ENTROPY BOUNDS FOR ENDOMORPHISMS COMMUTING WITH K ACTIONS

G. MORRIS AND T. WARD

ABSTRACT. Shereshevsky has shown that a shift–commuting homeomorphism from the two–dimensional full shift to itself cannot be expansive, and asked if such a homeomorphism can have finite positive entropy. We formulate an algebraic analogue of this problem, and answer it in a special case by proving the following: if $T : X \to X$ is a mixing endomorphism of a compact metrizable abelian group X, and T commutes with a completely positive entropy Z^2–action S on X by continuous automorphisms, then T has infinite entropy.

1. INTRODUCTION

Let $\Sigma = \{0, 1, \ldots, k-1\}^{\mathbb{Z}^2}$ be the full two–dimensional shift on k symbols, and let $h : \Sigma \to \Sigma$ be a shift–commuting continuous map (or *cellular automaton*) on Σ. Shereshevsky [13] has shown that h cannot act expansively, and has conjectured that the topological entropy of h must lie in $\{0, \infty\}$. A special case of this conjecture concerns the case where h is an endomorphism of the group structure on Σ (see Lemma 1 below). A natural algebraic version of Shereshevsky's problem is the following (notice that for $e > 1$ a mixing algebraic $\mathbb{N}^e$–action does not automatically have positive entropy).

Problem. If T is a positive entropy mixing $\mathbb{N}^e$–action on a compact abelian group, commuting with a completely positive entropy $\mathbb{Z}^d$–action, and $1 \le e \le d-1$, can T have finite entropy?

Here and below we restrict attention to metrizable compact groups, and use "entropy" to mean either topological entropy or entropy with respect to Haar measure (which is maximal for ergodic compact group endomorphisms by Berg's theorem [1]).

A related problem is *Lehmer's problem*, originally stated in [4]: if

$$p(x) = (x - \lambda_1) \ldots (x - \lambda_n)$$

is a monic polynomial in $\mathbb{Z}[x]$ with constant term ± 1, can the quantity

$$M(p) = \prod_{|\lambda_i| > 1} |\lambda_i|$$

be made arbitrarily close to 1? Lind [6] Theorem 9.3, has shown that if the answer to Lehmer's problem is "yes" then for every $r \in (0, \infty]$ there is an ergodic automorphism of a compact abelian group with entropy r, and in [5] that if the answer is

"no" then every ergodic automorphism of the infinite torus $\mathbb{T}^\infty$ must have infinite entropy.

The partial result we prove is the following.

Theorem 1. *Let $T : X \to X$ be a mixing endomorphism of the compact abelian group X, that commutes with a $\mathbb{Z}^2$–action S with completely positive entropy. Then T has infinite entropy.*

2. Notation and background

Following Lind in [5] we adopt the following terminology. An action U (of $\mathbb{N}$, or $\mathbb{Z}^2$ and so on) by monomorphisms of a countable discrete abelian group M is *ergodic, mixing, has positive entropy, completely positive entropy, infinite entropy* if and only if the dual action $\widehat{U}$ (of $\mathbb{N}$, or $\mathbb{Z}^2$ and so on) on the compact metrizable abelian group $X = \widehat{M}$ respectively is ergodic, mixing, has positive entropy, completely positive entropy, infinite entropy. If $N \leq M$ is a U–invariant subgroup, then the surjective homomorphism $\widehat{M} \to \widehat{N} = \widehat{M}/N^\perp$ dual to the inclusion $N \hookrightarrow M$ realizes the action $\widehat{V}$ on $\widehat{N}$ as a *factor* of the original action $\widehat{U}$ on $\widehat{M}$, where V denotes the action U restricted to N.

For example, in this terminology, $h(U \text{ on } M) \geq h(V \text{ on } N)$ is the statement corresponding to the observation that the entropy $h(\widehat{V})$ of the factor dynamical system $\widehat{V}$ is less than or equal to the entropy $h(\widehat{U})$ of $\widehat{U}$.

Since an ergodic endomorphism of a compact abelian group has completely positive entropy [11], if U is an ergodic monomorphism of a countable discrete group M, and $N \leq M$ is a U–invariant subgroup, then $U|_N$ has (completely) positive entropy.

Following Kitchens and Schmidt [3] there is an algebraic description of any $\mathbb{Z}^2 \times \mathbb{N}$–action on a compact abelian group X. Let $S_{(1,0)}$ and $S_{(0,1)}$ be generators for the $\mathbb{Z}^2$–action S on X, and let $T = T_1$ be the S–commuting generator of the $\mathbb{N}$–action on X. Then $\widehat{S_{(1,0)}}$, $\widehat{S_{(0,1)}}$ and $\widehat{T}$ are commuting monomorphisms of $M = \widehat{X}$, the first two of which are also surjective. By identifying the action of these three maps with multiplication by x, y, and t, the additive group M takes on the structure of an $\mathfrak{S}^+$–module, where $\mathfrak{S}^+ = \mathbb{Z}[x^{\pm 1}, y^{\pm 1}, t]$.

