Dynamical constraints on group actions

Gary Morris

A thesis submitted at the University of East Anglia
in partial fulfilment of the requirements for the degree of
Doctor of Philosophy.

July 1998

To my family, Pat, Percy, Chyrisse, and Shaun.

Acknowledgements

I would like to thank my supervisor, Tom Ward, for his technical expertise, proof reading, encouragement, and patience. I acknowledge the financial support of the E.P.S.R.C. for the three years of this research.

Abstract

We investigate whether groups of polynomial growth can act expansively by continuous maps on the circle. Also, whether the semi-group $\mathbf{Z}^+$ can act with finite positive entropy by maps determined by Laurent polynomials on the full two dimensional two shift (two dimensional algebraic cellular automata). We go on to consider the more abstract setting of a mixing $\mathbf{Z}^+$-action by continuous group endomorphisms which commutes with a completely positive entropy $\mathbf{Z}^2$-action on a compact metric group. We extend cellular automata results of Hedlund from one to two dimensions and from full-shifts to subshifts. This is partly preparation for proving entropy preservation by certain cellular automata restricted to subshifts.

There are two appendices. The first is a short paper with Ward on mixing properties of invertible extensions that is not related to the material in the thesis. The second is a paper with Ward that is closely related to the work in Chapter 3.

Chapter 1 is standard material that may be found in the texts of Walters or Petersen for example. Chapter 2 contains original work on expansive actions on the circle, though it is likely that some of the results are known but unpublished. One important example of a solvable group action is due to Mozes (unpublished). Chapter 3 contains original work, inlcuding special cases of a conjecture by Shereshevsky. It also contains a connected analogue of this conjecture, and the results here are joint work with Ward. Chapters 4 and 5 are original. In these chapters, some of Hedlund's work has been generalised and some of these generalisations are routine.

Contents

Chapter 1

Introduction

We address some aspect of the question of what constraints are imposed on a group, or its actions, by dynamical considerations.

Throughout the text $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{I}$, and $\mathbf{S}$ will denote the natural numbers, integers, rational numbers, real numbers, complex numbers, the closed unit interval, and the unit circle respectively. By $\mathbf{Z}^+, \mathbf{Q}^+$, and $\mathbf{R}^+$ we mean the non-negative members (includes zero).

All spaces will always be assumed to be infinite. Topological spaces will always be assumed to be metrizable. Measure spaces will always be assumed to be Lebesgue.

1.1 Group actions

We use the abbreviation m.p.t. for measure preserving transformation. We shall be interested in *actions* of a group (or semi-group) G on two kinds of spaces: *topological actions*, where G acts on a compact metric space X by homeomorphisms (continuous maps), and *measurable actions*, where G acts on a probability space $(X, \mathcal{B}, \mu)$ by invertible m.p.t's. (m.p.t's. respectively). Thus, a topological action of G is a (semi) group homomorphism $\alpha : G \to \mathrm{Cts}(X)$ where $\mathrm{Cts}(X)$ is the (semi) group of continuous maps of X (if G is a group we may use $\mathrm{Homeo}(X)$, the group of homeomorphisms of X); a measurable action is a (semi) group homomorphism $\beta : G \to \mathrm{MPT}(X)$ where $\mathrm{MPT}(X)$ is the (semi) group of measure-preserving transformations of the measure space X. If $G \cong \mathbf{Z}^d$ (or $\mathbf{N}^d$) for some $d \in \mathbf{N}$ then we write $\alpha : \mathbf{m} \to \alpha^{\mathbf{m}}$, otherwise we write $\alpha : g \to \alpha_g$, and similarly for β.

Notation 1.1 For $i = 1, 2$ and sets X_i carrying G-actions $\gamma_i : G \to \mathrm{Cts}(X_i)$ (or $\mathrm{MPT}(X_i)$) we denote the systems by (X_i, γ_i) and reserve the notation $T : (X_1, \gamma_1) \to (X_2, \gamma_2)$ for a map $T : X_1 \to X_2$ to mean that $(\gamma_2)_g(T(x)) = T((\gamma_1)_g(x))$ for all $g \in G$ and $x \in X_1$. In this case we say that T is a (measure-preserving/continuous/etc) *map from* (X_1, γ_1) *to* (X_2, γ_2) (if the actions are measurable, this intertwining condition is only required to hold almost everywhere). Clearly, if $(X_1, \gamma_1) = (X_2, \gamma_2) = (X, \gamma)$ then $T : X \to X$ is a (measure-preserving/etc) *map of* (X, γ) means that T commutes with γ_g for all $g \in G$.

Definition 1.1 If, for $i = 1, 2$, X_i are topological spaces, topological groups, or measure spaces respectively, and $T_i : X_i \to X_i$ are continuous maps, continuous group homomorphisms, or measure-preserving transformations respectively then we say that (X_1, T_1) is, respectively, *topologically conjugate to, topological group conjugate to,* or *measure conjugate to* (X_2, T_2) if there is homeomorphism, homeomorphic group isomorphism, or invertible measure-preserving transformation respectively, $\theta : X_1 \to X_2$ such that $\theta \circ T_1 = T_2 \circ \theta$. Two Γ-actions by the appropriate respective morphisms are defined to be *topologically conjugate, topological group conjugate,* or *measure conjugate* when, for each $\gamma \in \Gamma$, the respective images of γ under the two Γ-actions are appropriately conjugate for the same conjugating map.

1.2 Expansiveness

Definition 1.2 A topological action $\alpha : G \to \mathrm{Homeo}(X, \rho)$ is *expansive* if there is a constant $\delta > 0$ with the property that for any pair of points $x \neq y \in X$, there is a group element $g \in G$ for which $\rho(\alpha_g(x), \alpha_g(y)) > \delta$. We call such a δ an *expansive constant for the action.*

From now on G will always be a finitely generated group whereas Γ will be any (not necessarily countable) group. By $G = \langle g_1, \ldots, g_n \rangle$ we will mean that the group

G is generated by the elements $g_1, \ldots, g_n$ and no proper subset of these elements generates it. We reserve the notation $\langle\langle \alpha_{g_1}, \ldots, \alpha_{g_n} \rangle\rangle$ to refer to the group $\alpha(G)$ of maps in the image of the G-action α. Note that G and $\alpha(G)$ are isomorphic exactly when the action α is faithful (has trivial kernel).

Let $G = \langle g_1, ..., g_n \rangle$. For arbitrary $g \in G$ let

$$\|g\| = \min\{k \in \mathbf{N} : g = h_1 \ldots h_k \text{ where } h_i \in \{id, g_1^{\pm 1}, \cdots, g_n^{\pm 1}\} \text{ for } i = 1, \cdots, k\};$$

(the inclusion of the identity id in the choices for the h_i is optional for our purposes, the only difference it makes is that $\|id\| = 1$ instead of 2). Notice that $\| \cdot \|$ is dependent upon the generating set. For a natural number m define the *ball*

$$\mathrm{B}(m) = \{g \in G : \|g\| \leq m\}$$

and let $b(m)$ be the cardinality of $\mathrm{B}(m)$.

If there exist constants $A, C > 0$ and $k \in \mathbf{N}$ such that,

$$Am^k \leq b(m) \leq Cm^k \text{ for all } m \in \mathbf{N} \tag{1}$$

for some finite generating set, then the same property holds (with different A and C) for <u>any</u> generating set (see Bass [4]), so we may consistently make the following definition.

Definition 1.3 The group G is said to have *polynomial growth of degree k* if there exist constants $A, C > 0$ such that (1) holds.

See Bass [4], Gromov [19], Shereshevsky [61] for discussions of polynomial growth. Any finitely generated abelian group, and in particular the additive group $\mathbf{Z}^d$ for $d \in \mathbf{N}$, is clearly of polynomial growth. Wolf [67] showed that any finitely generated nilpotent group has polynomial growth. Gromov extended this to finitely generated groups containing a nilpotent subgroup of finite index along with proving the converse.

Theorem 1.1 *Let G be a finitely generated group. Then G has a nilpotent subgroup of finite index if and only if G has polynomial growth.*

Proof. See Gromov [19].

We are interested in to what extent certain characteristics, such as growth, of the acting group are determined by dynamical constraints, such as expansiveness, of the action upon the space.

For example it is known, Reddy [51], that a single homeomorphism (a continuous $\mathbf{Z}$-action by homeomorphisms) cannot act expansively on the unit circle, $\mathbf{S}$, while there are solvable group expansive actions on $\mathbf{S}$ (the example, for instance, of Theorem 2.3). A natural problem is the following.

Problem 1.1 *Can a group of polynomial growth act expansively on* $\mathbf{S}$*?*

By Theorem 1.1, if the answer is "no", then it is enough to show that nilpotent groups cannot act expansively on $\mathbf{S}$.

Along the way to partial results (for the specific case of $\mathbf{Z}^d$-actions) we show that, for an arbitrary (possibly uncountable) group Γ, if a Γ-action α by homeomorphisms of $\mathbf{S}$ is expansive then the set of points of $\mathbf{S}$ that are fixed by non-trivial members of $\alpha(\Gamma)$ is dense in $\mathbf{S}$ (the converse does not hold). We also provide an answer to this problem for what we call finitely generated Möbius groups, and discuss some geometrically natural actions on the circle.

1.3 Topological entropy and commuting maps

Recall that $\{Q_n\}_{n\in\mathbf{N}}$ is defined to be a *Følner sequence in* $\mathbf{Z}^d$ exactly when Q_n is a finite subset of $\mathbf{Z}^d$ for all $n \in \mathbf{N}$ and

$$\lim_{n\to\infty} \frac{|Q_n \bigtriangleup (\mathbf{m} + Q_n)|}{|Q_n|} = 0 \text{ for all } \mathbf{m} \in \mathbf{Z}^d.$$

Definition 1.4 Let $\alpha : \mathbf{Z}^d \to \mathrm{Homeo}(X, \rho)$ be a continuous $\mathbf{Z}^d$-action on a compact metric space. Let $\{Q_n\}_{n\in\mathbf{N}}$ be a *Følner sequence in* $\mathbf{Z}^d$ such that $\bigcup_{n\in\mathbf{N}} Q_n = \mathbf{Z}^d$ and, for all $n \in \mathbf{N}$, let $Q_n \subset Q_{n+1}$. A set $E \subset X$ is (Q_n, ρ, δ)*-spanning* for α if there exists, for every $x \in X$, an $x' \in E$ such that $\rho(\alpha^{\mathbf{m}}(x), \alpha^{\mathbf{m}}(x')) < \delta$ for all $\mathbf{m} \in Q_n$, and $D \subset X$ is (Q_n, ρ, δ)*-separated* if there exists, for every pair $x \neq x'$ in D, an $\mathbf{m} \in Q_n$

with $\rho(\alpha^{\mathbf{m}}(x), \alpha^{\mathbf{m}}(x')) \geq \delta$. Let $r_{Q_n}(\rho,\delta)$ be the smallest cardinality of a (Q_n,ρ,δ)-spanning set, and $s_{Q_n}(\rho,\delta)$ the largest cardinality of a (Q_n,ρ,δ)-separated set. Notice that both of these quantities are finite by compactness. Define the *(topological) entropy*[1], $h(\alpha)$, of α on X to be

$$\begin{aligned} h(\alpha) &= \lim_{\delta\to 0}\limsup_{n\to\infty}\frac{1}{|Q_n|}\log r_{Q_n}(\rho,\delta) = \lim_{\delta\to 0}\limsup_{n\to\infty}\frac{1}{|Q_n|}\log s_{Q_n}(\rho,\delta) \\ &= \lim_{\delta\to 0}\liminf_{n\to\infty}\frac{1}{|Q_n|}\log r_{Q_n}(\rho,\delta) = \lim_{\delta\to 0}\liminf_{n\to\infty}\frac{1}{|Q_n|}\log s_{Q_n}(\rho,\delta). \end{aligned}$$

To see that the limits above are equal, and independent of the Følner sequence used, we refer the reader to the proof of Proposition 13.1 in Schmidt [60] and Shereshevsky [61].

The definition for the topological entropy of a $(\mathbf{Z}^+)^d$-action by continuous maps of (X,ρ) is analogous to that of a $\mathbf{Z}^d$-action, replacing all occurrences of $\mathbf{Z}^d$ by $(\mathbf{Z}^+)^d$.

We prove (cf. Theorem 3.1) that if $T: X \to X$ is a uniformly continuous surjective group endomorphism (that is, a $\mathbf{Z}^+$-action) of a metric (not necessarily compact) group (X,ρ) with translation invariant metric ρ (in which case $h(T)$ can be defined consistently with Definition 1.4) then $h(T) \geq \log(|\ker(T)|)$ with $h(T) = \infty$ if $|\ker(T)| = \infty$.

Definition 1.5 Fix $d, k \in \mathbf{N}$. Put $\mathcal{S} = \mathcal{S}(k) = \mathbf{Z}_{/k} = \mathbf{Z}/k\mathbf{Z} = \{0,\cdots,k-1\}$. Let $\Omega = \Omega_k(d) = \mathcal{S}^{\mathbf{Z}^d} = \prod_{\mathbf{m}\in\mathbf{Z}^d}\mathcal{S}$ be the Cartesian product of $\mathbf{Z}^d$ copies of $\mathcal{S}$ with the product topology ($\mathcal{S}$ itself has the discrete topology). A typical element $\mathbf{x} \in \Omega$ is given by $\mathbf{x} = (x_{\mathbf{n}})_{\mathbf{n}\in\mathbf{Z}^d}$ where $x_{\mathbf{n}} \in \mathcal{S}$ for all $\mathbf{n} \in \mathbf{Z}^d$. The set Ω becomes a topological group under the obvious coordinate-wise addition mod k. Thus Ω is a compact metric group under any metric for which elements of Ω are close together whenever their coordinates agree over a large bounded region containing the origin in $\mathbf{Z}^d$. We define the *shift*, $\sigma{:}\mathbf{Z}^d \to \mathrm{Homeo}(\Omega)$, to be the $\mathbf{Z}^d$-action given by $(\sigma^{\mathbf{m}}(\mathbf{x}))_{\mathbf{n}} = x_{\mathbf{n}+\mathbf{m}}$ for all $\mathbf{m},\mathbf{n} \in \mathbf{Z}^d$ and for all $\mathbf{x} \in \Omega$. Note that the shift is also a group automorphism. We call (Ω,σ) the *full d-dimensional k-shift.*

[1]This gives the same value as the open cover definition of topological entropy, see for example Proposition 13.1 of Schmidt [60].

Our second problem concerning constraints made upon an acting group by dynamical considerations, a conjecture made by Shereshevsky, is the following.

Problem 1.2 *It is conjectured that the group* $\mathbf{Z}$ *cannot act by continuous shift-commuting maps with finite positive entropy on the full two-dimensional* 2*-shift.*

We initially confirm the conjecture for the algebraic case (that is, where the map T of (Ω, σ) is a continuous homomorphism of the group structure on Ω) of Shereshevsky's conjecture (for which d, the dimension of the shift, is equal to 2) with Ω_2 replaced by Ω_p for general prime p. We then use this result in the joint paper [42] with Ward to solve the following related problem by Ward for the particular case $e = 1, d = 2$ (see Definition 1.7 for mixing).

Definition 1.6 A measurable $\mathbf{Z}^d$-action α on a probability space $(X, \mathcal{B}, \mu)$ is a *K-action* or, equivalently, has *completely positive entropy* if $h_\mu(\alpha, \mathcal{P}) > 0$ for any finite measurable partition $\mathcal{P}$ such that $H_\mu(\mathcal{P}) > 0$ *(see Definition 1.8 below for measure–theoretic entropy).*

Problem 1.3 *Can a mixing action of* $\mathbf{Z}^e$ *by continuous automorphisms of a compact metric abelian group that commutes with a* K*-action of* $\mathbf{Z}^d$ *by continuous automorphisms have finite positive entropy if* $e \leq d - 1$*?*

Definition 1.7 Let G be a countable group. Let $(X, \mathcal{B}, \mu)$ be a probability space and let $L^2(X, \mu)$ be the space of square integrable functions on $(X, \mathcal{B}, \mu)$. The G-action α is *ergodic* if any $f \in L^2(X, \mu)$ with $f(\alpha_g(x)) = f(x)$ a.e. for all $g \in G$ is constant a.e. We also then say that μ is an *ergodic measure* of $(X, \mathcal{B}, \alpha)$.

Let $\{g_n\}_{n \in \mathbf{N}}$ be an enumeration of G. For a real–valued expression $E(g)$ put

$$\lim_{g \to \infty} E(g) = \lim_{n \to \infty} E(g_n),$$

and note that the meaning is independent of the particular enumeration of G. The action α is *(strongly) mixing* if

$$\lim_{g \to \infty} \mu(B \cap \alpha_g(C)) = \mu(B)\mu(C) \text{ for all } B, C \in \mathcal{B}.$$

For a continuous group endomorphism of a compact group ergodicity and mixing coincide (see, for example, Theorem 1.28 in Walters [64]).

1.4 Measure-theoretic entropy

Definition 1.8 A *(measurable) partition* of $(X, \mathcal{B}, \mu)$ is a disjoint finite collection of non-empty measurable sets (the positive measure ones are called the *atoms* of the partition) whose union is X.

If $\mathcal{P}_1 = \{A_{1i} : i \in I_1\}, \ldots, \mathcal{P}_n = \{A_{ni} : i \in I_n\}$ are partitions, indexed by sets $I_1, \ldots, I_n$ respectively then their *join* is the partition whose elements are all those non-empty sets of the form $\bigcap_{j=1}^{n} A_{ji_j}$ where $i_j \in I_j$ for $j = 1, \ldots, n$, and is denoted by $\bigvee_{j=1}^{n} \mathcal{P}_j$.

For a measurable partition $\mathcal{P} = \{X_1, \ldots, X_m\}$ of $(X, \mathcal{B}, \mu)$ the *entropy of the partition* $\mathcal{P}$, $H_\mu(\mathcal{P})$, is defined to be $-\sum_{i=1}^{m} \mu(X_i)\log(\mu(X_i))$. Let α be a measure-preserving $\mathbf{Z}^d$-action ($(\mathbf{Z}^+)^d$-action) of $(X, \mathcal{B}, \mu)$. Define the *entropy of* α *with respect to* $\mathcal{P}$ by $h_\mu(\alpha, \mathcal{P}) = \lim_{n\to\infty} \frac{1}{|Q_n|} H_\mu(\bigvee_{\mathbf{m}\in Q_n} \alpha^{-\mathbf{m}}(\mathcal{P}))$ where $\{Q_n\}_{n\in\mathbf{N}}$ is a Følner sequence in $\mathbf{Z}^d$ (see Definition 1.4). The existence of this limit and its independence of the Følner sequence used is well-known (see, for example, Ward and Zhang [65], where a proof is given using methods from Kieffer [28] and Ornstein and Weiss in [47]). Finally, the *entropy of* α is $h_\mu(\alpha) = \sup_{\mathcal{P}\in\Xi} h_\mu(\alpha, \mathcal{P})$ where Ξ is the family of all finite measurable partitions of X.

As a prerequisite to another result we prove, for fixed $a, k, l \in \mathbf{N}$, that if $\{\mathcal{P}_n\}_{n\in\mathbf{N}}$ is a sequence of measurable partitions of $(X, \mathcal{B}, \mu)$ then the value, if it exists (it may be infinite), of $\lim_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{P}_n)$ is equal to $\lim_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{Q}_n)$ where, for all $n \in \mathbf{N}$, $\mathcal{Q}_n$ is a measurable partition of $(X, \mathcal{B}, \mu)$ and each atom of $\mathcal{Q}_n$ is a union of no more than $lk^{n^{d-1}}$ atoms of $\mathcal{P}_n$.

Example 1.1 Any ergodic automorphism of a compact metric group defines a $\mathbf{Z}$-action with completely positive entropy by Rokhlin [56].

1.5 Subshifts and maximal measures

Notation 1.2 For a compact space X let $\mathcal{B}(X)$ denote the Borel σ-algebra of X, and let $M(X)$ denote the set of Borel probability measures on X. If α is a continuous G-action of X let $M(X, \alpha)$ denote the α-invariant members of $M(X)$.

The set $M(X, \alpha)$ is non-empty for any amenable group by Theorem 2.24 of Paterson [50].

We have the following form of the variational principle for $\mathbf{Z}^d$-actions (and $(\mathbf{Z}^+)^d$-actions).

Proposition 1.1 *Let α be a $\mathbf{Z}^d$-action ($(\mathbf{Z}^+)^d$-action) by homeomorphisms (continuous maps) of the compact metric space X. Then $h(\alpha) = \sup\{h_\mu(\alpha) : \mu \in M(X, \alpha)\}$.*

Proof: This was originally proved by T.N.T. Goodman, [17], for $d = 1$, and extended to $d \geq 1$ by Elsanousi, [15]. Misiurewicz, [41], has a short proof for $d = 1$. Walters, [64], proves the $\mathbf{Z}^+$ case for the more elaborate notion of pressure.

Notation 1.3 Let X and α be as in Proposition 1.1. For all $h \in [0, h(\alpha)]$, let $M^h(X, \alpha) = \{\mu \in M(X, \alpha) : h_\mu(\alpha) = h\}$ and put $M^*(X, \alpha) = M^{h(\alpha)}(X, \alpha)$, the set of measures of maximal entropy.

Gurevič first showed that $M^*(X, \alpha)$ may be empty. Examples of maps for which $M^*(X, \alpha)$ is empty are given in Misiurewicz, [40], and Section 8.3 of Walters, [64].

We prove that, if $0 < h(\alpha) < \infty$, the members of $M^*(X, \alpha)$ are *continuous measures* (also known as *non-atomic measures*). That is, such measures have value zero on points of X.

Remark 1.1 If X is a compact abelian group, and the $\mathbf{Z}^d$-action α is by continuous group automorphisms, then Haar measure is a member of $M(X, \alpha)$ (as observed by Halmos [20]) and is, furthermore, in $M^*(X, \alpha)$ (see Misiurewicz [41] or Berg [5]).

Haar measure is also the <u>unique</u> member of $M^*(X, \alpha)$ if $d = 1$, α is ergodic, and $h(\alpha) < \infty$ (due to Berg [5]) or if α has completely positive entropy and $h(\alpha) < \infty$ (see Lind, Schmidt and Ward [34]).

