# Ergodic Theory and Number Theory

## The work of Elon Lindenstrauss

Klaus Schmidt

Elon Lindenstrauss was awarded the 2010 Fields Medal for his results on measure rigidity in ergodic theory, and their applications to number theory.

The web page of the ICM 2010[1] contains the following brief description of Elon Lindenstrauss' achievements: *Lindenstrauss has made far-reaching advances in ergodic theory, the study of measure preserving transformations. His work on a conjecture of Furstenberg and Margulis concerning the measure rigidity of higher rank diagonal actions in homogeneous spaces has led to striking applications. Specifically, jointly with Einsiedler and Katok, he established the conjecture under a further hypothesis of positive entropy. It has impressive applications to the classical Littlewood Conjecture in the theory of diophantine approximation. Developing these as well other powerful ergodic theoretic and arithmetical ideas, Lindenstrauss resolved the arithmetic quantum unique ergodicity conjecture of Rudnick and Sarnak in the theory of modular forms. He and his collaborators have found many other unexpected applications of these ergodic theoretic techniques in problems in classical number theory. His work is exceptionally deep and its impact goes far beyond ergodic theory.*

In this note I will concentrate on the work by Lindenstrauss and his collaborators on measure rigidity and the partial settlement of Littlewood's conjecture. Although the method of Lindenstrauss proof of arithmetic quantum unique ergodicity also uses ideas from measure rigidity, the concepts involved in explaining the latter problem and its solution would seriously overburden this exposition. I refer the interested reader to the original paper [19] for details. The paper [11] by Einsiedler and Lindenstrauss gives an excellent overview of the range of ideas spanning measure rigidity and quantum unique ergodicity.[2] A reasonably elementary proof of the arithmetical quantum unique ergodicity theorem for $\mathrm{SL}(2,\mathbb{Z})$ can be found in [12].

The connection between ergodic theory and number theory alluded to in the above desription of Lindenstrauss' achievements has a long history, with early landmarks like Hermann Weyl's work on uniform distribution [34] or Khinchine's study of continued fractions [18]. In recent decades the interplay between dynamics and arithmetical problems has stimulated a very interesting development in ergodic theory: the study of multiparametric (or *higher rank*) actions, i.e., of actions of $\mathbb{Z}^d$ or $\mathbb{R}^d$ with $d > 1$. Let me illustrate this transition from classical to multiparameter dynamics with a simple example, that of normal numbers.

**Normal numbers.** If $p > 1$ is a rational integer, then a real number $x \in I = [0, 1)$ is *normal in base* $p$ (or $p$-*normal*) if every possible block $b_1 \cdots b_L$ of digits $b_i \in \{0, \dots, p-1\}$ occurs with frequency $p^{-L}$ in the expansion of $x$ in base $p$. An elementary argument shows that $x$ is $p$-normal if and only if the sequence $\bigl(p^n x \pmod 1\bigr)_{n\ge1}$ is uniformly distributed in the unit interval $I = [0, 1)$.[3]

We identify the interval $I$ with $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ and write $T_m$ for multiplication by an integer $m$ on $\mathbb{T}$, corresponding to the map $x \mapsto mx \pmod 1$ on $I$. As remarked above, an element $x \in \mathbb{T}$ is $p$-normal if and only if $\lim_{N\to\infty} \frac{1}{N}\sum_{k=0}^{N-1} f(T_p^k x) = \int f\,d\lambda$ for every continuous function $f\colon \mathbb{T} \longrightarrow \mathbb{R}$, where $\lambda$ is the Lebesgue measure on $\mathbb{T}$. The individual ergodic theorem implies that $\lambda$-*a.e.* $x \in \mathbb{T}$ is $p$-normal, and by varying $p$ we see that $\lambda$-*a.e.* $x \in \mathbb{T}$ is $p$-normal for every integer $p > 1$.[4]

[1] http://www.icm2010.org.in/prize-winners-2010/fields-medal-elon-lindenstrauss
[2] See also http://www.ma.huji.ac.il/∼elon/Publications/TopErgThySp07.pdf
[3] The notion of normality was introduced in 1909 by É. Borel [3] and studied further by Sierpiński [32] and many others.
[4] The explicit construction of such an $x \in \mathbb{T}$ is nontrivial — cf., e.g., [32], [7].

Cassels and Wolfgang Schmidt asked whether one can find numbers $x \in \mathbb{T}$ which behave differently in different bases (cf. [5] and [31]).

**Theorem 1** ([31, Theorem 1])**.** *Let $p, q > 1$ be integers.*

*(1) If $p, q$ are multiplicatively dependent (i.e., if there exist integers $a, b$, not both equal to zero, such that $p^a = q^b$), then every $p$-normal number $x \in \mathbb{T}$ is also $q$-normal.*

*(2) If $p, q$ are multiplicatively independent, then there are uncountably many $x \in \mathbb{T}$ which are $p$-normal, but not $q$-normal.*

In order to discuss this result further we have to go a little deeper into ergodic theory. Recall that a set $B \subset \mathbb{T}$ is $T_p$*-invariant* if $B \subset T_p^{-1}B$. A probability measure $\mu$ on $\mathbb{T}$ is $T_p$*-invariant* if $\mu(T_p^{-1}B) = \mu(B)$ for every Borel set $B \subset \mathbb{T}$. A $T_p$-invariant probability measure $\mu$ on $\mathbb{T}$ is *ergodic* if $\mu(B) \in \{0, 1\}$ for every $T_p$-invariant Borel set $B \subset \mathbb{T}$.