It will be useful later to construct the natural invertible extension of the endomorphism T. Let $\mathfrak{M}$ denote the set $\{t^k\}_{k \geq 0}$ of powers of t. This is a multiplicative subset of $\mathfrak{S}^+$, and the localisation $\mathfrak{S}^+_{\mathfrak{M}}$ is $\mathfrak{S} = \mathbb{Z}[x^{\pm 1}, y^{\pm 1}, t^{\pm 1}]$. The $\mathfrak{S}^+$–module M also has a localisation, $M_{\mathfrak{M}}$, which is an $\mathfrak{S} = \mathfrak{S}^+_{\mathfrak{M}}$–module. It follows that the third generator of the $\mathbb{Z}^3$–action corresponding by duality to the $\mathfrak{S}$–module $M_{\mathfrak{M}}$ is the natural invertible extension $\tilde{T}$ of T, and $h(\tilde{T}) = h(T)$ by Section 3.3 of [10]. An alternative description of the invertible extension is via tensor products: there is a canonical isomorphism of $\mathfrak{S}$–modules between $M_{\mathfrak{M}}$ and $M \otimes_{\mathfrak{S}^+} \mathfrak{S}$ by Theorem 4.4 of [9].

Similarly, a $\mathbb{Z}^2$–action by automorphisms of a compact abelian group X gives the dual group $M = \widehat{X}$ the structure of an $\mathfrak{R}$–module, where $\mathfrak{R} = \mathbb{Z}[x^{\pm 1}, y^{\pm 1}]$. We shall use the canonical inclusion $\mathfrak{R} \subset \mathfrak{S}^+$ without comment.

The $\mathbb{Z}^2$–action corresponding to the cyclic $\mathfrak{R}$–module $\mathfrak{R}/\mathfrak{p}$ (where $\mathfrak{p}$ is a prime ideal in $\mathfrak{R}$) is known to have completely positive entropy if and only if the ideal $\mathfrak{p}$ is principal and not generated by a polynomial of the form $x^a y^b \phi(x^c y^d)$, where ϕ is a cyclotomic polynomial [7], Section 6. More generally, the $\mathbb{Z}^2$–action corresponding

to the $\mathfrak{R}$–module M has completely positive entropy if and only if for every prime ideal $\mathfrak{p}$ associated with M the action corresponding to the cyclic module $\mathfrak{R}/\mathfrak{p}$ has completely positive entropy by [7], Theorem 6.5. Notice that the set of associated prime ideals of M as an $\mathfrak{R}$–module is identical to the set of associated primes of $M_{\mathfrak{M}}$ as an $\mathfrak{R}$–module, so that passing to the invertible extension of the transformation T does not affect the completely positive entropy condition on S.

3. Proof in a special case

The special case for which we first prove Theorem 1 is that in which the completely positive entropy $\mathbb{Z}^2$–action S has a particularly simple form: in general, the actions S and T make $M = \widehat{X}$ into an $\mathfrak{S}^+$–module; assuming that the actions take the form of Lemma 1 or Lemma 2 amounts to assuming that the module M is of the form $\mathfrak{S}^+/\mathfrak{q}$, and that the ideal $\mathfrak{q}$ is of the form $\langle t - g(x,y), f(x,y) \rangle$ for polynomials $g, f \in \mathfrak{R}$. In Lemma 1 we assume in addition that the polynomial f is a constant, and in Lemma 2 that f is not a constant.

Lemma 1. *Let $X = \widehat{\mathfrak{R}/\mathfrak{p}}$ and let S be the corresponding $\mathbb{Z}^2$–action on X. Let T be a mixing, S–commuting endomorphism of X. Assume that $\mathfrak{p} = \langle p \rangle$ for a rational prime p or $\mathfrak{p} = \{0\}$. Then $h(T) = \infty$.*

Proof. If $\mathfrak{p} = \langle p \rangle$ then $X = \mathbb{F}_p^{\mathbb{Z}^2}$, and the $\mathbb{Z}^2$–action S is the full two–dimensional shift on p symbols. It follows that $T : X \to X$ is an algebraic cellular automaton determined by a polynomial $g \in \mathbb{F}_p[x^{\pm 1}, y^{\pm 1}]$ as follows. If $g = \sum_{(a,b) \in G} c_{(a,b)} x^a y^b$, where $G \subset \mathbb{Z}^2$ is the (finite) support of g, then $T = T_g$ is determined by

$$(T\mathbf{x})_{(n,m)} = \sum_{(a,b) \in G} c_{(a,b)} x_{(a+n, b+m)}$$

(where addition is performed in $\mathbb{F}_p$). Notice that T_g is mixing if and only if g is non–constant since multiplication by g can have a non–trivial finite orbit if and only if g is constant. The case $G = \{0\}$ cannot therefore occur.

