ISRAEL JOURNAL OF MATHEMATICS, Vol. 41, No. 4, 1982

ERGODIC GROUP AUTOMORPHISMS ARE EXPONENTIALLY RECURRENT

BY

D. A. LIND[†]

ABSTRACT

We show that ergodic automorphisms of compact abelian groups have the property that for every nonempty open set U, the measure of the set first returning to U after n iterates decays exponentially in n. This follows from a result about aperiodic automorphisms of countable abelian groups, whose proof employs p-adic analysis.

§1. Introduction

Many measure-preserving transformations also preserve a natural topology. Some that are known to be measurably isomorphic to a Bernoulli shift have recently been shown to be finitarily isomorphic as well, i.e. an isomorphism exists that is continuous off an invariant null set. The question that motivates this paper is whether ergodic automorphisms of compact metrizable abelian groups, which are known to be measurably Bernoulli [5], are finitarily Bernoulli. Hyperbolic toral automorphisms are finitarily Bernoulli because they have Markov partitions [1], [2]. However, even for the other ergodic toral automorphisms this question is not yet settled (see [7]).

Smorodinsky observed that a necessary condition for an automorphism to be finitarily Bernoulli is that it be exponentially recurrent, i.e. that open sets have exponentially decaying return times. He used this to construct a countable state Markov chain that is measurably but not finitarily Bernoulli.

We describe exponential recurrence in §2, and show that for a group automorphism it is implied via duality by a property we call lacunary independence for the dual automorphism. In §3 we verify that certain basic automorphisms are lacunarily independent. The interesting case is a linear transformation of a rational vector space, where p-adic analysis seems to play an essential

[†] Partially supported by NSF Grant MCS 7704915.
Received November 26, 1981

role. In §4 we describe how a general aperiodic automorphism can be obtained from the basic automorphisms using restrictions, increasing limits, and extensions. Lacunary independence is shown in §5 to persist under each of these processes, and therefore holds for all aperiodic automorphisms. Finally, in §6 we briefly discuss the strength of the mixing condition we obtain for group automorphisms.

§2. Exponential recurrence

Let X be a compact metric space and T be a homeomorphism of X that preserves a nonatomic Borel probability measure μ. We may and will assume that μ is positive on open subsets of X. For $U \subset X$ put $r_U(x) = \min\{j > 0 : T^j x \in U\}$. If $\mu(U) > 0$, then $r_U < \infty$ a.e. on U by Poincaré recurrence. Say that T is *exponentially recurrent* if for every (nonempty) open set U, $\mu\{x \in U : r_U(x) = n\} \to 0$ exponentially fast. If T is ergodic on (X, μ), another formulation of exponential recurrence is that for every open U, $\mu(U \cup TU \cup \cdots \cup T^n U) \to 1$ exponentially fast.

Let $p = (p_1, \cdots, p_r)$ be a probability vector, $\Sigma = \{1, \cdots, r\}^{\mathbf{Z}}$, σ be the shift on Σ, and $\nu = p^{\mathbf{Z}}$ be product measure on Σ. Say that T is *finitarily isomorphic* to the Bernoulli shift σ if there is a measurable conjugacy $\Phi : X \to \Sigma$ of T to σ that is a homeomorphism off appropriate invariant null sets in X and Σ. Call T *finitarily Bernoulli* if it is finitarily isomorphic to some Bernoulli shift.

PROPOSITION 1. *Finitarily Bernoulli transformations are exponentially recurrent.*

PROOF. Since exponential recurrence is preserved under finitary isomorphism, it suffices to show Bernoulli shifts are exponentially recurrent.

Let (Σ, σ, ν) be as above, and U be an open subset of Σ. There is a cylinder set $A = \{\omega \in \Sigma : \omega_k = a_k, \cdots, \omega_{k+m} = a_{k+m}\} \subset U$. Then

$$\nu\{r_U = n+1\} \leqq \nu\left(\bigcap_{j=1}^{[n/m]} \sigma^{mj} A^c\right) = \prod_{j=1}^{[n/m]} \nu(\sigma^{mj} A^c)$$
$$\leqq \{\nu(A^c)^{1/m}\}^n.$$

Our main goal is to prove the following result, giving some evidence that ergodic group automorphisms are finitarily Bernoulli.