Clearly, $T_p$ is not invertible on $\mathbb{T}$. However, if $\mu$ is a $T_p$-invariant probability measure on $\mathbb{T}$ it may happen that there exists a Borel set $A \subset \mathbb{T}$ with $\mu(A) = 1$ such that $A$ contains, for every $x \in A$, a *unique* element $y$ with $T_p y = x$. If this is the case we say that $\mu$ has *zero entropy.* In other words, $\mu$ has zero entropy if $T_p$ is invertible when restricted to a suitable Borel set $A \subset \mathbb{T}$ of full $\mu$-measure. If $\mu$ does not have zero entropy we say that it has *positive entropy* under $T_p$, denoted by $h_\mu(T_p) > 0$.[5]

It is not difficult to show that there exist $T_p$-invariant and ergodic probability measures $\mu \neq \lambda$ on $\mathbb{T}$ with positive entropy.[6]

**Theorem 2** ([14, Théorème 1])**.** *Let $p, q > 1$ be two relatively prime integers, and let $\mu \neq \lambda$ be a nonatomic probability measure on $\mathbb{T}$ which is invariant and ergodic under $T_p$. If $h_\mu(T_p) > 0$ then $\mu$-a.e. $x \in \mathbb{T}$ is $q$-normal, but not $p$-normal.*

Theorem 2 is closely related to (and, in fact, implies) a celebrated result by Rudolph about probability measures $\mu$ on $\mathbb{T}$ which are invariant and ergodic under the joint action of $T_p$ and $T_q$ with $(p, q) = 1$.[7]

**Theorem 3** ([29, Theorem 4.9])**.** *Let $p, q > 1$ be two relatively prime integers, and let $\mu$ be a nonatomic probability measure on $\mathbb{T}$ which is invariant and ergodic under the joint action of $T_p$ and $T_q$. If $h_\mu(T_p) > 0$ then $\mu = \lambda$.*

Leaving subtleties aside concerning the difference between the ergodicity assumptions in the Theorems 2 and 3 (which can be dealt with by using appropriate ergodic decompositions), Theorem 2 implies that $\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \mu \circ T_q^{-k} = \lambda$. If $\mu \neq \lambda$ then $\mu$ cannot be $T_q$-invariant.

What about $T_p$-invariant and ergodic probability measures with zero entropy in Theorem 2, or about zero entropy $(T_p, T_q)$-invariant measures in Theorem 3? This problem originates from a paper by Furstenberg [13] in which he proves that every infinite closed subset $C \subset \mathbb{T}$ which is invariant under both $T_p$ and $T_q$ must coincide with $\mathbb{T}$. An equivalent formulation is that the orbit $\{T_p^k T_q^l x : k, l \geq 0\}$ of every irrational $x \in \mathbb{T}$ is dense in $\mathbb{T}$ (if $x$ is rational, this orbit is obviously finite).[8] If closed jointly invariant subsets of $\mathbb{T}$ are scarce, what can one say about jointly invariant probability measures on $\mathbb{T}$? Is $\lambda$ the only nonatomic measure of this kind? This question, often referred to as *Furstenberg's* $\times 2$, $\times 3$ *conjecture*, has been open since 1967, and has been seminal for the development of 'algebraic' multiparameter ergodic theory for the past decades.

[5]For much of this note it will not be necessary to know the precise meaning of the number $h_\mu(T_p)$. Readers interested in the actual definition of measure-theoretic (or, as it is often called, *metric*) entropy of a finite measure preserving transformation $T$ should consult one of the standard text books on ergodic theory, such as [26] or [33]. The notion of entropy for finite measure preserving actions of more general groups is explained in [24] or [25], for example.

[6]Consider the one-sided shift space $\Sigma_p^+ = \{0, \dots, p-1\}^{\mathbb{N}}$ with the shift $\sigma$ given by $(\sigma x)_n = x_{n+1}$, $x = (x_n) \in \Sigma_p^+$. The map $\phi \colon \Sigma_p^+ \longrightarrow \mathbb{T}$ defined by $\phi(x) = \sum_{n\geq 1} x_n p^{-n} \pmod 1$ is almost one-to-one and sends any shift-invariant probability measure $\mu$ on $\Sigma_p^+$ to a $T_p$-invariant probability measure $\phi_*\mu$ on $\mathbb{T}$ such that $h_\mu(\sigma) = h_{\phi_*\mu}(T_p)$. By letting $\mu$ vary over the set of Markov measures on $\Sigma_p^+$, for example, one obtains uncountably many different ergodic $T_p$-invariant probability measures on $\mathbb{T}$ of any entropy between 0 and $\log p$.

[7]'Joint' ergodicity of $\mu$ means that $\mu(B) \in \{0, 1\}$ for every Borel set $B$ which is invariant under both $T_p$ and $T_q$.

[8]In contrast, there are many nontrivial infinite closed subsets $C \subset \mathbb{T}$ which are invariant under *one* of the maps $T_p, T_q$, and there are uncountably many irrationals whose orbits under one of these maps are not dense.

Results like Furstenberg's theorem in [13] or Rudolph's Theorem 3 above are referred to as *rigidity theorems.* Speaking loosely, 'rigidity' is the appearance of an algebraic structure *where one does not expect it.* Consider our present setting: $T_p$ and $T_q$ each have a wide variety of infinite closed invariant sets and nonatomic invariant probability measures. However, if we ask for *simultaneous* invariance of these objects under $T_p$ and $T_q$, they have to be (or are at least conjectured to be) invariant under translation by *every* element of $\mathbb{T}$, an a priori totally unexpected algebraic invariance property.

Although the theorems by Furstenberg and Rudolph are similar in spirit, their classical proofs have nothing in common. In the recent paper [4], Bourgain, Lindenstrauss, Michel and Venkatesh correct this situation by giving an 'effective' proof of Rudolph's theorem (or, more precisely, of a generalization of Rudolph's theorem due to Aimee Johnson in [15] in which $p$ and $q$ are not required to be relatively prime, but only multiplicatively independent), which they then use to prove an effective version of Furstenberg's result.

