbf{x} \in \mathbb{Z}^n \text{ contains } 0 \text{ in its closure,}$$

then (4) would follow immediately.

**2.3. Lattices.** (5) is rather nice, but a little unwieldy. We would rather deal with the  $H$ -orbit of a single point instead of an infinite collection. This can be done by “packaging” all  $\mathbf{x} \in \mathbb{Z}^n$  into a single object: a *lattice*.

A *lattice* in  $\mathbb{R}^n$  is simply a “grid containing the origin”, i.e. a set of all *integral* combinations of  $n$  linearly independent vectors  $\mathbf{v}_1, \dots, \mathbf{v}_n$ . Every such lattice is of the form  $g.\mathbb{Z}^n$  for some  $g \in \text{GL}(n, \mathbb{R})$ .

Let  $\tilde{\mathcal{L}}_n$  be the set of lattices<sup>6</sup> in  $\mathbb{R}^n$  and let  $\tilde{\mathcal{L}}_n[\varepsilon]$  be the set of lattices that contain  $\mathbf{v} \in \mathbb{R}^n$  with Euclidean length  $\|\mathbf{v}\| \leq \varepsilon$ . So  $\mathbb{Z}^n$  can be thought of as a point  $[\mathbb{Z}^n] \in \tilde{\mathcal{L}}_n$ . Then (5) would follow if:

$$(6) \quad H.[\mathbb{Z}^n] \cap \tilde{\mathcal{L}}_n[\varepsilon] \neq \emptyset, \text{ for all } \varepsilon > 0.$$

This is a statement that fits cleanly into the context of dynamics: does the orbit of the point  $[\mathbb{Z}^n] \in \tilde{\mathcal{L}}_n$ , under the group  $H$ , intersect the subset  $\tilde{\mathcal{L}}_n[\varepsilon]$ ? It is (6), which was proven by Margulis.

**2.4. Background on the space of lattices.** To each lattice we can assign a natural invariant, its *covolume*. Choosing generators  $\mathbf{v}_1, \dots, \mathbf{v}_n$  for the lattice, the covolume is the absolute value of the determinant of the matrix with rows  $\mathbf{v}_1, \dots, \mathbf{v}_n$ , that is to say, the volume of a fundamental parallelepiped  $\sum \lambda_i \mathbf{v}_i : \lambda_i \in [0, 1)$ . For  $g \in \text{GL}(n, \mathbb{R})$  and  $L \in \tilde{\mathcal{L}}_n$ , we observe that  $\text{covol}(g.L) = |\det g| \text{covol}(L)$ . In particular, because all  $h \in H$  have determinant 1, all elements in  $H.[\mathbb{Z}^n]$  have covolume 1. So  $H.[\mathbb{Z}^n]$  belongs to the subset

$$(7) \quad \mathcal{L}_n = \{L \in \tilde{\mathcal{L}}_n : L \text{ has covolume } 1\}.$$

The space  $\mathcal{L}_n$  is more pleasant to work with than  $\tilde{\mathcal{L}}_n$ . The map  $g \mapsto g.[\mathbb{Z}^n]$  identifies  $\tilde{\mathcal{L}}_n$  with the quotient  $\text{GL}(n, \mathbb{R})/\text{GL}(n, \mathbb{Z})$  and  $\mathcal{L}_n$  with the quotient  $\text{SL}(n, \mathbb{R})/\text{SL}(n, \mathbb{Z})$ . These identifications give rise to topologies on  $\tilde{\mathcal{L}}_n$  and  $\mathcal{L}_n$ ; indeed, they are given the structure of manifolds.

Although  $\mathcal{L}_n$  is not compact, it admits a natural  $\text{SL}(n, \mathbb{R})$ -invariant measure of finite volume, which is a reasonable substitute for compactness. Moreover, Mahler’s criterion – a consequence of reduction theory for lattices [23] – gives a precise description of how  $\mathcal{L}_n$  fails to be compact. Put  $\mathcal{L}_n[\varepsilon] := \tilde{\mathcal{L}}_n[\varepsilon] \cap \mathcal{L}_n$ .

<sup>5</sup>The idea that this should be exploitable was suggested by M. Raghunathan. It is also implicitly used in a paper of Cassels and Swinnerton-Dyer from the 1950s.

<sup>6</sup>We will later work almost exclusively with the subset of  $\tilde{\mathcal{L}}_n$  consisting of lattices of covolume 1. Therefore, for notational simplicity, we prefer to put a tilde for the whole space of lattices and omit it for the subset  $\mathcal{L}_n$ .

**Theorem 2.1.** *A subset  $K \subset \mathcal{L}_n$  is bounded (= precompact) if and only if it does not intersect  $\mathcal{L}_n[\varepsilon]$ , for some  $\varepsilon > 0$ .*

In words, it asserts that the only way that a sequence of lattices  $L_1, L_2, \dots$  in  $\mathcal{L}_n$  can degenerate (leave any compact set in  $\mathcal{L}_n$ ) is if there exist vectors  $\mathbf{v}_1 \in L_1, \mathbf{v}_2 \in L_2, \dots$  such that  $\|\mathbf{v}_i\| \rightarrow 0$ .

We may therefore rephrase (6): The Oppenheim conjecture would follow if

$$(8) \quad H.[\mathbb{Z}^n] \text{ is unbounded in } \mathcal{L}_n.$$

### 3. UNIPOTENTS ACTING ON LATTICES

Obviously, the statement (4) is false for  $Q$  positive definite and, as observed in footnote 4, (less obviously) false for  $Q$  in two variables. How are we to detect this difference when considering the problem from the dynamical viewpoint of (6) or (8)?

**3.1. Unipotents from Margulis to Ratner.** An important difference is that the group  $H$  is isomorphic to  $\mathrm{SO}(n) \subset \mathrm{GL}(n, \mathbb{R})$  in the first case, and  $\mathrm{SO}(1, 1) \subset \mathrm{GL}(2, \mathbb{R})$  in the second case. In either case, *the group  $H$  consists entirely of semi-simple elements.*<sup>7</sup> Margulis' idea was to exploit the fact that if  $Q$  is indefinite in  $n \geq 3$  variables, the group  $H$  contains *unipotent* elements, i.e.  $g \in \mathrm{GL}(n, \mathbb{R})$  for which all of the (generalized) eigenvalues of  $g$  are equal to 1.

At a vague level, the reason why these might be helpful is quite easy to state: if  $u \in \mathrm{GL}(n, \mathbb{R})$  is unipotent, the matrix entries of  $u^n$  grow only *polynomially* in  $n$ . This contrasts sharply with the behavior of a "typical" element  $g \in \mathrm{GL}(n, \mathbb{R})$ , when these entries will grow exponentially. This means that when studying the trajectory  $ux_0, u^2x_0, u^3x_0, \dots$ , we are able to "retain information" about it for much longer.