THEOREM 1. *Ergodic automorphisms of compact metrizable abelian groups are exponentially recurrent.*

We shall deduce this via duality from a property of aperiodic automorphisms of discrete countable abelian groups that may have independent interest. First some terminology. "Group" always means "abelian group". If G is a group and $\{E_j\}$ is a collection of subsets of G, say that $\{E_j\}$ is *independent* if whenever $e_{j_1} + \cdots + e_{j_m} = 0$ with $e_{j_i} \in E_{j_i}$ and the j_i distinct, then each $e_{j_i} = 0$. Note that independence refers to the sets E_j, not to the subgroup of G generated by them. If N is an integer, an increasing sequence of integers $\{n_j\}$ is N-*lacunary* if $n_{j+1} - n_j \geqq N$. An automorphism of a group is *aperiodic* if the only periodic element is the identity.

Definition. An aperiodic automorphism S of a group G is *lacunarily independent* if for every finite subset F of G there is an integer $N = N(S, F)$ such that for every N-lacunary sequence $\{n_j\}$ the sets $\{S^{n_j}F\}$ are independent.

Theorem 2. *Every aperiodic automorphism of a countable group is lacunarily independent.*

We conclude this section by deducing Theorem 1 from Theorem 2.

Proof of Theorem 1. Let T be an ergodic automorphism of the compact metrizable group X, and S be its dual automorphism of the countable dual group G. Ergodicity of T is equivalent to aperiodicity of S. Let U be open in G, and χ_U denote its indicator function. Using the Stone–Weierstrass theorem, one can find a trigonometric polynomial ψ on X involving a finite set F of characters in G such that $\psi \geqq \chi_{U^c}$ and $\int_X \psi d\mu = \eta < 1$. By Theorem 2, choose $N = N(S, F)$. Since $F, S^N F, S^{2N} F, \cdots$ are independent subsets of G, it follows that $\psi, T^N\psi, T^{2N}\psi, \cdots$ are mutually uncorrelated random variables. Thus, letting $m = [n/N]$, we have

$$\begin{aligned}\mu\{r_U = n+1\} &\leqq \mu\left(\bigcap_{j=1}^{m} T^{jN}U^c\right) = \int_X \prod_{j=1}^{m} T^{jN}\chi_{U^c}\,d\mu \\ &\leqq \int_X \prod_{j=1}^{m} T^{jN}\psi d\mu = \prod_{j=1}^{m} \int_X T^{jN}\psi d\mu \\ &= \eta^m \leqq (\eta^{1/N})^n.\end{aligned}$$

§3. Basic automorphisms

The building blocks for aperiodic automorphisms are group shifts and irreducible rational maps. In this section we show they are lacunarily independent.

If H is a group, and G is the countable direct sum of copies of H, call the shift S on G the *group shift on* H. If S is an aperiodic $\mathbf{Q}$-linear map of $\mathbf{Q}^d$ with characteristic polynomial that is irreducible over $\mathbf{Q}$, call S an *irreducible rational map.* A *basic automorphism* is one that is isomorphic to one of these.

PROPOSITION 2. *Basic automorphisms are lacunarily independent.*

PROOF. Since a finite subset of a countable direct sum depends on only finitely many coordinates, the result is clear for group shifts.

More interesting are irreducible rational maps. If $S \in \mathrm{GL}(d, \mathbf{Q})$ has a complex eigenvalue of norm $\neq 1$, then the same idea as in [7] will work. The novel feature here is that if all the complex eigenvalues of S have norm 1, then some p-adic eigenvalue of S will have p-adic norm $\neq 1$. The geometric idea in [7] then has an arithmetic counterpart when S is thought of as acting on the d-dimensional p-adic vector space instead of $\mathbf{C}^d$.