The various proofs of Rudolph's theorem and its generalizations all depend crucially — but sometimes subtly — on the hypothesis of positive entropy under at least one (and hence both) of the maps $T_p$ or $T_q$. In the absence of positive entropy the rigidity problem for nonatomic $(T_p, T_q)$-invariant probability measures on $\mathbb{T}$ remains as mysterious as ever.

**Commuting automorphisms of tori and solenoids.** For $p, q \geq 2$, the maps $T_p, T_q$ on $\mathbb{T}$ generate an abelian semigroup of surjective homomorphisms of $\mathbb{T}$. By using a standard construction one can find a compact abelian group $X$ and a continuous surjective homomorphism $\phi\colon X \longrightarrow \mathbb{T}$ such that $\phi\circ\bar{T}_p = T_p\circ\phi$ and $\bar{T}_q \circ \phi = \phi \circ T_q$, where $\bar{T}_p$ and $\bar{T}_q$ denote multiplication by $p$ and $q$ on $X$ (the group $X$ is, in fact, a $pq$-adic solenoid). Questions about invariant sets and measures of $T_p, T_q$ and of $\bar{T}_p, \bar{T}_q$ are essentially equivalent. This suggests a broader setting for the problems discussed so far: if $X$ is a compact abelian group and $\alpha\colon \mathbf{n} \mapsto \alpha^{\mathbf{n}}$ and action of $\mathbb{Z}^d$, $d > 1$, by continuous automorphisms of $X$, what are the dynamical properties of $\alpha$, and what, if any, rigidity properties may one expect such an action to have? This is the general setting developed and studied in the monograph [30]. It turns out that such *algebraic $\mathbb{Z}^d$-actions* exhibit a wide range of dynamical properties which can be studied quite effectively by combining tools from commutative algebra, arithmetic and dynamics. The connections between dynamics, arithmetical problems and rigidity phenomena central to Elon Lindenstrauss' work manifest themselves most clearly in the special case where $X$ is a finite-dimensional torus or solenoid, and where the action $\alpha$ is not *virtually cyclic* (which means that $\{\alpha^{\mathbf{n}} : \mathbf{n} \in \mathbb{Z}^d\}$ is not contained in the set of powers of a *single* automorphism $\beta$ of $X$).

The study of measure rigidity of higher rank algebraic $\mathbb{Z}^d$-actions by commuting toral automorphisms was initiated by Anatole Katok and Ralph Spatzier in [17] and brought into a definitive form by Manfred Einsiedler and Elon Lindenstrauss in the research announcement [10]. In order to keep statements simple I'll restrict myself to the totally irreducible case,[9] where the result is completely analogous to Theorem 3.

**Theorem 4** ([10, Theorem 1.1])**.** *Let $\alpha$ be a totally irreducible, not virtually cyclic action of $\mathbb{Z}^d$ by automorphisms of a (finite dimensional) solenoid $X$. Then every $\alpha$-invariant probability measure $\mu$ on $X$ is either equal to the normalized Haar measure $\lambda_X$ of $X$, or it has zero entropy under $\alpha^{\mathbf{n}}$ for every $\mathbf{n} \in \mathbb{Z}^d$.*

As was pointed out in [16, Theorem 5.2], the measure rigidity exhibited in Theorem 4 implies another remarkable rigidity property: the rigidity of isomorphisms and factor maps. I restrict myself to a particularly simple, but still instructive, special case of [10, Theorem 1.4] (cf. also [16, Theorem 5.2]).

**Theorem 5.** *Let $d \geq 2$, and let $\alpha$ and $\beta$ be irreducible and mixing actions of $\mathbb{Z}^d$ by automorphisms of solenoids $X$ and $Y$, respectively. We write $\lambda_X$ and $\lambda_Y$ for the normalized Haar measures on these groups. If $\phi\colon X \longrightarrow Y$ is a measurable map satisfying $\lambda_X\phi^{-1} = \lambda_Y$ and $\beta^{\mathbf{n}} \circ \phi = \phi \circ \alpha^{\mathbf{n}}$ $\lambda_X$-a.e., for every $\mathbf{n} \in \mathbb{Z}^d$, then $\phi$ coincides $\lambda_X$-a.e. with an affine map $A\colon X \longrightarrow Y$.*

[9]The $\mathbb{Z}^d$-action $\alpha$ is *totally irreducible* if there exists no finite index subgroup $\Lambda \subset \mathbb{Z}^d$ and no infinite closed subgroup $Y \subset X$ which is invariant under the automorphisms $\alpha^{\mathbf{n}}$, $\mathbf{n} \in \Lambda$.

One should compare Theorem 5 with the case of a single hyperbolic automorphism $A \in \mathrm{GL}(3, \mathbb{Z})$ of $\mathbb{T}^3$ with eigenvalues $\gamma_1, \gamma_2, \gamma_3$, say. Since $A$ preserves the Lebesgue measure (i.e., volume) $\lambda_{\mathbb{T}^3}$ on $\mathbb{T}^3$, $\det(A) = \gamma_1\gamma_2\gamma_3 = 1$, but $|\gamma_i| \neq 1$ for $i = 1, 2, 3$, by hyperbolicity. Hence either one or two of the eigenvalues of $A$ will have absolute value $> 1$, which is easily seen to imply that $A$ and $A^{-1}$ cannot be conjugate in $\mathrm{GL}(3, \mathbb{Q})$. General results about ergodic toral automorphisms imply, however, that $A$ and $A^{-1}$ are *measurably conjugate*, i.e., that there exists a measurable bijection $\phi\colon \mathbb{T}^3 \longrightarrow \mathbb{T}^3$ which preserves $\lambda_{\mathbb{T}^3}$ and satisfies that $A^{-1} \circ \phi = \phi \circ A$ $\lambda_{\mathbb{T}^3}$-*a.e.* The following example exhibits a subtle consequence of Theorem 5.