**3.2. Ratner's theorems.** We will not say anything about the specifics of Margulis' proof; see [1] for an elementary presentation. A far-reaching generalization of Margulis' result which has been of fundamental importance for later work is the following (special case of a) theorem of Ratner; see [21] and [22]:<sup>8</sup>

**Theorem 3.1.** *Let  $H \subset \mathrm{SL}(n, \mathbb{R})$  be generated by one-parameter unipotent subgroups.<sup>9</sup> The closure of the orbit  $\overline{H.[\mathbb{Z}^n]}$  inside  $\mathcal{L}_n$  is of the form  $H'.[\mathbb{Z}^n]$  for a closed subgroup  $H' \supseteq H$ . Moreover, there exists an  $H'$ -invariant probability measure on  $H'.[\mathbb{Z}^n]$ .*

This is a difficult theorem which settled a conjecture of M. Raghunathan. The orbit  $H.[\mathbb{Z}^n]$  can be extremely complicated. Ratner's theorem asserts that its closure is determined by a very simple piece of algebraic data: a subgroup intermediate between  $H$  and  $\mathrm{SL}(n, \mathbb{R})$ .

Let us see how this implies (6). The group  $H = \mathrm{SO}(Q)$  is *maximal* inside  $\mathrm{SL}(n, \mathbb{R})$ . So Theorem 3.1 means that either  $H.[\mathbb{Z}^n]$  is closed or  $H.[\mathbb{Z}^n]$  is dense in  $\mathcal{L}_n$ . It may be seen that  $H.[\mathbb{Z}^n]$  is closed only if the form  $Q$  is a multiple of a rational form. In this fashion, Theorem 3.1 implies the Oppenheim conjecture.

<sup>7</sup>i.e. conjugate to a diagonal matrix over the complex numbers.

<sup>8</sup>This theorem, in general, is not just about spaces like  $\mathcal{L}_n = \mathrm{SL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{Z})$ , but more general quotients of Lie groups by discrete subgroups.

<sup>9</sup>i.e. of the form  $\exp(tX)$  where  $X$  is a nilpotent matrix.

**3.3. An idea from the proof of Theorem 3.1: Measures not sets.** Although a fascinating topic, we shall limit our discussion of Theorem 3.1 to emphasizing a single philosophical point from the proof of Theorem 3.1 that has also been indispensable in later work.

(9) Measures are often easier to work with than sets.

To be a little more specific, let us comment on how Ratner’s proof of Theorem 3.1 works. Let us take the simple case when  $H$  consists *entirely* of unipotent elements. (A comprehensive exposition of the proof is to be found in [26].)

Ratner begins by classifying the *probability measures* on  $\mathcal{L}_n$  that are invariant under  $H$ . The topological statement of Theorem 3.1 is then *deduced* from the classification of  $H$ -invariant probability measures.

The relation between probability measures and invariant sets is quite simple: an invariant probability measure has a support which is a closed  $H$ -invariant set. Conversely, if  $Y \subset \mathcal{L}_n$  is an  $H$ -invariant closed set, it must support an  $H$ -invariant probability measure (average your favorite measure under  $H$  – note that this requires  $H$  to be amenable). This relation is a good deal more tenuous than one would like – the support of the measure constructed this way may be strictly smaller than  $Y$  – and the deduction of statements concerning invariant sets from statements about probability measures is not formal.

Nonetheless, what is gained by going through measures? Measures have much better formal properties than sets. A particularly important difference is that an  $H$ -invariant probability measure can be decomposed into “minimal” invariant measures (ergodic decomposition).<sup>10</sup> That property does not seem to have a clean analogy at the level of  $H$ -invariant closed sets. In particular, an  $H$ -invariant closed set always *contains* a minimal  $H$ -invariant closed set, but cannot be decomposed into minimal  $H$ -invariant closed sets in any obvious way.

This is not to say that it is necessarily impossible to prove Theorem 3.1 by purely topological methods. Indeed, Margulis’ original proof of (6) was purely topological (and utilized a study of minimal  $H$ -invariant closed sets). But, to my knowledge, no such proof has been carried out in the general case.

#### 4. THE DYNAMICS OF COORDINATE DILATIONS ON LATTICES, I: CONJECTURES AND ANALOGIES

We have seen that the assertion (4) about the values of the quadratic form  $x^2 + y^2 - \sqrt{2}z^2$  can be converted to the assertion (6) about the orbit of  $[\mathbb{Z}^n]$  under the group  $H = \text{SO}(Q)$ . We now briefly carry through the corresponding reasoning in the case of the Littlewood conjecture. This will lead us to study the action of the diagonal group  $A_3$  inside  $\text{SL}(3, \mathbb{R})$  on  $\mathcal{L}_3$ .

**4.1. Reduction to dynamics.** Let  $P(x_1, x_2, x_3) = x_1(\alpha x_1 - x_2)(\beta x_1 - x_3)$ . We have seen (see (3)) that the Littlewood conjecture is (almost, with a constraint  $x_1 \neq 0$ ) equivalent to the assertion that  $|P(\mathbf{x})| < \varepsilon$  is solvable in integers.

---

<sup>10</sup>The set of  $H$ -invariant probability measures forms, clearly, a convex set in the space of all probability measures. Any point in this convex set can be expressed as a convex linear combination of extreme points. These extreme points are called *ergodic* measures for  $H$  and are “minimal”, in the sense that they cannot be expressed nontrivially as an average of two other  $H$ -invariant probability measures. See [25] for a general introduction.

Let  $T$  be the *automorphism group of  $P$* , that is to say, the set of  $g \in \mathrm{GL}(3, \mathbb{R})$  such that  $P(g.\mathbf{x}) = P(\mathbf{x})$ .  $T$  contains a conjugated copy of the group of diagonal matrices.<sup>11</sup>

So  $P(a.\mathbf{x}) = P(\mathbf{x})$  for  $a \in T$ . It would appear to be enough to show that  $\{a.\mathbf{x} : a \in T, \mathbf{x} \in \mathbb{Z}^n\}$  approaches arbitrarily close to 0, or, repeating the line of implications (4)  $\Leftarrow$  (6)  $\Leftarrow$  (8), it seems to be enough to show that  $T.[\mathbb{Z}^n]$  is unbounded in  $\mathcal{L}_n$ .

This is not quite right, though:  $T.[\mathbb{Z}^n]$  being unbounded in  $\mathcal{L}_n$  indeed would produce solutions to  $|x_1(\alpha x_1 - x_2)(\beta x_1 - x_3)| < \varepsilon$  but, regrettably, provides no guarantee that  $x_1 \neq 0$ .

However, this can be avoided by replacing  $T$  with a certain subsemigroup  $T^+ \subset T$  engineered specifically to avoid this. Moreover, since  $T$  contains a conjugate copy of  $A_3$  (the diagonal subgroup of  $\mathrm{SL}_3(\mathbb{R})$ ) as a finite index subgroup, we can rephrase this assertion in terms of the dynamics of  $A_3$ , not of  $T$ .