So first assume that some complex eigenvalue of S has norm $\neq 1$. Since S has irreducible characteristic polynomial, if W is a proper S-invariant subspace of $\mathbf{C}^d$, then $W \cap \mathbf{Q}^d = \{0\}$. By replacing S with S^{-1} if necessary, we may assume that some eigenvalue λ has $|\lambda| < 1$. A Jordan block of S corresponding to λ splits $\mathbf{C}^d$ into an S-invariant decomposition $V \oplus W$, where

$$\| S^n |_V \| \leqq C |\lambda|^n \tag{1}$$

for a suitable constant C. Let $\pi : \mathbf{C}^d \to V$ denote projection along W.

Suppose $F \subset \mathbf{Q}^d$ is finite. We may assume $0 \in F$. Since $W \cap \mathbf{Q}^d = \{0\}$, there are $\delta, \Delta > 0$ such that

$$\delta < \| \pi x \| < \Delta \qquad \text{if } 0 \neq x \in F.$$

Choose $N = N(S, F)$ so that $C|\lambda|^N < \delta(1 - |\lambda|)/2\Delta$. Suppose $\{n_j\}$ is N-lacunary, and that $\sum_{j=0}^m S^{n_j} x_j = 0$ with $x_j \in F$. If some $x_j \neq 0$, we may assume $n_0 = 0$ and $x_0 \neq 0$. Then

$$\begin{aligned} 0 < \delta < \| \pi x_0 \| &= \left\| \sum_{j=1}^m S^{n_j} \pi x_j \right\| \leqq C \sum_{j=1}^m |\lambda|^{n_j} \Delta \\ &\leqq C\Delta \sum_{k=N}^\infty |\lambda|^k = \frac{C\Delta |\lambda|^N}{1 - |\lambda|} < \frac{\delta}{2}. \end{aligned}$$

Hence each $x_j = 0$, and so $\{S^{n_j} F\}$ is independent, completing the proof in this case.

Now suppose that all the complex eigenvalues of S have norm 1. Let $f(t) = t^d + a_1 t^{d-1} + \cdots + a_d \in \mathbf{Q}[t]$ be the characteristic polynomial of S. We claim that there must be a prime p that occurs in the denominator of one of the a_j, i.e. that $|a_j|_p > 1$ for some p and j. Here $|\cdot|_p$ denotes the p-adic norm on $\mathbf{Q}$. For a very readable introduction to p-adic analysis, the reader should enjoy Koblitz' book [3].

If our claim were not true, then each $a_j \in \mathbf{Z}$. But a theorem of Kronecker [4] shows that if all the conjugates of an algebraic integer have complex norm 1, then it must be a root of unity. This is ruled out by aperiodicity of S, so not all the a_j are integers.

Let p be a prime with $|a_j|_p > 1$, and let $\bar{\mathbf{Q}}_p$ denote the algebraic closure of the p-adic field $\mathbf{Q}_p$. It turns out that $|\cdot|_p$ extends uniquely to $\bar{\mathbf{Q}}_p$ so that $|x+y|_p \leqq \max\{|x|_p, |y|_p\}$ and $|xy|_p = |x|_p|y|_p$. Since $f(t)$ is irreducible over $\mathbf{Q}$, it splits over $\bar{\mathbf{Q}}_p$ into distinct linear factors as $f(t) = (t-\lambda_{1,p})\cdots(t-\lambda_{d,p})$. Since a_j is the jth symmetric function in the $\lambda_{i,p}$ we have

$$\begin{aligned} 1 < |a_j|_p &= |\lambda_{1,p}\cdots\lambda_{j,p} + \cdots|_p \\ &\leqq \max\{|\lambda_{1,p}\cdots\lambda_{j,p}|_p, \cdots\} \\ &\leqq \Big(\max_{1\leqq k\leqq d} |\lambda_{k,p}|_p\Big)^j. \end{aligned}$$

Hence $|\lambda_{k,p}|_p > 1$ for some k. By replacing S with S^{-1}, we may assume $|\lambda_{k,p}|_p < 1$. Now the proof above goes through exactly as before, except that $\bar{\mathbf{Q}}_p^d$ replaces $\mathbf{C}^d$, completing the proof.