Assume first that the set $G \cup \{0\}$ does not lie on a line. We shall find a sequence $\{X_n\}_{n \in \mathbb{N}}$ of closed T_g–invariant subgroups of $X = \mathbb{F}_p^{\mathbb{Z}^2}$ such that for every $n \in \mathbb{N}$, $T|_{X_n}$ is an expansive map, and $\mathrm{Fix}_K(T|_{X_n}) \geq p^{Kn}$ for all $K, n \in \mathbb{N}$ (here Fix_K denotes the number of points with period K). Then the basic inequality

$$h(U) \geq \limsup_{K \to \infty} \frac{1}{K} \log \mathrm{Fix}_K(U) \tag{1}$$

for expansive maps U [2] applies to show that $h(T|_{X_n}) \geq \lim_{K \to \infty} \frac{1}{K} \log p^{nK} = n \log p$, so that as $n \to \infty$, $h(T) \geq h(T|_{X_n}) \to \infty$.

To construct the groups $\{X_n\}$, notice that since the points in $G \cup \{0\}$ do not lie on a line, we may find a line ℓ through 0, with rational slope, which has non–empty intersection with the interior (in $\mathbb{R}^2$) of the convex hull of $G \cup \{0\}$, and is not parallel to any of the faces of the convex hull of $G \cup \{0\}$. Since expansiveness of a continuous function on a compact metric space is a topological property, we may use any metric on $X = \mathbb{F}_p^{\mathbb{Z}^2}$ compatible with the product topology. For any $r \geq 0$, let $S(r)$ be the closed square in $\mathbb{R}^2$ with side length r, centre 0 and two sides parallel to ℓ. For any $\mathbf{x}, \mathbf{y} \in X$, let $\rho(\mathbf{x}, \mathbf{y}) = 0$ if $\mathbf{x} = \mathbf{y}$, and $\rho(\mathbf{x}, \mathbf{y}) = 2^{-I(\mathbf{x}, \mathbf{y})}$ if not, where

$$I(\mathbf{x}, \mathbf{y}) = \inf\{r \geq 0 \mid x_{\mathbf{n}} \neq y_{\mathbf{n}} \text{ for some } \mathbf{n} \in \mathbb{Z}^2 \cap S(r)\}.$$

Now choose a unit vector $\mathbf{v} \in \mathbb{R}^2$ normal to ℓ. Let $r' > 0$, $r'' > 0$ be the greatest distances, in the directions of $\mathbf{v}$ and $-\mathbf{v}$ respectively, between ℓ and a line parallel to ℓ meeting G (by construction, these lines meet G in exactly one point each: call these points $\mathbf{m}_1$ and $\mathbf{m}_2$). Now let $G = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_c\}$. Let $r''' > 0$ be the distance between adjacent points in $\ell \cap \mathbb{Z}^2$, and select a point $\mathbf{k} \in \ell \cap \mathbb{Z}^2 \backslash \{0\}$ closest to 0. For any $R > \max\{2r', 2r'', r'''\}$, and for any $n \in \mathbb{N}$ such that $n\mathbf{k}$ is distance strictly less than R from 0, put

$$X_n = \{\mathbf{x} = (x_\mathbf{n}) \in X \mid x_\mathbf{m} = x_{\mathbf{m}+n\mathbf{k}} \text{ for all } \mathbf{m} \in \mathbb{Z}^2\}.$$

Let ℓ_1 and ℓ_2 be the lines parallel to ℓ containing sides of the square $S(R)$. If $\rho(\mathbf{x}, \mathbf{y}) \leq 2^{-R}$ for any $\mathbf{x} \neq \mathbf{y}$ in X_n then $x_\mathbf{n} \neq y_\mathbf{n}$ for some $\mathbf{n}$ outside the interior of $S(R)$. Moreover, $\mathbf{n}$ cannot lie between ℓ_1 and ℓ_2 by construction. Since ℓ has rational gradient, there is a least real $R' \geq R$ and a line ℓ' parallel to ℓ and distance $R'/2$ from ℓ such that $x_{\mathbf{n}''} \neq y_{\mathbf{n}''}$ for some $\mathbf{n}'' \in \ell' \cap \mathbb{Z}^2$, so there exists $\mathbf{n}' \in S(R') \cap \mathbb{Z}^2$ such that $x_{\mathbf{n}'} \neq y_{\mathbf{n}'}$ and then $\rho(\mathbf{x}, \mathbf{y}) = 2^{-R'}$. By construction, we know that for $j = 1$ or 2, $x_{\mathbf{n}'+\mathbf{m}_i-\mathbf{m}_j} = y_{\mathbf{n}'+\mathbf{m}_i-\mathbf{m}_j}$ for all $i \in \{1, 2, \ldots, c\} \backslash \{j\}$.