We will not go through the details, but rather will explicate the result of going through this process: if  $L_{\alpha, \beta} \subset \mathbb{R}^3$  is the lattice spanned by  $(1, \alpha, \beta), (0, 1, 0)$  and  $(0, 0, 1)$ , the Littlewood conjecture for  $(\alpha, \beta)$  is equivalent to:

(10)  $A_3^+.L_{\alpha, \beta}$  is unbounded in  $\mathcal{L}_n$ ,

$$A_3^+ = \left\{ \begin{pmatrix} x & 0 & 0 \\ 0 & y & 0 \\ 0 & 0 & z \end{pmatrix} : xyz = 1, x \leq 1, y \geq 1, z \geq 1 \right\}.$$

The reader can easily verify (10) directly.

We are led, more generally, to study the action of the group of diagonal matrices with determinant 1, denoted  $A_n$ , on  $\mathcal{L}_n$ , and, in particular, to seek an analogue of Theorem 3.1. The obstacle will be that the analogue of Theorem 3.1 *totally fails* for (conjugates of)  $A_2$  acting on  $\mathcal{L}_2$ . There exists a plethora of orbit closures that do not correspond to closed orbits of intermediate subgroups  $A_2 \leq H \leq \mathrm{SL}(2, \mathbb{R})$ . (This corresponds roughly to the fact that there are many  $\alpha$  for which  $\liminf n\|\alpha\| > 0$ ; i.e. the “one variable” Littlewood conjecture is false.)

**4.2. An analogy with  $\times 2 \times 3$  on  $S^1$ .** Let us reprise: we are studying the action of the group  $A_n$  (diagonal matrices of size  $n$ , with determinant 1) on the space  $\mathcal{L}_n = \mathrm{SL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{Z})$ , or, geometrically, we are studying the action of *coordinate dilations* on grids in  $\mathbb{R}^n$ .

A very helpful analogy in studying the action of  $A_n$  on  $\mathcal{L}_n$  is the following:

(11) Action of  $A_2$  on  $\mathcal{L}_2$  behaves like  $x \mapsto 2x$  on  $\mathbb{R}/\mathbb{Z}$ ;

(12) Action of  $A_3$  on  $\mathcal{L}_3$  behaves like  $x \mapsto 2x, x \mapsto 3x$  on  $\mathbb{R}/\mathbb{Z}$ .

Note that  $A_3$  is a two-parameter (continuous) group, whereas  $x \mapsto 2x, x \mapsto 3x$  generate a two-parameter (discrete) semigroup. We will often use the notation “ $\times 2$ ” or “ $\times 2 \times 3$ ” as a shorthand for the dynamical systems  $x \mapsto 2x$  or  $x \mapsto 2x, x \mapsto 3x$  on  $\mathbb{R}/\mathbb{Z}$ .

The analogies (11) and (12) – we will make precise statements to illustrate them in a moment – appear to be quite strong, although I do not know of any entirely

---

<sup>11</sup>In a suitable coordinate system,  $P$  becomes  $P(x_1, x_2, x_3) = x_1 x_2 x_3$ . But the set of linear transformations that preserve  $(x_1, x_2, x_3) \mapsto x_1 x_2 x_3$  consist of all permutation matrices whose determinant is  $\pm 1$  according to the sign of the permutation.

satisfying “reason” for them. The analogy between  $(A_2, \mathcal{L}_2)$  and  $(\times 2, \mathbb{R}/\mathbb{Z})$  is particularly strong: in a fairly precise sense,<sup>12</sup> the action of a suitable element  $a \in A_2$  on  $\mathcal{L}_2$  behaves like a shift on  $\{0, 1\}^{\mathbb{Z}}$ , whereas the action of  $x \mapsto 2x$  behaves like a shift on  $\{0, 1\}^{\mathbb{N}}$ . We will list in the next section some results and questions in both the  $\mathcal{L}$  and  $\mathbb{R}/\mathbb{Z}$  cases and will see they are quite analogous.

For the moment, let us just observe that the action of  $x \mapsto 2x$  on  $\mathbb{R}/\mathbb{Z}$  is fundamentally different from the simultaneous action of  $x \mapsto 2x, x \mapsto 3x$ . Indeed, the trajectory  $\{2^n x\}$  of a point under  $x \mapsto 2x$  essentially encodes the binary expansion of  $x$ , which can be arbitrarily strange (cf. Lemma 4.1). For instance, there exist uncountably many possibilities for the closure  $\overline{\{2^n x\}}$ . On the other hand, it is much more difficult to arrange that the binary and ternary expansions of a given  $x$  be *simultaneously* strange. This means it is much harder to arrange that the orbit of  $x$  under  $x \mapsto 2^n 3^m x$  be strange, and indeed it is known that the possibilities for the closure  $\overline{\{2^n 3^m x\}}$  are very simple (see Theorem 4.1).

Correspondingly, one might hope that the fact that Theorem 3.1 fails for  $(A_2, \mathcal{L}_2)$ , as commented on at the end of §4.1, might be a phenomenon that vanishes when one passes to  $(A_n, \mathcal{L}_n)$  for  $n \geq 3$ . Indeed, this is believed to be largely the case.

**4.3. A short detour on entropy.** In order to enunciate precise theorems about our dynamical systems, we shall need to make use of the notion of *positive entropy*. Let us briefly give an incomplete survey of this notion; for more, see [6, Section 3] (in the context of homogeneous spaces) and [25] (as a general reference).

We motivate it by considering the map  $\times 2$ . We have already noted that (via binary expansion) this amounts to a shift on  $\{0, 1\}^{\mathbb{N}}$ . In particular, the number of possibilities for the collection of first binary digits of a trajectory  $(x, 2x, 4x, \dots, 2^n x)$  grows *exponentially* in  $n$ . This is not a general feature of dynamical systems: if we take  $T(x) = x + \sqrt{7}$ , the number of possibilities for the first binary digits of  $(x, Tx, T^2x, \dots, T^n x)$  grows at most linearly with  $n$ . The *entropy* will be an invariant of a dynamical system that detects this exponential growth; it will be positive in the case of  $\times 2$  and zero in the case of  $T(x) = x + \sqrt{7}$ .

More precisely, the theory of metric entropy assigns to a measure-preserving transformation  $T$  of a probability space  $(X, \mu)$  a non-zero number, the *entropy*  $h_\mu(T)$  of  $T$ . We briefly reprise the definition. If  $\mathcal{P}$  is a partition of the probability space  $(X, \mu)$ , the entropy of  $\mathcal{P}$  is defined as  $H_\mu(\mathcal{P}) := \sum_{S \in \mathcal{P}} -\mu(S) \log \mu(S)$ . We define the ergodic theoretic entropy of the transformation  $T$  as:

$$(13) \quad h_\mu(T) = \sup_{\mathcal{P}} \lim_{n \rightarrow \infty} \frac{H_\mu(\mathcal{P} \vee T^{-1}\mathcal{P} \vee \dots \vee T^{-(n-1)}\mathcal{P})}{n},$$

where the supremum is taken over all finite partitions of  $X$ . Here  $\vee$  denotes the minimal common refinement of two partitions.

We might think of this as follows: Suppose, for simplicity, that  $\mathcal{P} = \{P_1, \dots, P_r\}$  attains the supremum in (13). For  $y \in X$ , write  $[y] \in \{1, \dots, r\}$  for the index of the part of  $\mathcal{P}$  containing  $y$ .