Definition 1.9 A system (X, α), where X is a compact space and $\alpha : X \to X$ is a continuous $\mathbf{Z}^d$-action such that $h(\alpha) < \infty$ and $|M^*(X, \alpha)| = 1$, is called *intrinsically ergodic*.

The unique maximal measure of an intrinsically ergodic system is ergodic. In general, $M^*(X, \alpha)$ is *convex* (if $\mu, \nu \in M^*(X, \alpha)$ and $m \in \mathbf{I}$ then $m\mu + (1-m)\nu \in M^*(X, \alpha)$ where $(m\mu + (1-m)\nu)(B) = m\mu(B) + (1-m)\nu(B)$ for all $B \in \mathcal{B}(X)$). Furthermore, if $h(\alpha) < \infty$ the ergodic members of $M^*(X, \alpha)$ are exactly the extremal points (see Walters [64, Section 8.3], for example).

Definition 1.10 Let $d, k \in \mathbf{N}$, $\mathcal{S} = \{0, \cdots, k-1\}$, and let $\Sigma \subset \Omega = \mathcal{S}^{\mathbf{Z}^d}$ be a closed shift invariant ($\sigma(\Sigma) = \Sigma$) subset of Ω. We call $(\Sigma, \sigma|_\Sigma) = (\Sigma, \sigma)$, or simply Σ, a *subshift*.

For $E \subset \mathbf{Z}^d$ and $\mathbf{x} = (x_\mathbf{n})_{\mathbf{n} \in \mathbf{Z}^d}$ let $\pi_E(\mathbf{x}) = (x_\mathbf{n})_{\mathbf{n} \in E} \in \mathcal{S}^E$ be the projection of $\mathbf{x}$ onto the coordinates in E.

Let F be a finite subset of $\mathbf{Z}^d$ and Σ a subshift of Ω. If there is a set $P \subset \mathcal{S}^F$ such that

$$\Sigma = \{\mathbf{x} \in \Omega = \Omega_k : \pi_F(\sigma_\mathbf{n}(\mathbf{x})) \in P \ \forall \ \mathbf{n} \in \mathbf{Z}^d\}$$

then Σ is a *subshift of finite type* (cf. Schmidt [59, Chapter 5]).

Now let $d = 1$ and let $A = (a_{ij})$ be a $k \times k$ matrix of ones and zeros such that no row or column of A contains all zeros. Put

$$\Sigma = \{(x_n)_{n \in \mathbf{Z}} \in \Omega = \Omega_k : a_{x_n x_{n+1}} = 1 \text{ for all } n \in \mathbf{Z}\}.$$

Then Σ is a subshift of finite type. We call it a *matrix subshift of finite type*.

If, for all $1 \leq i, j \leq k$, there is an $n \in N$ such that $a^n(i, j) > 0$ (where $a^n(i, j)$ is the (i, j)th entry of A^n) then A is *irreducible*, and the corresponding matrix subshift of finite type is *irreducible*.

Furthermore, for $d = 1$, any subshift of finite type is topologically conjugate to a matrix subshift of finite type. The conjugate system may have a different value for k.

Parry [49] has shown that irreducible matrix subshifts of finite type are intrinsically ergodic and exhibited the measure of maximal entropy, the *Parry measure*.

In particular, for the one-dimensional full shift (clearly this is an irreducible matrix subshift) we have that the Parry measure is the well-known equidistributed Bernoulli measure (which coincides with the Haar measure on the natural compact group structure).

Coven and Paul [14] have shown that for intrinsically ergodic systems $(X,T),(W,S)$ with maximal measures μ,ν respectively, (X,W are compact metrizable spaces) where T,S are continuous $\mathbf{Z}$-actions (i.e. single homeomorphisms), if R is a continuous surjective map from (X,T) onto (W,S) (see Notation 1.1) then the map $\hat{R}: M(X,T) \to M(W,S)$ defined by $(\hat{R}(\lambda))(B) = \lambda(R^{-1}(B))$ for all $\lambda \in M(X,T)$ and $B \in \mathcal{B}(W)$ is surjective, see Goodwyn [18], and $\hat{R}(\mu) = \nu$.

Definition 1.11 Let X be a topological space and α a $\mathbf{Z}^d$-action by homeomorphisms of X. We say that (X,α) is *transitive* if there is an $x \in X$ such that the *α-orbit of x*, $\mathcal{O}_\alpha(x) = \{\alpha^{\mathbf{n}}(x) : \mathbf{n} \in \mathbf{Z}^d\}$, is dense in X.

To generalize the notion of irreducibility to $d \geq 1$ we use the well known fact (referred to in Markley and Paul [37, Section 5], for example) that a one dimensional matrix subshift of finite type (Σ,σ) is irreducible if and only if it is transitive and the set $\{x \in \Sigma : |\mathcal{O}_\sigma(x)| < \infty\}$ is dense in Σ.

Burton and Steif have exhibited [8] a subshift of finite type (Σ,σ) for $d=2$ which has these properties (transitivity and dense set of points with finite σ-orbit) that are equivalent (in the case $d=1$) to irreducibility and yet is not intrinsically ergodic: it has exactly two maximal ergodic measures. Furthermore, there is a continuous, surjective map of (Σ,σ) which swaps the two maximal ergodic measures.

In the light of Coven and Paul's result we ask (for $d=2$) if, for all continuous maps T of (Σ,σ) (recall Notation 1.1: this requires that T commute with σ), $\hat{T}(M^*(\Sigma,\sigma)) = M^*(\Sigma,\sigma)$. For an interesting class of continuous maps called corner permutative subcellular automata we prove that $\hat{T}(M^h(\Sigma,\sigma)) \subset M^h(\Sigma,\sigma)$ for all $h \in [0,h(\sigma)]$, with equality holding if the map is surjective.

This is similar to a result by Newton and Parry [44], for more general measure spaces X_1,X_2 with the two dimensional shift replaced by general single invertible measure-preserving maps S_1,S_2 where $T:(X_1,S_1) \to (X_2,T_2)$ is countable to one almost everywhere. However, our result is for $d = 2$, does not insist that T is onto, and also does not require that T is countable-to-one almost everywhere.

Partly as pre-requisites for the above work, we generalise some of Hedlund's results [21] for one-dimensional *cellular automata* (continuous maps of (Ω, σ)) to continuous maps of (Σ, σ), where (Σ, σ) is a two-dimensional subshift of finite type (we use the term two-dimensional *subcellular automata* to refer to such maps).

We also show (for $d = 2$) that any corner permutative map T of (Ω, σ) is surjective and, adding support to Shereshevsky's conjecture for the general (not necessarily algebraic) case, cannot have finite positive entropy. The algebraic case also follows from this result.

1.6 Related results

We mention here some standard examples of dynamical constraints on group actions.

Rokhlin [53] proved that $\mathbf{Z}$ cannot act ergodically and with zero entropy by continuous homomorphisms on any compact abelian group.

Kushnirenko showed that $\mathbf{Z}$ cannot act with infinite entropy by smooth maps of a smooth manifold. The relevant definitions and a proof of this can be found in sections 1 and 12 of Arnold and Avez's book [2].

An interesting example of group constraints dates back to a famous open algebraic problem first posed by Lehmer [31] in 1933. It is well known (see, for example Walters [64, Section 0.8]) that any continuous group automorphism of the n-dimensional additive torus group $\mathbf{S}^n$ (viewed as the direct product of n copies of $[0, 1)$ with coordinatewise addition (mod 1) and the obvious topology) acts on points $v \in \mathbf{S}^n$ by $v \mapsto A \cdot v$ where A is an $n \times n$-matrix with integer entries and determinant ± 1. The entropy of the automorphism given by A (which we also denote by A) is given by $h(A) = \sum_{i=1}^{k} \log \lambda_i$, where $\lambda_1, \cdots, \lambda_k$ are those complex eigenvalues of A whose moduli exceed one (see for example Arov [3], Sinai [62], or Yuzvinskii [25]). Lehmer's problem amounts to asking if this entropy value can be positive but arbitrarily small. Thus, a negative answer to Lehmer's problem would imply that there exists some positive ϵ such that, for any $n \in \mathbf{N}$, $\mathbf{Z}$ cannot act ergodically and with entropy less than ϵ by continuous group homomorphisms on $\mathbf{S}^n$ (that $\mathbf{Z}$ cannot act ergodically and with zero entropy on any compact abelian group was mentioned earlier).

Lind [32] observes that an automorphism of the infinite torus can be constructed by multiplying (in the obvious way) automorphisms of finite tori and that the resulting automorphism is ergodic if and only if each of the automorphisms of the finite tori of which it is composed are ergodic. The entropy of the resulting automorphism is then the sum of the automorphisms from which it is composed. So a positive answer to Lehmer's problem would give an ergodic $\mathbf{Z}$-action by continuous homomorphisms on $\mathbf{S}^{\mathbf{N}}$ with finite entropy. Lind [32] also proves the converse: a negative answer to Lehmer's problem would mean that $\mathbf{Z}$ cannot act ergodically and with finite entropy by continuous homomorphisms on the infinite torus $\mathbf{S}^{\mathbf{N}}$.

An interesting dynamical constraint arises for certain amenable groups. Amenable groups date back to a question asked by Lebesgue in 1904, and their history and theory is given a detailed treatment in Paterson's monograph [50]. Følner gave an equivalent condition to amenability (which in the case of a countable group amounts to the existence of a Følner sequence as in Definition 1.4). With some strengthening of Følner's condition, Ornstein and Weiss [47] were able to give a consistent definition of measure theoretic entropy for the actions, by measure preserving maps, of a large class of (though not all) amenable groups. With an example of a group action due to Rudolph [57] in mind, they then showed that there are amenable groups for which the entropy of their action by measure preserving maps on measure spaces can be defined and they are not able to act with entropy less than some constant (the value of which depends on the group) on any measure space. Furthermore, the constant may be infinity.

Section 6 of Conze's paper [13] shows that, given a $\mathbf{Z}^d$-action by measure preserving maps on a probability space which has positive entropy, any subgroup action (in the obvious sense) of smaller rank must have infinite entropy.

Schmidt [58, Section 3] and Bergelson and Rosenblatt [6, Section 3] characterise groups for which ergodicity of an action automatically implies a certain degree of mixing.

Chapter 2

Expansive group actions on the circle

2.1 The “North-East-South-West action”

We refer the reader to Section 1.2 of the introduction for some of the definitions used in, and relevant background to, this chapter.

Consider $\mathbf{S}$ with diametrically opposite North and South pole, N and S respectively, and a copy, $\mathbf{R}^{\infty}_{N}$, of the one point compactification of the real line, tangential at $0 \in \mathbf{R}^{\infty}_{N}$ to $S \in \mathbf{S}$. For arbitrary $x \in \mathbf{S}$ let $r \in \mathbf{R}^{\infty}_{N}$ be the N-stereographic projection of x (r is where the straight line through N and x meets $\mathbf{R}^{\infty}_{N}$). Let $\Phi_N : \mathbf{S} \to \mathbf{R}^{\infty}_{N}$ be this N-stereographic projection from the North pole and note that (i) Φ_N is a homeomorphism and (ii) $\Phi_N(N) = \pm\infty$. The “North-South Map” $\Psi_N : \mathbf{S} \to \mathbf{S}$ is given by $\Psi_N(x) = \Phi_N^{-1}(2\Phi_N(x))$ for all $x \in \mathbf{S}$ (that is, the North-South Map is that unique map on the circle which is topologically conjugate, under N-stereographic projection, to the map $f : r \mapsto 2r$ on $\mathbf{R}^{\infty}_{N}$). See Walters [64] for more on the North-South map: note that the usual convention is that the inverse of our map is called the North-South map.

If we place the East and West Poles, E and W respectively in the obvious locations on $\mathbf{S}$ and consider an “East-West Map”, $\Psi_E : \mathbf{S} \to \mathbf{S}$ defined as above, but with ‘North’, ‘South’, ‘N’, and ‘S’ replaced by ‘East’, ‘West’, ‘E’, and ‘W’ respectively, then $\langle\langle \Psi_N, \Psi_E \rangle\rangle$ is given by a continuous group action α of some group G on $\mathbf{S}$. In this section we answer the questions (i) what abstract group is G and (ii) is the action expansive?

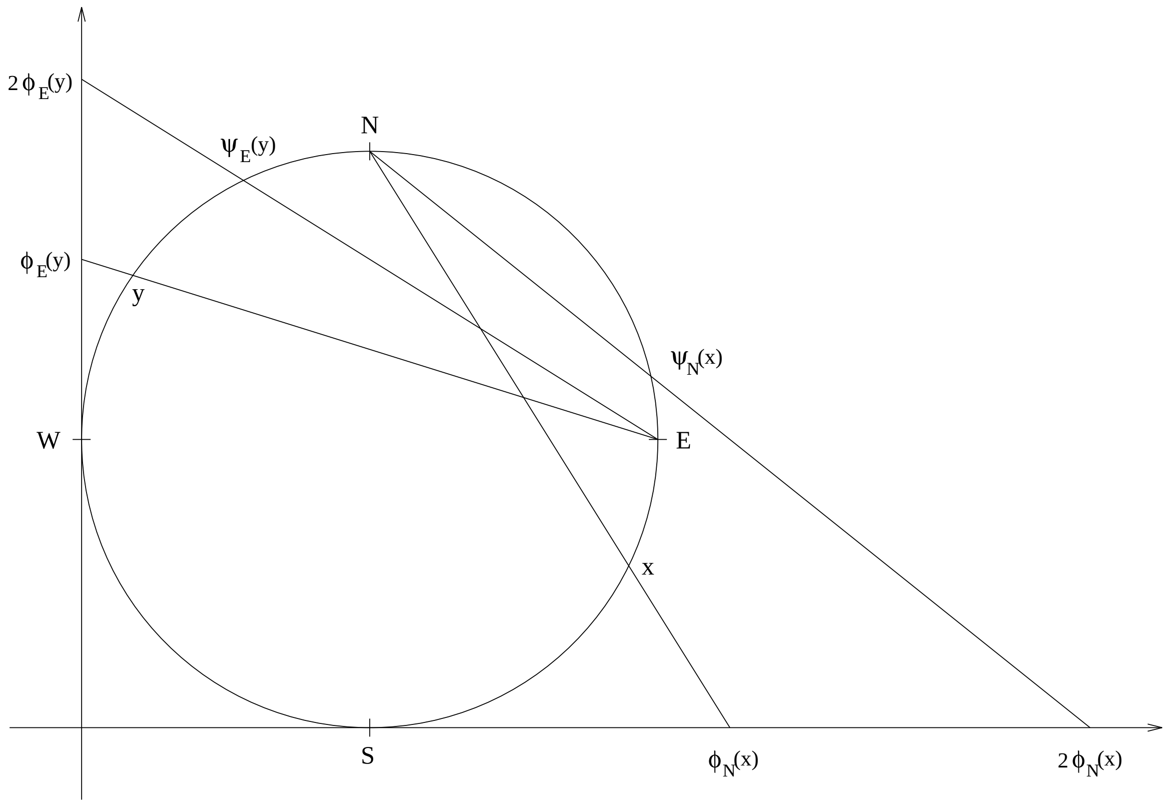

Figure 1: The "North–South–East–West" action.

To prove that α is expansive we identify points on the circle with the real value of their image under the N-stereographic projection, so that the points at N, E, S, and W are represented by $\infty, 2, 0$, and -2 respectively. Given $r \in \mathbf{R}_N^\infty$ then, to know the effect of Ψ_E on r, we need to know the value of $\Phi_N(\Psi_E(\Phi_N^{-1}(r))) = \Phi_N(\Phi_E^{-1}(2\Phi_E(\Phi_N^{-1}(r))))$.

Given arbitrary $x \in \mathbf{S}$ we can uniquely identify x by the angle $\theta_N = < SNx$ (respectively $\theta_E = < WEx$) $\in (-\pi/2, \pi/2]$ that x and S (respectively W) subtend at N (respectively E), with the convention that clockwise angles from the NS (respectively EW) line segment are negative so, for example, we may associate $\infty \in \mathbf{R}_N^\infty$ with $\theta_N = \pi/2$ and $\theta_E = -\pi/4$ (the angle , at E, between the lines EW and EN, where N corresponds to ∞).

If $x \in \mathbf{S}$ is positioned on one of those three quadrants such that $\theta_N \in (-\pi/2, \pi/4]$ (respectively $\theta_E \in (-\pi/4, \pi/2]$) then $\theta_N - \theta_E = -\pi/4$. In the remaining quadrant we have that $\theta_N - \theta_E = 3\pi/4 = \pi/2 + \pi/4 = -\pi/2 + \pi/4 = -\pi/4$ due to the identification of ∞, $-\infty$, $\pi/2$, and $-\pi/2$ (bearing in mind the π-periodicity of the tan function).

Considering the effects that Ψ_N and Ψ_E have on the representations θ_N and θ_E respectively of points in $\mathbf{S}$ we have that $\Psi_N(\theta_N) = \tan^{-1}(1/2(2(2\tan(\theta_N)))) = \tan^{-1}(2\tan(\theta_N))$ and, similarly, $\Psi_E(\theta_E) = \tan^{-1}(2\tan(\theta_E))$, and the effect on $\mathbf{R}_N^\infty$ of Ψ_E is given by $g : \mathbf{R}_N^\infty \to \mathbf{R}_N^\infty$ where, for all $r \in \mathbf{R}_N^\infty$,

$$g(r) = 2\tan(-\pi/4 + \tan^{-1}(2\tan(\pi/4 + \tan^{-1}(r/2)))) =$$
$$2\tan\left(-\frac{\pi}{4} + \tan^{-1}\left(2\frac{1+r/2}{1-r/2}\right)\right) = 2\frac{-1+2\frac{2+r}{2-r}}{1+2\frac{2+r}{2-r}} = \frac{4+6r}{6+r}.$$

From now on we abuse notation slightly by using the maps $f : \mathbf{R}_N^\infty \to \mathbf{R}_N^\infty$ and $g : \mathbf{R}_N^\infty \to \mathbf{R}_N^\infty$ to refer to the maps Ψ_N and Ψ_E on $\mathbf{S}$, and we shall use values of points on $\mathbf{R}_N^\infty$ to refer to their respective images, under Φ_N^{-1}, in $\mathbf{S}$; i.e. we are merely identifying $(\mathbf{S}, \Psi_N, \Psi_E)$ with $(\mathbf{R}_N^\infty, f, g)$.

Note that $g^{-1}(r) = \frac{-4+6r}{6-r}$ and we have $g(\infty) = 6$, $g(-6) = \infty$, $g(2) = 2$, $g(-2) = -2$, $f(0) = 0$, and $f(\infty) = \infty$.

So g is a real function with asymptotic axes $x = -6$ and $y = 6$ and gradient positive everywhere, and fixing 2 and -2 which refer to the East and West poles respectively. Also, f sends all non-zero points closer to ∞ and g sends all points in $(-2, -6)$ closer to $-\infty$, all points in $(-6, -\infty)$ into $(6, \infty)$, all points in $(2, \infty)$ closer to 2, and all points in $(-2, 2)$ closer to 2.

Note that $\{0, \infty\} \cup \{[f^n(i), f^{n+1}(i)) : n \in \mathbf{Z} \text{ and } i \in \{2, -2\}\}$ (respectively $\{2, -2\} \cup \{[g^n(i), g^{n+1}(i)) : n \in \mathbf{Z} \text{ and } i \in \{0, \infty\}\}$) is a partition of $\mathbf{S}$. If, for some $m \in \mathbf{Z}$, $g^m(x)$ and $g^m(y)$ (respectively $f^m(x)$ and $f^m(y)$) lie in different atoms of the partition then, for suitable $n \in \mathbf{Z}$, exactly one of $f^n g^m(x)$ and $f^n g^m(y)$ (respectively $g^n f^m(x)$ and $g^n f^m(y)$) lies in $[-2, 2)$ (respectively $[0, \infty)$), they can then be separated by g^k (respectively f^k) for suitable $k \in \mathbf{Z}$.

The difficulty in proving expansiveness lies in the possibility of two distinct points always (after any finite combination of repeated applications of $f^{\pm 1}$ and $g^{\pm 1}$) remaining close together <u>and</u> in common atoms of the respective partitions for both the

f-orbit and the g-orbit. Using the algorithm below we show that this does not occur.

First note that given $\epsilon > 0$ there exists $\delta > 0$ such that if $r, s \in (-2, 2) \subset \mathbf{R}_N^\infty$ and $|r - s| > \epsilon$ then those points on $\mathbf{S}$ corresponding to r and s are greater than δ apart with respect to the standard metric on $\mathbf{S}$, so it is sufficient to separate points by some specified amount ϵ within the bounded interval $(-2, 2)$ of $\mathbf{R}_N^\infty$. For our algorithm we use $\epsilon = 1$.

Algorithm 2.1 (i) Given distinct $r, s \in \mathbf{R}_N^\infty$, IF (a) $r = \infty$ or $s = \infty$ then apply f^{-n} for sufficiently large $n \in \mathbf{N}$ and we are done, ELSE (b) apply f^{-n} for sufficiently large $n \in \mathbf{N}$ to get $f^{-n}(r)$ and $f^{-n}(s) \in (-2, 2)$. Next apply g^m for sufficiently large $m \in \mathbf{N}$ to get $r_1 = g^m(f^{-n}(r)) \in (0, 2)$ and $s_1 = g^m(f^{-n}(s)) \in (0, 2)$. Set i=1.

(ii) IF $\{r_i, s_i\} \cap (0, 1) \neq \phi$(the empty set) then apply f^m where $m \in \mathbf{N}$ is such that $\{f^m(r_i), f^m(s_i)\} \cap (0, 1) = \phi$ but $\{f^{m-1}(r_i), f^{m-1}(s_i)\} \cap (0, 1) \neq \phi$ and put $r_{i+1} = f^m(r_i)$ and $s_{i+1} = f^m(s_i)$ ELSE put $r_{i+1} = g^{-1}(r_i)$ and $s_{i+1} = g^{-1}(s_i)$. Increment i.

