ISRAEL JOURNAL OF MATHEMATICS, Vol. 37, No. 3, 1980

A DISCRETE ANALOGUE OF A THEOREM OF KATZNELSON

BY

JUSTIN PETERS

ABSTRACT

In this paper we sharpen an earlier result of the author's concerning entropy of automorphism on discrete groups. We show that the entropy of an automorphism of Z^m can be approximated arbitrarily well on a subset on which some power of α acts as a discrete shift.

Katznelson [2] showed that ergodic automorphisms of the m-torus $\bar{T}^m$ are isomorphic to bernoulli shifts. By duality, an automorphism $\alpha \in \mathrm{Aut}(\bar{T}^m)$ may be viewed as an automorphism of the m-dimensional integer lattice Z^m. What we will show here is that α can be approximated arbitrarily closely by discrete bernoulli shifts in powers of α contained in Z^m. First, however, we will define what we mean by a discrete bernoulli shift and show how this arises naturally from Pontryagin duality.

Let G be a (discrete) group written additively and $0 \in S_i \subset G$ $(i \in Z)$ a collection of subsets of G. The set $B = \sum_{i=-\infty}^{\infty} S_i = \{\sum s_i : s_i \in S_i$ and all but finitely many of the s_i are zero$\}$ is called the direct sum of the S_i's, written $B = \bigoplus_{i=-\infty}^{\infty} S_i$, if each $x \in B$ has a unique expression $x = \sum_i s_i$ $(s_i \in S_i)$. Suppose $B = \bigoplus_{i=-\infty}^{\infty} S_i$ and $\alpha : B \to B$ is a bijection such that $\alpha S_i = S_{i+1}$ for all $i \in Z$. Then we say α is a discrete (left) bernoulli shift on B with state space $S = S_0$. In that case we define the entropy of α on B, $h(\alpha, B)$, to be $\log(\mathrm{card}\, S)$ if S has finite cardinality and $+\infty$ otherwise.

Let G again be a discrete abelian group and Γ the character group of G, which is compact in the topology of pointwise convergence on G. If α is an automorphism of G, the adjoint ${}^t\alpha$ is defined on Γ by ${}^t\alpha(\gamma)(x) = \gamma(\alpha^{-1}(x))$. We define the entropy of α on G as follows: let $E \subset G$ be any finite subset, and for each positive integer n set

$$E_{\alpha,n} = E + \alpha^{-1}E + \cdots + \alpha^{-(n-1)}E,$$

Received May 31, 1979 and in revised form April 13, 1980

and

$$(*) \qquad h(\alpha, G) = \sup_{E \subset G \text{ finite}} \lim_n \frac{1}{n} \log |E_{\alpha,n}|$$

where $|\cdot|$ denotes cardinality. Then $h(\alpha,G)$ equals the Kolmogorov–Sinai entropy of $'\alpha$ on Γ with respect to haar measure or, equivalently, the topological entropy of $'\alpha$ on Γ. (See [4], [5].)

If $G = \bigoplus_{i=-\infty}^{\infty}(Z_p)_i$, where for all i, $(Z_p)_i = Z_p$ is the group of integers modulo p and α is the left shift, then the two definitions we have given above agree. Indeed, in this example the supremum in $(*)$ is attained by taking $E = (Z_p)_0 = S_0$, the state space, and

$$\lim_n \frac{1}{n} \log |E_{\alpha,n}| = \lim_n \frac{1}{n} \log p^n = \log p = \log \operatorname{card}(S_0).$$

In general, it follows from definition $(*)$ that if α is an automorphism of a discrete abelian group G and there is a subset $B \subset G$ on which α acts as a bernoulli shift, then $h(\alpha, B) \leqq h(\alpha, G)$. Next we list some properties of discrete entropy; the proofs are straightforward and can be found in [4]:

(a) $h(\alpha^n, G) = nh(\alpha, G)$, n a positive integer;

(b) $h(\alpha^{-1}, G) = h(\alpha, G)$;

(c) $h(\iota, G) = 0$, $\iota(x) = x$ is the identity;

(d) if G_i are discrete abelian groups and $\alpha_i \in \operatorname{Aut}(G_i)$, $i = 1,2$, then $h(\alpha_1 \times \alpha_2, G_1 \times G_2) = h(\alpha_1, G_1) + h(\alpha_2, G_2)$;

(e) if $\alpha_1, \alpha_2 \in \operatorname{Aut}(G)$ are conjugate (so $\alpha_2 = \beta\alpha_1\beta^{-1}$ for some $\beta \in \operatorname{Aut}(G)$), then $h(\alpha_1, G) = h(\alpha_2, G)$.