Pick a random  $x \in X$  – *random* according to  $\mu$  – and write down the sequence  $[Tx], \dots, [T^n x]$ . In this way, we get a probability measure on  $\{1, \dots, r\}^n$ , which tells us how probable a sequence of digits is to occur. Let  $H(n)$  be the cardinality

---

<sup>12</sup>e.g. the systems are measure-theoretically isomorphic.

of the smallest subset of  $\{1, \dots, r\}^n$  that occurs with probability  $> 0.9$  (or any fixed number in  $(0, 1)$ ); if  $\mu$  is ergodic, then  $\frac{\log H(n)}{n}$  will converge to the entropy.

We will make one more remark – rather imprecisely, since we will use it only in a sketchy way – to try to illustrate the content of positive entropy. We claim that:

(14) If  $[Tx], \dots, [T^n x]$  determines  $[x]$  with high probability,  
then  $h_\mu(T)$  is small.

(Formal version: if there existed a function  $f : \{1, \dots, r\}^n \rightarrow \{1, \dots, r\}$  with the property that  $[x] = f([Tx], [T^2x], \dots, [T^n x])$  with probability  $\geq 1 - \varepsilon$ , then the entropy is bounded in terms of  $\varepsilon$ , this bound approaching 0 as  $\varepsilon$  does.) Indeed, the assumption implies that (replacing  $x$  by  $T^{-n-1}x$ ) that “[ $T^{-1}x$ ],  $\dots$ , [ $T^{-n}x$ ] determines [ $T^{-n-1}x$ ] with high probability”, which shows by a counting argument that the entropy of  $T^{-1}$  is small. However, the entropy of  $T$  and  $T^{-1}$  are equal.

We can restate (14) in the following way: positive entropy arises from the possibility of different points having similar forward trajectories.

**4.4. Conjectures and results for  $\times 2 \times 3$  and for  $A_n$ .** Recall that a probability measure  $\nu$  invariant under a group  $G$  is said to be  $G$ -ergodic if any  $G$ -invariant measurable subset  $S$  has either  $\nu(S) = 1$  or  $\nu(S) = 0$ . An equivalent definition is found in footnote 10.

We observe that a classification of  $G$ -invariant ergodic probability measures is as good as a classification of  $G$ -invariant probability measures, for any  $G$ -invariant probability measure can be expressed as a convex combination of  $G$ -invariant ergodic probability measures.

These definitions are also good for non-invertible transformations and semigroups of such. Then it is easier (for me) to think in terms of functions. If  $G$  is a semigroup, a measure  $\nu$  is said to be  $G$ -invariant if the integrals of  $f(x)$  and  $x \mapsto f(gx)$  coincide, for all  $g \in G$  and all continuous functions  $f$ . We say that a measure is  $G$ -ergodic if any  $\nu$ -measurable function which is invariant under  $G$  is constant (modulo sets of measure 0). In what follows, we shall speak of a measure  $\nu$  on  $\mathbb{R}/\mathbb{Z}$  being invariant or ergodic under  $x \mapsto 2x, x \mapsto 3x$ . By this, we mean that it is invariant or ergodic under the semigroup generated by these transformations.

Formalizations of some of the intuitions we suggested in the previous section are to be found in the following results. They state, in that order, that:

- There are a huge number of closed invariant sets for  $x \mapsto 2x$ .
- There are very few closed invariant sets for  $x \mapsto 2x, x \mapsto 3x$  simultaneously (and a clean classification).
- Conjecturally, there are very few invariant probability measures under  $x \mapsto 2x, x \mapsto 3x$ .
- One can prove the third assertion under an additional assumption on the measure, positive entropy.

**Lemma 4.1.** *There exist orbit closures  $\{\overline{2^n x}\}_{n \geq 0}$  of any Hausdorff dimension between 0 and 1.*

Similarly, there exist “very many” probability measures on  $\mathbb{R}/\mathbb{Z}$  invariant under  $x \mapsto 2x$ .

**Theorem 4.1** (Furstenberg). *The orbit closure  $\overline{\{2^n 3^m x\}}_{n, m \geq 0}$  is  $\mathbb{R}/\mathbb{Z}$  or finite, according to whether  $x$  is irrational or rational.*

**Conjecture 4.1** (Furstenberg). *Let  $\mu$  be a probability measure on  $\mathbb{R}/\mathbb{Z}$  that is invariant under  $x \mapsto 2x$  and  $x \mapsto 3x$  and ergodic w.r.t.  $x \mapsto 2x, x \mapsto 3x$ . Then  $\mu$  is either Lebesgue measure or supported on a finite set of rationals.*

**Theorem 4.2** (Rudolph). *Let  $\mu$  be a probability measure on  $\mathbb{R}/\mathbb{Z}$  that is invariant under  $x \mapsto 2x$  and  $x \mapsto 3x$  and ergodic w.r.t.  $x \mapsto 2x, x \mapsto 3x$ , and such that either  $\times 2$  or  $\times 3$  acts with positive entropy. Then  $\mu$  is Lebesgue measure.*

Now let us enunciate the analogues of these statements for  $A_n$  acting on  $\mathcal{L}_n$ . They state, in this order, that:

- There are a huge number of orbit closures and invariant measures for  $A_2$  acting on  $\mathcal{L}_2$ .
- Conjecturally, there are very few closed sets for  $A_n$  acting on  $\mathcal{L}_n$  when  $n \geq 3$ . The statement here is not as clean as in the  $(\times 2 \times 3, \mathbb{R}/\mathbb{Z})$  case.
- Conjecturally, there are very few invariant probability measures on  $\mathcal{L}_n$  under  $A_n$  when  $n \geq 3$ .
- One can prove the third assertion under an additional assumption on the measure, positive entropy.

**Lemma 4.2.** *There exist orbit closures  $\overline{A_2 \cdot x}$  of any Hausdorff dimension between 1 and 3.*

Similarly, there exist “very many” probability measures on  $\mathcal{L}_2$  invariant by  $A_2$ .

The following conjectures are stated (in a considerably more general form) in [17].

**Conjecture 4.2** (Margulis). *The orbit closure  $\overline{A_n \cdot x}$  (for  $n \geq 3$  and  $x \in \mathcal{L}_n$ ) is, if compact, a closed  $A_n$ -orbit.<sup>13</sup>*

**Conjecture 4.3** (Margulis). *Suppose  $n \geq 3$  and let  $\mu$  be a probability measure on  $\mathcal{L}_n$  that is invariant under  $A_n$  and ergodic w.r.t.  $A_n$ . Then<sup>14</sup>  $\mu$  is algebraic:  $\mu$  coincides with the  $H'$ -invariant probability measure on a closed orbit  $H'x_0$ , for some closed subgroup  $A_n \leq H' \leq \mathrm{SL}(n, \mathbb{R})$ .*

**Theorem 4.3** (Einsiedler-Katok-Lindenstrauss). *Suppose  $n \geq 3$  and let  $\mu$  be a probability measure on  $\mathcal{L}_n$  that is invariant under  $A_n$  and ergodic w.r.t.  $A_n$ , such that some element of  $A_n$  acts with positive entropy. Then  $\mu$  is algebraic.*

Theorem 4.3 is the main theorem of [5]. The result concerning Littlewood’s conjecture is deduced from it. It should be noted that while Theorem 4.3 is closely analogous to Theorem 4.2, the technique of proof is quite different.