(iii) Since $f((0, 1)) = (0, 2)$ and $g^{-1}([1, 2)) = [\frac{2}{5}, 2)$ we still have at least one of $r_i, s_i \in (0, 2)$, IF (a) one of them is not (this would be because f^m sent it into $[2, \infty)$) we can separate them adequately by applying g^{-n} for sufficiently large $m \in \mathbf{N}$ ELSE IF (b) $|r_i - s_i| > 1$ then we are done ELSE (c) repeat step (ii).

Theorem 2.1 *The "North-East-South-West Action" is expansive on* $\mathbf{S}$.

Proof. Apply algorithm 2.1. If we do not escape at (i)(a) or eventually escape at (iii)(a) then, after sufficiently many repetitions of step (ii), we must have that $|r_i - s_i| > 1$. This is because $|f^m(r_i) - f^m(s_i)| = 2^m |r_i - s_i|$ and, without loss of generality, $1 \leq r_i < s_i < 2$ implies that $g^{-1}(s_i) - g^{-1}(r_i) =$

$$\frac{-4 + 6s_i}{6 - s_i} - \frac{-4 + 6r_i}{6 - r_i} = \frac{32(s_i - r_i)}{36 - 6(s_i + r_i) + s_i r_i}$$

$$\geq \frac{32(s_i - r_i)}{36 + \sup_{t \in [1,2)}(-12t + t(t+1))} = \frac{32(s_i - r_i)}{36 - 10} = \frac{16(s_i - r_i)}{13}.$$

So step (ii) always increases $|s_i - r_i|$ by a factor of at least 16/13. $\square$

We use the following lemma, for the proof of which we are indebted to Morris Newmann, to prove that the "North-East-South-West Group" $\langle\langle \Psi_N, \Psi_E\rangle\rangle$ is a free group.

Lemma 2.1 *The group* $\langle G, F\rangle$ *is a free group, where*

$$G = \frac{1}{4\sqrt{2}}\begin{pmatrix} 6 & 4 \\ 1 & 6 \end{pmatrix} \quad \text{and} \quad F = \frac{1}{\sqrt{2}}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

Proof. Set $S = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, put

$$E = SGS^{-1} = \frac{1}{2\sqrt{2}}\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$$

and $F = SFS^{-1}$. It now suffices to show that $\langle E, F\rangle = \langle SGS^{-1}, SFS^{-1}\rangle$ is free.

Now $E = UFU$, where

$$U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is a square root of the identity. So any non-empty word-string of E's and F's equal to the identity matrix gives a non-empty word-string of U's and F's equal to the identity. We claim that this word-string may be assumed to be of the form $UF^{k_1}U\cdots UF^{k_n}$ for some $n \in \mathbf{N}$ and $k_1, \cdots, k_n \in \mathbf{Z}\backslash\{0\}$. This is because (where I is the identity matrix)

(i) $F^{k_1}U\cdots UF^{k_n} = I$ implies that $UF^{k_2}U\cdots UF^{k_n+k_1} = I$,

(ii) $F^{k_1}U\cdots UF^{k_n}U = I$ implies that $UF^{k_2}U\cdots UF^{k_n}UF^{k_1} = I$, and

(iii) $UF^{k_1}U\cdots UF^{k_n}U = I$ implies that $F^{k_1}U\cdots UF^{k_n} = I$, which in turn implies that $UF^{k_2}U\cdots UF^{k_n+k_1} = I$.

Here cancellations due to the possibility of $k_1 = -k_n$, and in general $k_i = -k_{n+1-i}$ for either $1 \leq i \leq n/2$ for n even or $1 \leq i \leq (n-1)/2$ for n odd leaves, at worst, $U = I$ if n is even and $F^{k_{(n+1)/2}} = I$ if n is odd, neither of which is possible. So we may assume that $UF^{k_1}U\cdots UF^{k_n} = I$ for some $n \in \mathbf{N}$ and $k_1, \cdots, k_n \in \mathbf{Z}\backslash\{0\}$.

Let $A \sim B$ in $GL(2, \mathbf{R})$ if and only if there exists $r \in \mathbf{R}\backslash\{0\}$ such that $A = rB$. Then, for $k \in \mathbf{Z}\backslash\{0\}$,

$$UF^k \sim \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \sqrt{2}^{\,k} & 0 \\ 0 & \sqrt{2}^{\,-k} \end{pmatrix} = \begin{pmatrix} \sqrt{2}^{\,k} & \sqrt{2}^{\,-k} \\ \sqrt{2}^{\,k} & -\sqrt{2}^{\,-k} \end{pmatrix}$$

which is equivalent, with respect to $\sim$, to both

$$\begin{pmatrix} \sqrt{2}^{\,2k} & 1 \\ \sqrt{2}^{\,2k} & -1 \end{pmatrix} = \begin{pmatrix} 2^k & 1 \\ 2^k & -1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & \sqrt{2}^{\,-2k} \\ 1 & -\sqrt{2}^{\,-2k} \end{pmatrix} = \begin{pmatrix} 1 & 2^{-k} \\ 1 & -2^{-k} \end{pmatrix}.$$

For $i = 1, \cdots, n$, put $A_i = \begin{pmatrix} 2^{k_i} & 1 \\ 2^{k_i} & -1 \end{pmatrix}$ if $k_i > 0$ and put $A_i = \begin{pmatrix} 1 & 2^{-k_i} \\ 1 & -2^{-k_i} \end{pmatrix}$ if $k_i < 0$. Clearly, since we have $UF^{k_1}U \cdots UF^{k_n} = I$, it follows that $A_1 \cdots A_n \sim I$. But the product $A_1 \cdots A_n$ is a matrix with only integer entries, so $A_1 \cdots A_n = c \cdot I$ where $c \in \mathbf{Z}\backslash\{0\}$. It then follows that $A_1 \cdots A_n = I$ or $0 \pmod 2$, where 0 is the zero matrix. But each $A_i = P$ or $Q \pmod 2$, where

$$P = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } Q = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

Furthermore, $P^2 = P, Q^2 = Q, PQ = Q$, and $QP = P$, which contradicts $A_1 \cdots A_n = I$ or $0 \pmod 2$. Thus, there cannot exist any non-empty word-string of E's and F's equal to the identity matrix and, hence, $\langle E, F \rangle$ is a free group. $\square$

Theorem 2.2 *The "North-East-South-West Group" $\langle\langle \Psi_N, \Psi_E \rangle\rangle$ is a free group.*

Proof. Note that all elements of the group $\langle\langle \psi_N, \psi_E \rangle\rangle$ are of the form $g : x \mapsto \frac{ax+b}{cx+d}$ where $a, b, c, d \in \mathbf{R}$ and $ad - bc \neq 0$ (simply check that ψ_N and ψ_E are of this form and that if g_1, g_2 are of this form then so is $g_1 \circ g_2$). The typical element, g of $\langle\langle \psi_N, \psi_E \rangle\rangle$ is clearly unaffected if each of a, b, c, and d is multiplied by the same non-zero real number r: $ad - bc$ is merely scaled by r^2.

We thus construct a well defined map $\theta : \langle\langle \psi_N, \psi_E \rangle\rangle \to \mathcal{S} = (SL(2, \mathbf{R}), \sim)$ by

$$\theta(g) = \frac{1}{\sqrt{ad - bc}} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where, for $A, B \in SL(2,\mathbf{R})$, $A \sim B$ if and only if $A = \pm B$ and note that θ is a group homomorphism with trivial kernel, $\ker\theta = \{x \mapsto \frac{r\cdot x+0}{0\cdot x+r} : r \in \mathbf{R}\backslash\{0\}\}$. Thus, the restriction of θ to $\langle\langle\psi_N, \psi_E\rangle\rangle$ gives a group isomorphism between $\langle\langle\psi_N, \psi_E\rangle\rangle$ and $\langle F, G\rangle$, where F and G are as in Lemma 2.1. $\square$

Thus the geometrically natural action generated by the N-S and E-W maps is an expansive action of a free group. A natural question is whether "smaller" groups can act expansively.

Example 2.1 The group action generated by an irrational rotation of $\mathbf{S}$ and the North-South map on $\mathbf{S}$ is clearly expansive. However, it is not clear whether this group of transformations is free.

2.2 An expansive solvable group action

What relations can we impose upon the elements of the group and still retain expansiveness? We now describe an example due to Shahar Mozes (unpublished) of a solvable group action which is easily shown to act expansively.

Remaining with the terminology (and identification of $(\mathbf{S}, \Psi_N)$ with $(\mathbf{R}_N^\infty, f)$) from Section 2.1 define $\Psi_H : \mathbf{S} \to \mathbf{S}$ by $\Psi_H = \Phi_N^{-1} h \Phi_N$ where $h : \mathbf{R}_N^\infty \to \mathbf{R}_N^\infty$ is given by $h : r \mapsto r + 1$.

Theorem 2.3 *The group action $\langle\langle\Psi_N, \Psi_H\rangle\rangle$ by homeomorphisms of the circle is an expansive action by a solvable, but not nilpotent, group.*

Proof. Note that, for all $g \in \langle\langle f, h\rangle\rangle$, $g(r) = 2^m r + a$ for all $r \in \mathbf{R}_N^\infty$ where $a = 2^n b$, for some $m, n, b \in \mathbf{Z}$. Using the restriction of the injective group homomorphism θ in theorem 2.2 to $\langle\langle f, h\rangle\rangle$ we represent the typical member $g \in \langle\langle f, h\rangle\rangle$ by

$$G = \frac{1}{\sqrt{2^m}} \begin{pmatrix} 2^m & a \\ 0 & 1 \end{pmatrix}$$

and see that $\langle\langle f, h\rangle\rangle$ is represented by

$$\langle F, H\rangle = \left\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Note that all commutators of this group are are of the form $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ where $a \in \mathbf{Q}$ and, hence, that all elements of the commutator subgroup are of this form. Furthermore such elements clearly commute, so certainly $\langle\langle \Psi_N, \Psi_H \rangle\rangle = \langle\langle f, h \rangle\rangle$ is solvable.

Suppose nilpotency of class n where n is minimal (clearly, F and H do not commute), so the n^{th} commutator subgroup γ_n is contained in the centre of $\langle F, H \rangle$. Let $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ where $a \in \mathbf{Q}$, be a typical member of γ_n (clearly all elements of each commutator group are of this form). Then if A commutes with F, $a = 0$, so $\gamma_n = \{id\}$, contradicting the minimality of n.

Expansiveness is clear; given any two distinct real numbers we can, if necessary, apply f^m to both of them for suitable integer m so that they are real distance greater than one but less than or equal to two apart (recall that f is the map on the extended real line), then apply h^n (which is an isometry on $\mathbf{R}$) to each of the resultant points for suitable integer n so that the two resultant points are within the interval $(-2, 2)$. Expansiveness follows, by the paragraph preceding Algorithm 2.1. $\square$

2.3 Möbius groups and nilpotency

The maps f, g, and h of $\mathbf{R}_N^\infty$ in Sections 2.1 and 2.2 are specific examples of *Möbius maps*.

Definition 2.1 A real map of the form $x \mapsto \frac{ax+b}{cx+d}$ for all $x \in \mathbf{R}^\infty$, the one point compactification of the reals, for some $a, b, c, d \in \mathbf{R}$ with $ad - bc \neq 0$ is called a *Möbius map*. We represent such a map by a *Möbius matrix*

$$\frac{1}{\sqrt{ad-bc}} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S} = (SL(2, \mathbf{R}), \sim)$$

where Möbius matrices A and B are considered equivalent, $A \sim B$, if and only if $A = \pm B$. We call a group generated by such matrices with the equivalence relation $\sim$ a *Möbius group*.

Clearly, if the Möbius matrices $A_1, \ldots, A_n$ represent the Möbius maps $f_1, \ldots, f_n$ of $\mathbf{R}^\infty$ then $\langle\langle f_1, \ldots, f_n \rangle\rangle$ is a faithful $\langle A_1, \ldots, A_n \rangle$-action, and we call it a *Möbius action.*

We have seen from Theorem 2.3 that finitely generated Möbius groups can be solvable, but what about nilpotency? We now prove that the only finitely generated nilpotent Möbius groups are abelian. It will then follow from Theorem 2.9 below that any finitely generated Möbius group which acts expansively on the circle cannot have polynomial growth.

Theorem 2.4 *Let G be a finitely generated Möbius group. If G is nilpotent then it is commutative.*

Proof: Let

$$G = \left\langle A_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \mathcal{S} : a_i d_i - b_i c_i = 1 \text{ for } i \in \{1, \ldots, k\} \right\rangle .$$

We first prove the theorem for the special case

$$H = \left\langle A_i = \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix} \in \mathcal{S} : a_i d_i = 1 \text{ for } i \in \{1, \ldots, k\} \right\rangle .$$

The special case where c_i is not necessarily zero but $b_i = 0$ for $1 \leq i \leq k$ follows by an analogous (and hence omitted) argument. We then finally prove it for the general case.

Suppose that H is nilpotent and not commutative. Then $\{I\} \neq \gamma_n(H) \subset Z(H)$ for some $n \in \mathbf{N}$. Let $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ be a non-identity member of $\gamma_n(H)$. Since $A \in Z(H)$ we have that $ab_i + bd_i = a_i b + b_i d$, or $b(d_i - a_i) = b_i(d - a)$, for $1 \leq i \leq k$. If $b = 0$ then $ab_i = b_i d$ for $1 \leq i \leq k$. Since H is not commutative we can't have $b_i = 0$ for all i such that $1 \leq i \leq k$. It follows that $a = d$ equals 1 or -1 (since $ad = ad - b \cdot 0 = 1$). But $A \not\sim I$, so we can't have $b = 0$.

Hence $b(d_i - a_i) = b_i(d - a)$ gives $b_j b(d_i - a_i) = b_j b_i(d - a) = bb_i(d_j - a_j)$ and $b \neq 0$ then gives $a_j b_i + b_j d_i = a_i b_j + b_i d_j$ for $1 \leq i, j \leq k$, which can't be so because

H is not commutative. This contradiction proves the theorem for the special case of H. The theorem is similarly shown to be true for the case where $b_i = 0$ for $1 \leq i \leq k$.

Finally suppose that G is nilpotent but not commutative. Then $\{I\} \neq \gamma_n(G) \subset Z(G)$ for some $n \in \mathbf{N}$. Take $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq I$ in $\gamma_n(G)$. So $bc_i = b_i c$, $b_i(a-d) = b(a_i - d_i)$, and $c_i(a-d) = c(a_i - d_i)$ for $1 \leq i \leq k$.

Suppose $c = 0$, then $bc_i = 0$ for $1 \leq i \leq k$. If $b = 0$ we have $(a-d)b_i = 0 = (a-d)c_i$ for $1 \leq i \leq k$. We can't have $c_i = 0$ for $1 \leq i \leq k$ (this was H), so we must have $a = d$ and, hence, $a = d = \pm 1$ since $ad = ad - bc = 1$, but $A \not\sim I$, so we must have $b \neq 0$. But, then, $bc_i = 0$ gives $c_i = 0$ again for $1 \leq i \leq k$ (case H again), so we can't have $c = 0$. The case for supposing that $b = 0$ (before any restrictions on c) is similarly dealt with.

So, finally, suppose $b \neq 0 \neq c$. Then, by the same method used earlier, we get $b_i(a_j - d_j) = b_j(a_i - d_i)$, $c_i(a_j - d_j) = c_j(a_i - d_i)$, and $b_j c_i = b_i c_j$ for $1 \leq i, j \leq k$, which is sufficient for G to be commutative. Thus, it is not possible for our group to be nilpotent unless it is commutative. □

2.4 Expansive group actions on the circle and fixed points

In Section 2.5 we consider (finitely generated) commutative groups. We first prove a result for expansive actions of continuous maps by arbitrary (not necessarily countable) groups which will help us show that commutative groups cannot act expansively on the circle.

Definition 2.2 Let S be $\mathbf{I}$, $\mathbf{S}$, or $\mathbf{R}$. A set $A \subset S$ is *nowhere dense* if it is dense in no interval of S.

Lemma 2.2 *A finite union of nowhere dense subsets of S is nowhere dense, where S is $\mathbf{I}$, $\mathbf{S}$, or $\mathbf{R}$.*

Proof: Take any interval, B say, of S. Let the nowhere dense sets be $A_1, \cdots, A_n$ for some $n \in \mathbf{N}$. There exists an open set $C_1 \subset B$ such that $A_1 \cap C_1 = \emptyset$. There exists an open set $C_2 \subset C_1$ such that $A_2 \cap C_2 = \emptyset$. $\cdots$. There exists an open set $C_n \subset C_{n-1}$ such that $A_n \cap C_n = \emptyset$. Clearly $(\bigcup_{i=1}^{n} A_i) \cap C_n = \emptyset$ and $C_n \subset B$. So $\bigcup_{i=1}^{n} A_i$ is not dense in arbitrarily chosen $B \subset S$. $\square$

Theorem 2.5 *If an action $\alpha : \Gamma \to \mathrm{Homeo}(\mathbf{S})$, for arbitrary group Γ, is expansive then there is a dense set of elements in $\mathbf{S}$, each of which is fixed by a non-trivial element of $\alpha(\Gamma)$. That is, the closure of*

$$\{x \in \mathbf{S} : \alpha_\gamma(x) = x \text{ for some } \gamma \in \Gamma \text{ such that } \alpha_\gamma \neq id\}$$

is all of $\mathbf{S}$.

Proof. Assume α is expansive with expansive constant δ. We shall presently think of $\mathbf{S}$ as the unit interval, $[0,1]$, with 0 and 1 identified and metric ρ given by $\rho(x,y) = \min(|x-y|, 1-|x-y|)$. Partition $\mathbf{S}$ into a finite number, m say, of disjoint positive length intervals (it doesn't matter whether any particular interval is open, closed, or closed at one end and open at the other end) $\{I_1, \ldots, I_m\}$ each of length less than $\delta/2$.

Fix a sequence $\{\epsilon_n\}$ such that $\epsilon_n \in (0, 1/2)\, \forall n \in \mathbf{N}$ and $\lim_{n\to\infty} \epsilon_n = 0$. Given $x \in \mathbf{S}$ put $x_n = x + \epsilon_n (\mathrm{mod} 1)$ for all $n \in \mathbf{N}$. By expansiveness there exists a sequence $\{\gamma_n\} \subset \Gamma$ such that $\rho(\alpha_{\gamma_n}(x), \alpha_{\gamma_n}(x_n)) > \delta$ for all $n \in \mathbf{N}$. Therefore there exists $m_x \in \{1, \ldots, m\}$ and a subsequence $\{\gamma_{n_k}\} \subset \{\gamma_n\}$ such that $I_{m_x} \subset (\alpha_{\gamma_{n_k}}(x), \alpha_{\gamma_{n_k}}(x_{n_k}))$ for all $k \in \mathbf{N}$. Since $\{\epsilon_n\}$ is fixed, the least such m_x is uniquely determined by x.

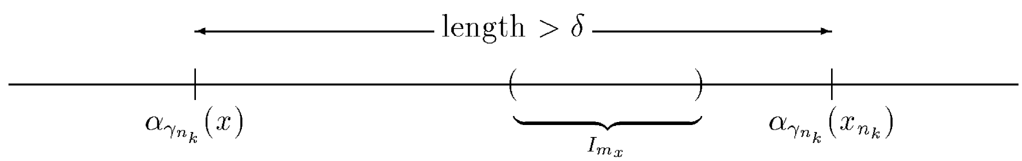

Figure 2: First step in Theorem 2.5.

Now suppose that E is an arbitrary interval of $\mathbf{S}$. Partition the points of E into disjoint subsets $U_1, \ldots, U_m$ according to the rule $x \in U_n$ if and only if $n = m_x$, the unique element of $\{1, \ldots, m\}$ chosen as above. By Lemma 2.2 there exists a proper interval $D \subset E$ and there exists $m_0 \in \{1, \ldots, m\}$ such that U_{m_0} is dense in D (else $E = \bigcup_{i=1}^{m} U_i$ would be nowhere dense).

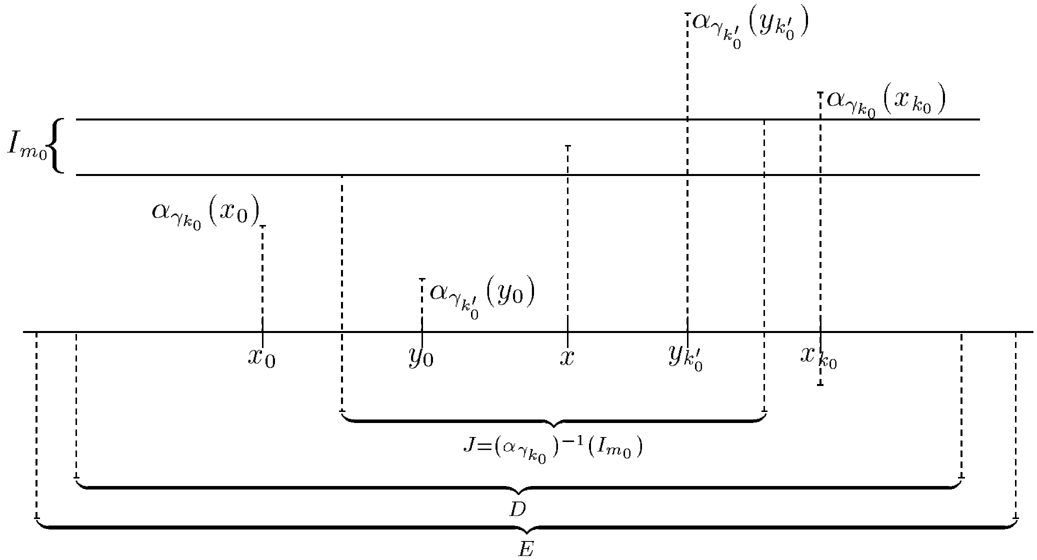

Figure 3: Second step in Theorem 2.5.

Now select an interior point $x_0 \in D \cap U_{m_0}$ of D. Then there exist sequences $\{x_k\} \subset \mathbf{S} \backslash \{x_0\}$ and $\{\gamma_k\} \subset \Gamma$ such that $\lim_{k \to \infty} x_k = x_0$ and $I_{m_0} \subset (\alpha_{\gamma_k}(x_0), \alpha_{\gamma_k}(x_k)) \, \forall \, k \in \mathbf{N}$. Select $k_0 \in \mathbf{N}$ such that $x_{k_0} \in D$. So $(x_0, x_{k_0}) \subset D$ and $I_{m_0} \subset (\alpha_{\gamma_{k_0}}(x_0), \alpha_{\gamma_{k_0}}(x_{k_0}))$.