It follows that $(T_g(\mathbf{x}))_{\mathbf{n}'-\mathbf{m}_j} \neq (T_g(\mathbf{y}))_{\mathbf{n}'-\mathbf{m}_j}$ for $j = 1, 2$. If $\rho(T_g(\mathbf{x}), T_g(\mathbf{y})) \leq 2^{-R}$ then, by the construction of X_n, $\rho(T_g(\mathbf{x}), T_g(\mathbf{y})) = 2^{-R'+2r_1}$ for some r_1 with $r' \leq r_1 \leq r''$. (We are assuming without loss of generality that $r' \leq r''$.)

So, inductively, we argue that if $2^{-R'+2r_1+\cdots+2r_k} = \rho(T_g^k(\mathbf{x}), T_g^k(\mathbf{y})) \leq 2^{-R}$ for some $k \in \mathbb{N}$ with $r' \leq r_i \leq r''$ for $i \leq k$, then

$$\rho(T_g^{k+1}(\mathbf{x}), T_g^{k+1}(\mathbf{y})) \leq 2^{-R} \implies \rho(T_g^{k+1}(\mathbf{x}), T_g^{k+1}(\mathbf{y})) = 2^{-R'+2r_1+\cdots+2r_{k+1}}$$

for some $r' \leq r_{k+1} \leq r''$. Eventually, we must get $R' - 2(r_1 + \cdots + r_k) < R$ for some $k \in \mathbb{N}$, which gives $\rho(T_g^k(\mathbf{x}), T_g^k(\mathbf{y})) > 2^{-R}$. So the map T_g restricted to X_n is expansive, with expansive constant $\delta = 2^{-R}$.

Notice that R (and hence $|n\mathbf{k}|$, and hence n) may be chosen arbitrarily large without affecting the expansiveness of T_g restricted to X_n.

We may therefore apply (1) to the map T_g restricted to X_n for all $n \geq 1$.

Since $\mathbb{F}_p$ is an integral domain, the convex hull of the support G_K of the polynomial defining T_g^K is given by scaling the convex hull of G by K, centred at 0.

Now $\mathbf{x} \in X$ is fixed by T_g^K if and only if

$$x_\mathbf{n} = \sum_{\mathbf{m} \in G_K} c_\mathbf{m}^{(K)} x_{\mathbf{n}+\mathbf{m}} \mod p$$

for suitable coefficients $c_\mathbf{m}^{(K)} \in \mathbb{F}_p$ and for all $\mathbf{n} \in \mathbb{Z}^2$. Let $\mathbf{k}' \in ((r' + r'')\mathbf{v} + \ell) \cap \mathbb{Z}^2$, and let ℓ'' be the line through 0 and $\mathbf{k}'$. Given $K, n \in \mathbb{N}$, let $R(K, n)$ be the semi–closed quadrilateral in $\mathbb{R}^2$ with vertices 0, $n\mathbf{k}$, $K\mathbf{k}'$, and $n\mathbf{k} + K\mathbf{k}'$ including only those border points in ℓ and ℓ''. A point $\mathbf{x}$ in X_n fixed by T_g^K may now be constructed by choosing $x_\mathbf{n}$ freely for all $\mathbf{n} \in R(K, n)$. This gives a total of $p^{C(K,n)}$ choices, where $C(K, n) = |R(K, n) \cap \mathbb{Z}^2| = KnC$ for some $C = C(1, 1) \geq 1$. It follows that

$$\text{Fix}_K(T_g \text{ on } X_n) \geq p^{|R(K,n)|} = p^{KnC} \geq p^{Kn}.$$

By (1), letting $K \to \infty$, we deduce that

$$h(T_g) \geq h(T_g \text{ on } X_n) \geq n \log p$$

for all n, so $h(T_g) = \infty$.

If $\{0\} \neq G \cup \{0\} \subset \ell$ for some line $\ell = \{\ldots, \mathbf{n}(-1), \mathbf{n}(0) = 0, \mathbf{n}(1), \ldots\} \subset \mathbb{Z}^2$ then we may write $\mathbb{Z}^2 = \bigcup_{i \in \mathbb{Z}} \ell_i$ and $\mathbb{F}_p^{\mathbb{Z}^2} = \prod_{i \in \mathbb{Z}} \mathbb{F}_p^{\ell_i}$ where each ℓ_i is some translate of $\ell = \ell_0$. For each $n \geq 1$ the subgroup

$$L_n = \prod_{i < -n} \{0\}^{\ell_i} \times \mathbb{F}_p^{\ell_{-n}} \times \cdots \times \mathbb{F}_p^{\ell_n} \times \prod_{i > n} \{0\}^{\ell_i}$$