The assumption concerning positive entropy translates, as we shall see later, to the exceptional set in Theorem 1.1; removing this assumption from the theorem would establish the Littlewood conjecture unconditionally. Indeed, as we have already seen in (10), starting from an exception to the Littlewood conjecture, we produce a point in  $\mathcal{L}_3$  with “strange” behavior under  $A_3$ ; and, by the philosophy discussed in §3.3, one can also produce an  $A_3$ -invariant measure on  $\mathcal{L}_3$  which fails to be algebraic. It turns out that, given a *sufficiently thick* set of counterexamples to the Littlewood conjecture, one can produce a “sufficiently thick”  $A_3$ -invariant

<sup>13</sup>This is not quite as good as a complete classification of orbit closures, and, indeed, [17] posits a more precise classification. Conjecture 4.2 is just a simple clean statement that can be extracted from this classification.

<sup>14</sup>i.e. “the measure-theoretic analogue of Theorem 3.1 holds for  $A_n$  acting on  $\mathcal{L}_n$ ”.

measure on  $\mathcal{L}_3$  which fails to be algebraic, and the meaning of “sufficiently thick” amounts precisely to positive entropy. We discuss this in a little more detail at the end of the next (and final) section – see §5.6 and §5.7.

## 5. COORDINATE DILATIONS ACTING ON LATTICES, II: THE PRODUCT LEMMA OF EINSIEDLER-KATOK

The remainder of the paper is impressionistic; it should be regarded simply as a motivation for looking at the original proof!

The main thing which the reader might come away with is the importance and naturality of *conditional measures*.

The study and usage of conditional measures is a formalization of the following natural idea: given an  $A_3$ -invariant measure  $\mu$  on  $\mathcal{L}_3$ , study  $\mu$  along slices transverse to  $A_3$ . Note that the action of  $A_3$  contracts part of these slices and dilates other parts. Also, certain elements  $a \in A_3$  may leave slices neither contracted nor dilated (“partial hyperbolicity”).

**5.1. Some ideas in the general proof.** We are going to focus on the case of  $A_3$  acting on  $\mathcal{L}_3$  and moreover focus on just one of the ideas from the proof of Theorem 4.3: the “product lemma” contained in the paper [4].

The proof of Theorem 4.3 in its entirety draws on many ideas and tools from different areas and the work of several prior authors (see comments after Theorem 1.1). We note, in addition, the usage of the theory of ergodic theoretic entropy; unipotent dynamics on homogeneous spaces, including ideas and results from the work of M. Ratner; and ideas from the theory of hyperbolic and partially hyperbolic actions. In the end, two distinct methods – the high entropy method developed by Einsiedler and Katok [4] and the low entropy method developed by Lindenstrauss [15] – fit together to yield the result. (For a brief discussion of how they fit together, see the discussion between Theorem 5.1 and Theorem 5.2.)

Therefore, it must be emphasized that we are simply focussing on *one ingredient among several*: I have tried to choose an idea that captures some of the general flavour.

**5.2. Closed sets.** Before we embark on describing some of the ideas in [4], we begin by explaining how one might try to approach the analysis of  $A_3$ -invariant closed sets. We then explain – in the spirit of §3.3 – why it might be helpful to switch to measures.

Suppose  $\sigma \subset \mathcal{L}_3$  is an  $A_3$ -invariant closed set.

We wish to study the behavior of  $\sigma$  in directions transverse to  $A_3$ . Let  $e_{ij}$  be the elementary matrix with a 1 in the  $(i, j)$  position and 0s everywhere else; for  $i \neq j$  let  $n_{ij}(x) = \exp(x.e_{ij})$ . Then  $N_{ij} = \{n_{ij}(x) : x \in \mathbb{R}\}$  is a subgroup of  $SL_3(\mathbb{R})$ .

A natural way of studying how  $\sigma$  behaves *transverse to  $A_3$*  is to consider the subsets:

$$\sigma_x^{ij} := \{t \in \mathbb{R} : n_{ij}(t)x \in \sigma\} \subset \mathbb{R}.$$

This set is a closed subset of  $\mathbb{R}$  and is defined for all  $x \in \mathcal{L}_3$ .

Now, we wish to use the fact that a typical element  $a \in A_3$  can contract some of the subgroups  $N_{ij}$  and expand others.

Let us take an explicit example: the matrix  $a = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$ . It centralizes  $N_{12}$ ; that is to say,  $an_{12}(x)a^{-1} = n_{12}(x)$ . On the other hand, it *shrinks*  $N_{23}$ ; that

is to say:

$$a.n_{23}(x).a^{-1} = n_{23}(x/8).$$

This is an example of partial hyperbolicity: an element that contracts in certain transverse directions and leaves other transverse directions neutral.

Now consider two points  $x_1, x_2 \in \sigma$  which lie along the  $N_{23}$  direction from one another, i.e.  $x_2 \in N_{23}x_1$ . Let us compare  $\sigma_{x_1}^{12}$  and  $\sigma_{x_2}^{12}$ . Because our element  $a$  centralizes  $N_{12}$ ,

$$(15) \quad \sigma_{x_1}^{12} = \sigma_{ax_1}^{12} = \sigma_{a^2x_1}^{12} = \dots \text{ and } \sigma_{x_2}^{12} = \sigma_{ax_2}^{12} = \sigma_{a^2x_2}^{12} = \dots$$

But  $a^kx_1$  and  $a^kx_2$  are becoming very close as  $k \rightarrow \infty$ , because  $a$  shrinks the direction  $N_{23}$ . Therefore, if we had some version of the statement

$$(16) \quad \text{Wishful thinking: as } x \text{ approaches } y, \sigma_x^{12} \text{ approaches } \sigma_y^{12},$$

we could deduce from (15) – by considering  $a^kx_1, a^kx_2$  as  $k \rightarrow \infty$  – the following surprising fact:

$$(17) \quad \sigma_{x_1}^{12} = \sigma_{x_2}^{12} \quad (\text{NOT proved, based on wishful thinking!})$$

In other words, were some version of (16) true, we would have a rather weak version of the following statement: the behavior of a closed set  $\sigma$  in the  $N_{12}$ -direction is constant along the  $N_{23}$ -direction. It is not immediate how to *use* this, but nonetheless it is an important structural fact. (See discussion after Lemma 5.1 for an indication of how the measure-theoretic version of this fact is used.) It is quite surprising, because we assumed nothing about the behavior of  $\sigma$  besides  $A_3$ -invariance.

In order to get any mileage, of course, we need to be able to find points  $x_1, x_2$  which differ in the  $N_{23}$  directions, or, equivalently, the sets  $\sigma_x^{23}$  should have more than one point. So in order to have any hope of using this entire setup, we should also have:

$$(18) \quad \text{The sets } \sigma_x^{ij} \text{ should not always be singletons.}$$

Let me emphasize that the above is, indeed, essentially wishful thinking and is based on the rather baselessly optimistic (16). The surprising fact is that, by working with measures, we can salvage a version of (16).