Now let $J = (\alpha_{\gamma_{k_0}})^{-1}(I_{m_0})$ and take $y_0 \in J \cap U_{m_0}$ such that y_0 is an interior point of J, so there exist respective sequences $\{y_k\} \subset \mathbf{S} \backslash \{y_0\}$ and $\{\upsilon_k\} \subset \Gamma$ such that $\lim_{k \to \infty} y_k = y_0$ and $I_{m_0} \subset (\alpha_{\upsilon_k}(y_0), \alpha_{\upsilon_k}(y_k)) \, \forall \, k \in \mathbf{N}$, and there exists an appropriate $k_0' \in \mathbf{N}$ such that $y_{k_0'}$ is an interior point of J and I_{m_0} is a proper subset of $(\alpha_{\upsilon_{k_0'}}(y_0), \alpha_{\upsilon_{k_0'}}(y_{k_0'}))$. Clearly $\alpha_{\upsilon_{k_0'}} \neq \alpha_{\upsilon_{k_0}}$ since $(\alpha_{\gamma_{k_0}}(y_0), \alpha_{\gamma_{k_0}}(y_{k_0'}))$ is a proper subset of I_{m_0}. In fact,

$$\alpha_{\upsilon_{k_0'}}(y_0) < \alpha_{\gamma_{k_0}}(y_0) \text{ and } \alpha_{\gamma_{k_0}}(y_{k_0'}) < \alpha_{\upsilon_{k_0'}}(y_{k_0'}) \tag{2}$$

(but note that it is possible that $\alpha_{\gamma_{k_0}}(y_0) > \alpha_{\gamma_{k_0}}(y_{k_0'})$: i.e. it is possible that $\alpha_{\gamma_{k_0}}$ does not preserve the orientation of $\mathbf{S}$) where the ordering relation is used locally in the obvious sense on proper subintervals of $\mathbf{S}$ (if $\alpha_{\upsilon_{k_0'}}$ reverses orientation, of course, we'd have $>$ instead of $<$ in the above two inequalities). By the Intermediate Value Theorem, there exists $x \in (y_0, y_{k_0'})$ such that x is fixed by the non-trivial homeomorphism $\alpha_{(\gamma_{k_0}^{-1} \upsilon_{k_0'})}$. $\square$

Remark 2.1 The proof of Theorem 2.5 is clearly still valid when $\mathbf{S}$, with its usual metric, is replaced by $\mathbf{I}$, with its usual metric.

Remark 2.2 By (2) we have actually shown that, given any interval, we can find a non trivial element α_γ of $\alpha(\Gamma)$ and three distinct points in the interval such that the middle (in the obvious sense) point is fixed by α_γ and the other two points are not.

2.5 Commutative group-actions on the circle

So far we know that solvable groups can act expansively on $\mathbf{S}$ but have no evidence that any groups of polynomial growth (or nilpotent groups) can. We now show that finitely generated abelian groups cannot act expansively on $\mathbf{S}$ and, by a previous result, non-expansiveness also follows for all Möbius groups of polynomial growth. After eliminating any torsion elements (elements of finite order and clearly of no influence on expansiveness or non-expansiveness of commutative groups) we may consider any commutative group to be isomorphic with $\mathbf{Z}^d$ for some $d \in \mathbf{N}$, so we consider faithful $\mathbf{Z}^d$-actions only.

We continue to view $\mathbf{S}$ as $[0, 1]$ with 0 and 1 identified and keep the metric ρ from the proof of Theorem 2.5 (but see the notation below), and δ will always represent a candidate for an expansive constant. We begin with a concept of generator for continuous countable group actions analogous to Keynes and Robertson's [27] generator for a single homeomorphism of a compact metric space.

Notation 2.1 When considering intervals, $I = [a, b]$ say, of $\mathbf{S}$ we are sometimes interested in the interval as a metric space in its own right, with points ordered in the obvious manner (as elements of $\mathbf{R}$). For arbitrary $x \leq y$ in I let $\mu(x, y)$ be the Lebesgue measure (normalised on $\mathbf{S}$, not I) of the interval $[x, y]$ considered as an interval in $\mathbf{S}$. This is useful because if $\mu(x, y) \leq 1/2$ then $\rho(x, y) = \mu(x, y)$ and $\mu(x, y) \leq \delta < 1/2 \Rightarrow \rho(u, v) \leq \delta$ for all $u, v \in [x, y]$, which wouldn't necessarily be true if we merely had $\rho(x, y) \leq \delta < 1/2$. We therefore always assume that $\delta < 1/2$ from now on and must initially prove the main theorem for intervals with the μ-metric (that is, $\mu(x, y)$ is the Lebesgue measure of the interval with end points x and y for any points x and y in the interval).

Definition 2.3 A finite open cover ξ is a *generator* for a continuous Γ-action α on a compact metric space X if, for every $\{X_\gamma\}_{\gamma\in\Gamma} \subset \xi^\Gamma$ (where $X_\gamma \in \xi\ \forall\gamma \in \Gamma$), $|\bigcap_{\gamma\in\Gamma} \alpha_\gamma(\overline{X_\gamma})| \leq 1$. If we only insist that $|\bigcap_{\gamma\in\Gamma} \alpha_\gamma(X_\gamma)| \leq 1$ then we call ξ a *weak generator*.

Theorem 2.6 *A continuous countable group action has a generator if and only if it has a weak generator.*

Proof: As in Theorem 5.20 in Walters [64] (all generators are weak generators. If ξ is a weak generator with Lebesgue number ϵ and ξ' is an open cover of X with $\mathrm{diam}(A) \leq \epsilon$ for all $A \in \xi'$ then ξ' is a generator). $\square$

Observation 2.1 If $\{\mathbf{m}_1, \ldots, \mathbf{m}_d\} \subset \mathbf{Z}^d$ form a basis in $\mathbf{R}^d$ then for all $\mathbf{m}_0 \in \mathbf{Z}^d$ there exists $(n_1, \ldots, n_d) \in \mathbf{Z}^d$ and $\mathbf{k} \in \mathbf{P}$ (the semi-closed d-dimensional parallelogram in $\mathbf{Z}^d$ formed by the set of vectors $\{\overrightarrow{\mathbf{0m}}_i \colon i \in \{1, \ldots, d\}\}$) such that

$$\mathbf{m}_0 = n_1\mathbf{m}_1 + \ldots + n_d\mathbf{m}_d + \mathbf{k}.$$

Theorem 2.7 *A continuous countable* Γ*-action on a compact metric space is expansive if and only if it has a generator if and only if it has a weak generator.*

Proof: Completely analogous to Walters [64, Theorem 5.22] and due to Reddy [51] and Keynes and Robertson [27] for the case $\Gamma = \mathbf{Z}$.

The next result shows that expansiveness, or non-expansiveness, is unaffected if we replace an $\mathbf{R}^d$-basis $\{\mathbf{m}_1, \cdots, \mathbf{m}_d\} \subset \mathbf{Z}^d$ by the standard orthonormal basis $\{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$.

Corollary 2.1 *Let* $\{\mathbf{m}_1, \ldots, \mathbf{m}_d\} \subset \mathbf{Z}^d\backslash\{\mathbf{0}\}$ *be a basis in* $\mathbf{R}^d$*. Then the* $\mathbf{Z}^d$*-action* α *on a compact metric space* X *is expansive if and only if* β *is expansive on* X*, where, for all* $\mathbf{n} = (n_1, \ldots, n_d) \in \mathbf{Z}^d$, $\beta^{\mathbf{n}} = (\alpha^{\mathbf{m}_1})^{n_1} \ldots (\alpha^{\mathbf{m}_d})^{n_d} = \alpha^{n_1\mathbf{m}_1+\cdots+n_d\mathbf{m}_d}$.

Proof: ($\Leftarrow$) A generator for β is a generator for α.

($\Rightarrow$) By Observation 2.1, given $\mathbf{m}_0 \in \mathbf{Z}^d$ there exists $\mathbf{n} = (n_1, \ldots, n_d) \in \mathbf{Z}^d$ and $\mathbf{k} \in \mathbf{P}$ such that $\alpha^{\mathbf{m}_0} = (\alpha^{\mathbf{m}_1})^{n_1} \ldots (\alpha^{\mathbf{m}_d})^{n_d} \alpha^{\mathbf{k}} = \beta^{\mathbf{n}} \alpha^{\mathbf{k}}$. So if ξ is a generator for α then the refinement $\bigvee_{\mathbf{k} \in \mathbf{P}} \alpha^{\mathbf{k}}(\xi)$ is a generator for β. $\square$

Remark 2.3 The expansive constant for β may have a different value to that for α in the event that α is expansive.

Observation 2.2 Let $\{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$ be the standard orthonormal basis for $\mathbf{Z}^d$. Given $\mathbf{m} \in \mathbf{Z}^d \backslash \{\mathbf{0}\}$, $\{\mathbf{m}\} \bigcup (\{\mathbf{e}_1, \cdots, \mathbf{e}_d\} \backslash \{\mathbf{e}_j\})$ is a basis in $\mathbf{R}^d$ for some $1 \leq j \leq d$. So, putting $\mathbf{m}_i$ in corollary 2.1 equal to $\mathbf{e}_i$ for $i \neq j$ and putting $\mathbf{m}_j = \mathbf{m}$, we have $\beta^{\mathbf{e}_j} = \alpha^{\mathbf{m}}$. That is, if $\alpha^{\mathbf{m}}$ has some property for some $\mathbf{m} \in \mathbf{Z}^d \backslash \{\mathbf{0}\}$ then we may assume that $\alpha^{\mathbf{e}_j}$ has that same property for some $1 \leq j \leq d$, without affecting the expansiveness or non-expansiveness of α.

Observation 2.3 Let $\{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$ be the standard orthonormal basis for $\mathbf{Z}^d$. By Corollary 2.1 we may replace $\{2\mathbf{e}_1, \ldots, 2\mathbf{e}_d\}$ by $\{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$ and assume that all elements of our group act by orientation preserving homeomorphisms of $\mathbf{S}$ without affecting expansiveness.

Notation 2.2 Let α be a $\mathbf{Z}^d$-action by homeomorphisms of an arbitrary set X. For $\mathbf{n} \in \mathbf{Z}^d \backslash \{\mathbf{0}\}$ put $F_{\mathbf{n}} = F_{\mathbf{n}}(\alpha) = \{x \in X : \alpha^{\mathbf{n}}(x) = x\}$, $F_\alpha = \bigcap_{\mathbf{n} \in \mathbf{Z}^d} F_{\mathbf{n}}$, $P_{\mathbf{n}} = P_{\mathbf{n}}(\alpha) = \bigcup_{m \in \mathbf{Z} \backslash \{0\}} F_{m\mathbf{n}}$, and $P_\alpha = \bigcup_{\mathbf{n} \in \mathbf{Z}^d \backslash \{\mathbf{0}\}} F_{\mathbf{n}}$.

If $X = \mathbf{S}$ and α is an expansive $\mathbf{Z}^d$-action then P_α is dense in $\mathbf{S}$ (Theorem 2.5).

Note that, with respect to Corollary 2.1, if $\beta^{\mathbf{n}}(x) = x$ for all x in some set S then $\alpha^{n_1\mathbf{m}_1 + \cdots + n_d\mathbf{m}_d}(x) = x$ for all x in S. That is, there exists $\mathbf{n}' \in \mathbf{Z}^d \backslash \{\mathbf{0}\}$ such that all points fixed by $\beta^{\mathbf{n}}$ are also fixed by $\alpha^{\mathbf{n}'}$. In particular:

Observation 2.4 The property that $|F_{\mathbf{n}}| < \infty$ for all $\mathbf{n} \in \mathbf{Z}^d \backslash \{\mathbf{0}\}$ is preserved if we replace an $\mathbf{R}^d$-basis in $\mathbf{Z}^d$ by the standard orthonormal basis.

Notation 2.3 Let $\{\mathbf{e}_1, \cdots, \mathbf{e}_d\}$ be the standard orthonormal basis for $\mathbf{Z}^d$. For $Y \subset X$ and $i \leq j$ in $\{1, \cdots, d\}$ put $\mathcal{O}_i^j(Y) = \{\alpha^{n_i\mathbf{e}_i + n_{i+1}\mathbf{e}_{i+1} + \cdots + n_j\mathbf{e}_j}(Y) : (n_i, n_{i+1}, \cdots, n_j) \in \mathbf{Z}^{j-i+1}\}$. Put $\mathcal{O}_i = \mathcal{O}_i^i$. If $Y = \{x\}$, a singleton set, we denote $\mathcal{O}_i^j(\{x\})$ and $\mathcal{O}_i(\{x\})$ by $\mathcal{O}_i^j(x)$ and $\mathcal{O}_i(x)$ respectively.

If $j \in \{1, \cdots, d\}$ is fixed and, for $i \in \{1, \cdots, d\}$, the $\mathbf{R}^d$-basis $\{\mathbf{m}_1, \cdots, \mathbf{m}_d\}$ in Corollary 2.1 is such that $\mathbf{m}_i = \mathbf{e}_i$ if $i \neq j$ and $\mathbf{m}_j = \mathbf{m}$ for some $\mathbf{m} = (m_1, \cdots, m_d) \in \mathbf{Z}^d$ (so $m_j \neq 0$) then note that $\beta^{\mathbf{e}_j} = \alpha^{\mathbf{m}}$ and, for all $i \in \{1, \cdots, d\} \backslash \{j\}$ and $n \in \mathbf{Z}$, $\beta^{n\mathbf{e}_i} = \alpha^{n\mathbf{e}_i}$. That is:

Observation 2.5 If $i \neq j$ and $m_j \neq 0$ then $\mathcal{O}_i(Y)$, for all $Y \subset X$, and $F_{\mathbf{e}_i}$ are unaffected if $\mathbf{m} = (m_1, \cdots, m_d)$ is replaced by $\mathbf{e}_j$. What was "$F_{\mathbf{m}}$" before replacement becomes "$F_{\mathbf{e}_j}$".

It is known that a $\mathbf{Z}$-action (action generated by a single homeomorphism) on the circle cannot be expansive, see for example Walters [64, Theorem 5.27] which is based upon Reddy's proof [51]. Theorem 2.5 gives rise to the following different proof of this.

Theorem 2.8 *A continuous $\mathbf{Z}$-action T on the circle $\mathbf{S}$ cannot be expansive.*

Proof: Suppose T is expansive and without loss of generality assume T preserves orientation. If $|F_m| < \infty$ for all $m \in \mathbf{Z}\backslash\{0\}$ then take $m \in \mathbf{Z}\backslash\{0\}$ with $F_m \neq \emptyset$ and assume without loss of generality that $m = 1$. We can find an interval $[x_1, x_2]$ of non-zero length in $\mathbf{S}$ with $F_1 \cap [x_1, x_2] = \{x_1, x_2\}$ (x_1 and x_2 may be the same point, giving unit length). Since T is strictly monotone on the open interval (x_1, x_2), all interior points of $[x_1, x_2]$ must have infinite T-orbit, contradicting Theorem 2.5. Therefore there must exist $m_0 \in \mathbf{Z}\backslash\{0\}$ with $|F_{m_0}| = \infty$. Assume without loss of generality that $m_0 = 1$. Then given any $\delta > 0$ there exists $x, y \in F_1$ with $\rho(x, y) \leq \delta$, so that $\rho(T^n x, T^n y) = \rho(x, y) \leq \delta$ for all $n \in \mathbf{Z}$, contradicting expansiveness. □

To prove the same result for arbitrary $\mathbf{Z}^d$-actions on $(\mathbf{S}, \rho)$ we first prove it for $\mathbf{Z}$ on $(\mathbf{I}, \mu)$ and then for $\mathbf{Z}^d$ on $(\mathbf{I}, \mu)$ for arbitrary intervals $\mathbf{I}$ in $\mathbf{S}$ and the metric μ of Lebesgue measure (normalised on $\mathbf{S}$).

Proposition 2.1 *A continuous* $\mathbf{Z}$*-action* T *on a closed interval with the Lebesgue measure metric* μ *cannot be expansive.*

Proof: Everything in Theorem 2.5 and Theorem 2.8 carries through to $(\mathbf{I}, \mu)$. $\square$

Proposition 2.2 *A continuous* $\mathbf{Z}^d$*-action* α *cannot act expansively on a closed interval* $\mathbf{I}$ *with the Lebesgue measure metric* μ.

Proof: We note that the statement is true for $d = 1$, by Proposition 2.1, and proceed by induction. Assume that $d > 1$ and that the statement is true for $\mathbf{Z}^k$-actions for all $k < d$. We consider two separate cases (A) and (B). The latter breaks down into two further cases, (i) and (ii), and (ii) itself breaks down further into cases (a) and (b). Thus we have cases (A), (B)(i), (B)(ii)(a), and (B)(ii)(b). Throughout we assume, for a contradiction, that the $\mathbf{Z}^d$-action α is expansive (and hence that P_α is dense) and we assume, without loss of generality, that orientation is preserved.

(A) First assume that $|F_{\mathbf{m}}|$ is finite for all $\mathbf{m} \in \mathbf{Z}^d \backslash \{\mathbf{0}\}$. Now $\alpha^{\mathbf{e}_1}$ clearly permutes $F_{\mathbf{m}}$ for any $\mathbf{m} \in \mathbf{Z}$, so take $\mathbf{m} \in \mathbf{Z}\backslash\{0\}$ such that $F_{\mathbf{m}} \neq \emptyset$. Some iterate of $\alpha^{\mathbf{e}_1}$ fixes $F_{\mathbf{m}}$ pointwise, this may as well be $\alpha^{\mathbf{e}_1}$ itself. So $F_{\mathbf{e}_1} \neq \emptyset$ (this we know to be true for a $\mathbf{Z}^d$-action on a closed interval, before this replacement, since orientation preservation implies that the end points are fixed, but this replacement IS needed in Theorem 2.9 which refers to this proof, but with the closed interval replaced by the circle). Since $0 < |F_{\mathbf{e}_1}| < \infty$ (by Observation 2.4) we may assume without loss of generality that only the end points of interval I of positive Lebesgue measure (unit measure if $|F_{\mathbf{e}_1}| = 1$ and hence the end points are the same point) are fixed by $\alpha^{\mathbf{e}_1}$. Then $\alpha^{\mathbf{e}_1}$ must be strictly monotone on the interior of our I so that the $\alpha^{\mathbf{e}_1}$-orbit of every interior point is infinite. Expansiveness implies that there exists $\mathbf{n} \in \mathbf{Z}^d\backslash\{0\}$ and an interior point of I which belongs to $F_{\mathbf{n}}$. But $|F_{\mathbf{n}}| < \infty$ (by Observation 2.4), contradicting the infinite $\alpha^{\mathbf{e}_1}$-orbit, since $F_{\mathbf{n}}$ is $\alpha^{\mathbf{e}_1}$-invariant.

(B) Suppose that $|F_{\mathbf{m}}| = \infty$ for some $\mathbf{m} \in \mathbf{Z}^d\backslash\{\mathbf{0}\}$. Without loss of generality we may replace $\mathbf{m}$ by $\mathbf{e}_1$. Clearly $F_{\mathbf{e}_1}$ is a closed subset of our interval: if it is dense then it implies that $\alpha^{\mathbf{e}_1}$ is the identity, giving a $\mathbf{Z}^{d-1}$-action and we appeal to our induction hypothesis. So, since $F_{\mathbf{e}_1}$ is closed, we may assume that there exists distinct $x_1, y_1 \in \mathbf{I}$ such that $[x_1, y_1] \cap F_{\mathbf{e}_1} = \{x_1, y_1\}$. We observe two possibilities.

(i) Since $|F_{\mathbf{e}_1}| = \infty$, if there exists only finitely many intervals such as (x_1, y_1) then $F_{\mathbf{e}_1}$ must be dense over some interval of positive Lebesgue measure in the compliment of this finite set of open intervals and hence must contain some such interval in this compliment, since $F_{\mathbf{e}_1}$ is closed. So $F_{\mathbf{e}_1}$ must consist of a finite number of isolated points (possibly none) and also a finite number (but at least one) of positive Lebesgue measure, closed, pointwise $\alpha^{\mathbf{e}_1}$-invariant intervals which are maximal in that they are not proper sub-intervals of any other intervals which are contained in $F_{\mathbf{e}_1}$, let I be one of these intervals.

For each $2 \leq i \leq d$, since $\alpha^{\mathbf{e}_i}$ permutes $F_{\mathbf{e}_1}$ and is a homeomorphism it must also send these proper intervals to one another. But there are only finitely many intervals such as I. So clearly, for all $i \in \{2, \ldots, d\}$, there exists $m_i \in \mathbf{N}$ such that $\alpha^{m_i \mathbf{e}_i}(I) = I$ (though not necessarily pointwise). Assume without loss of generality that $m_i = 1$ for $2 \leq i \leq d$. Since I is pointwise fixed by $\alpha^{\mathbf{e}_1}$ we now have that the restriction $\alpha|_I$ is a $\mathbf{Z}^{d-1}$-action on I and so is non-expansiveness, by the induction hypothesis. It clearly follows that α itself is non-expansive.

(ii) So suppose that there exists an infinite family $\mathcal{F} = \{I_n\}_{n\in\mathbf{N}} = \{[x_n, y_n]\}_{n\in\mathbf{N}}$ of intervals such that $I_n \cap F_{\mathbf{e}_1} = \{x_n, y_n\}$ for all $n \in \mathbf{N}$. Since, for all $\mathbf{m} \in \mathbf{Z}^d \backslash \{0\}$, $\alpha^{\mathbf{m}}$ clearly permutes $F_{\mathbf{e}_1}$ and is a homeomorphism it must also permute $\mathcal{F}$. Furthermore the distinct members of $\mathcal{F}$ may clearly only intersect at end points. We consider two cases.