is closed and T–invariant, so $h(T) \geq h(T|_{L_n}) = (2n+1)h(T|_{L_0})$. Let $\mathbf{m} \in \ell \backslash \{0\}$ be an end–point of the set $G \cup \{0\}$. Pick $\epsilon > 0$ with the property that if $\mathbf{x} = (x_{\mathbf{n}(j)}), \mathbf{y} = (y_{\mathbf{n}(j)})$ are points in $\mathbb{F}_p^{\ell}$, with $x_{\mathbf{n}(0)} \neq y_{\mathbf{n}(0)}$ then $\rho(\mathbf{x}, \mathbf{y}) > \epsilon$ for the natural metric on $\mathbb{F}_p^{\ell}$. That is, $\rho(\mathbf{x}, \mathbf{y}) = 2^{-L(\mathbf{x},\mathbf{y})}$ where $L(\mathbf{x}, \mathbf{y}) = \min\{|\mathbf{n}(i)| \mid x_{\mathbf{n}(j)} = y_{\mathbf{n}(j)} \forall |j| \leq |i|\}$ for $\mathbf{x} \neq \mathbf{y}$, and $\rho(\mathbf{x}, \mathbf{y}) = 0$ for $\mathbf{x} = \mathbf{y}$. It follows that for any $K \geq 1$, the set

$$S_K = \{\mathbf{x} \in \mathbb{F}_p^{\ell} \mid x_{\mathbf{n}} = 0 \text{ if } \mathbf{n} \notin \{0, \mathbf{m}, 2\mathbf{m}, \ldots, (K-1)\mathbf{m}\}\}$$

is (K, ρ, ϵ')–separated for all $0 < \epsilon' < \epsilon$, and $|S_K| = p^K$ (notice that T_g restricted to ℓ is permutative on the end–point $\mathbf{m}$). It follows that $h(T|_{L_0}) \geq \log p$, and so $h(T) \geq (2n+1)\log p$ for all n, hence $h(T_g) = \infty$.

If $\mathfrak{p} = \{0\}$, then T is defined by a polynomial $g \in \mathbb{Z}[x^{\pm 1}, y^{\pm 1}]$: $\widehat{T}(m) = g \cdot m$ in $\mathfrak{R}/\mathfrak{p} = \mathfrak{R}$. Since T is mixing, the polynomial g is not a constant, so for a large enough prime p, the reduction $\bar{g}$ of g mod p is a non–constant element of $\mathbb{F}_p[x^{\pm 1}, y^{\pm 1}]$, which therefore defines a mixing map $\bar{m} \to \bar{g} \cdot \bar{m}$ from $\mathfrak{R}/\langle p \rangle$ to $\mathfrak{R}/\langle p \rangle$ dual to a mixing endomorphism $\bar{T}$. The dual of the surjective map $\mathfrak{R} \to \mathfrak{R}/\langle p \rangle$ embeds a copy of $\mathbb{F}_p^{\mathbb{Z}^2}$ as a closed subgroup of $X = \mathbb{T}^{\mathbb{Z}^2}$, so it is clear from the separated set definition of topological entropy that $h(T) \geq h(\bar{T})$. On the other hand (by the choice of p above) $\bar{T}$ is mixing, so the first part of the proof applies to show that $h(\bar{T}) = \infty$. $\qquad\square$

The remaining possibility is that $\mathfrak{p} = \langle f \rangle$ for some non–constant non–cyclotomic irreducible polynomial f.

Lemma 2. *Let $X = \widehat{\mathfrak{R}/\mathfrak{p}}$ and let S be the corresponding $\mathbb{Z}^2$–action on X. Let T be a mixing, S–commuting endomorphism of X. Assume that $\mathfrak{p} = \langle f \rangle$ for a non–constant non–cyclotomic irreducible polynomial f. Then $h(T) = \infty$.*

Proof. In this case the group $X = \widehat{\mathfrak{R}/\langle f \rangle}$ is an infinite–dimensional connected group. Lemma 3.1 of [8] extends to this setting, and shows that if $X^{(\mathbb{Q})}$ is the group dual to $\mathfrak{R}/\langle f \rangle \otimes_{\mathbb{Z}} \mathbb{Q}$, then T extends to an endomorphism $T^{(\mathbb{Q})} = T \otimes_{\mathbb{Z}} 1 : X^{(\mathbb{Q})} \to X^{(\mathbb{Q})}$ with $h(T^{(\mathbb{Q})}) = h(T)$.