**Example 5.1.** Take a closed subset  $S$  of the square  $[0, 1]^2$ . Let  $\pi : [0, 1]^2 \rightarrow [0, 1]$  be the projection onto the first coordinate. For each  $x \in [0, 1]$  we can consider the set  $S_x = \pi^{-1}(\{x\}) \cap S$ . There is no reason that if  $x, x'$  are close, then  $S_x, S_{x'}$  should be similar; this is the failure of (16).

However, a measure-theoretic version of this *is valid*. If  $\mu$  is a probability measure on  $[0, 1]^2$ , we can disintegrate it along fibers: we can write  $\mu = \int_{x \in [0, 1]} \mu_x d\nu(x)$ , where  $\nu = \pi_*\mu$  is the pushed-down measure on  $[0, 1]$  and  $\mu_x$  is a probability measure supported on the fiber  $\pi^{-1}(\{x\})$ . The measures  $\mu_x$  are the measure-theoretic analogue of  $S_x$ , and:

$$(19) \quad \text{On a set of measure } 0.999999 \text{ the function } x \mapsto \mu_x \text{ is continuous.}$$

In other words, throwing away a set of small measure, we can think of the measures  $\mu_x$  as satisfying a version of (16).

**5.3. What comes next.** Einsiedler and Katok implement the strategy discussed in §5.2, but in the world of measures, not sets.

- Rather than an  $A_3$ -invariant *closed set*  $\sigma$ , we start with an  $A_3$ -invariant probability measure  $\mu$ .
- The analogue of  $\sigma_x^{N_{ij}} \subset \mathbb{R}$  is played by *conditional measures*  $\mu_x^{ij} \in \text{Measures}(\mathbb{R})$  discussed in §5.4. (Note that these are *not* probability measures in general and may have infinite mass.)
- The assumption (18) that  $\sigma_x^{ij}$  not be singletons is replaced by the assumption that  $\mu_x^{ij}$  not be *atomic* (a multiple of a point mass), which will be needed in both Theorem 5.1 and Theorem 5.2.
- One can prove the analogue of (17): it is the *product-lemma*, Lemma 5.1.

**5.4. Conditional measures: the analogue of the  $\sigma_x^{ij}$  for measures.** Let a nice group  $G$  (e.g.  $G = N_{ij}$ ) act on a nice space  $X$  (e.g.  $X = \mathcal{L}_3$ ).

Given a closed subset  $S \subset X$ , we can define the sets  $\sigma_x^G = \{g \in G : gx \in S\}$ , which isolates behavior of  $S$  along the  $G$ -direction. Now we want to define a similar concept, but with the set  $S$  replaced by a probability measure  $\mu$ , and replace the closed subset  $\sigma_x^G \subset G$  by a measure  $\mu_x^G$  (or just  $\mu_x$ ) on  $G$ .

This can indeed be done in a canonical way, except that the measures  $\mu_x$  are defined only *up to scaling by a positive number*. In other words, there exists an association  $x \mapsto \mu_x$  from points of  $X$  to measures on  $G$ , referred to as *conditional measures* along  $G$ , with the following properties (see [5, Section 2]):

- (1) The map  $x \mapsto \mu_x$  (thought of as a map from  $X$  to measures on  $G$ ) is itself measurable.
- (2) For  $g \in G$  and  $x \in X$  such that both  $\mu_{gx}$  and  $\mu_x$  are defined, the measures  $\mu_{g \cdot x}$  and  $g \cdot \mu_x$  are proportional, written  $\mu_{g \cdot x} \propto g \cdot \mu_x$ <sup>15</sup> (one would like to say “equal”, but everything is defined only up to a positive scalar).
- (3) Let  $B$  be any open ball containing the identity in  $G$ . Then  $\mu_x(B) > 0$  for almost all  $x \in X$ .
- (4)  $\mu$  is invariant under the  $G$ -action if and only if  $\mu_x$  is a Haar measure on  $G$  for almost all  $x \in X$ .

Let’s briefly describe how to do this when  $X$  is general but  $G$  is finite. In that case, one can normalize the  $\mu_x$  canonically by requiring them to be probability measures on the finite set  $G$ . We will just describe the function  $x \mapsto \mu_x(\{1\})$ ; then (2) determines  $\mu_x$  totally (in this case, after normalizing the  $\mu_x$ , the  $\propto$  of (2) becomes equality).

Average  $\mu$  under  $G$  to get a measure  $\nu$ , with respect to which  $\mu$  is absolutely continuous. Therefore, by the theorem of Radon and Nikodym, there exists a function  $f \in L^1(\nu)$  such that  $\mu = f \cdot \nu$ ; i.e.  $\mu(S) = \int_S f d\nu$ . Then  $f(x) = \mu_x(\{1\})$  almost everywhere when matters are normalized such that  $\mu_x$  is a probability measure.

Returning to the context of an  $A_3$ -invariant measure  $\mu$  on  $\mathcal{L}_3$ , we denote by  $\mu_x^{ij}$  the measure on  $N_{ij} \cong \mathbb{R}$  defined by the process described above, applied to the action of  $N_{ij}$  on  $\mathcal{L}_3$ .

**5.5. From product lemma to unipotent invariance.** Let  $\mu$  be an  $A_3$ -invariant measure on  $\mathcal{L}_3$ . The following is established in [4], corollary to Proposition 5.1.

<sup>15</sup>Here  $g \cdot \mu_x$  is the measure defined as  $g \cdot \mu_x(S) = \mu_x(Sg)$  for a subset  $S \subset G$ .

**Lemma 5.1** (Product lemma). *Let  $\mu$  be an  $A_3$ -invariant measure on  $\mathcal{L}_3$ . Then, for  $(k, \ell) \neq (i, j), (j, i)$  we have  $\mu_{n_{k\ell}(t)x}^{ij} \propto \mu_x^{ij}$ , for  $\mu_x^{k\ell}$ -almost all  $t \in \mathbb{R}$  and for  $\mu$ -almost every  $x \in \mathcal{L}_3$ .*

Recall that  $n_{kl}$  was defined at the start of §5.2. The reasoning is a measure-theoretic version of that already discussed in §5.2. Thus Lemma 5.1 is “just” a consequence of the fact that it is possible to “shrink” the  $N_{k\ell}$  while leaving  $N_{ij}$  unchanged.

We say that  $\mu_x^{ij}$  is *trivial* if it is proportional to the Dirac measure supported at 0, i.e. if  $\mu_x^{ij}(f) \propto f(0)$  for every continuous function  $f$  on the real line. To make use of the  $\mu_x^{ij}$ s, one really needs them to be *non-trivial* for almost all  $x$ . This is the analogue of (18).