(a) If $\mathcal{O}_2^d(I_m) = \{\alpha^{n_1\mathbf{e}_2 + \ldots + n_{d-1}\mathbf{e}_d}(I_m) : (n_1, \ldots, n_{d-1}) \in \mathbf{Z}^{d-1}\}$ is a finite collection of intervals for all $m \in \mathbf{N}$ then $\mathcal{F}$ is an infinite union of such orbits and, given potential expansive constant $\delta > 0$, there exists $m \in \mathbf{N}$ such that $\mathcal{O}_2^d(I_m)$ contains only intervals of Lebesgue measure less than δ, contradicting expansiveness on x_m and y_m, since each interval in $\mathcal{O}_2^d(I_m)$ is also $\alpha_{\mathbf{e}_1}$-invariant (end points of such intervals are in $F_{\mathbf{e}_1}$ and orientation is preserved).

(b) So finally assume that $\mathcal{O}_2^d(I_m) = \{\alpha^{n_1\mathbf{e}_2 + \ldots + n_{d-1}\mathbf{e}_d}(I_m) : (n_1, \ldots, n_{d-1}) \in \mathbf{Z}^{d-1}\}$ is an infinite collection of intervals for some $m \in \mathbf{N}$. Put $I = I_m$. If $|\mathcal{O}_i(I)| < \infty$ for $2 \leq i \leq d$ then $|\mathcal{O}_2^d| < \infty$ so, without loss of generality, assume that there exists $j \in \{2, \cdots, d\}$ such that $i \in \{2, \cdots, j-1\}$ implies that $|\mathcal{O}_i(I)| = a_i \in \mathbf{N}$ and $i \in \{j, \cdots, d\}$ implies that $|\mathcal{O}_i(I)| = \infty$.

By observation 2.5 we may incrementally replace $a_i\mathbf{e}_i$ by $\mathbf{e}_i$ for $i = 2$ then for $\cdots$ then for $i = j-1$ so that $\mathcal{O}_1^{j-1}(I) = \{I\}$ and $|\mathcal{O}_i(I)| = \infty$ for $i \in \{j, \cdots, d\}$. If the members of $\mathcal{O}_j^d$ are not all distinct we apply the following step (with the initial value $k = 1$) which may be applied inductively until we do have this desired condition.

In general if, for some $k \in \{1, \cdots, d-j\}$, $\mathcal{O}_1^{j+k-2}(I) = \{I\}$, $|\mathcal{O}_i| = \infty$ for $i \in \{j+k-1, \cdots, d\}$, and there exists $\mathbf{n} = (n_1, \cdots, n_{d-j-k+2}) \in \mathbf{Z}^{d-j-k+2}\backslash\{0\}$ such that $\alpha^{n_1\mathbf{e}_{j+k-1}+\cdots+n_{d-j-k+2}\mathbf{e}_d}(I) = I$ (not necessarily point-wise of course) then we may assume, without loss of generality, that $n_1 \neq 0$ and replace $\mathbf{n}$ by $\mathbf{e}_{j+k-1}$ so that, by observation 2.5, $\mathcal{O}_1^{j+k-1}(I) = \{I\}$ and $|\mathcal{O}_i(I)| = \infty$ for $i \in \{j+k, \cdots, d\}$.

Thus, eventually we must get, for some $m \in \{0, \cdots, d-j\}$, that $\mathcal{O}_1^{j+m-1}(I) = \{I\}$ and that $\mathcal{O}_{j+m}^d(I)$ is an infinite family of <u>distinct</u> closed intervals whose interiors are mutually disjoint (if we get as far as $m = d-j$ then we'd have that $|\mathcal{O}_{j+1}^d(I)| = |\mathcal{O}_d^d(I)| = |\mathcal{O}_d(I)| = \infty$ so that, certainly, $\alpha^{n_1\mathbf{e}_{j+m}}(I) = \alpha^{n_1\mathbf{e}_d}(I) \neq I$ for all $n_1 \in \mathbf{Z}\backslash\{0\}$).

Now I is (not necessarily pointwise) invariant under the action of the map-group $G = \langle\langle\alpha^{n_1\mathbf{e}_1+\ldots,n_{j+m-1}\mathbf{e}_{j+m-1}} : (n_1, \ldots, n_{j+m-1}) \in \mathbf{Z}^{j+m-1}\rangle\rangle$ where $j+m-1 \leq d-1$ and so, by our induction hypothesis, the restriction of this action to I, β say, is not expansive.

Furthermore, given a potential expansive constant $\delta > 0$, all but a finite subset, $\{\alpha^{\mathbf{n}_i}(I) : 1 \leq i \leq p\}$ say (where $p \in \mathbf{Z}^+$), of members of $\mathcal{O}_{j+m}^d(I)$ must have Lebesgue measure less than δ. But, for $1 \leq i \leq p$, by uniform continuity of $\alpha^{\mathbf{n}_i}$ there exists δ_i such that $u, v \in I$ and $\mu(u,v) < \delta_i$ implies that $\mu(\alpha^{\mathbf{n}_i}(u), \alpha^{\mathbf{n}_i}(v)) < \delta$. But by non-expansiveness of β we can find distinct $u_0, v_0 \in I$ such that $\mu(\gamma(u_0), \gamma(v_0)) < \min\{\delta_i : 1 \leq i \leq p\}$ for all $\gamma \in G$. $\square$

Remark 2.4 The above inductive argument cannot be directly applied to $\mathbf{S}$ because in assuming the induction hypothesis and applying it to I in the last sentence of part (B)(i) the metric ρ_I on I itself would have to be assumed to be like the circle metric ρ in that two points x and y could be δ close according to ρ_I because they are each, for example, within $\delta/2$ of the opposite ends of I so that $\rho_I(x,y) \leq \delta$ and yet $\rho(x,y) > \delta$, the interval I may be arbitrarily close to the whole of $\mathbf{S}$. Similar remarks apply, in part (B)(ii), for intervals whose end points are less than or equal to δ apart in the circle metric.

This brings us to the main result of the chapter.

Theorem 2.9 *A continuous $\mathbf{Z}^d$-action α on the circle cannot be expansive.*

Proof: Apply the proof of Proposition 2.2 with $\mathbf{I}$ replaced by $\mathbf{S}$ and μ replaced by ρ, but at the stage in part (B)(i) referred to in Remark 2.4 appeal to the statement of Proposition 2.2 for I as an interval with metric μ on $I \subset \mathbf{S}$ but normalised on $\mathbf{S}$. For $\mu(x,y) \leq \delta < 1/2$ we are then assured that $\rho(x,y) = \mu(x,y) \leq \delta$. In part (B)(ii), we can be assured that not only are $\rho(x_1, y_1) \leq \delta$ and $\rho(g(x_1), g(y_1)) \leq \delta$ for all g in the co-finite subset $\alpha(\mathbf{Z}^d)\backslash G$ of the action but that the Lebesgue measure of, without loss of generality, the respective intervals is less than or equal to δ, thus ensuring that, for $\delta < 1/2$, $\rho(u,v) \leq \delta$ and $\rho(g(u), g(v)) \leq \delta$ for all g in $\alpha(\mathbf{Z}^d)\backslash G$, for any chosen u, v in $[x_1, y_1]$. For the uniform continuity argument we again apply the statement of Proposition 2.2 to I as an interval with metric μ on $I \subset \mathbf{S}$ normalised on $\mathbf{S}$ and also put the μ-metric, normalised on $\mathbf{S}$, on each of the respective finite set of intervals and then appeal to uniform continuity. $\square$

Corollary 2.2 *A finitely generated Möbius group G of polynomial growth cannot act expansively on the circle.*

Proof: By Theorem 1.1 such a group must contain a nilpotent subgroup of finite index so, for purposes of non-expansiveness, we can assume G to be finitely generated nilpotent and Möbius. Theorem 2.4 then tells us that G is commutative, so we apply Theorem 2.9. $\square$

Remark 2.5 Work of Witte [66] shows that certain lattices in Lie groups cannot act faithfully by homeomorphisms of the circle. For example, if Γ is a subgroup of finite index in $SL_n(\mathbf{Z})$ with $n \geq 3$ then Γ has no continuous faithful actions on $\mathbf{S}$ (see Corollary 2.4$'$ in Witte [66]).

Chapter 3

Topological entropy and commuting maps on metric groups

3.1 A result for translation invariant metrics

Remark 3.1 For $\alpha = T$, the $\mathbf{N}$-action generated by a single uniformly continuous map $T : X \to X$, the non-invertible analogue of Definition 1.4 makes sense when the metric space, X, is not necessarily compact (here, $Q_n = \{0, \cdots, n-1\}$ for all $n \in \mathbf{N}$). See, for example Walters [64, Section 7.2] for this fact which is due to Bowen. Thus, X in the following theorem is not necessarily compact.

Theorem 3.1 *Suppose $T : X \to X$ is a uniformly continuous surjective group endomorphism of a metric group (X, ρ) with translation invariant metric (that is, if $x, y, z \in X$ then $\rho(xz, yz) = \rho(x, y)$). Then $h(T) \geq \log(|\ker(T)|)$, with $h(T) = \infty$ if $|\ker(T)| = \infty$.*

Example 3.1 The one-sided (non-invertible) full-shift on p symbols has entropy $\log p$, exactly the logarithm of the size of the kernel.

Example 3.2 The only continuous endomorphisms of the circle group (viewed additively (mod 1)) are of the form $x \mapsto mx \pmod 1$ for all $x \in \mathbf{S}$, for some $m \in \mathbf{Z}$. The corresponding entropy is $\log m$, exactly the logarithm of the size of the kernel.

Example 3.3 The only continuous endomorphisms of the d-dimensional toral group $\mathbf{S}^d$ (viewed additively (mod 1) in the obvious coordinatewise manner) are of the form $\mathbf{x} \mapsto A\mathbf{x}$ (mod 1) for all $\mathbf{x} \in \mathbf{S}^d$, for some non-singular integer $d \times d$ matrix A. The corresponding entropy is the logarithm of the product of those eigenvalues of A that have modulus greater than one. The size of the kernel of this map is the product of <u>all</u> of the eigenvalues of A and hence its logarithm is less than or equal to the entropy of the map.

Proof of Theorem 3.1: By surjectivity, $T^{-1}(x) \neq \emptyset$ for all $x \in X$ and thus, since T is a group homomorphism, $|T^{-1}(x)| = |\ker(T)|$ for all $x \in X$.

Furthermore, for fixed $x_0 \in T^{-1}(x)$, $T^{-1}(x) = \{x_0 z : z \in \ker(T)\}$ and so by translation invariance of ρ, $T^{-1}(x)$ is isometric to $\ker(T)$ for all $x \in X$.

For any finite subset $A \subset \ker(T)$ there clearly exists $\epsilon > 0$ such that $\rho(a_1, a_2) > \epsilon$ for all $a_1, a_2 \in A$ and, by the isometry between $T^{-1}(x)$ and $\ker(T)$ for all $x \in X$ there exists $A^x \subset T^{-1}(x)$ with the same property for the same value of ϵ for all $x \in X$.

If $|\ker(T)| = \infty$ then take a strictly increasing (A_n is a proper subset of A_{n+1} for all $n \in \mathbf{N}$) sequence $\{A_n\}_{n\in\mathbf{N}}$ of subsets of $\ker(T)$ with respective sequence $\{\epsilon_n > 0\}_{n\in\mathbf{N}}$ such that A_n is $(0, \rho, \epsilon_n)$-separated, as is some appropriate set A_n^x, which is isometric (to A_n), for all $x \in X$, for all $n \in \mathbf{N}$. We may assume that $\lim_{n\to\infty} \epsilon_n = 0$ (necessary if X is compact).

For $|\ker(T)| < \infty$ there exists $\epsilon_0 > 0$ such that $\epsilon_0 > \epsilon > 0$ implies that $\ker(T)$ is $(0, \rho, \epsilon)$-separated and we assume that $A_n = \ker(T)$ and $\epsilon_0 > \epsilon_n > 0$ for all $n \in \mathbf{N}$, and that $\lim_{n\to\infty} \epsilon_n = 0$.

So, for all $n \in \mathbf{N}$ and for all $x \in X$, A_n^x is $(0, \rho, \epsilon_n)$-separated. Furthermore if, for $k \in \mathbf{Z}^+$, some set B is (k, ρ, ϵ_n)-separated then $\bigcup_{x\in B} A_n^x$ is $(k+1, \rho, \epsilon_n)$-separated since, if $x_1 \neq x_2$ in $\bigcup_{x\in B} A_n^x$ then EITHER x_1 and x_2 are both from the same A_n^x so that $\rho(x_1, x_2) > \epsilon_n$ (since A_n^x is $(0, \rho, \epsilon_n)$-separated) OR $T(x_1) \neq T(x_2)$, in which case there exists $i \in \{0, 1, \cdots, n-1\}$ such that $\rho(T^i(T(x)), T^i(T(x))) > \epsilon_n$, since $T(x_1), T(x_2) \in B$ and B is (k, ρ, ϵ_n)-separated. Thus, $S_{k+1}(\rho, \epsilon_n) \geq |A_n| S_k(\rho, \epsilon_n)$. So

$$h(T) = \lim_{\epsilon\to 0} \limsup_{k\to\infty} \frac{\log S_k(\rho, \epsilon)}{k} \geq \lim_{n\to\infty} \lim_{k\to\infty} \frac{\log(|A_n|^k S_0(\rho, \epsilon_n))}{k}$$

$$\geq \lim_{n\to\infty} \lim_{k\to\infty} \frac{\log(|A_n|^{k+1})}{k} = \lim_{n\to\infty} \log|A_n| = \log|\ker(T)| \ \text{ or } \ \infty$$

depending on whether $|\ker(T)|$ is finite or infinite respectively. □

3.2 Actions by the semi-group N and inverse limits

Recall that $(\Omega_p(d), \sigma)$, or just $\Omega_p(d)$, is the d-dimensional full shift on p symbols.

Shereshevsky's conjecture, Problem 1.2, suggests that $\mathbf{Z}$ cannot act by continuous shift commuting maps with finite positive entropy on $(\Omega_2(2), \sigma)$, or simply Ω, the full two dimensional two shift as in Definition 1.5.

We prove a form of Shereshevsky's conjecture, for Ω_p instead of Ω_2 where p is any fixed prime, and use the result in the joint paper [42] (an account of which constitutes the latter part of this chapter) with Ward to answer (for the case $d = 2$ and $e = 1$) Problem 1.3; that a mixing action of $\mathbf{Z}^e$ by continuous automorphisms of a compact metric abelian group that commutes with a K-action of $\mathbf{Z}^d$ by continuous automorphisms cannot have finite positive entropy if $e \leq d - 1$.

We initially address Shereshevsky's Conjecture, formulated instead for continuous $\mathbf{N}$-actions (not necessarily invertible maps), for an interesting class of continuous maps T of (Ω, σ) (see Notation 1.1), the class of *algebraic cellular automata*. These maps are all of the form

$$(T(x))_{\mathbf{n}} = \sum_{\mathbf{m}\in\mathbf{Z}^2} c_f(\mathbf{m}) x_{\mathbf{n}+\mathbf{m}} \ (\mathrm{mod}\ p)$$

for all $\mathbf{n} \in \mathbf{Z}^2$, where $c_f(\mathbf{n}) \in \{1, \cdots, p-1\}$ for finitely many $\mathbf{n} \in \mathbf{Z}^2$ and $c_f(\mathbf{n}) = 0$ otherwise; they are clearly cellular automata in the sense given at the end of Section 1.5. So, for all $\mathbf{n} \in \mathbf{Z}^2$, $c_f(\mathbf{n})$ can be considered to be the coefficient of $u^{\mathbf{n}}$ in

$$f = \sum_{\mathbf{n}\in\mathbf{Z}^2} c_f(\mathbf{n}) u^{\mathbf{n}} \in \mathcal{R}_{2,p} = \mathbf{Z}_{/p}[u_1^{\pm 1}, u_2^{\pm 1}],$$

where $\mathcal{R}_{2,p}$ is the ring of Laurent polynomials in commuting variables u_1, u_2 with coefficients in $\mathbf{Z}_{/p}$ and $u^{\mathbf{n}} = u_1^{n_1} u_2^{n_2}$ for all $\mathbf{n} = (n_1, n_2) \in \mathbf{Z}^2$. The polynomial f uniquely determines T, and T uniquely determines f.

Notice that maps of the form T are continuous group endomorphisms of the compact metric abelian group Ω. There is an extensively developed theory for such algebraic dynamical systems with the $\mathbf{N}$-action $\{T^n : n \in \mathbf{N}\}$ replaced by general $\mathbf{Z}^d$-actions by continuous group automorphisms and Ω replaced by various other interesting compact metric groups (see the monograph [60] by Schmidt).

An example of such a $\mathbf{Z}^d$-action is the inverse limit $(\widetilde{\Omega}, \widetilde{\sigma}, \widetilde{T})$ of the case we are considering, (Ω, σ, T). That is, the $\mathbf{Z}$-action generated by the shift component $\widetilde{T} = \sigma^{(0,0,1)}$ on the subshift of finite type and subgroup $\widetilde{\Omega} = \Sigma(3)$ of $\Omega(3)$ (i.e. $d = 3$ for the inverse limit system) given by

$$\widetilde{\Omega} = \Sigma(3) = \{x \in \Omega(3) : x_{(n_1,n_2,n_3+1)} = (T((x_{(m_1,m_2,n_3)})_{(m_1,m_2)\in\mathbf{Z}^2}))_{(n_1,n_2)}$$

for all $(n_1, n_2, n_3) \in \mathbf{Z}^3\}$, where the original two dimensional shift is represented by

$$\widetilde{\sigma} = \{\sigma^{(n_1,n_2,0)} : (n_1, n_2) \in \mathbf{Z}^2\}.$$

These actions in general originate from Ledrappier's [30] example of the shift action σ of $\mathbf{Z}^2$ on the closed shift invariant subgroup

$$\{x \in \Omega_2(2) : x_{(n_1,n_2)} + x_{(n_1+1,n_2)} + x_{(n_1,n_2+1)} = 0 \,(\mathrm{mod}\, 2) \text{ for all } (n_1, n_2) \in \mathbf{Z}^2\}$$

(so d=2 and p=2) of the full two-dimensional two-shift.

Ledrappier's example is the inverse limit of the $\mathbf{N}$-action generated by the map T' of $(\Omega, \sigma) = (\Omega_2(1), \sigma)$ given by $(T'(x))_n = x_n + x_{n+1} \,(\mathrm{mod}\, 2)$ for all $x \in \Omega$ and $n \in \mathbf{Z}$. A natural progression from this action to the type that we are considering is $T : \Omega_2(2) \to \Omega_2(2) = \Omega$ given by

$$(T(x))_{(n_1,n_2)} = x_{(n_1,n_2)} + x_{(n_1+1,n_2)} + x_{(n_1,n_2+1)} \;(\mathrm{mod}\, 2)$$

for all $x \in \Omega$ and $(n_1, n_2) \in \mathbf{Z}^2$. Here the original space is $\{0,1\}^{\mathbf{Z}}$ and the inverse limit space constructed inside $\{0,1\}^{\mathbf{Z}^2}$ may be identified with $\{0,1\}^{\mathbf{Z}\times\mathbf{N}}$ since the rule T determines every point $x_{(n_1,n_2,n_3)}$ with $n_3 > 0$ from the values of $x_{(n_1,n_2,0)}$. The respective polynomial in $\mathcal{R}_2$ for T is $f = 1 + u_1 + u_2$. The behaviour of such shift commuting maps is everywhere determined by the appropriate translates of the set of values of $\mathbf{n} \in \mathbf{Z}^2$ for which $c_f(\mathbf{n}) \neq 0$, in this case $(0,0)$, $(1,0)$, and $(0,1)$. Note that these points are not co-linear in $\mathbf{Z}^2$, the significance of which will become apparent as our argument develops.

We answer Shereshevsky's Conjecture for $\mathbf{N}$-actions for our class of examples by appealing to the well-known Theorem below (the earliest explicit proof we found is in Conze [12] for instance).

Theorem 3.2 *Let T be a continuous map of a compact metric space X. If the $\mathbf{N}$-action generated by T on X is expansive then*

$$\limsup_{n\to\infty} \frac{\log F_n(T)}{n} \leq h(T) \tag{3}$$

where $F_n(T)$ is the number of elements of X fixed by T^n for all $n \in \mathbf{N}$.

Proof: See Conze [12].

Example 3.4 For the special case of an axiom A diffeomorphism, Bowen [7] showed that we have equality in (3).

Example 3.5 The existence of an irreducible shift space with no periodic points and positive entropy is alluded to in Lind and Marcus [33, Exercise 4.1.11]. Hence the inequality in (3) may be strict for expansive maps.

Example 3.6 In many algebraic settings, the inequality (3) holds even without expansiveness; see Chothi, Everest and Ward [11, Section 6].

3.3 Convex maps and expansiveness

We consider maps on the 2-dimensional p-shift space $\Omega = \Omega_p(2)$, where p is any fixed prime.

Definition 3.1 Let the continuous map $T : \Omega \to \Omega$ be determined by the polynomial $f \in \mathcal{R}_{2,p}$, and suppose that $c \in \mathbf{N}$ and the set of points, $\{\mathbf{m}_i : 1 \leq i \leq c\} \subset \mathbf{Z}^2$ for which $c_f(\mathbf{m}_i) \neq 0$ along with the origin $\mathbf{0} \in \mathbf{Z}^2$ are not co-linear in $\mathbf{R}^2$. Then T is a *convex* map of Ω *with hull H* where H is the convex hull formed by $\{\mathbf{0}, \mathbf{m}_1, \dots, \mathbf{m}_c\}$.

For the sake of illustration, Proposition 3.1, Theorem 3.3, and Theorem 3.4 are proved for $p = 2$. Note that the proofs readily extend to a general prime p.