Write $\Sigma = \widehat{\mathbb{Q}}$ for the one–dimensional solenoid; the group $X^{(\mathbb{Q})}$ then has the following explicit description. Let P_1 and P_2 be a pair of parallel lines in $\mathbb{Z}^2$ with the property that P_1 and P_2 meet the support of the polynomial f in points, and they are the most widely separated lines amongst those normal to a fixed vector with that property. Let A denote the subset of points in $\mathbb{Z}^2$ that lie on P_1 or strictly between P_1 and P_2. Now $X^{(\mathbb{Q})}$ is a closed, shift–invariant subgroup of $\Sigma^{\mathbb{Z}^2}$, and by construction the map from $X^{(\mathbb{Q})}$ to Σ^A sending a point to its restriction to the co–ordinates in A is a group isomorphism. That is, a point in $X^{(\mathbb{Q})}$ is completely determined by the co–ordinates in A, and these may be chosen freely.

So, as a group

$$X^{(\mathbb{Q})} \cong \Sigma^A. \tag{2}$$

Choose a finite set $Q \subset A$ and a vector $\mathbf{n} \in \mathbb{Z}^{\mathbf{2}}$ with the property that the sets

$$\ldots, Q - \mathbf{n}, Q, Q + \mathbf{n}, Q + 2\mathbf{n}, \ldots$$

are all disjoint, and $A = \bigcup_{k \in \mathbb{Z}} Q + k\mathbf{n}$. Then by (2), $X^{(\mathbb{Q})} \cong \left(\Sigma^Q\right)^{\mathbb{Z}}$; the endormorphism $T^{(\mathbb{Q})} : X^{(\mathbb{Q})} \to X^{(\mathbb{Q})}$ under this isomorphism becomes the map dual to the infinite matrix

$$B = \begin{bmatrix} \ddots & \ddots & \ddots & \ddots & & & \\ & A_1 & A_2 & \ldots & A_r & & \\ & & A_1 & A_2 & \ldots & A_r & \\ & & & A_1 & A_2 & \ldots & A_r \\ & & & \ddots & \ddots & \ddots & \ddots \end{bmatrix} \tag{3}$$

where each matrix A_i is a $|Q| \times |Q|$ rational matrix (the elements of $\widehat{\Sigma^Q} = \mathbb{Q}^Q$ are written here as column vectors of length $|Q|$, and the dual of the direct product $\left(\Sigma^Q\right)^{\mathbb{Z}}$ is the direct sum $\bigoplus_{\mathbb{Z}} \widehat{\Sigma^Q}$). We also know that $T^{(\mathbb{Q})}$ is ergodic, so if Lehmer's problem were known to have the answer "no", we could deduce at once that $h(T^{(\mathbb{Q})}) = \infty$ by [5]. However, the special band structure of the matrix in (3) allows us to compute the entropy directly.

Write Γ for the group $\bigoplus_{\mathbb{Z}} \mathbb{Q} \cong \bigoplus_{\mathbb{Z}} \mathbb{Q}^Q = \widehat{\left(\Sigma^Q\right)^{\mathbb{Z}}}$ (where elements of $\mathbb{Q}^Q$ are written as column vectors), and consider the action of the matrix B on Γ thought of as an infinite–dimensional vector space over $\mathbb{Q}$.

Assume first that there is some vector $\gamma \in \Gamma \backslash \{0\}$ with the property that some polynomial in B annihilates γ. Then the subspace $W \leq \Gamma$ spanned by $\{B^k \gamma\}_{k \in \mathbb{N}}$ is finite–dimensional. Let $\sigma : \Gamma \to \Gamma$ denote the shift operator. Since W is finite–dimensional, there exists $k \geq 1$ such that the subspaces

$$W, \sigma^{k|Q|}W, \sigma^{2k|Q|}W, \ldots, \sigma^{(K-1)k|Q|}W$$

are all linearly independent for any $K \geq 1$, and are all B–invariant. Moreover, from the band structure of the matrix B, the action of B restricted to the subspace $\sigma^{j|Q|}W$ is isomorphic to the action of B on W. Finally, the B–invariant subspace $W \oplus \cdots \oplus \sigma^{(K-1)k|Q|}W$ determines a factor of the action of $T^{(\mathbb{Q})}$ on $X^{(\mathbb{Q})}$, so

$$h(T) \geq h(B \text{ on } \bigoplus_{j=0,\ldots,K-1} \sigma^{j|Q|}W) = \sum_{j=0}^{K-1} h(B \text{ on } W) = K \cdot h(B \text{ on } W).$$

On the other hand, B acting on W is itself dual to a non–trivial factor of $T^{(\mathbb{Q})}$, and so has positive entropy. Since K was arbitrary, we deduce that $h(T) = \infty$.