**Example 6** ([16, Example 2a])**.** Consider the commuting matrices

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 6 & -3 \end{pmatrix}, \qquad B = \begin{pmatrix} 2 & -4 & -1 \\ 1 & -4 & -1 \\ 1 & -5 & -1 \end{pmatrix}.$$

in $\mathrm{GL}(3, \mathbb{Z})$. The $\mathbb{Z}^2$-action $\alpha\colon \mathbf{n} = (n_1, n_2) \mapsto \alpha^{\mathbf{n}} = A^{n_1}B^{n_2}, \mathbf{n} = (n_1, n_2) \in \mathbb{Z}^2$ on $\mathbb{T}^3$ preserves Lebesgue measure and is ergodic.

If $V = \begin{pmatrix} 2 & -2 & -1 \\ 0 & -3 & 0 \\ 1 & -4 & -2 \end{pmatrix}$, then the matrices

$$A' = VAV^{-1} = \begin{pmatrix} 1 & 2 & -1 \\ -1 & -2 & 2 \\ 2 & 5 & -2 \end{pmatrix}, \qquad B' = VBV^{-1} = \begin{pmatrix} 1 & -1 & -1 \\ -1 & -2 & -1 \\ -1 & -4 & -2 \end{pmatrix},$$

generate a $\mathbb{Z}^2$-action $\beta\colon \mathbf{n} = (n_1, n_2) \mapsto \beta^{\mathbf{n}} = A'^{n_1}B'^{n_2}$ on $\mathbb{T}^3$. This action has the property that $\beta^{\mathbf{n}}$ is measurably conjugate to $\alpha^{\mathbf{n}}$ for every $\mathbf{n} \in \mathbb{Z}^2$, but the action $\alpha$ and $\beta$ are not measurably conjugate, since they are not algebraically conjugate in the sense of Theorem 5 ($\alpha$ and $\beta$ are obviously conjuagte in $\mathrm{GL}(3, \mathbb{Q})$, but not in $\mathrm{GL}(3, \mathbb{Z})$).

Results about isomorphism rigidity of $\mathbb{Z}^d$-actions by automorphisms of more general compact abelian groups can be found in [1] and [2].

**Homogeneous dynamics.** Apart from commuting group automorphisms, there is a second source of examples of 'algebraic' multiparametric actions with a rich theory and deep arithmetical connections: actions of higher rank diagonalizable subgroups of semisimple Lie groups on homogeneous spaces. More specifically, let $G$ be a linear algebraic group over the field $\Bbbk = \mathbb{R}$, and let $\Gamma \subset G$ be a lattice, i.e., a discrete subgroup with finite covolume (such as $\mathrm{SL}(n, \mathbb{Z}) \subset \mathrm{SL}(n, \mathbb{R})$). Every subgroup $H \subset G$ acts by right multiplication on the homogeneous space $X = \Gamma\backslash G$, and one can attempt to classify the $H$-invariant probability measures on $X$. Our assumptions on $\Gamma$ guarantee that there exists a (unique) $G$-invariant probability measure $\lambda_X$ on $X$.

A celebrated result by Marina Ratner [27] describes the probability measures which are invariant under unipotent subgroups of $G$.

**Theorem 7.** *Let $\Gamma \subset G$ be as above, and let $H \subset G$ be a unipotent subgroup. Then every $H$-invariant and ergodic probability measure on $X = \Gamma\backslash G$ is homogeneous in the sense that there exists a closed subgroup $L \subset G$ containing $H$ such that $\mu$ is the $L$-invariant probability measure supported on a single orbit of $L$.*

If the group $H$ is generated by (partially) hyperbolic elements the problem of classifying the $H$-invariant probability measures is open, even under much stronger hypotheses. The following conjecture is attributed to Furstenberg, Katok-Spatzier and Margulis.

**Conjecture 8** ([23])**.** *Let $A$ be the group of diagonal matrices in $\mathrm{SL}(n, \mathbb{R})$, $n \geq 3$. Then every $A$-invariant and ergodic probability measure on $X_n = \mathrm{SL}(n, \mathbb{Z})\backslash\mathrm{SL}(n, \mathbb{R})$ is homogeneous in the sense of Theorem 7.*

The following remarkable analogue of Rudolph's thoerem by Manfred Einsiedler, Anatole Katok and Elon Lindenstrauss represents at least partial progress towards this conjecture.

**Theorem 9** ([9, Theorem 1.3])**.** *Let $A$ be the group of diagonal matrices in $\mathrm{SL}(n, \mathbb{R})$, $n \geq 3$. Every $A$-invariant and ergodic probability measure $\mu$ on $X_n = \mathrm{SL}(n, \mathbb{Z})\backslash\mathrm{SL}(n, \mathbb{R})$ satisfies one of the following conditions:*

*(1) The measure $\mu$ is a homogeneous and not supported on a compact $A$-orbit;*

*(2) For every one-parameter subgroup $(a_t)_{t\in\mathbb{R}} \subset A$, $h_\mu(a_t) = 0$ for every $t \in \mathbb{R}$.*

One can classify the potential homogeneous measures arising in Conjecture 8 (cf. [21]). For example, if $n$ is prime, then any $A$-invariant homogeneous probability measure on $X_n$ is either the obvious invariant measure on a compact $A$-orbit, or equal to the $G$-invariant probability measure $\lambda_{X_n}$ on $X_n$.

In general, [21, Theorem 1.3] guarantees that no $\mu$ satisfying Condition (1) in Theorem 9 can be compactly supported.