An instructive example is $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 6/5 \end{smallmatrix}\right]$ acting on $\mathbf{Q}^2$. The complex eigenvalues are $\frac{3}{5} \pm \frac{4}{5}i$, so the first proof fails. Now $f(t) = t^2 - \frac{6}{5}t + 1$, and $p = 5$. Over $\bar{\mathbf{Q}}_5$, $f(t) = (t-\lambda_{1,5})(t-\lambda_{2,5})$ where each $|\lambda_{j,5}|_5 > 1$. Here increasing divisibility of the denominators of S^n by the prime 5 replaces the geometric contraction of (1).

§4. The structure of aperiodic automorphisms

Call an aperiodic automorphism of a countable group *derivable* if it can be obtained from the basic automorphisms using the *basic operations* of restriction, increasing limit, and extension. Alternatively, the derivable automorphisms form the smallest collection of automorphisms containing the basic ones and which is closed under the basic operations. Recall that "group" means "abelian group".

PROPOSITION 3. *All aperiodic automorphisms of countable groups are derivable.*

PROOF. Let S be an aperiodic automorphism of the countable group G. For an S-invariant subgroup H of G, we denote the corresponding restriction and quotient automorphisms by S_H and $S_{G/H}$. Note that $S_{G/H}$ need not be aperiodic. Aperiodicity of certain quotient automorphisms below is checked directly.

Let G_t be the torsion subgroup of G, which is clearly S-invariant. It is easy to check that S is aperiodic on G/G_t. Since S is an extension of S_{G/G_t} by S_{G_t}, it suffices to consider only the torsion and torsion-free cases.

First suppose that G is a torsion group. Then the p-primary component G_p of G is S-invariant. Since $G = \bigoplus_p G_p$, we need only prove that S_{G_p} is derivable.

Thus we may assume that each element of G is annihilated by a power of p. Let $G(n) = \{g \in G : p^n g = 0\}$. Since $G(n) \nearrow G$, we only need that each $S_{G(n)}$ is derivable.

Now $G(1)$ is a vector space over $\mathbf{Z}/p$, so under the action of S is a module over $\mathbf{Z}/p[x, x^{-1}] = R_p$, as in [5, p. 235]. Aperiodicity of S implies that $G(1)$ is R_p-torsion-free. Let H_j be an increasing sequence of finitely generated R_p-submodules of $G(1)$ whose union is $G(1)$. Since R_p is a principle ideal domain, every finitely generated torsion-free R_p-module is R_p-free. Hence each S_{H_i} is a product of p-shifts, so is derivable. Thus $S_{G(1)}$ is derivable.

Assume inductively that $S_{G(n)}$ is derivable. It is easy to verify that $S_{G(n+1)/G(n)}$ is aperiodic, so the previous paragraph shows that it is derivable. Thus $S_{G(n+1)}$ is derivable, completing the proof in the torsion case.

Now consider the case when G is torsion-free. Embed G into the $\mathbf{Q}$-vector space $G \otimes_{\mathbf{Z}} \mathbf{Q}$, to which S extends as an automorphism. Since restriction is a basic operation, we can assume that G is already a $\mathbf{Q}$-vector space. Using the action of S, G becomes a module over $\mathbf{Q}[x, x^{-1}] = R$, as in [5, p. 238].

Let G_0 be the R-torsion submodule of G, and K_j be R-finitely generated submodules of G_0 increasing to G_0. Then S_{K_j} is a linear map of a finite-dimensional rational vector space. The rational canonical form for S_{K_j} shows that K_j invariantly splits into $L(q_1) \oplus \cdots \oplus L(q_r)$, where the q_i are the irreducible factors of the minimal polynomial of S_{K_j}, and $S_{L(q_i)}$ has minimal polynomial a power of q_i. As shown in [5, p. 215], each $S_{L(q_i)}$ is a sequence of extensions of an irreducible rational map, so is derivable. Hence each S_{K_j} is derivable, and therefore so is S_{G_0}.