If there is no vector $\gamma \in \Gamma \backslash \{0\}$ which is annihilated by some polynomial in B, then there is a vector $\gamma \in \Gamma$ with the property that the subspace spanned by $\{B^k \gamma\}_{k \in \mathbb{Z}}$ is a copy of $\sum_{\mathbb{Z}} \mathbb{Q}$ on which B acts as the shift. Dual to this subgroup is a factor of $T^{(\mathbb{Q})}$ isomorphic to the full shift with infinite alphabet Σ, so $h(T) = \infty$ again. $\qquad\square$

4. GENERAL CASE

For the general case we use results of Schmidt on how "big" a group must be in order to carry a completely positive entropy $\mathbb{Z}^2$–action. Let X, S, T be as in Theorem 1. The additive group $M = \widehat{X}$ then has the structure of an $\mathfrak{S}^+$–module. By tensoring M with $\mathfrak{S}$ we may pass to the natural invertible extension of the map

T, and so assume that M is an $\mathfrak{S}$–module. Since $\mathfrak{S}$ is Noetherian as a ring, the module M has associated primes (see Theorem 6.1 in [9]). Let $\mathfrak{q} \subset \mathfrak{S}$ be a prime ideal associated to M, so there is an $m \in M$ such that

$$\mathfrak{q} = \{f \in \mathfrak{S} \mid f \cdot m = 0_M\}.$$

The map $f \mapsto f \cdot m$ from $\mathfrak{S}$ to M has as image an isomorphic copy of $\mathfrak{S}/\mathfrak{q}$, so the original $\mathbb{Z}^2 \times \mathbb{Z}$–action has a factor of the form $X = X_{\mathfrak{S}/\mathfrak{q}}$.

Some terminology: a subgroup $\Gamma \leq \mathbb{Z}^3$ is *primitive* if the quotient $\mathbb{Z}^3/\Gamma$ is torsion–free.

First assume that the ring $\mathfrak{S}/\mathfrak{q}$ has positive characteristic p. Then, since X carries a $\mathbb{Z}^2$–action with (completely) positive entropy, by Proposition 24.1 of [12] the entropy "dimension" s of the $\mathbb{Z}^3$–action generated by S and T is 2 or 3. So, by Proposition 8.2 of [12] there is a primitive subgroup $\Gamma \leq \mathbb{Z}^3$ with rank s, and a finite set $Q \subset \mathbb{Z}^3$ such that $Q \cap Q + \mathbf{m} = \emptyset$ for all $\mathbf{m} \in \Gamma \backslash \{\mathbf{0}\}$, and the projection from $X \subset \mathbb{F}_p^{\mathbb{Z}^3}$ to the co–ordinates in $\bar{\Gamma} = \Gamma + Q$ is a continuous group isomorphism. Under this isomorphism, we see that if $s = 3$ the automorphism T is a full shift with infinite alphabet, or if $s = 2$, is an invertible extension of a mixing algebraic cellular automaton of a full 2–dimensional full shift. In the former case the entropy is clearly infinite, and in the latter case it is infinite by Lemma 1.

Now assume that the ring $\mathfrak{S}/\mathfrak{q}$ has zero characteristic. For simplicity, let $\mathfrak{S}^{(\mathbb{Q})} = \mathfrak{S} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[x^{\pm 1}, y^{\pm 1}, t^{\pm 1}]$, and extend T as before (start of proof of Lemma 2) to an automorphism $T^{(\mathbb{Q})}$ of $X^{(\mathbb{Q})} = \widehat{\mathfrak{S}^{(\mathbb{Q})}/\mathfrak{q}}$. Since $X^{(\mathbb{Q})}$ carries a $\mathbb{Z}^2$–action with completely positive entropy, by Proposition 24.3 of [12] the entropy "dimension" s of the $\mathbb{Z}^3$–action generated by S and T is 1 or 2. By Lemma 8.3 of [12] there is a primitive subgroup $\Gamma \leq \mathbb{Z}^3$ with rank s, and a finite set $Q \subset \mathbb{Z}^3$ such that $Q \cap Q + \mathbf{m} = \emptyset$ for all $\mathbf{m} \in \Gamma \backslash \{\mathbf{0}\}$, and the projection from $X \subset \mathbb{T}^{\mathbb{Z}^3}$ to the co–ordinates in $\bar{\Gamma} = \Gamma + Q$ is a continuous group isomorphism. Under this isomorphism, if $s = 1$ then $T^{(\mathbb{Q})}$ is the invertible extension of an endomorphism of the infinite–dimensional solenoid $(\widehat{\mathbb{Q}})^{\Gamma}$, with the band structure of (3). It follows by the argument used in the proof of Lemma 2 that the entropy must be infinite.