The proof of Theorem 9 is a *tour de force*, based on a detailed analysis of the conditional measures induced by $\mu$ on the leaves of certain $A$-invariant foliations of $X_n$. The definition of these 'leaf measures' is in itself a little subtle, since the leaves of these foliations are typically noncompact and dense in $X_n$.[10]

The details of the proof of Theorem 9 fall under the definition of a *P2C2E* in the terminology of [28]: a process too complicated to explain here. The proof is based on a combination of two methods, referred to as the *high* and *low entropy* methods, respectively. I will try to give a very superficial impression of these two methods.

*The high entropy method.* In [8], M. Einsiedler and A. Katok prove that — under appropriate hypotheses — any $A$-invariant probability measure of sufficiently high entropy under some element of the $A$-action must be equal to $\lambda_{X_n}$.

**Theorem 10** ([8, Theorem 4.1], [11, Theorem 9.20])**.** *Let $n \geq 3$, $\Gamma \subset \mathrm{SL}(n,\mathbb{R})$ a lattice, $X = \Gamma\backslash G$, $A \subset G$ the diagonal subgroup and $\mu$ an $A$-invariant and ergodic probability measure on $X$. Then there exists, for every $a \in A$, an $h_0 < h_\lambda(a)$ such that $h_\mu(a) > h_0$ implies that $\mu = \lambda$. Furthermore, if $h_\mu(a) > 0$ for every $a \in A$, $a \neq 1_G$, then $\mu = \lambda$.*

*For $n = 3$ the existence of an $a \in A$ with $h_\mu(a) > \frac{1}{2}h_\lambda(a)$ implies that $\mu = \lambda_X$.*

For the proof of Theorem 10 I will follow the exposition in [11] and consider the eigenvalues (or *weights*) of the adjoint action $A$ on the Lie algebra $\mathfrak{g}$ of $G$: each of these eigenvalues is a homomorphism $\eta\colon A$ to $\mathbb{R}^\times$ for which there exists an $x \in \mathfrak{g}$ with $\mathrm{Ad}_a(x) = \eta(a)x$ for every $a \in A$. For a given weight $\eta$, the corresponding *eigenspace* consisting of all such $x \in \mathfrak{g}$ is denoted by $\mathfrak{g}^\eta$. If $\Phi$ is the set of these weights, then $\mathfrak{g} = \bigoplus_{\eta\in\Phi} \mathfrak{g}^\eta$. Note that $[\mathfrak{g}^\eta, \mathfrak{g}^{\eta'}] \subset \mathfrak{g}^{\eta\eta'}$ for $\eta, \eta' \in \Phi$.

For each $a \in A$, the *stable subspace* $\mathfrak{g}_a^- = \bigoplus_{\{\eta\in\Phi:|\eta(a)|<1\}} \mathfrak{g}^\eta$ of $a$ is a nilpotent subalgebra which the exponential map sends bijectively to the *stable horospherical subgroup* $G_a^- \subset G$ of $a$.

Two weights $\eta, \eta' \in \Phi$ are *equivalent* ($\eta \sim \eta'$) if $\eta^m = \eta'^n$ for some positive integers $m, n$. For every $\eta \in \Phi$ the equivalence class $[\eta]$ of $\eta$ is called a *coarse Lyapunov weight*, and $\mathfrak{g}^{[\eta]} = \bigoplus_{\eta'\sim\eta} \mathfrak{g}^{\eta'}$ is a Lie subalgebra of $\mathfrak{g}$, called the *coarse Lyapunov subalgebra* of $\eta$. The exponential map defines a homeomorphism between $\mathfrak{g}^{[\eta]}$ and a unipotent subgroup $G^{[\eta]}$ of $G$, called the *coarse unipotent subgroup* corresponding to $\eta$.

One chooses an order $[\eta_1] < \cdots < [\eta_l]$ of these coarse Lyapunov weights in such a way that there exists, for every $i = 1, \dots, l$, a $b \in A$ with $\eta_i(b) = 1$ and $|\eta_j(b)| < 1$ for $i < j \leq l$ (such an order is called *allowed*). Then the following is true.

**Theorem 11** ([11, Theorem 9.8], [8])**.** *Let $n \geq 3$, $\Gamma \subset \mathrm{SL}(n,\mathbb{R})$ a lattice, $X = \Gamma\backslash G$, $A \subset G$ the diagonal subgroup, and $\mu$ an $A$-invariant and ergodic probability measure on $X$. Fix some $a \in A$ and choose an allowed order $[\eta_1'] < \cdots < [\eta_s']$ of the coarse Lyapunov algebras contained in $\mathfrak{g}_a^-$ as described above. Then the leaf measures[11] $\mu_x^{G_a^-}$ and $\mu_x^{G^{[\eta_i']}}$, $i = 1, \dots, s$, satisfy that $\mu_x^{G_a^-}$ is proportional to the image of the product measure $\prod_{i=1}^s \mu_x^{G^{[\eta_i']}}$ for $\mu$-a.e. $x \in X$ under the product map $(g_1, \dots, g_s) \mapsto g_1 \cdots g_s$ from $\prod_{i=1}^s G^{[\eta_i']}$ to $G_a^-$.*

[10] In order to appreciate this difficulty the reader might consider the foliation of the space $X = \mathbb{T}^2$ given by the cosets of a noncompact dense subgroup $Y \cong \mathbb{R}$ of $X$ (e.g., $Y = \{(s, \sqrt{2}s) \pmod 1 : s \in \mathbb{R}\}$). Any probability measure $\mu$ on $X$ can be decomposed into Borel measures $\{\nu_x, x \in X\}$, such that $\nu_x$ is concentrated on the coset $Y + x$ for $\mu$-*a.e.* $x \in X$. However, these measures $\nu_x$ are typically not finite, and they are determined only up to scalar multiples. In general, they will not satisfy the condition that $\nu_x$ is equal to (or even equivalent to) $\nu_y$ if $x$ and $y$ lie on the same leaf of the foliation: in this case, $\nu_x$ can only be expected to be a multiple of $\nu_y$, translated by $x - y$.