Proposition 3.1 *Let T be a convex map of Ω. Then there exists $\mathbf{k} \in \mathbf{Z}^2 \backslash \{\mathbf{0}\}$ such that, for any $n \in \mathbf{N} \backslash \{0\}$, the $\mathbf{N}$-action generated by the restriction of T to the closed shift-invariant subgroup $\Omega^{n\mathbf{k}} = \{x \in \Omega : x_{\mathbf{n}} = x_{\mathbf{n}+n\mathbf{k}}$ for all $\mathbf{n} \in \mathbf{Z}^2\}$ of Ω is expansive.*

Example 3.7 Consider $\Omega = \Omega_2(2)$ and the convex map $T : \Omega \to \Omega$ given by, for all $\mathbf{x} \in \Omega$, $(T(\mathbf{x}))_{\mathbf{m}} = x_{\mathbf{m}} + x_{\mathbf{m}+(0,1)} + x_{\mathbf{m}+(1,0)} \pmod 1$ for all $\mathbf{m} \in \mathbf{Z}^2$. If $\mathbf{k} = (1,1)$ then, given $n \in \mathbf{N}$, let $S \subset \mathbf{R}^2$ be the strip parallel to the $(1,1)$ direction, centered at $(0,0)$, and of thickness $n\sqrt{2}$. Let $D \subset \mathbf{R}^2$ be the square with two of its sides parallel to the $(1,1)$ direction, centered at $(0,0)$, and of side-length $n\sqrt{2}$, any two points $\mathbf{x}, \mathbf{y} \in \Omega^{n\mathbf{k}}$ such that $x_{\mathbf{n}} \neq y_{\mathbf{n}}$ for some $\mathbf{n} \in S$ must also have $x_{\mathbf{m}} \neq y_{\mathbf{m}}$ for some $\mathbf{m} \in D$, by the construction of $\Omega^{n\mathbf{k}}$. But if $\mathbf{u}, \mathbf{v} \in \Omega^{n\mathbf{k}}$ and $R \subset \mathbf{R}^2$ is the thinnest strip centered at $(0,0)$ and parallel to the strip S such that $u_{\mathbf{q}} \neq v_{\mathbf{q}}$ for some $\mathbf{q} \in \mathbf{Z}^2$ which lies on an edge of R then, clearly, $(T(\mathbf{u}))_{\mathbf{p}} \neq (T(\mathbf{v}))_{\mathbf{p}}$ for some $\mathbf{p} \in \mathbf{Z}^2$ which lies on an edge of that strip in $\mathbf{R}^2$ parallel to R and thinner than R by $\sqrt{2}$. We can repeat this until $(T^b(\mathbf{u}))_{\mathbf{c}} \neq (T^b(\mathbf{v}))_{\mathbf{c}}$ for some $b \in \mathbf{N}$ and $\mathbf{c} \in S \cap \mathbf{Z}^2$ and, without loss of generality, $\mathbf{c} \in D \cap \mathbf{Z}^2$. Expansiveness follows.

Remark 3.2 The method of "approximating" subdynamics in a $\mathbf{Z}$-action by restriction to subshifts of a large shift-period in some direction is used in Chothi, Everest and Ward [11].

Proof of Proposition 3.1: Let T be determined by $f \in \mathcal{R}_{2,2}$ and let $\{\mathbf{m}_i : 1 \leq i \leq c\}$, for some $c \in \mathbf{N}$, be the set of points for which $c_f(\mathbf{m}_i) \neq 0$. Suppose T has hull H in $\mathbf{Z}^2$. Choose a line L through $\mathbf{0}$ of rational gradient in $\mathbf{R}^2$ that has non empty intersection in $\mathbf{R}^2$ with the interior of H and is therefore not parallel to any of the faces of H.

By Theorem 2.7 and Definition 1.5, we may use any metric ρ which makes points $x, y \in \Omega$ close when $x(\mathbf{n})$ and $y(\mathbf{n})$ agree for all $\mathbf{n} \in \mathbf{Z}^2$ within a large radius of the origin $\mathbf{0} \in \mathbf{Z}^2$.

For any real number $r \geq 0$ let $S(r)$ be the closed (in $\mathbf{R}^2$) square of side length r, centered at $\mathbf{0}$ and with two of its sides parallel to L. For any x, y in Ω let $\rho(x, y) = 0$ if $y = x$ and $(1/2)^{I(x,y)}$ otherwise, where

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

So ρ is greatest when $x_{\mathbf{0}} \neq y_{\mathbf{0}}$, giving $\rho(x, y) = 1$.

Let the unit length vector $\mathbf{v} \in \mathbf{R}^2$ represent the direction perpendicular to L. Let $r' > 0$ and $r'' > 0$ in $\mathbf{R}$ be the greatest distances in the directions of $-\mathbf{v}$ and $\mathbf{v}$ respectively between L and a line parallel to L and containing one (by the construction of L it will be a single point) of the points $\{\mathbf{m}_i : 1 \leq i \leq c\}$; without loss of generality assume that the points are $\mathbf{m}_1$ and $\mathbf{m}_2$ respectively. Let $r''' \in \mathbf{R}$ be the distance between $\mathbf{0}$ and its nearest neighbour, $\mathbf{k}$ say, in $L \cap \mathbf{Z}^2$.

It may help to refer to the diagram on the next page for the remainder of the argument.

For any real number $R > \max\{2r', 2r'', r'''\}$, choose any $n \in \mathbf{N}$ such that $n\mathbf{k}$ is distance strictly less than R from $\mathbf{0}$. Put

$$\Omega^{n\mathbf{k}} = \{x \in \Omega : x_{\mathbf{n}} = x_{\mathbf{n}+n\mathbf{k}} \,\text{for all}\, \mathbf{n} \in \mathbf{Z}^2\}.$$

Let the distinct lines L_1, L_2 in $\mathbf{R}^2$ be those two lines that are each parallel to L and each contain a side of the square $S(R)$.

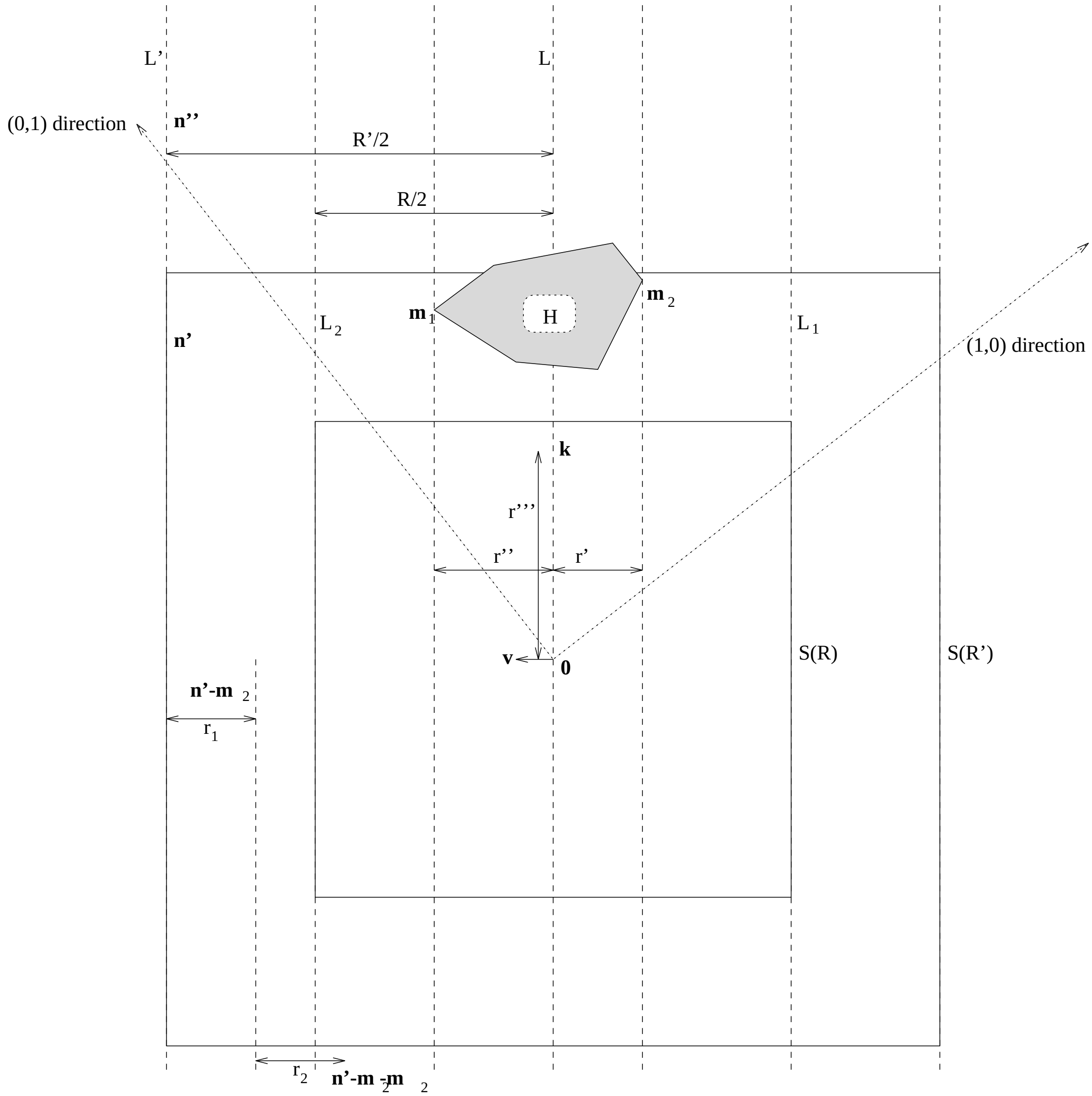

Figure 4: Proof of Proposition 3.1.

If $\rho(x,y) \le (1/2)^R$ for any $x \ne y$ in $\Omega^{n\mathbf{k}}$ then $x_{\mathbf{n}} \ne y_{\mathbf{n}}$ for some $\mathbf{n} \in \mathbf{Z}^2$ outside, or on the boundary of, $S(R)$. Furthermore, any such $\mathbf{n}$ cannot lie between L_1 and L_2, by the construction of $\Omega^{n\mathbf{k}}$. Since L has rational gradient there exists some minimal real number $R' \ge R$ and a line L' parallel to L and distance (in the direction of $\mathbf{v}$ or $-\mathbf{v}$) $R'/2$ from L such that $x_{\mathbf{n}''} \ne y_{\mathbf{n}''}$ for some $\mathbf{n}'' \in L' \bigcap \mathbf{Z}^2$ and so, furthermore, there exists $\mathbf{n}' \in S(R') \cap \mathbf{Z}^2$ (in fact, $\mathbf{n}' \in \partial(S(R')) \cap L' \cap \mathbf{Z}^2$, where $\partial(S(R'))$ is the boundary of $S(R')$) such that $x_{\mathbf{n}'} \ne y_{\mathbf{n}'}$ and clearly $\rho(x,y) = (1/2)^{R'}$. By our construction we know that, for $j=1$ or $j=2$, $x_{\mathbf{n}'+\mathbf{m}_i-\mathbf{m}_j} = y_{\mathbf{n}'+\mathbf{m}_i-\mathbf{m}_j}$ for all $i \in \{1,\ldots,c\} \backslash \{j\}$.

It follows that $(T(x))_{\mathbf{n}'-\mathbf{m}_j} \ne (T(y))_{\mathbf{n}'-\mathbf{m}_j}$. If $\rho(T(x),T(y)) \le (1/2)^R$ then, by the construction of $\Omega^{n\mathbf{k}}$, $\rho(T(x),T(y)) = (1/2)^{R'-2r_1}$ for some real r_1 such that $r' \le r_1 \le r''$ (without loss of generality, we are assuming that $r' \le r''$).

So we may inductively argue that if $(1/2)^{R'-2(r_1+\ldots+r_k)} = \rho(T^k(x),T^k(y)) \le (1/2)^R$ for some $k \in \mathbf{N}$ where $r' \le r_i \le r''$ for $1 \le i \le k$ then

$$\rho(T^{k+1}(x),T^{k+1}(y)) \le (1/2)^R \Rightarrow (1/2)^{R'-2(r_1+\ldots+r_{k+1})} = \rho(T^{k+1}(x),T^{k+1}(y))$$

where also $r' \le r_{k+1} \le r''$. Eventually we must get $R' - 2(r_1 + \ldots + r_{k'}) < R$ for some $k' \in \mathbf{N}$ and $r' \le r_i \le r''$ for $1 \le i \le k'$ giving $\rho(T^{k'}(x),T^{k'}(y)) > (1/2)^R$. So the $\mathbf{N}$-action generated by T is expansive on $\Omega^{n\mathbf{k}}$ with expansive constant $\delta = (1/2)^R$. Finally note that we could have selected R, and hence $|n\mathbf{k}|$, arbitrarily large (though for $n' \ne n''$ the expansive constants for T restricted to $\Omega^{n'\mathbf{k}}$ and $\Omega^{n''\mathbf{k}}$ respectively are not necessarily the same). $\square$

3.4 Shereshevsky's conjecture

Let $\mathcal{A}$ be any set and p any prime number. Partition $\mathcal{A}^p$ into equivalence classes according to the equivalence relation, $\sim$, given by $(a_0,\cdots,a_{p-1}) \sim (b_0,\cdots,b_{p-1})$ if and only if there exists $i \in \{0,\cdots,p-1\}$ such that, for all $j \in \{0,\cdots,p-1\}$, $a_j = b_{j+i\,(\mathrm{mod}\,p)}$. Furthermore, let $i : \mathcal{A} \to \mathcal{A}^p$ be the canonical embedding given by $i : a \mapsto (a,\cdots,a)$.

Lemma 3.1 *With the above notation, $\mathcal{A}^p \backslash i(\mathcal{A})$ is partitioned, by $\sim$, into equivalence classes each of cardinality p.*

Proof. Clearly, no equivalence class can have cardinality greater than p. If $a_j = a_{j+i\,(\mathrm{mod}\,p)}$ for all $j \in \{0, \cdots, p-1\}$ then $a_0 = a_i = a_{2i\,(\mathrm{mod}\,p)} = \cdots = a_{(p-1)i\,(\mathrm{mod}\,p)}$. But, since p is prime, $\{ki\,(\mathrm{mod}\,p) : 0 \leq k \leq p-1\} = \{0, \cdots, p-1\}$ unless $i = 0$. So if $i \neq 0$ and $a_j = a_{j+i\,(\mathrm{mod}\,p)}$ for all $j \in \{0, \cdots, p-1\}$ then $a_0 = \cdots = a_{p-1}$. In other words, if $a_k \neq a_l$ for some distinct $k, l \in \{0, \cdots p-1\}$ then, for all $i \in \{1, \cdots, p-1\}$, there exists $j = j(i) \in \{1 \cdots, p-1\}$ such that $a_j \neq a_{j+i\,(\mathrm{mod}\,p)}$. So, for all distinct $i, j \in \{0, \cdots, p-1\}$, $(a_i, \cdots, a_{i+p-1\,(\mathrm{mod}\,p)}) \neq (a_j, \cdots, a_{j+p-1\,(\mathrm{mod}\,p)})$ unless $a_0 = \cdots = a_{p-1}$. $\square$

Corollary 3.1 *Fermat's little theorem.*

Proof. Fix any $n \in \mathbf{N}$. With the above notation, let $\mathcal{A} = \{1, \cdots, n\}$. Then $n^p - n = |\mathcal{A}^p| - |\mathcal{A}| = |\mathcal{A}^p \backslash i(\mathcal{A})| = kp$ for some $k \in \mathbf{Z}^+$. $\square$

Lemma 3.1 is used in the multiple summation in the following observation, where $\mathcal{A} = \{1, \cdots, q\}$. The sums of the form $\mathbf{n}_{i_1} + \cdots + \mathbf{n}_{i_q}$, as $(i_1, \cdots, i_p)$ runs through $\mathcal{A}^p \backslash i(\mathcal{A})$, can be partitioned into equivalence classes (of cyclic permutations) of cardinality p. Furthermore, each member of any such equivalence class will correspond with the same coefficient product. It follows that all such terms cancel $(\mathrm{mod}\,p)$. The following line then uses Fermat's little theorem.

Observation 3.1 If, for some $q \in \mathbf{N}$, T is represented by

$$f = c_f(\mathbf{n}_1)u^{\mathbf{n}_1} + \cdots + c_f(\mathbf{n}_q)u^{\mathbf{n}_q} \in \mathcal{R}_{2,p} \text{ then } (T^p(x))_{\mathbf{n}} =$$

$$c_f(\mathbf{n}_1)(T^{p-1}(x))_{\mathbf{n}+\mathbf{n}_1} + \cdots + c_f(\mathbf{n}_q)(T^{p-1}(x))_{\mathbf{n}+\mathbf{n}_q}\,(\mathrm{mod}\,p) = \cdots =$$

$$\sum_{i_1=1}^{q} \cdots \sum_{i_p=1}^{q} c_f(\mathbf{n}_{i_p}) \cdots c_f(\mathbf{n}_{i_1}) x_{\mathbf{n}+\mathbf{n}_{i_1}+\cdots+\mathbf{n}_{i_p}}\,(\mathrm{mod}\,p) =$$

$$(c_f(\mathbf{n}_1))^p x_{\mathbf{n}+p\mathbf{n}_1} + \ldots + (c_f(\mathbf{n}_q))^p x_{\mathbf{n}+p\mathbf{n}_q}\,(\mathrm{mod}\,p) =$$

$$c_f(\mathbf{n}_1) x_{\mathbf{n}+p\mathbf{n}_1} + \cdots + c_f(\mathbf{n}_q) x_{\mathbf{n}+p\mathbf{n}_q}\,(\mathrm{mod}\,p)$$

which is represented by

$$f^p = c_f(\mathbf{n}_1)u^{p\mathbf{n}_1} + \ldots + c_f(\mathbf{n}_q)u^{p\mathbf{n}_q} \in \mathcal{R}_{2,p}.$$

We thus inductively show that, for all $k \in \mathbf{N}$, T^{p^k} is represented by

$$f^{p^k} = c_f(\mathbf{n}_1)u^{p^k \mathbf{n}_1} + \ldots + c_f(\mathbf{n}_q)u^{p^k \mathbf{n}_q}.$$

Remark 3.3 This tight control over the support of iterates of T is exactly where the algebraic case becomes much easier than the general case.

Theorem 3.3 *The* $\mathbf{N}$*-action generated by any convex map on the full two dimensional* 2*-shift has infinite entropy.*

Proof: Remaining with the notation of the arbitrary convex map T in Proposition 3.1 note that, by Observation 3.1, $x \in \Omega$ is fixed by T^{2^k} for any $k \in \mathbf{N}$ if and only if $x_{\mathbf{n}} = x_{\mathbf{n}+2^k\mathbf{m}_1} + \ldots + x_{\mathbf{n}+2^k\mathbf{m}_c} \pmod{p}$ for all $\mathbf{n} \in \mathbf{Z}^2$ and that T^{2^k} is a convex map with hull $2^k H$.

There exist points in $((r' + r'')\mathbf{v} + L) \cap \mathbf{Z}^2$, let $\mathbf{k}'$ be one of them, and let M be the line through $\mathbf{0}$ and $\mathbf{k}'$. Given $k, n \in \mathbf{N}$ let $R(k, n)$ be the semi closed quadrilateral in $\mathbf{R}^2$ with vertices $\mathbf{0}$, $n\mathbf{k}$, $2^k\mathbf{k}'$, and $n\mathbf{k} + 2^k\mathbf{k}'$ including points on the two borders contained in L and M only.

We are free to start to construct a point x in $\Omega^{n\mathbf{k}}$ that is fixed by T^{2^k} by putting $x_{\mathbf{n}} = 0$ or 1 for all $\mathbf{n} \in R(k, n) \cap \mathbf{Z}^2$ because (i) if some $\mathbf{n}$ is in $R(k, n)$ then $\mathbf{n} + \mathbf{k}$ can't be and (ii) some corner of any hull of the form $\mathbf{m} + 2^k H$ ($\mathbf{m} \in \mathbf{Z}^2$) must always lie outside of $R(k, n)$. This gives a total of $2^{C(k,n)}$ choices where $C(k, n)$ is the cardinality of $R(k, n) \bigcap \mathbf{Z}^2$. One readily sees that, for all $k, n \in \mathbf{N}$, $C(k, n) = 2^k n C(0, 1) = 2^k nC$ for some $C \neq 0$.

By Proposition 3.1, for all $n \in \mathbf{N} \backslash \{0\}$, the restriction of T to $\Omega^{n\mathbf{k}}$, is expansive and so, by Theorem 3.2, $h(T) \geq h(T|_{\Omega^{n\mathbf{k}}})$

$$\geq \limsup_{N\to\infty} \frac{\log F_N(T|_{\Omega^{n\mathbf{k}}})}{N} \geq \lim_{k\to\infty} \frac{\log F_{2^k}(T|_{\Omega^{n\mathbf{k}}})}{2^k} = \lim_{k\to\infty} \frac{\log 2^{2^k nC}}{2^k} = nC \log 2. \ \square$$

Theorem 3.4 *No* $\mathbf{N}$*-action on* Ω *generated by a map* T *which is determined by a polynomial* $f \in \mathcal{R}_{2,2}$ *can have finite positive entropy.*

Proof: For convex maps this is Theorem 3.3. If T is not convex then either it is the identity, the zero map (both entropy zero), or $\mathbf{0}$ and all $\mathbf{m}$ for which $c_f(\mathbf{m}) \neq 0$ lie on a unique rational line K, which is isomorphic to $\mathbf{Z}$. We thus think of Ω as $\mathbf{Z}$ copies of $\Omega_1 = \mathbf{Z}_{/2}^{\mathbf{Z}}$ where T acts on Ω by acting individually on each copy of Ω_1 and a simple entropy calculation tells us that $h(T) = \infty$ when non-convex T is not the identity or the zero map. $\square$

Remark 3.4 This result also follows from our more general result of Theorem 5.8.

3.5 The algebraic case in general

The remainder of the chapter gives the proof of the result of the joint work, [42], with Tom Ward.

Recall Problem 1.3. We solve this for $e = 1, d = 2$, and for endomorphisms rather than just automorphisms. That is;

Theorem 3.5 *If T is a mixing continuous group endomorphism of (X, α), where X is a compact metric Abelian group and α is a completely positive entropy Z^2-action by continuous group automorphisms, then $h(T) = \infty$.*

Note that we may drop the possibility (for the case of general $d \geq 2$ and $e \leq d-1$) of $h(T) = 0$, since a single mixing continuous group endomorphism (an $\mathbf{N}$-action) of a compact metric Abelian group has positive entropy by Rokhlin [53].