If $s = 2$ the automorphism $T^{(\mathbb{Q})}$ is the invertible extension of a shift–commuting endomorphism of the full two–dimensional shift with solenoid alphabet, which may be treated similarly. Notice that the dual group is isomorphic to $\sum_{\mathbb{Z}^2} \mathbb{Q} = \sum_{\mathbb{Z}} \sum_{\mathbb{Z}} \mathbb{Q}$ (that is, choose a basis for the dual group using vertical strips). The map $T^{(\mathbb{Q})}$ is then dual to an infinite matrix of the form

$$C = \begin{bmatrix} \ddots & \ddots & \ddots & \ddots & & & \\ & A_1 & A_2 & \dots & A_r & & \\ & & A_1 & A_2 & \dots & A_r & \\ & & & A_1 & A_2 & \dots & A_r \\ & & & \ddots & \ddots & \ddots & \ddots \end{bmatrix} \tag{4}$$

in which each submatrix A_i is finite, but the entries in each A_i are themselves bi–infinite rational matrices. Exactly as in the proof of Lemma 2, if there is a vector $\gamma \neq 0$ with the property that some polynomial in C annihilates γ, then we may find arbitrarily many finite–dimensional C–invariant subspaces, on each of which C restricts to a fixed positive entropy map. If there is no such vector, then there is a vector γ with the property that the factor of the original dynamical system

corresponding to the C–invariant subspace spanned by $\{C^k\gamma\}_{k\in\mathbb{Z}}$ is a full shift with alphabet $\widehat{\mathbb{Q}}^{\mathbb{Z}}$. In both cases we see that the entropy is infinite. $\square$

Remark 1. (1) If the words "commutes with" are replaced by "carries" in Theorem 1, the result no longer holds. In the disconnected case, there are mixing endomorphisms of the group $\mathbb{F}_p^{\mathbb{Z}^2}$ with entropy $\log p$. In the connected case, the result remains true if the answer to Lehmer's problem is "no".

(2) In the proof of Lemma 2, both cases occur for the possible dimensions of invariant subspaces of Γ. Let $f = \langle 1 + x + y \rangle$ and choose $P_1 = \{(a,b) \mid a = b\}$, $P_2 = \{(a,b) \mid a = b - 2\}$, $Q = \{(0,0),(0,1)\}$ and $\mathbf{n} = (1,1)$. Then the group $X^{(\mathbb{Q})}$ is given by

$$X^{(\mathbb{Q})} = \{\mathbf{x} \in \hat{\mathbb{Q}}^{\mathbb{Z}^2} \mid x_{(n,m)} + x_{(n+1,m)} + x_{(n,m+1)} = 0 \text{ for all } n,m\},$$

with the $\mathbb{Z}^2$–action S given by the shift. If the endomorphism T is defined by $(T(\mathbf{x}))_{(a.b)} = x_{(a,b+1)}$, then the corresponding infinite matrix consists of a diagonal line of 1's shifted one away from the diagonal, which has no finite–dimensional invariant subspaces. On the other hand, if T is defined by $(T(\mathbf{x}))_{(a.b)} = 2x_{(a,b)}$, the corresponding infinite matrix has infinitely many 1–dimensional invariant subspaces.

References

[1] K. Berg, Convolution of invariant measures, maximal entropy, *Math. Sys. Th.* **3** (1969), 146–151.

[2] J.P. Conze, Points périodiques et entropie topologique, *Comptes Rendus Acad. Sci. Paris, Ser. A* **267** (1968), 149–152.

[3] B. Kitchens & K. Schmidt, Automorphisms of compact groups, *Ergodic Theory and Dynamical Systems* **9** (1989), 691-735.

[4] D.H. Lehmer, Factorisation of certain cyclotomic functions, *Annals of Math.* **34** (1933), 461–479.

[5] D.A. Lind, Ergodic automorphisms of the infinite torus are Bernoulli, *Israel J. of Math.* **17** (1974), 162–168.

[6] D.A. Lind, The structure of skew products with ergodic group automorphisms, *Israel J. of Math.* **28** (1977), 205-248.

[7] D.A. Lind, K. Schmidt & T. Ward, Mahler measure and entropy for commuting automorphisms of compact groups, *Inventiones Math.* **101**, (1990) 593–629.

[8] D.A. Lind & T. Ward, Automorphisms of solenoids and p-adic entropy, *Ergodic Theory and Dynamical Systems* **8** (1988), 411–419.

[9] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, Cambridge, 1986.

[10] V.A. Rokhlin, Exact endomorphisms of a Lebesgue space, *American Math. Society Transl.* (2) **39** (1964), 1–36.

[11] V.A. Rokhlin, Metric properties of endomorphisms of compact commutative groups *American Math. Society Transl.* (2) **64** (1967), 244–252.

[12] K. Schmidt, *Dynamical Systems of Algebraic Origin*, Birkhäuser, Basel, 1995.

[13] M.A. Shereshevsky, Expansiveness, entropy and polynomial growth for groups acting on subshifts by automorphisms, *Indag. Mathem.* **4** (1993), 203–210.

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, U.K.
E-mail address: `t.ward@uea.ac.uk`