In the case where $\mu = \lambda_{\mathbb{T}^2}$ these leaf measures are multiples of one-dimensional Lebesgue measures located on the 'lines' $Y + x$. Conversely, if $\mu$ is a probability measure whose leaf measures are *a.e.* multiples of Lebesgue measure, then $\mu = \lambda_{\mathbb{T}^2}$.

[11] The leaves in question are the orbits of the respective groups $G_a^-$ and $G^{[\eta_i']}$ in $X$.

By varying the allowed order of the coarse Lyapunov weights and exploring the commutators of the leaves corresponding to orbits of $G^{[\eta_i']}$ and $G^{[\eta_j']}$ one obtains the following result from this product structure of $\mu_x^{G_a^-}$.

**Theorem 12** (High entropy theorem – cf. [11, Theorem 9.14], [8])**.** *Let $\mu$ an $A$-invariant and ergodic probability measure on $X$. Let $[\eta]$ and $[\eta']$ be coarse Lyapunov weights such that $[\eta] \neq [\eta']$ and $[\eta^{-1}] \neq [\eta']$. Then for $\mu$-a.e. $x \in X$, $\mu$ is invariant under the group generated by the commutator $[\operatorname{supp}(\mu_x^{G^{[\eta']}}), \operatorname{supp}(\mu_x^{G^{[\eta']}})]$ of the supports of $\mu_x^{G^{[\eta]}}$ and $\mu_x^{G^{[\eta']}}$.*

We return to the proof of Theorem 10: the product formula in Theorem 11 shows that the conditional entropy of $a$ with respect to the foliation by $G_a^-$-orbits (whose integral is equal to $h_\mu(a)$) is the sum of the integrals of the conditional entropies of $a$ with respect to the foliations by $G^{[\eta_i']}$-orbits. If one of the measures $\mu_x^{G^{[\eta_i']}}$ is trivial, then its contribution to the entropy $h_{\mu_x^{G_a^-}}(a)$ is zero, which makes $h_\mu(a)$ smaller than $h_\lambda(a)$ by a specified amount. Hence, if $h_\mu(a)$ is sufficiently close to $h_\lambda(a)$, then $\mu_x^{G^{[\eta_i']}}$ is nontrivial for every $i = 1, \dots, s$ and $\mu$-*a.e.* $x \in X$. By playing around with commutators one obtains from Theorem 12 the invariance of $\mu$ under the various coarse unipotent subgroups $G^{[\eta]} \subset G_a^-$, which is enough to prove that $\mu = \lambda$.

*The low entropy method* was first introduced by Lindenstrauss in [19]. It studies the behaviour of the measure $\mu$ under the unipotent subgroups of $G$ normalized by $A$, even though these subgroups do not necessarily preserve the measure. Instead of *invariance*, this approach is based on *recurrence properties* of the measure $\mu$ under these subgroups.[12]

The following result is a special case of [19, Theorem 1.1] and gives a flavour of this approach.

**Theorem 13** ([19, Theorem 1.6])**.** *Let $X = \Gamma\backslash G$, where $\Gamma$ is an irreducible lattice in $G = G_1 \times G_2$ with $G_i = \mathrm{SL}(2, \mathbb{R})$ for $i = 1, 2$. Let $A = \left\{ \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \times 1_{G_2} \right\}$ be the embedding of the (one-parameter) diagonal subgroup of $G_1$ in $G$. Suppose that $\mu$ is an $A$-invariant probability measure on $X$ which is recurrent under $1_{G_1} \times G_2$, and such that a.e. ergodic component of $\mu$ (under $A$) has positive entropy. Then $\mu = \lambda_X$.*

The basic philosophy for concluding invariance from recurrence is the following: let $G$ and $H$ be locally compact groups acting on a space $X$, and let $\mu$ be a $G$-invariant and ergodic probability measure on $X$. Suppose that $\mathcal{F}$ is a foliation of $X$ which is preserved by $G$, and that each leaf of $\mathcal{F}$ is fixed by $H$. If $\mu$ is recurrent under $H$, then $\mu$ should be $H$-invariant — given appropriate conditions concerning the 'normalization' of the $H$-action by the action of $G$.

This approach appears to go back to [14], where Host used it for an alternative proof of Rudolph's Theorem 3. Another application can be found in [20], where it is used to show that any probability measure $\mu$ on $\mathbb{T}^n$ which is invariant under an irreducible ergodic nonhyperbolic toral automorphism $A$ and recurrent under the central foliation of that automorphism (i.e., under translation by the dense subgroup of $\mathbb{T}^n$ on which $A$ acts isometrically), is equal to Lebesgue measure.

I regret that the geometric considerations necessary even in the special case of Theorem 13 would overburden this brief account. The reader is referred to [11, §10] and, of course, to [9] for details.