Now let us briefly – and very heuristically – indicate how one might use Lemma 5.1. The assertion 5.1 says, in particular, that the value of  $x \mapsto \mu_x^{13}$  is “the same” (at least, proportional) at  $x$  and at  $n_{12}(t)x$ , except for a set of  $t$  of  $\mu_x^{12}$ -measure 0. If  $\mu_x^{12}$  is far from being atomic, we can find plenty of  $t \neq 0$  for which this will be true. Similarly, if  $\mu_x^{23}$  is far from being atomic, we can find plenty of  $s$  for which the value of  $x \mapsto \mu_x^{13}$  is the same at  $x$  and at  $n_{23}(s)x$ .

Applying this argument repeatedly, we may hope to find  $t, s$  with the property that  $\mu^{13}$  takes proportional values at  $x$  and  $n_{12}(t)n_{23}(s)n_{12}(-t)n_{23}(-s)x$ . But the groups  $N_{12}$  and  $N_{23}$  do not commute: indeed  $n_{12}(t)n_{23}(s)n_{12}(-t)n_{23}(-s) = n_{13}(ts)$ . This shows that  $\mu_x^{13}$  is proportional at  $x$  and at  $n_{13}(ts)x$ .

This says something quite strong: the measure  $\mu_x^{13}$  on the real line is proportional to its translate under  $ts$ ! An auxiliary argument shows that we can find enough  $(t, s)$  to force  $\mu_x^{13}$  to be Lebesgue measure on  $\mathbb{R}$ , so (by property (4) of conditional measures)  $\mu$  is *invariant by  $N_{13}$* . At this point we have invariance in a *unipotent* direction, and one may apply the measure-theoretic version of Theorem 3.1 (see also discussion of §3.3) to classify possibilities for  $\mu$ .<sup>16</sup>

In words, Lemma 5.1 combines with the non-commutativity of the subgroups  $N_{ij}$  to show that  $\mu$  is invariant in a unipotent direction.

The conclusion of this line of reasoning is the following, part of [4, Theorem 4.2]:

**Theorem 5.1.** *Suppose  $\mu$  is an  $A_3$ -ergodic measure on  $\mathcal{L}_3$  such that, for every  $i \neq j$  and for a positive measure set of  $x \in \mathcal{L}_3$ , the measure  $\mu_x^{ij}$  is non-trivial. Then  $\mu$  is Haar measure.*

Here *Haar measure* refers to the unique  $\mathrm{SL}_3(\mathbb{R})$ -invariant probability measure on  $\mathcal{L}_3$ .

In his work on the quantum unique ergodicity problem [15], Lindenstrauss introduced a different way of analyzing this type of situation, termed the “low entropy” method. It turns out that this complements the methods in the proof of Theorem 5.1 and – in the context of the present paper – allows the analysis of the case (loosely speaking) when *some* but not all  $\mu_x^{ij}$  are non-trivial. The strategy of the proof in this case is, also, to find some directions  $N_{ij}$  in which  $\mu$  is invariant; one may then apply the theorem of Ratner classifying measures invariant by a unipotent subgroup. However, the proof of unipotent invariance is established by a strategy that is very different to the non-commutativity idea above; it uses, among other

<sup>16</sup>In fact, in [4], the use of Ratner’s theorem was avoided by applying this argument repeatedly, with 13 replaced by various  $ij$ .

things, certain ideas from work of Ratner, e.g. [20]. We will not attempt to describe this strategy at all here.

Combining ideas from [4] and [15] led eventually to the following theorem, which is equivalent up to rephrasing to Theorem 4.3. (We discuss this equivalence in §5.7; it relies on an adaptation [18] of a special case of the Ledrappier-Young entropy formula.)

**Theorem 5.2.** *Suppose  $\mu$  is an  $A_3$ -ergodic measure on  $\mathcal{L}_3$  such that, for at least one pair  $i \neq j$  and for a positive measure set of  $x \in \mathcal{L}_3$ , the measure  $\mu_x^{ij}$  is non-trivial. Then  $\mu$  is Haar measure.*

Suitable analogues of these theorems are true replacing  $(A_3, \mathcal{L}_3)$  by  $(A_n, \mathcal{L}_n)$ . In that case there are, in general, more possibilities for  $\mu$  besides Haar measure, as in the statement of Theorem 4.3.

The question of removing the assumption in Theorem 5.2 seems to be a very difficult and fundamental one. If one could do so, the Littlewood conjecture (without any set of exceptions) would follow.

**5.6. Back to Theorem 1.1.** Now let's return to Theorem 1.1, which can be attacked using Theorem 5.2 and the relation between sets and measures.

We claim that for any fixed positive  $\delta$ ,

$$(20) \quad \text{BoxDimension} \{(\alpha, \beta) : \inf_{n \geq 1} n \cdot \|n\alpha\| \cdot \|n\beta\| \geq \delta\} = 0.$$

From this it is easy to deduce Theorem 1.1.

We saw that in the discussion preceding (10) that the failure of the Littlewood conjecture for a fixed pair  $(\alpha, \beta)$  would correspond to the  $A_3^+$ -orbit of a certain  $L_{\alpha, \beta} \in \mathcal{L}_3$  being bounded. If (20) fails, indeed, there exists a set of lattices  $L_{\alpha, \beta}$  of box dimension  $\geq 0.01$  (say) whose  $A_3^+$ -orbits all remain within a fixed bounded set inside  $\mathcal{L}_3$ .

So the closure  $Y$  of  $A_3^+ \cdot \{L_{\alpha, \beta}\}$  is a bounded,  $A_3^+$ -invariant closed set on  $\mathcal{L}_3$  with box dimension  $\geq 2.01$  (the extra 2 comes from taking the  $A_3$ -orbit; in words, it means that  $Y$  has thickness transverse to the  $A_3$ -direction).

In what follows, let us ignore the distinction between  $A_3^+$  and  $A_3$  for simplicity. The necessity of dealing with  $A_3^+$  complicates the argument slightly. So, let us assume that  $Y$  was actually  $A_3$ -invariant.

We construct an  $A_3$ -invariant measure  $\mu$  supported on  $Y$ . It turns out that the fact that  $Y$  has thickness transverse to the  $A_3$ -direction translates into the fact that it is possible to choose  $\mu$  with at least one of the conditional measures  $\mu_x^{ij}$  non-trivial (for almost all  $x$ ). But then Theorem 5.2 shows that  $\mu$  has to be Haar measure. So the support of  $\mu$  is all of  $\mathcal{L}_3$ , and  $\mu$  cannot be supported on the bounded set  $Y$  – a contradiction.

We observe that the need to allow a set of exceptions in Theorem 1.1 arises from the assumption in Theorem 5.2 concerning conditional measures (equivalently, the positive entropy condition). Removing that condition would settle the Littlewood conjecture in whole.

**5.7. Conditional measures and entropy.** Finally, let us observe that Theorem 4.3 and Theorem 5.2 are truly the same:

**Theorem 5.3.** *Let  $\mu$  be an  $A_3$ -invariant probability measure on  $\mathcal{L}_3$ . Then  $h_\mu(a) = 0$  for all  $a \in A_3$  if and only if, for almost all  $x \in \mathcal{L}_3$  and all  $(i, j)$ , the conditional measures  $\mu_x^{ij}$  are trivial.*

This is a (slight adaptation of a) special case of the “Ledrappier-Young entropy formula” [12, 13] and is of great importance, for the Theorems 5.1 and 5.2 are not useful without a reasonable way to verify the conditions on  $\mu_x^{ij}$ . The above result provides this, and, indeed, in many applications it is Theorem 4.3 rather than Theorem 5.2 which is directly applicable. Indeed, even the discussion in §5.6 is made rigorous using entropy.