Finally, one checks that S_{G/G_0} is aperiodic. Thus is suffices to assume that G is R-torsion-free. Since R is a principle ideal domain, each finitely generated R-submodule is R-free, so a product of $\mathbf{Q}$-shifts. Thus G is the increasing limit of products of $\mathbf{Q}$-shifts, so is derivable.

REMARKS. (1) The proof requires only shifts on $\mathbf{Z}/p$ and $\mathbf{Q}$, not general group shifts.

(2) This proposition distills the algebraic reductions used in [5] and [6] to analyse the ergodic theory of compact group automorphisms.

§5. Lacunary independence under basic operations

We complete the proof of Theorem 2 with the following fact.

PROPOSITION 4. *Lacunary independence is preserved under the basic operations.*

PROOF. This is obvious for restriction and increasing limits.

Suppose $H \subset G$ is an S-invariant subgroup, and that S_H and $S_{G/H}$ are lacunarily independent. Let $\pi : G \to G/H$ be the quotient map. Suppose $F \subset G$ is finite, and assume without loss that $0 \in F$. Put

$$N(S, F) = \max\{N(S_{G/H}, \pi F), N(S_H, F \cap H)\}.$$

Let $\{n_j\}$ be $N(S, F)$-lacunary, and suppose that

$$\sum_{j=0}^{m} S^{n_j} x_j = 0$$

with $x_j \in F$. Applying π gives

$$\sum_{j=0}^{m} S_{G/H}^{n_j}(\pi x_j) = 0.$$

Since $N(S, F) \geqq N(S_{G/H}, \pi F)$, we obtain $\pi x_j = 0$, i.e. $x_j \in F \cap H$ for each j. Then $N(S, F) \geqq N(S_H, F \cap H)$ implies that each $x_j = 0$.

§6. Some questions

If X is a compact metrizable abelian group, then the trigonometric polynomials form a subalgebra A of $L^\infty(X)$ that is dense in $L^1(X)$. Each finite dimensional subspace of A involves only a finite set of characters. If T is an ergodic automorphism of X, then Theorem 2 applied to the dual of T shows that T has the following property:

(*) There is a T-invariant subalgebra A of $L^\infty(X)$, dense in $L^1(X)$, such that if V is a finite-dimensional subspace of A, then there is an $N = N(T, V)$ such that if $f_j \in V$ and $\{n_j\}$ is N-lacunary, then $\{T^{n_j} f_j\}$ are mutually uncorrelated.

If T is a measure-preserving transformation of a Lebesgue space X, it is meaningful to ask whether it has property (*). This is a lot to ask of T. For example, (∗) immediately implies that T is mixing of all orders. Bernoulli shifts have (∗). Must a T with (∗) have positive entropy? Must it be a Kolmogorov automorphism? A Bernoulli shift?

References

1. M. Keane and M. Smorodinsky, *Bernoulli schemes of the same entropy are finitarily isomorphic*, Ann. of Math. (2), **109** (1979), 397–406.

2. M. Keane and M. Smorodinsky, *The finitary isomorphism theorem for Markov shifts*, Bull. Am. Math. Soc. (N. S.) **1** (1979), 436–438.

3. Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta Functions*, Springer, New York, 1977.

4. L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **53** (1857), 173–175.

5. D. A. Lind, *The structure of skew products with ergodic group automorphisms*, Isr. J. Math. **28** (1977), 205–248.

6. D. A. Lind, *Split skew products, a related functional equation, and specification*, Isr. J. Math. **30** (1978), 236–254.

7. D. A. Lind, *Dynamical properties of quasihyperbolic toral automorphisms*, to appear.

Department of Mathematics
University of Washington
Seattle, WA 98195 USA