Finally we come to the problem of *combining the high and low entropy methods* for a proof of Theorem 9. The assumption of positive entropy of $\mu$ under some appropriately chosen $a \in A$ in the statement of Theorem 9 implies that the measures induced by $\mu$ on the contracting leaves of $a$ (i.e., on the orbits of $G_a^-$) are nontrivial for *a.e.* orbit of $G_a^-$. By using a product structure result in [8] and a geometrical argument one obtains a unipotent subgroup $U$ of $G_a^-$ such that the leaf measure induced by $\mu$ on *a.e.* $U$-orbit is nontrivial (which implies recurrence of $\mu$ under $U$). Leaving further subtleties aside one then deduces that $\mu$ is either $U$-invariant (in which case one can apply Ratner's classification theorem for invariant measures of unipotent groups), or one obtains a second unipotent subgroup $V$ of $A$ such that *a.e.* leaf measure induced by $\mu$ on the $V$-orbits is nontrivial. The latter condition leads to invariance under the commutator $[U, V]$ of $U$ and $V$. An argument similar to that used in the proof of Theorem 10 finally shows that $\mu = \lambda$.

[12] If $T\colon g \mapsto T_g$ is an action of a locally compact group $G$ on a standard Borel space $(X, \mathcal{S})$, then a probability measure $\nu$ on $X$ is *recurrent* under $G$ if there exist, for every compact set $K \subset G$ and every Borel set $B \subset X$ with $\mu(B) > 0$, a $g \in G \smallsetminus K$ and an $x \in B$ with $T_g x \in B$.

*Towards Littlewood's Conjecture.* Around 1930, Littlewood conjectured the following diophantine result.

**Conjecture 14** (Littlewood)**.** *For every $u, v \in \mathbb{R}$,*

$$\liminf_{n\to\infty} n\|nu\|\|nv\| = 0, \tag{1}$$

*where $\|w\| = \min_{n\in\mathbb{Z}} |w-n|$ is the distance of $w \in \mathbb{R}$ to the nearest integer.*

We set $G = \mathrm{SL}(3,\mathbb{R})$, $\Gamma = \mathrm{SL}(3,\mathbb{Z})$, $X = \mathrm{SL}(3,\mathbb{Z})\backslash\mathrm{SL}(3,\mathbb{R})$ and write $A$ for the group of diagonal matrices in $G$. As usual, the $G$-invariant probability measure on $X$ will be denoted by $\lambda$.

**Proposition 15** ([9, Proposition 11.1], [11, Proposition 12.5])**.** *For every $s, t \in \mathbb{R}$ we set*

$$a(s,t) = \begin{pmatrix} e^{s+t} & 0 & 0 \\ 0 & e^{-s} & 0 \\ 0 & 0 & e^{-t} \end{pmatrix} \in A.$$

*A point $(u,v) \in \mathbb{R}^2$ satisfies* (1) *if and only if the closure of the orbit $xA^+$ of the point*

$$x_{u,v} = \Gamma \cdot \begin{pmatrix} 1 & u & v \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in X$$

*under the semigroup $A^+ = \{a(s,t) : s,t \geq 0\}$ is noncompact.*

*Furthermore, if $\delta > 0$, then there exists a compact set $C_\delta \subset X$ which contains every $x_{u,v}$ with $\liminf_{n\to\infty} n\|nu\|\|nv\| \geq \delta$.*

The proof of Proposition 15 uses *Mahler's compactness criterion*: a set $E \subset X_n = \mathrm{SL}(n,\mathbb{Z})\backslash\mathrm{SL}(n,\mathbb{R})$ is bounded if and only if there is an $\varepsilon > 0$ such that $E$ contains no lattices $\Gamma g$ with $\min\{\|\mathbf{w}\| : \mathbf{w} \in (\mathbb{Z}^d \smallsetminus \mathbf{0}) \cdot g\} < \varepsilon$ (where $\mathbf{v} \cdot g \in \mathbb{R}^n$ is the product of a row vector $\mathbf{v} \in \mathbb{Z}^d$ with the matrix $g \in \mathrm{GL}(n,\mathbb{R})$).

The next step in deriving a partial solution of Littlewood's conjecture depends crucially on Theorem 9, combined with the variational principle[13] and semicontinuity properties of measure-theoretic entropy on $X_n$. We set $a_{\sigma,\tau}(t) = a(\sigma t, \tau t)$ with $a(s,t)$ as in Proposition 15.

**Proposition 16** ([11, Proposition 12.12])**.** *Suppose that $(u,v) \in \mathbb{R}^2$ does not satisfy* (1)*. Then for any $\sigma, \tau \geq 0$, the topological entropy of $a_{\sigma,\tau}$ on the compact set $\overline{\{x_{u,v}a_{\sigma,\tau}(t) : t \geq 0\}} \subset X$ vanishes.*

With very little further work one arrives at the remarkable partial solution of Littlewood's conjecture by Einsiedler, Katok and Lindenstrauss.

**Theorem 17** ([9, Theorem 1.5], [11, Theorem 12.10])**.** *For any $\delta > 0$, the set $\Xi_\delta = \{(u,v) \in [0,1)^2 : \liminf_{n\to\infty} n\|nu\|\|nv\| \geq \delta\}$ has zero upper box dimension.*[14]

It is worth noting that Littlewood's conjecture would follow from Conjecture 8. For a discussion of this connection, which goes back in essence to Cassels and Swinnerton-Dyer, see [6], [22] and [23].

# References


[1] S. Bhattacharya, *Isomorphism rigidity of commuting automorphisms*, Trans. Amer. Math. Soc. **360** (2008), 6319–6329.

[2] S. Bhattacharya and K. Schmidt, *Homoclinic points and isomorphism rigidity of algebraic $\mathbf{Z}^d$-actions on zero-dimensional compact abelian groups*, Israel J. Math. **137** (2003), 189–209.

[3] É. Borel, *Les probabilités dénombrables et leurs applications arithmétiques*, Rend. Circ. Mat. Palermo **27** (1909), 247–271.


[13] The version of the variational principle relevant here is that the topological entropy of a continuous flow on a compact metric space is bounded by the measure-theoretic entropies of its invariant probability measures.