Theorem 3.5 will be proved after some preparations. Certain Pontryagin duality results on compact metric groups will be used. All may be found in Hewitt and Ross [23] or Morris [43].

Let $M = \widehat{X}$ be the *dual group* or *character group* of X; that is, the group of continuous group homomorphisms from X into the unit circle with the compact open topology (see Morris [43]). By the Pontryagin-van Kampen duality Theorem, for each $x \in X$, the map $x' : M \to \mathbf{S}$ given by $x'(m) = m(x)$ for all $m \in M$ is an element of $\widehat{M}$ and the map sending each x to x' is a topological group isomorphism, which gives the identification $\widehat{\widehat{X}} = \widehat{M} = X$. We thus identify x with x' for all $x \in X$ and hence have $m(x) = x(m)$ under this identification for all $m \in M$ and $x \in X$. It also follows from this identification that, for a continuous group homomorphism $\alpha : X \to X$, we may identify $\widehat{\widehat{\alpha}}$ and α.

For work on commutative algebra including ring-modules, Noetherian rings, and associated prime ideals, see Atiyah and MacDonald [1], Lang [29], or Matsumura [38].

Let $\mathcal{R}$ be a ring and M an $\mathcal{R}$-module.

Definition 3.2 A prime ideal $\wp$ of $\mathcal{R}$ is said to be an *associated prime ideal* of M if there exists $m \in M$ such that $\wp = \{f \in \mathcal{R} : f \cdot m = 0 = 0_M\}$.

Definition 3.3 The module M is said to be *Noetherian* if, whenever $M_1 \subset M_2 \subset \ldots$ is an increasing sequence of submodules of M, there exists $n \in \mathbf{N}$ such that $M_n = M_{n+1} = \ldots$.

The ring $\mathcal{R}$ is said to be *Noetherian* if it is Noetherian as the canonical $\mathcal{R}$-module over itself. Equivalently, if whenever $\ell_1 \subset \ell_2 \subset \ldots$ is an increasing sequence of ideals of $\mathcal{R}$, there exists $n \in \mathbf{N}$ such that $\ell_n = \ell_{n+1} = \ldots$.

Theorem 3.6 *If $\mathcal{R}$ is a Noetherian ring then any $\mathcal{R}$-module not equal to $\{0\}$ has an associated prime ideal.*

Proof. See Corollary 4.7 of Lang [29].

Much of the algebraic dynamics which we use is from Schmidt's book [60] where the following notation is described.

Let X be a compact metric group. The dual group (or character group) $M = \widehat{X}$ of X is countable and discrete. We shall treat the unit circle as an additive group here, so that the character group operation is given, for all $m_1, m_2 \in M$, by $(m_1+m_2)(x) = m_1(x) + m_2(x) (\operatorname{mod} 1)$ for all $x \in X$, the $(\operatorname{mod} 1)$ often being taken for granted and omitted. Given a $\mathbf{Z}^d$-action, α, by continuous group automorphisms of X recall that the dual, $\widehat{\alpha}$, of α is given by $(\widehat{\alpha}^{\mathbf{n}}(m))(x) = m(\alpha^{\mathbf{n}}(x))$ for all $\mathbf{n} \in \mathbf{Z}^d, m \in M$ and $x \in X$. If $\mathcal{R}_d = \mathbf{Z}[u_1^{\pm 1}, \cdots, u_d^{\pm 1}]$, the ring of Laurent polynomials in commuting variables $u_1, \cdots, u_d$ with coefficients in $\mathbf{Z}$, then M becomes an $\mathcal{R}_d$-module under the action $f \cdot m = \sum_{\mathbf{n} \in \mathbf{Z}^d} c_f(\mathbf{n}) \widehat{\alpha}^{\mathbf{n}}(m)$ for all $m \in M$ and for all $f \in \mathcal{R}_d$, where $c_f(\mathbf{n})$ is the coefficient of $u^{\mathbf{n}} = u_1^{n_1} \cdots u_d^{n_d}$ in f for all $\mathbf{n} = (n_1, \cdots, n_d) \in \mathbf{Z}^d$. Conversely, if M is an $\mathcal{R}_d$-module (always countable) then we may define the $\mathbf{Z}^d$-action, β, by continuous automorphisms of M by $\beta^{\mathbf{n}}(m) = u^{\mathbf{n}} \cdot m$ for all $m \in M$ for all $\mathbf{n} \in \mathbf{Z}^d$ and obtain the $\mathbf{Z}^d$-action $\alpha = \widehat{\beta}$ by continuous automorphisms of X.

Consider the map $\theta : \mathcal{R}_d \to \mathbf{Z}_{\mathbf{Z}^d} \cong \widehat{\mathbf{S}^{\mathbf{Z}^d}}$ (here, the notation $\mathbf{Z}_{\mathbf{Z}^d}$ refers to the direct sum of $\mathbf{Z}^d$ copies of $\mathbf{Z}$) given by $(\theta(f))((x_{\mathbf{n}})_{\mathbf{n}\in\mathbf{Z}^d}) = \sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) \cdot x_{\mathbf{n}} \pmod 1$ (recall that $c_f(\mathbf{n})$ is the coefficient of $\mathbf{u}^{\mathbf{n}}$ in f) for all $f \in \mathcal{R}_d$. Then $(\theta(f+g))((x_{\mathbf{n}})) = \sum_{\mathbf{n}\in\mathbf{Z}^d} c_{f+g}(\mathbf{n}) \cdot x_{\mathbf{n}} = \sum_{\mathbf{n}\in\mathbf{Z}^d}(c_f(\mathbf{n} + c_g(\mathbf{n}) \cdot x_{\mathbf{n}} = \sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n} \cdot x_{\mathbf{n}} + \sum_{\mathbf{n}\in\mathbf{Z}^d} c_g(\mathbf{n} \cdot x_{\mathbf{n}} = (\theta(f))((x_{\mathbf{n}})) + (\theta(g))((x_{\mathbf{n}})) = (\theta(f) + \theta(g))((x_{\mathbf{n}}))$ for all $(x_{\mathbf{n}}) \in \mathbf{S}^{\mathbf{Z}^d}$ and for all $f, g \in \mathcal{R}_d$. So θ is a homomorphism of discrete groups, and hence continuous.

Furthermore, $\theta(f) = \theta(g)$ implies that, for all $(x_{\mathbf{n}}) \in \mathbf{S}^{\mathbf{Z}^d}$, $\sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) \cdot x_{\mathbf{n}} = \sum_{\mathbf{n}\in\mathbf{Z}^d} c_g(\mathbf{n}) \cdot x_{\mathbf{n}}$ so that $\sum_{\mathbf{n}\in\mathbf{Z}^d} c_{f-g}(\mathbf{n}) \cdot x_{\mathbf{n}} = 0$. Fixing arbitrary $\mathbf{m} \in \mathbf{Z}^d$ and constructing $(x_{\mathbf{n}}) \in \mathbf{S}^{\mathbf{Z}^d}$ such that $x_{\mathbf{m}} \in \mathbf{S}$ is irrational and $x_{\mathbf{n}} = 0$ for all $\mathbf{n} \neq \mathbf{m}$ we get that $c_{f-g}(\mathbf{m}) \cdot x_{\mathbf{m}} = 0 \pmod 1$, so $c_{f-g}(\mathbf{m}) = 0$ and $c_f(\mathbf{m}) = c_g(\mathbf{m})$. Since $\mathbf{m}$ was chosen arbitrarily we have that $f = g$ and hence θ is injective.

Dual to θ we have $\widehat{\theta} : \mathbf{S}^{\mathbf{Z}^d} \to \widehat{\mathcal{R}_d}$ given by $(\widehat{\theta}((x_{\mathbf{n}})))(f) = (x_{\mathbf{n}})(\theta(f)) = (\theta(f))((x_{\mathbf{n}}))$. So $\widehat{\theta}((x_{\mathbf{n}})) = \widehat{\theta}((y_{\mathbf{n}}))$ implies that, for all $f \in \mathcal{R}_d$, $(\widehat{\theta}((x_{\mathbf{n}})))(f) = (\widehat{\theta}((y_{\mathbf{n}})))(f)$, so that $(x_{\mathbf{n}})(\theta(f)) = (y_{\mathbf{n}})(\theta(f))$ and hence $(\theta(f))(x_{\mathbf{n}}) = (\theta(f))(y_{\mathbf{n}})$, so that $\sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) \cdot (x_{\mathbf{n}} - y_{\mathbf{n}}) = 0 \pmod 1$. So taking $f = \mathbf{u}^{\mathbf{m}}$ for arbitrary $\mathbf{m} \in \mathbf{Z}^d$ we have that $x_{\mathbf{m}} = y_{\mathbf{m}}$. So $(x_{\mathbf{n}}) = (y_{\mathbf{n}})$, since $\mathbf{m} \in \mathbf{Z}^d$ was arbitrary. That is, $\widehat{\theta}$ is injective, so θ is a continuous group isomorphism and we may consider $f \in \mathcal{R}_d$ as an element of $\widehat{\mathcal{S}^{\mathbf{Z}^d}}$ under the identification of f with $\theta(f)$. That is, $f((x_{\mathbf{n}})_{\mathbf{n}\in\mathbf{Z}^d}) = \sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) \cdot x_{\mathbf{n}} \pmod 1$ for all $(x_{\mathbf{n}}) \in \mathbf{S}^{\mathbf{Z}^d}$.

Let $\wp$ be a prime ideal in $\mathcal{R}_d$. The dual, $\widehat{\mathcal{R}_d/\wp}$, of $\mathcal{R}_d/\wp$ is isomorphic to the annihilator, $\wp^{\perp} = \{(x_{\mathbf{n}}) \in \mathbf{S}^{\mathbf{Z}^d} = \widehat{\mathcal{R}_d} : (x_{\mathbf{n}})(f) = 0 \text{ for all } f \in \mathcal{R}_d\}$, of $\wp$ in $\widehat{\mathcal{R}_d}$. This is $\{(x_{\mathbf{n}}) \in \mathbf{S}^{\mathbf{Z}^d} : \sum_{\mathbf{n}\in\mathbf{Z}^d} c_p(\mathbf{n}) \cdot x_{\mathbf{m}+\mathbf{n}} = 0 \text{ for all } \mathbf{m} \in \mathbf{Z}^d\}$, when $\wp = (p)$ is principal.

Let $\beta^{\mathbf{n}} : \widehat{\mathcal{R}_d} \to \widehat{\mathcal{R}_d}$ be the dual of multiplication by $\mathbf{u}^{\mathbf{n}}$ on $\mathcal{R}_d$. Now $((\beta^{\mathbf{m}} \circ \widehat{\theta})((x_{\mathbf{n}})))(f) = (x_{\mathbf{n}})(\widehat{(\beta^{\mathbf{m}} \circ \widehat{\theta})}(f)) = (x_{\mathbf{n}})(\theta \circ \widehat{\beta^{\mathbf{m}}})(f)) = (x_{\mathbf{n}})(\theta(\mathbf{u}^{\mathbf{m}} \cdot f)) = (\theta(\mathbf{u}^{\mathbf{m}} \cdot f))(x_{\mathbf{n}}) = \sum_{\mathbf{n}\in\mathbf{Z}^d} c_{\mathbf{u}^{\mathbf{m}}\cdot f}(\mathbf{n}) \cdot x_{\mathbf{n}} = \sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n} - \mathbf{m}) \cdot x_{\mathbf{n}} = \sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) \cdot x_{\mathbf{m}+\mathbf{n}} = (\theta(f))((x_{\mathbf{m}+\mathbf{n}})) = ((x_{\mathbf{m}+\mathbf{n}}))(\theta(f)) = (\widehat{\theta}((x_{\mathbf{m}+\mathbf{n}})))(f) = (\widehat{\theta} \circ \sigma^{\mathbf{m}}((x_{\mathbf{n}})))(f)$ for all $f \in \mathcal{R}_d$, for all $(x_{\mathbf{n}}) \in \mathbf{S}^{\mathbf{Z}^d}$.

So, under the identification given by θ, β is the shift on $\mathbf{S}^{\mathbf{Z}^d}$. Similarly, the dual of multiplication by $\mathbf{u}^{\mathbf{n}}$ on $\mathcal{R}_d/\wp$ is the shift, $\sigma^{\mathbf{n}}$, on $\widehat{\mathcal{R}_d/\wp} = \{(x_{\mathbf{n}}) \in \mathbf{S}^{\mathbf{Z}^d} = \widehat{\mathcal{R}_d} :$ $(x_{\mathbf{n}})(f) = 0$ for all $f \in \mathcal{R}_d\}$.

Let $\hat{t} : \widehat{\mathcal{R}_d/\wp} \to \widehat{\mathcal{R}_d/\wp}$ be a continuous group homomorphism that commutes with the shift σ on $\widehat{\mathcal{R}_d/\wp}$. Note that, for $f \in \mathcal{R}_d$, $t(f+\wp) = t(\sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) \cdot \mathbf{u}^{\mathbf{n}} + \wp) = \sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) \cdot t(\mathbf{u}^{\mathbf{n}}) + \wp = (\sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) \cdot \mathbf{u}^{\mathbf{n}} + \wp) \cdot t(1+\wp) = (f+\wp)\cdot(h+\wp)$, where $h + \wp = t(1+\wp)$. So t commutes with multiplication by $\mathbf{u}^{\mathbf{n}}$ on $\mathcal{R}_d/\wp$.

So the duals t of algebraic cellular automata such as $\hat{t}$ are merely multiplication by polynomials in $\mathcal{R}_d$. It follows that $(\hat{t}((x_{\mathbf{n}}))(f) = (x_{\mathbf{n}})(t(f)) = (x_{\mathbf{n}})(f \cdot h) = \sum_{\mathbf{m}\in\mathbf{Z}^d} c_{f\cdot h}(\mathbf{m})\cdot x_{\mathbf{m}} = \sum_{\mathbf{m}\in\mathbf{Z}^d} \sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) c_h(\mathbf{m}-\mathbf{n})\cdot x_{\mathbf{m}} = \sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n})(\sum_{\mathbf{m}\in\mathbf{Z}^d} c_h(\mathbf{m}-\mathbf{n}) \cdot x_{\mathbf{m}}) = (y_{\mathbf{n}})(f)$, for all $f \in \mathcal{R}_d$, for all $(x_{\mathbf{n}}) \in \mathbf{S}^{\mathbf{Z}^d}$, where $(y_{\mathbf{n}}) \in \mathbf{S}^{\mathbf{Z}^d}$ is such that $y_{\mathbf{n}} = \sum_{\mathbf{m}\in\mathbf{Z}^d} c_h(\mathbf{m}-\mathbf{n}) \cdot x_{\mathbf{m}} = \sum_{\mathbf{m}\in\mathbf{Z}^d} c_h(\mathbf{m}) \cdot x_{\mathbf{m}+\mathbf{n}}$ for all $\mathbf{n} \in \mathbf{Z}^d$. So algebraic cellular automata such as $\hat{t}$ are the polynomial maps on $\widehat{\mathcal{R}_d/\wp}$; $\hat{t}$ is determined by the polynomial $h \in \mathcal{R}_d$.

To prove Theorem 3.5 we need three more results (Theorem 3.7, Theorem 3.8, and Theorem 3.9).

Definition 3.4 A subgroup $\Gamma \subset \mathbf{Z}^d$ is *primitive* if the quotient $\mathbf{Z}^d/\Gamma$ is torsion free.

For notational compactness, $\mathbf{F}_p$ below is $\mathbf{Z}_{/p} = \mathbf{Z}/(p\mathbf{Z})$.

Theorem 3.7 *Suppose $d \in \mathbf{N}$, $\wp$ is a positive characteristic prime ideal in $\mathcal{R}_d$, of characteristic p, and the shift σ on*

$$\widehat{\mathcal{R}_d/\wp} = \{(x_{\mathbf{n}})_{\mathbf{n}\in\mathbf{Z}^d} \in \mathbf{S}^{\mathbf{Z}^d} : \sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) x_{\mathbf{n}} = 0 \pmod 1 \text{ for all } f \in \wp\} \subset \mathbf{F}_p^{\mathbf{Z}^d}$$

is ergodic. Then there exists an integer $r = r(\wp) \in \{1, \cdots, d\}$, a primitive subgroup $\Gamma = \Gamma(\wp) \subset \mathbf{Z}^d$, and a finite set $Q = Q(\wp) \subset \mathbf{Z}^d$ such that $\Gamma \cong \mathbf{Z}^r$, $\mathbf{0} \in Q$, $Q \cap (Q + \mathbf{m}) = \emptyset$ whenever $\mathbf{0} \neq \mathbf{m} \in \Gamma$ and, if

$$\overline{\Gamma} = \Gamma + Q = \{\mathbf{m} + \mathbf{n} : \mathbf{m} \in \Gamma, \mathbf{n} \in Q\},$$

then the coordinate projection $\pi_{\overline{\Gamma}} : \widehat{\mathcal{R}_d/\wp} \to \mathbf{F}_p^{\overline{\Gamma}}$, which restricts any point $x \in \widehat{\mathcal{R}_d/\wp}$ to its coordinates in $\overline{\Gamma}$, is a topological group isomorphism; in particular, if $\{\mathbf{n}_1, \cdots, \mathbf{n}_r\}$

is a basis for Γ *then the* $\mathbf{Z}^r$*-action generated by* $\{\sigma^{\mathbf{n}_1}, \cdots, \sigma^{\mathbf{n}_r}\}$ *is isomorphic to the shift on* $(\mathbf{F}_p^Q)^{\mathbf{Z}^r}$*.*

Furthermore, for any $s \in \mathbf{R}^+$*,*

$$\sup_{\mathcal{P}\in\Xi} \lim_{m\to\infty} \frac{1}{(2m)^s} H_\lambda\Big(\bigvee_{\mathbf{m}\in Q(m)} \sigma^{-\mathbf{m}}(\mathcal{P})\Big) = \begin{cases} \infty & \text{if and only if } s < r(\wp) \\ 0 & \text{if and only if } s > r(\wp), \end{cases} \tag{4}$$

where Ξ *is the set of all finite measurable partitions of* $\widehat{\mathcal{R}_d/\wp}$ *and* λ *is Haar measure on* $\widehat{\mathcal{R}_d/\wp}$*. The integer* $r = r(\wp)$ *does not depend on the choice of primitive subgroup* $\Gamma = \Gamma(\wp) \subset \mathbf{Z}^d$*, and is a measurable conjugacy invariant.*

Example 3.8 If $d = 2$ and $\wp = (2, p) = (2, 1 + u_1 + u_2)$ (so $c_p((0,1)) = c_p((0,0)) = c_p((1,0)) = 1$) then $\widehat{\mathcal{R}_d/\wp} =$

$$\{(x_\mathbf{n}) \in \mathbf{S}^{\mathbf{Z}^2} : 2x_\mathbf{m} = 0 \text{ and } x_{\mathbf{m}+(0,1)} + x_{\mathbf{m}+(0,0)} + x_{\mathbf{m}+(1,0)} = 0 \pmod 1 \text{ for all } \mathbf{m} \in \mathbf{Z}^2\}$$

$$\cong \{(x_\mathbf{n}) \in \{0,1\}^{\mathbf{Z}^2} : x_{\mathbf{m}+(0,1)} + x_{\mathbf{m}+(0,0)} + x_{\mathbf{m}+(1,0)} = 0 \pmod 2 \text{ for all } \mathbf{m} \in \mathbf{Z}^2\}.$$

Consideration of a lower-left to upper-right bi-infinite diagonal strip in $\mathbf{R}^2$, thick enough for any translate to always contain exactly two adjacent bi-infinite diagonal lines of points of $\mathbf{Z}^2$, gives a one-to-one correspondence between points of $\widehat{\mathcal{R}_d/\wp}$ and all possible combinations of 0's and 1's on the lattice points in the strip. So, by Theorem 5.4 with $\xi = \{A_1, A_2\}$ where $A_i = \{(x_\mathbf{n}) \in \widehat{\mathcal{R}_d/\wp} : x_{(0,0)} = i\}$ for $i = 1, 2$, equation (4) with $s = 1$ gives value $2\sqrt{2}\log 2$ so, by Theorem 3.7, $r(\wp) = 1$.

Example 3.9 If $d = 2$ and $\wp = (2 - u_1, 3 - u_2)$ (so the shift on $\widehat{\mathcal{R}_d/\wp}$ is the invertible extension of $(\mathbf{S}, S, T)$ where S and T are multiplication by 2 and 3, respectively, (mod 1)) then, by Theorem 5.4 with $\xi = \{A_1, \cdots, A_6\}$ where $A_i = \{(x_\mathbf{n}) \in \widehat{\mathcal{R}_d/\wp} : x_{(0,0)} \in [(i-1)/6, i/6)\}$ for $i = 1, \cdots, 6$, equation (4) with $s = 1$ gives value $\log 6$ so, by Theorem 3.7, $r(\wp) = 1$.

Proof of Theorem 3.7. Proposition 8.2 and Theorem 24.1 of Schmidt [60].

The case where the prime ideal $\wp$ has characteristic zero involves looking at the shift component $\sigma^{(0,0,1)}$ on $\widehat{\mathcal{Q}_3/\wp'} \cong \{(x_\mathbf{n}) \in \Sigma^{\mathbf{Z}^3} : \sum_{\mathbf{n}\in\mathbf{Z}^3} c_p(\mathbf{n}) \cdot x_\mathbf{n} = 0 =$

0_Σ for all $p \in \wp'\}$ (the identification being analogous to the $\mathcal{R}_3/\wp$ case) where Σ is the full solenoid $\widehat{\mathbf{Q}}$, $\mathcal{Q}_3 = \mathbf{Q}[u_1^{\pm 1}, \cdots, u_3^{\pm 1}]$, and $\wp'$ is the canonical ideal in $\mathcal{Q}_3$ which corresponds to the ideal $\wp$ in $\mathcal{R}_3$.