In the next theorem we will show it is possible to have a bernoulli shift contained in Z^m $(m \geqq 2)$ in which the state space is not a subgroup. Let $0 \neq b \in Z^m$ and p a positive integer; following [1] we will denote $[b]_p = \{0, b, 2b, \cdots, (p-1)b\}$ the "p-cyclic set" generated by b. (There should be no confusion between $[b]_p$ and the greatest integer function $[\cdot]$ below.)

1. Theorem. *Let $\alpha \in \operatorname{Aut}(Z^m) = \mathrm{GL}(m, Z)$ have characteristic polynomial $p(x)$ which is irreducible over Z. Suppose $\{\lambda_1, \cdots, \lambda_k\}$ is a subset of the zeroes of $p(x)$, $|\lambda_1| \geqq |\lambda_2| \geqq \cdots \geqq |\lambda_k|$, such that $p_j = [|\lambda_j|/2j] - 1$ is a positive integer, $1 \leqq j \leqq k$. Set $p = \Pi_{j=1}^k p_j + 1$. Then for any $0 \neq b \in Z^m$, $B = \Sigma_{i=-\infty}^{\infty}[\alpha^i b]_p$ is a direct sum on which α acts as a discrete bernoulli shift.*

Proof. We show $B = \Sigma_{i=-\infty}^{\infty}[\alpha^i b]_p$ is actually a direct sum. For suppose we had

$$\sum_{i=n_1}^{n_2} c_i\alpha^i b = \sum_{i=n_1'}^{n_2'} c_i'\alpha^i b, \qquad c_i, c_i' \in \{0, 1, \cdots, p-1\}.$$

Combining and multiplying by an appropriate power of α, we obtain $\Sigma_{i=0}^n a_i\alpha^i b = 0$, where $a_i \in Z$, $|a_i| < p$, and $a_0a_n \neq 0$. Now

$$0 = \alpha^j\left(\sum_{i=0}^n a_i\alpha^i b\right) = \sum_{i=0}^n a_i\alpha^i(\alpha^j b),$$

and since by the irreducibility of α, $\{b, \alpha b, \cdots, \alpha^{m-1}b\}$ span a subgroup of finite index in Z^m, we must have $\Sigma_{i=0}^n a_i\alpha^i = 0$. Thus the characteristic polynomial $p(x)$ of α, which is also the minimal polynomial, must divide $f(x) = \Sigma_{i=0}^n a_i x^i$. However that is impossible by Lemma 2.

In the proof of the following lemma we will make repeated use of a theorem due to Montel [3; 33.2]: *Let* $f(z) = a_0 + a_1z + \cdots + a_nz^n$ *be a polynomial with complex coefficients and r an integer,* $1 \leqq r \leqq n$, *such that* $a_r \neq 0$. *Then at least r zeroes of* $f(z)$ *lie in the disk* $|z| < 1/(1 - Q_r^q)$, *where* $Q_r = N_r/(1 + N_r)$, $N_r = \max_{0\leqq j\leqq r-1}|a_j/a_r|$ *and* $q = 1/(n - r + 1)$.