[14] This means that, for every $\varepsilon > 0$ and $0 < r < 1$, one can cover $\Xi_\delta$ by $O_{\delta,\varepsilon}(r^{-\varepsilon})$ boxes of size $r \times r$. Note that zero upper box dimension for every $\Xi_\delta$, $\delta > 0$, trivially implies zero Lebesgue measure for the set of exceptions to Littlewood's conjecture.

[4] J. Bourgain, E. Lindenstrauss, P. Michel and A. Venkatesh, *Some effective results for $\times a$ $\times b$*, Ergod. Th. & Dynam. Sys. **29** (2009), 1705–1722.

[5] J.W.S. Cassels, *On a problem of Steinhaus about normal numbers*, Colloq. Math. **7** (1959), 95–101.

[6] J.W.S. Cassels and H.P.F. Swinnerton-Dyer, *On the product of three homogeneous linear forms and indefinite ternary quadratic forms*, Philos. Trans. Roy. Soc. London Ser. A **248** (1955), 73–96.

[7] D.G. Champernowne, *The construction of decimals normal in the scale of ten*, J. London Math. Soc. **8** (1933), 254–260.

[8] M. Einsiedler and A. Katok, *Invariant measures on $G/\Gamma$ for split simple Lie groups $G$*, Comm. Pure Appl. Math. **56** (2003), 1184–1221.

[9] M. Einsiedler, A. Katok and E. Lindenstrauss, *Invariant measures and the set of exceptions to Littlewood's conjecture*, Ann. of Math. **164** (2006), 513–560.

[10] M. Einsiedler and E. Lindenstrauss, *Rigidity properties of $\mathbf{Z}^d$-actions on tori and solenoids*, Electron. Res. Announc. Amer. Math. Soc. **9** (2003), 99–110.

[11] M. Einsiedler and E. Lindenstrauss, *Diagonalizable flows on locally homogeneous spaces*, in: Homogeneous flows, moduli spaces and arithmetic, Clay Math. Proc., vol. 10, American Mathematical Society, Providence, R.I., 2010, 155–241.

[12] M. Einsiedler and T. Ward, *Arithmetic quantum unique ergodicity for* $\Gamma\backslash\mathbb{H}$. http://swc.math.arizona.edu/aws/10/2010EinsiedlerNotes.pdf

[13] H. Furstenberg, *Disjointness in ergodic theory, minimal sets, and a problem in diophantine approximation*, Math. Systems Theory **1** (1967), 1–49.

[14] B. Host, *Nombres normaux, entropie, translations*, Israel J. Math. **91** (1995), 419–428.

[15] A.S.A. Johnson, *Measures on the circle invariant under multiplication by a nonlacunary subsemigroup of the integers*, Israel J. Math. **77** (1992), 211–240.

[16] A. Katok, S. Katok and K. Schmidt, *Rigidity of measurable structure for algebraic actions of higher-rank abelian groups*, Comment. Math. Helv. **77** (2002), 718–745.

[17] A. Katok and R.J. Spatzier, *Invariant measures for higher-rank hyperbolic abelian actions*, Ergod. Th. & Dynam. Sys. **16** (1996), 751–778; *Corrections*, **18** (1998), 507–507.

[18] A. Khinchine, *Metrische Kettenbruchprobleme*, Compositio Math. **1** (1935), 361–382.

[19] E. Lindenstrauss, *Invariant measures and arithmetic quantum unique ergodicity*, Ann. of Math. **163** (2006), 165–219.

[20] E. Lindenstrauss and K. Schmidt, *Invariant measures of nonexpansive group automorphisms*, Israel J. Math. **144** (2004), 29–60.

[21] E. Lindenstrauss and B. Weiss, *On sets invariant under the action of the diagonal group*, Ergod. Th. & Dynam. Sys. **21** (2001), 1481–1500.

[22] G.A. Margulis, *Oppenheim conjecture*, in: Fields Medallists' Lectures, World Sci. Ser. 20th Century Math., vol. 5, World Scientific Publishers, River Edge, New Jersey, 1997, 272–327.

[23] G. Margulis, *Problems and conjectures in rigidity theory*, in: Mathematics: Frontiers and Perspectives, American Mathematical Society, Providence, R.I., 2000, 161–174.

[24] J. Moulin-Ollagnier, *Ergodic theory and statistical mechanics*, Lecture Notes in Mathematics, vol. 1115, Springer Verlag, Berlin-Heidelberg-New York, 1985.

[25] D.S. Ornstein and B. Weiss, *Entropy and isomorphism theorems for actions of amenable groups*, J. Analyse Math. **48** (1987), 1–141.

[26] K. Petersen, *Ergodic theory*, Cambridge University Press, Cambridge, 1983.

[27] M. Ratner, *On Raghunathan's measure conjecture*, Ann. of Math. **134** (1991), 545–607.

[28] S. Rushdie, *Haroun and the Sea of Stories*, Puffin Books, Penguin Books Ltd., London, 1993.

[29] D.J. Rudolph, $\times 2$ *and* $\times 3$ *invariant measures and entropy*, Ergod. Th. & Dynam. Sys. **10** (1990), 395–406.

[30] K. Schmidt, *Dynamical systems of algebraic origin*, Birkhäuser Verlag, Basel-Berlin-Boston, 1995.

[31] W.M. Schmidt, *On normal numbers*, Pacific J. Math. **10** (1960), 661–672.

[32] W. Sierpiński, *Démonstration élémentaire d'un théorème de M. Borel sur les nombres absolument normaux et détermination effective d'un tel nombre*, Bull. Soc. Math. France **45** (1917), 127–132.

[33] P. Walters, *An introduction to ergodic theory*, Graduate Texts in Mathematics, vol. 79, Springer Verlag, Berlin-Heidelberg-New York, 1982.

[34] H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. **77** (1916), 313–352.