We shall simply motivate the idea behind this result. Recall that we remarked (end of §4.3) that positive entropy arises from the possibility of points having “similar” forward trajectories. In the context of  $(A_n, \mathcal{L}_n)$  there is a simple reason this could happen: if  $x = n_{ij}x'$  and  $a \in A_n$  contracts  $n_{ij}$  (cf. discussion near (15)), then the points  $a^kx, a^kx'$  become very close as  $k \rightarrow \infty$ . This leads to the theorem above.

#### ACKNOWLEDGEMENTS

I would like to thank Einsiedler, Lindenstrauss and Gregory Margulis for very many fruitful discussions and explanations relating to their work on this topic. I would also like to thank Sinan Güntürk for his comments on this paper and the referee for very helpful comments.

#### ABOUT THE AUTHOR

Akshay Venkatesh is an associate professor at the Courant Institute in New York. His research interests are in number theory and related topics. Most recently, he has been studying connections between ergodic theory on homogeneous spaces and analytic number theory.

#### REFERENCES

- [1] S. G. Dani and G. A. Margulis. Limit distributions of orbits of unipotent flows and values of quadratic forms. In *I. M. Gelfand Seminar*, volume 16 of *Adv. Soviet Math.*, pages 91–137. Amer. Math. Soc., Providence, RI, 1993. MR1237827 (95b:22024)
- [2] J. Ellenberg and A. Venkatesh. Local-global principles for representations of quadratic forms. [arxiv: math.NT/0604232](https://arxiv.org/abs/math/0604232).
- [3] M. Einsiedler and A. Katok. Rigidity of measures – the high entropy case, and non-commuting foliations. *Israel J. Math.*, 148 (2005), 169–238. MR2191228 (2007d:37034)
- [4] M. Einsiedler and A. Katok. Invariant measures on  $G/\Gamma$  for split simple Lie-groups  $G$ . *Comm. Pure Appl. Math.*, 56 (8) (2003), 1184–1221. MR1989231 (2004e:37042)
- [5] M. Einsiedler, A. Katok, and E. Lindenstrauss. Invariant measures and the set of exceptions to Littlewood’s conjecture. *Ann. of Math. (2)*, 164 (2006), no. 2, 513–560. MR2247967
- [6] Manfred Einsiedler and Elon Lindenstrauss. Diagonalizable flows on locally homogeneous spaces and number theory. *Proceedings of the International Congress of Mathematicians*. International Congress of Mathematicians. Vol. II, 1731–1759, Eur. Math. Soc., Zürich, 2006. MR2275667
- [7] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel and Akshay Venkatesh. The distribution of periodic torus orbits on homogeneous spaces. [arxiv: math.DS/0607815](https://arxiv.org/abs/math/0607815).
- [8] Boris Kalinin and Ralf Spatzier. Rigidity of the measurable structure for algebraic actions of higher-rank Abelian groups. *Ergodic Theory Dynam. Systems*, 25 (2005). MR2122918 (2005k:37008)
- [9] Anatole Katok and Ralf Spatzier. Invariant measures for higher-rank hyperbolic abelian actions. *Ergodic Theory Dynam. Systems*, 16 (1996), no. 4, 751–778. MR1406432 (97d:58116)

- [10] Corrections to: “Invariant measures for higher-rank hyperbolic abelian actions”. *Ergodic Theory Dynam. Systems*, 18 (1998), no. 2, 503–507. MR1619571 (99c:58093)
- [11] Y. Katznelson. Chromatic numbers of Cayley graphs on  $\mathbb{Z}$  and recurrence. *Combinatorica*, 21 (2001). MR1832446 (2002h:05065)
- [12] F. Ledrappier and L.-S. Young. The metric entropy of diffeomorphisms. I. Characterization of measures satisfying Pesin’s entropy formula. *Ann. of Math. (2)*, 122 (1985), no. 3, 509–539. MR819556 (87i:58101a)
- [13] F. Ledrappier and L.-S. Young. The metric entropy of diffeomorphisms. II. Relations between entropy, exponents and dimension. *Ann. of Math. (2)*, 122 (1985), no. 3, 540–574. MR819557 (87i:58101b)
- [14] Elon Lindenstrauss. Arithmetic quantum unique ergodicity and adelic dynamics. Proceedings of Current Developments in Mathematics conference (2004), to appear.
- [15] Elon Lindenstrauss. Invariant measures and arithmetic quantum unique ergodicity. *Annals of Math. (2)*, 163 (2006). MR2195133 (2007b:11072)
- [16] Elon Lindenstrauss. Rigidity of multiparameter actions. *Israel J. of Math.*, 149 (2005). MR2191215 (2006j:37007)
- [17] Gregory Margulis. Problems and conjectures in rigidity theory. In *Mathematics: Frontiers and perspectives*, pages 161–174. Amer. Math. Soc., Providence, RI, 2000. MR1754775 (2001d:22008)
- [18] G. A. Margulis and G. Tomanov. Invariant measures for actions of unipotent groups over local fields on homogeneous spaces. *Invent. Math.*, 116 (1994), nos. 1-3, 347–392. MR1253197 (95k:22013)
- [19] Andrew Pollington and Sanju Velani. On a problem in simultaneous Diophantine approximation: Littlewood’s conjecture. *Acta. Math.*, 185 (2000). MR1819996 (2002a:11076)
- [20] M. Ratner. Horocycle flows, joinings and rigidity of products. *Ann. of Math. (2)*, 118 (2) (1983), 277–313. MR717825 (85k:58063)
- [21] Marina Ratner. On Raghunathan’s measure conjecture. *Ann. of Math. (2)*, 134 (3) (1991), 545–607. MR1135878 (93a:22009)
- [22] Marina Ratner. Raghunathan’s topological conjecture and distributions of unipotent flows. *Duke Math. J.*, 63 (1) (1991), 235–280. MR1106945 (93f:22012)
- [23] Carl Siegel. Lectures on the geometry of numbers. Springer-Verlag, Berlin, 1989. MR1020761 (91d:11070)
- [24] Lior Silberman and Akshay Venkatesh. On quantum unique ergodicity for locally symmetric spaces. [math.RT/0407413](#), to appear, *GAF*, 17 (3) (2007), 960–998.
- [25] P. Walters. An introduction to ergodic theory. Graduate Texts in Mathematics, 79. Springer-Verlag, 1982. MR648108 (84e:28017)
- [26] David Witte. Ratner’s theorems on unipotent flows. Chicago Lectures in Mathematics Series, University of Chicago Press, Chicago, IL, 2005.

DEPARTMENT OF MATHEMATICS, COURANT INSTITUTE, NEW YORK UNIVERSITY, NEW YORK, NEW YORK 10012