2. Lemma. *Let* $\lambda_1, \lambda_2, \cdots, \lambda_k$ $(k \geqq 1)$ *be complex numbers arranged so that* $|\lambda_1| \geqq |\lambda_2| \geqq \cdots \geqq |\lambda_k|$. *Set* $p_j = [|\lambda_j|/2j] - 1$, $1 \leqq j \leqq k$, *where* $[\cdot]$ *denotes the greatest integer function. Assume* $p_k \geqq 1$. *Let* $f(z) = a_0 + a_1a + \cdots + a_nz^n$ *be any polynomial with integral coefficients* a_j *satisfying* $|a_j| \leqq \Pi_{i=1}^k p_i$. *Then* $\lambda_1, \cdots, \lambda_k$ *cannot all be zeroes of* $f(z)$; *in other words,* $(z - \lambda_1)(z - \lambda_2)\cdots(z - \lambda_k)$ *does not divide* $f(z)$ *in the ring* $\mathbf{C}[z]$ *of polynomials with complex coefficients.*

Proof. Consider the function

$$\omega(t) = \frac{1}{1 - \left(\dfrac{t}{t+1}\right)^q}, \qquad t > 0 \quad \text{and} \quad 0 < q \leqq 1.$$

$\omega'(t) \geqq 0$, so $\omega(t)$ is nondecreasing. Suppose now that for some polynomial $f(z)$ satisfying the conditions of the lemma, the conclusion fails; i.e. $(z - \lambda_1)(z - \lambda_2)\cdots(z - \lambda_k)$ divides $f(z)$. We claim then it must be the case that $|a_n| = 1$, $|a_{n-1}| \leqq p_1, \cdots, |a_{n-j}| \leqq p_1 \cdots p_j$, $0 \leqq j \leqq k$. For if

$$|a_{n-k+1}| > \begin{cases} p_1 \cdots p_{k-1}, & \text{if } k > 1 \\ 1, & \text{if } k = 1 \end{cases},$$

set $N_{k+1} = \max_{0\leqq j\leqq n-k}|a_j/a_{n-k+1}|$, so $N_{n-k+1} \leqq p_k$. By the remark that $\omega(t)$ is nondecreasing we may as well take $N_{n-k+1} = p_k$. Thus $Q_{n-k+1} = p_k/(1 + p_k)$ and by Montel's Theorem at most $k - 1$ zeroes lie outside the disk $|z| <$

$1/(1-(p_k/(1+p_k))^{1/k})$. But

$$\frac{1}{1-\left(\frac{p_k}{1+p_k}\right)^{1/k}}=\frac{(1+p_k)^{1/k}}{(1+p_k)^{1/k}-p_k^{1/k}}$$

$$=(1+p_k)^{1/k}[(1+p_k)^{(k-1)/k}+p_k^{1/k}(1+p_k)^{(k-2)/k}+\cdots+p_k^{k-1/k}]<k(1+p_k)<|\lambda_k|.$$

But if $(z-\lambda_1)(z-\lambda_2)\cdots(z-\lambda_k)$ divides $f(z)$, at least k zeroes of f satisfy $|z|\geqq|\lambda_k|$. Suppose inductively that $|a_{n-i}|\leqq p_1\cdots p_i$, $k-1\leqq i\leqq j+1$. We show $|a_{n-j}|\leqq p_1\cdots p_j$. Suppose on the contrary that $|a_{n-j}|>p_1\cdots p_j$. Define the polynomial $g_j(z)=f(p_{j+1}z)$. Applying Montel's Theorem to $g_j(z)=p_{j+1}^n a_n z^n+p_{j+1}^{n-1}a_{n-1}z^{n-1}+\cdots+a_n$, for $i>j$ we have

$$\left|\frac{p_{j+1}^{n-i}a_{n-i}}{p_{j+1}^{n-j}a_{n-j}}\right|=\left|\frac{a_{n-i}}{p_{j+1}^{i-j}a_{n-j}}\right|<\frac{p_1\cdots p_i}{p_1\cdots p_j}\frac{p_{j+1}\cdots p_i}{p_{j+1}^{i-j}}\leqq 1$$

so all but at most j zeroes of g_j satisfy

$$|z|<\frac{1}{1-\left(\frac{1}{2^{1/j+1}}\right)}=\frac{2^{1/j+1}}{2^{1/j+1}-1}<2(j+1).$$

(Here we are using that $p_1\geqq p_2\geqq\cdots\geqq p_k\geqq 1$.) Hence at most j zeroes of $f(z)$ lie outside the disk

$$|z|<\frac{2^{1/j+1}}{2^{1/j+1}-1}p_{j+1}<|\lambda_{j+1}|.$$

This contradicts the assumption $(z-\lambda_1)\cdots(z-\lambda_{j+1})$ divides $f(z)$. So we have established the claim. Now one final application of Montel's Theorem shows us that no such $f(z)$ can exist. For set $g_0(z)=f(p_1z)=p_1^n a_n z^n+p_1^{n-1}a_{n-1}z^{n-1}+\cdots+a_0$. Then

$$\left|\frac{p_1^{n-i}a_{n-i}}{p_1^n a_n}\right|=\left|\frac{a_{n-i}}{p_1^i a_n}\right|\leqq\frac{p_1p_2\cdots p_i}{p_1^i}\leqq 1$$

holds for $1\leqq i\leqq k$. For $k<i\leqq n$, the ratio on the left is trivially $\leqq 1$, and so all the zeroes of g_0 satisfy $|z|<2$, and consequently, all the zeroes of f lie in $|z|<2p_1<|\lambda_1|$, an impossibility.

3. Corollary. *The entropy $h(\alpha,Z^m)$ of α on Z^m can be approximated arbitrarily closely by the entropy of discrete bernoulli shifts in α^n, for large n. In other words, given $\varepsilon>0$ there is an integer n and a discrete bernoulli shift $B\subset Z^m$*

in α^n so that

$$0 < h(\alpha, Z^m) - \frac{1}{n} h(\alpha^n, B) < \varepsilon.$$

PROOF. We may assume that the characteristic polynomial of α is irreducible for otherwise we could find an α-invariant subgroup H of Z^m of finite index which decomposes into a direct sum of α-irreducible subgroups H_i $(1 \leqq i \leqq r)$, and we would have $h(\alpha, Z^m) = h(\alpha, H) = \Sigma_{i=1}^r h(\alpha, H_i)$.

Now $h(\alpha, Z^m) = \Sigma_{i=1}^k \log|\lambda_i|$ where $\{\lambda_1, \cdots, \lambda_k\}$ are the eigenvalues of α satisfying $|\lambda| > 1$, which we arrange so $|\lambda_1| \geqq |\lambda_2| \geqq \cdots \geqq |\lambda_k|$. This formula follows from the fact that $h(\alpha, Z^m) = h({}^t\alpha, \bar{T}^m)$ ([4]) along with Kolmogorov's formula for the entropy of an automorphism of the m-torus. Choose n so large that both (i) $|\lambda_k|^n \geqq 8k$ and (ii) $(k \log(4k))/n < \varepsilon$ are satisfied. By (i),

$$p_j = \left[\frac{|\lambda_j|^n}{2j}\right] - 1 \geqq \frac{|\lambda_j|^n}{4k}, \qquad 1 \leqq j \leqq k.$$

Set $p = \Pi_{j=1}^k p_j + 1$ and $B = \Sigma_{i=-\infty}^{\infty} [\alpha^{ni} b]_p = \bigoplus_{i=-\infty}^{\infty} [\alpha^{ni} b]_p$, where $0 \neq b \in Z^m$. Then

$$h(\alpha^n, B) = \sum_{i=1}^k \log p_i \geqq \sum_{i=1}^k \log|\lambda_i|^n - k \log(4k).$$

By (ii)

$$0 < h(\alpha, Z^m) - \frac{1}{n} h(\alpha^n, B) < \frac{k \log(4k)}{n} < \varepsilon.$$

REFERENCES

1. L. Fuchs, *Abelian Groups*, Hungarian Academy of Sciences, Budapest, 1958.

2. Y. Katznelson, *Ergodic automorphisms of $\bar{T}^m$ are Bernoulli shifts*, Israel J. Math. **10** (1971), 186–195.

3. M. Marden, *Geometry of Polynomials*, Mathematical Surveys Number 3, American Mathematical Society, Providence, Rhode Island, 1966.

4. J. Peters, *Entropy on discrete abelian groups*, Advances in Math. **33** (1979), 1–13.

5. M. Weiss, *Algebraic and other entropies of group endomorphisms*, Math. Systems Theory **8** (1975), 243–248.

DEPARTMENT OF MATHEMATICS
IOWA STATE UNIVERSITY
AMES, IOWA 50011 USA