The dual of $(\{(x_\mathbf{n}) \in \Sigma^{\mathbf{Z}^3} : \sum_{\mathbf{n}\in\mathbf{Z}^3} c_p(\mathbf{n}) \cdot x_\mathbf{n} = 0 = 0_\Sigma \text{ for all } p \in \wp'\}, \sigma^{(0,0,1)})$ is $(\mathcal{Q}_3/\wp', t)$ where t represents multiplication by u_3. We need to show that the entropy of $(\{(x_\mathbf{n}) \in \Sigma^{\mathbf{Z}^3} : \sum_{\mathbf{n}\in\mathbf{Z}^3} c_p(\mathbf{n}) \cdot x_\mathbf{n} = 0 = 0_\Sigma \text{ for all } p \in \wp'\}, \sigma^{(0,0,1)})$ is equal to that of $(\{(x_\mathbf{n}) \in \mathbf{S}^{\mathbf{Z}^3} : \sum_{\mathbf{n}\in\mathbf{Z}^3} c_p(\mathbf{n}) \cdot x_\mathbf{n} = 0 = 0_\mathbf{S} \pmod 1 \text{ for all } p \in \wp\}, \sigma^{(0,0,1)})$.

We shall prove the more general Theorem 3.8 which is used (for the case of an automorphism) elsewhere, though no proof has been found. We'll need the following four lemmas (Lemma 3.2, Lemma 3.3, Lemma 3.4, and Lemma 3.5).

The first lemma which we prove (so as to exhibit the isomorphism involved) concerns a compact metric group, G, a normal closed subgroup H, of G, endowed with the subspace topology ($U \subset H$ open if and only if $U = H \cap V$ for some open $V \subset G$), the annihilator $H^\perp = \{\chi \in \widehat{G} : \chi(H) = \{0\}\}$ of H in $\widehat{G}$, and the quotient group, G/H (see, for example, Higgins [24] for the theory on topological groups). The quotient group, G/H, is given the quotient topology; $U \subset G/H$ is open in G/H if and only if $q^{-1}(U)$ is open in G, where $q : G \to G/H$ is the quotient map. The quotient topology makes G/H into a topological group. The quotient map, q, is automatically continuous.

The quotient map, q, is open since $U \subset G$ open in G implies $q^{-1}(q(U)) = \{g \in G : g + H = u + H \text{ for some } u \in U\} = \{g \in G : g - u \in H \text{ for some } u \in U\} = \{g \in G : g = u + h \text{ for some } u \in U, h \in H\} = \bigcup_{h\in H}\{h + u : u \in U\}$ is a union of open sets in G and hence open. It follows that $q(U)$ is open in G/H, by definition of the quotient topology and, hence, q is an open map.

The quotient map, q, is closed because; H being closed is sufficient to make G/H Hausdorff, and any continuous map from a compact space to a Hausdorff space is a closed map.

Lemma 3.2 *With the above notation (H a normal closed subgroup of G with the subspace topology), $\widehat{G}/H^\perp \cong \widehat{H}$.*

Proof. Let $i : H \to G$ be the inclusion map, automatically continuous because

H has the subspace topology. Dual to i we have the continuous endomorphism $\widehat{i}:\widehat{G}\to\widehat{H}$. Define $\theta:\widehat{G}/H^{\perp}\to\widehat{H}$ by $\theta(\chi+H^{\perp})=\widehat{i}(\chi)$ for all $\chi\in\widehat{G}$.

Firstly, not that if, for $\chi,\,\tau\in\widehat{G}$, $\chi-\tau\in H^{\perp}$ then, for all $h\in H$, $(\widehat{i}(\chi)-\widehat{i}(\tau))(h)=(\widehat{i}(\chi))(h)-(\widehat{i}(\tau))(h)=\chi(h)-\tau(h)=(\chi-\tau)(h)=0$, so that $\theta(\chi+H^{\perp})=\widehat{i}(\chi)=\widehat{i}(\tau)=\theta(\tau+H^{\perp})$ and, hence, θ is well defined. We will show that θ is a topological group isomorphism.

Surjectivity of θ follows from surjectivity of $\widehat{i}$ and continuity is trivial upon noting that the definition of the quotient topology and the discrete topology of $\widehat{G}$ means that $\widehat{G}/H^{\perp}$ has the discrete topology. Furthermore, for all $h\in H$, $(\theta((\chi+H^{\perp})+(\tau+H^{\perp})))(h)=(\widehat{i}(\chi+\tau))(h)=(\chi+\tau)(h)=\chi(h)+\tau(h)=(\widehat{i}(\chi))(h)+(\widehat{i}(\tau))(h)=(\theta(\chi+H^{\perp}))(h)+(\theta(\tau+H^{\perp}))(h)$, so that θ is a group homomorphism. Finally, if $\theta(\chi+H^{\perp})=0$ then, for all $h\in H$, $\chi(h)=(\widehat{i}(\chi))(h)=(\theta(\chi+H^{\perp}))(h)=0$, so that $\chi\in H^{\perp}$ and, hence, θ is injective. □

The proof of Lemma 13.6 in Schmidt [60] (concerning a $\mathbf{Z}^d$-action by continuous group automorphisms) works also for a single group endomorphism. We give here a more detailed proof (Lemma 3.5 below), but first we need the following lemma, which is used implicitly in Lemma 13.6 of [60]. For a topological space X let $\mathcal{B}(X)$ denote its Borel σ-algebra. For σ-algebras, $\mathcal{B}_n$, for $n\in\mathbf{N}$, on some common topological space, $\bigvee_{n\in\mathbf{N}}\mathcal{B}_n$ is the smallest σ-algebra containing $\bigcup_{n\in\mathbf{N}}\mathcal{B}_n$.

Lemma 3.3 *Let $\{H_n\}_{n\in\mathbf{N}}$ be a decreasing ($H_{n+1}\subset H_n$ for all $n\in\mathbf{N}$) sequence of closed, normal subgroups of G such that $\bigcap_{n\in\mathbf{N}}H_n=\{0\}$ and, for all $n\in\mathbf{N}$, let $\theta_n:G\to G/H_n$ be the quotient map. Then $\{\theta_n^{-1}(\mathcal{B}(G/H_n))\}_{n\in\mathbf{N}}$ is an increasing sequence of σ-algebras on G and $\bigvee_{n\in\mathbf{N}}\theta_n^{-1}(\mathcal{B}(G/H_n))=\mathcal{B}(G)$.*

Proof. Fix $n\in\mathbf{N}$ and note that, since H_{n+1} is a subgroup of H_n, $H_n=\bigcup_{h\in H_n}\{f+h:f\in H_{n+1}\}$. Let $U\subset G$ be the pre-image, under the quotient map θ_n, of an open set in G/H_n. So $U=\theta_n^{-1}(\theta_n(U))=\{g\in G:g-u\in H_n \text{ for some } u\in U\}=\{g\in G:g-u\in\bigcup_{h\in H_n}\{f+h:f\in H_{n+1}\}\text{ for some } u\in U\}=\bigcup_{h\in H_n}\{g\in G:g-u\in\{f+h:f\in H_{n+1}\}\text{ for some } u\in U\}=\bigcup_{h\in H_n}\{g\in G:g-(h+u)\in H_{n+1}\}\text{ for some } u\in U\}=\bigcup_{h\in H_n}\theta_{n+1}^{-1}(\theta_{n+1}(\{h+u:u\in U\}))=\theta_{n+1}^{-1}(\bigcup_{h\in H_n}\theta_{n+1}(\{h+u:u\in U\}))$.

But $\bigcup_{h\in H_n}\theta_{n+1}(\{h+u : u\in U\})$ is open in G/H_{n+1}. So $U\in\theta_{n+1}^{-1}(\mathcal{B}(G/H_{n+1}))$, which proves that $\{\theta_n^{-1}(\mathcal{B}(G/H_n))\}_{n\in\mathbf{N}}$ is an increasing sequence of σ-algebras on G.

We now show that $\bigvee_{n\in\mathbf{N}}\theta_n^{-1}(\mathcal{B}(G/H_n)) = \mathcal{B}(G)$. If V is open in G/H_n then $\theta_n^{-1}(V)$ is open in G, by definition of the quotient topology on G/H_n. It follows that $\bigvee_{n\in\mathbf{N}}\theta_n^{-1}(\mathcal{B}(G/H_n))\subset\mathcal{B}(G)$.

To prove the reverse inclusion, let C be a closed subset of G. First note that $C\subset\theta_n^{-1}(\theta_n(C))$ for all $n\in\mathbf{N}$, so that $C\subset\bigcap_{n\in\mathbf{N}}\theta_n^{-1}(\theta_n(C))$. Conversely if, for all $n\in\mathbf{N}$, $g+H_n\in\{c+H_n : c\in C\}$, for some $g\in G$, then there exists a sequence $\{c_n\}_{n\in\mathbf{N}}$ in C such that, for all $n\in\mathbf{N}$, $g-c_n\in H_n$. Since G is compact, $\{g-c_n\}_{n\in\mathbf{N}}$ contains a convergent subsequence which, without loss of generality, we assume to be the sequence itself. Fix arbitrary $m\in\mathbf{N}$ then, for all $n\geq m$, $g-c_n\in H_n\subset H_m$, since $\{H_n\}_{n\in\mathbf{N}}$ is decreasing. Thus, $\lim_{n\to\infty} g-c_n\in H_m$, since H_m is closed. Since m was chosen arbitrarily we have that $\lim_{n\to\infty} g-c_n\in\bigcap_{n\in\mathbf{N}}H_n=\{0\}$, so that $g=\lim_{n\to\infty}c_n$. But this limit is in C (this was our motivation for concentrating on the closed sets of G which, of course, also generate its Borel σ-algebra). Thus $g\in C$ and, hence, $\bigcap_{n\in\mathbf{N}}\theta_n^{-1}(\theta_n(C))=C$.

By the paragraph preceding Lemma 3.2, for all $n\in\mathbf{N}$, $\theta_n(C)$ is closed in G/H_n and, hence, $C=\bigcap_{n\in\mathbf{N}}\theta_n^{-1}(\theta_n(C))$ is a member of $\bigvee_{n\in\mathbf{N}}\theta_n^{-1}(\mathcal{B}(G/H_n))$. Thus, $\mathcal{B}(G)\subset\bigvee_{n\in\mathbf{N}}\theta_n^{-1}(\mathcal{B}(G/H_n))$, which is the reverse inclusion required. □

The proof of Lemma 3.5 uses the *conditional entropy of $\mathcal{P}$ with respect to $\mathcal{F}$*, $H_\mu(\mathcal{P}|\mathcal{F})$ for a finite measurable (with respect to the σ-algebra, $\mathcal{B}$) partition $\mathcal{P}$ of a probability space $(X,\mathcal{B},\mu)$, where $\mathcal{F}$ is a sub-σ-algebra of $\mathcal{B}$. See, for example, Walters [64, Section 4.3] for the the motivation for, definition of, and some theory concerning conditional entropies. The results used here are:

Since $\mathcal{P}$ is measurable with respect to $\mathcal{B}$, $H_\mu(\mathcal{P}|\mathcal{B})=0$.

For a measure preserving transformation, T, of $(X,\mathcal{B},\mu)$, $h_\mu(T,\mathcal{P})\leq h_\mu(T,\mathcal{P}')+H_\mu(\mathcal{P}|\mathcal{P}')$ for finite measurable partitions $\mathcal{P}$ and $\mathcal{P}'$ of $(M,\mathcal{B},\mu)$ (we have license to place the finite partition $\mathcal{P}'$ in place of a σ-algebra due to the canonical one-to-one correspondence between finite σ-algebras and finite partitions, see Walters [64]).

Lemma 3.4 *With the above notation, if $\{\mathcal{F}_n\}_{n\in\mathbf{N}}$ is an increasing ($\mathcal{F}_n\subset\mathcal{F}_{n+1}$ for all*

$n \in \mathbf{N}$) sequence of sub-σ-algebras of $\mathcal{B}$ with $\bigvee_{n\in\mathbf{N}} \mathcal{F}_n = \mathcal{F}$ then $\lim_{n\to\infty} H_\mu(\mathcal{P}|\mathcal{F}_n) =$ *$H_\mu(\mathcal{P}|\mathcal{F})$.*

Proof. Follows (see, for example, Walters [64, Theorem 4.7]) from Doob's martingale theorem.

Lemma 3.5 *Let T be a continuous group endomorphism of a compact metric group G, and let $\{H_n\}_{n\in\mathbf{N}}$ be a decreasing sequence of closed, normal, T-invariant subgroups of G such that $\bigcap_{n\in\mathbf{N}} H_n = \{0\}$. Then $h(T) = \lim_{n\to\infty} h(T_n)$ where, for all $n \in \mathbf{N}$, the continuous group endomorphism $T_n : G/H_n \to G/H_n$ is defined by $T_n(g + H_n) = T(g) + H_n$ for all $g \in G$.*

Proof. First note that, for all $n \in \mathbf{N}$, if $T(f)-T(g) \in H_n$ then $T_n(f+H_n)-T_n(g+H_n) = (T(f)+H_n)-(T(g)+H_n) = (T(f)-T(g))+H_n = 0$, so that T_n is well defined. Since, for all $n \in \mathbf{N}$, for all g, $h \in G$, $T_n((g + H_n) + (h + H_n)) = T(g + h) + H_n = (T(g) + T(h)) + H_n = (T(g) + H_n) + (T(h) + H_n) = T_n(g + H_n) + T_n(h + H_n)$, T_n is a group homomorphism. Surjectivity follows trivially from surjectivity of T. Furthermore, for all open $U \subset G/H_n$, $U = \{v+H_n : v \in V$ for some V open in $G\}$ and $\theta_n^{-1}(U) = \{g \in G : g+H_n = v+H_n$ for some $v \in V\}$ is open in G, by definition of the quotient topology on G/H_n, where $\theta_n : G \to G/H_n$ is the quotient map. Therefore, $T_n^{-1}(U) = \{g + H_n \in G/H_n : T(g) + H_n = v + H_n$ for some $v \in V\} = \{\theta_n(g) : g \in G$ and $T(g)+H_n = v+H_n$ for some $v \in V\} = \theta_n(\{g \in G : T(g)+H_n = v+H_n$ for some $v \in V\}) = \theta_n(T^{-1}(\{g \in G : g + H_n = v + H_n$ for some $v \in V\}))$ is open in G/H_n since T is continuous and θ_n is an open map by the paragraphs preceding Lemma 3.2. Thus, T_n is a continuous group endomorphism on G/H_n.

By the variational principle for continuous maps of compact metric spaces (see, for example, Walters [64]) and Remark 1.1 we have that $h(T) = h_\mu(T)$ and $h(T_n) = h_{\mu_n}(T_n)$ where, for all $n \in \mathbf{N}$, μ on G (and μ_n on G/H_n respectively) is Haar measure.

For all $n \in \mathbf{N}$, the quotient map $\theta_n : G \to G/H_n$ is a continuous (recall that G/H_n is endowed with the quotient topology) group endomorphism of compact groups and, thus, preserves the respective Haar measures. Furthermore, $\theta_n \circ T(g) = T(g) + H_n =$

$T_n(g+H_n) = T_n \circ \theta_n(g)$, for all $g \in G$, so $(G/H_n, T_n)$ is a factor of (G,T) and, hence, $h(T) \geq h(T_n)$ for all $n \in \mathbf{N}$. Thus $h(T) \geq \lim_{n\to\infty} h(T_n)$.

Conversely, let Ξ be the set of all finite Borel measurable partitions of G, suppose that $\epsilon > 0$ is given, and take $\mathcal{P} = \mathcal{P}(\epsilon) \in \Xi$, such that $h_\mu(T) - h_\mu(T,\mathcal{P}) = \sup_{\mathcal{O}\in\Xi} h_\mu(T,\mathcal{O}) - h_\mu(T,\mathcal{P}) < \epsilon/4$. By Lemma 3.3 $\{\theta_n^{-1}(\mathcal{B}(G/H_n))\}_{n\in\mathbf{N}}$ is an increasing sequence of σ-algebras on G and $\bigvee_{n\in\mathbf{N}} \theta_n^{-1}(\mathcal{B}(G/H_n)) = \mathcal{B}(G)$. For $n \in \mathbf{N}$, let $\mathcal{B}_n = \theta_n^{-1}(\mathcal{B}(G/H_n))$. It follows from Lemma 3.4 that $\lim_{n\to\infty} H_\mu(\mathcal{P}|\mathcal{B}_n) = H_\mu(\mathcal{P}|\mathcal{B}(G))$. But $H_\mu(\mathcal{P}|\mathcal{B}(G)) = 0$ by the results preceding Lemma 3.4. Thus, there exists $n = n(\mathcal{P},\epsilon) \in \mathbf{N}$ such that $m \geq n$ implies that $H_\mu(\mathcal{P},\mathcal{B}_m) < \epsilon/4$. Since Haar measure, μ, is a Borel probability measure and G is a metric space it follows (see, for example, Walters [64, Theorem 6.1]) that $(G,\mathcal{B}(G),\mu)$ has a countable measure basis (that is, a countable subset $\{B_n\}_{n\in\mathbf{N}} \subset \mathcal{B}(G)$ such that, for all $B \in \mathcal{B}(G)$ and for all $\delta > 0$, there exists $n \in \mathbf{N}$ such that $\mu(B\backslash B_n \bigcup B_n\backslash B) < \delta$). We may (see, for example, [64]) therefore take an increasing sequence, $\{\mathcal{A}_n\}_{n\in\mathbf{N}}$, of finite sub-algebras such that $\bigvee_{n\in\mathbf{N}} \mathcal{A}_n = \mathcal{B}_m$ so that, again by Lemma 3.4, there exists $k \in \mathbf{N}$ such that $H_\mu(\mathcal{P}|\mathcal{A}_k) - H_\mu(\mathcal{P}|\mathcal{B}_m) < \epsilon/4$. Also, $H_\mu(\mathcal{P}|\theta_m^{-1}(\mathcal{P}')) - H_\mu(\mathcal{P}|\mathcal{A}_k) < \epsilon/4$, where $\mathcal{P}'$ is the unique finite measurable partition of $(G/H_k, \mathcal{B}(G/H_k))$ such that $\theta_m^{-1}(\mathcal{P}')$ generates (in the obvious sense) $\mathcal{A}_k$. It follows, by the result preceding Lemma 3.4, that $h_\mu(T,\mathcal{P}) \leq h_\mu(T,\theta_m^{-1}(\mathcal{P}')) + H_\mu(\mathcal{P}|\mathcal{B}_m) + \epsilon/2 = h_{\mu_m}(T_m,\mathcal{P}') + H_\mu(\mathcal{P}|\mathcal{B}_m) + \epsilon/2$. Hence, $h_\mu(T) = \sup_{\mathcal{O}\in\Xi} h_\mu(T,\mathcal{O}) < h_\mu(T,\mathcal{P}) + \epsilon/4 < h_{\mu_m}(T_m,\mathcal{P}') + \epsilon \leq h_{\mu_m}(T_m) + \epsilon$. Hence, $h(T) = h_\mu(T) \leq \lim_{m\to\infty} h_{\mu_m}(T_m) + \epsilon = \lim_{m\to\infty} h(T_m) + \epsilon$. But ϵ was arbitrary, so $h(T) \leq \lim_{m\to\infty} h(T_m)$. □

Recall $\wp'$ introduced in the paragraph after Theorem 3.7.

Before proving Theorem 3.8 note that a general shift commuting (that is, commuting with multiplication by $\mathbf{u^n}$) group homomorphism, t (respectively s), of $\mathcal{R}_d/\wp$ (respectively $\mathcal{Q}_d/\wp'$) is easily shown to be multiplication by an element of $\mathcal{R}_d/\wp$ (respectively $\mathcal{Q}_d/\wp'$). Furthermore if the characteristic of $\mathcal{R}_d/\wp$ is zero then, since the ideal $\wp \in \mathcal{R}_d$ is prime, the map $\phi : \mathcal{R}_d/\wp \to \mathcal{Q}_d/\wp'$ given by $f + \wp \mapsto f + \wp'$ is injective.

Theorem 3.8 *With the above notation and $\wp$ a prime ideal with characteristic zero, if $\widehat{t}$ is a shift commuting topological group endomorphism of $\widehat{\mathcal{R}_d/\wp}$ then t is simply* *multiplication by $h+\wp$ in $\mathcal{R}_d/\wp$ for some $h \in \mathcal{R}_d$ and $h(\widehat{s}) = h(\widehat{t})$ where s is simply multiplication in $\mathcal{Q}_d/\wp'$ by $h+\wp' = \phi(h+\wp)$. Also, t is mixing if and only if s is mixing.*

Proof. First let $G = \widehat{\mathcal{Q}_2/\wp'}$ and $H_n = ((\frac{1}{n!}\mathcal{R}_2)/\wp')^\perp = \{\chi \in G : \chi((\frac{1}{n!}\mathcal{R}_2)/\wp') = \{0\}\}$ for all $n \in \mathbf{N}$. Since $\{(\frac{1}{n!}\mathcal{R}_2)/\wp'\}_{n\in\mathbf{N}}$ can be considered as an increasing sequence of subgroups of $\mathcal{Q}_2/\wp'$ with $\bigcup_{n\in\mathbf{N}}(\frac{1}{n!}\mathcal{R}_2)/\wp' = \mathcal{Q}_2/\wp'$ it follows that the annihilators form a decreasing sequence $\{H_n\}_{n\in\mathbf{N}}$ of closed normal subgroups of G with $\bigcap_{n\in\mathbf{N}} H_n = 0$. Therefore, by Lemma 3.5, the entropy $h(\widehat{t})$ of the system $(G, \widehat{s})$ is $\lim_{n\to\infty} h(T_n)$ where $T_n : G/H_n \to G/H_n$ is given by $T_n(\chi + H_n) = \widehat{s}(\chi) + H_n$ for all $\chi \in G$.

Also, by Lemma 3.2, for all $n \in \mathbf{N}$, $G/H_n \cong \widehat{(\frac{1}{n!}\mathcal{R}_2)/\wp'}$ under the topological group isomorphism $\theta_n(\chi + H_n) = \widehat{i_n}(\chi)$ for all $\chi \in G$, where $i_n : (\frac{1}{n!}\mathcal{R}_2)/\wp' \to \mathcal{Q}_2/\wp'$ is the respective inclusion map. Furthermore, $(\frac{1}{n!}\mathcal{R}_2)/\wp'$ is a s invariant subgroup of $\mathcal{Q}_2/\wp'$ (since $s(f+\wp') = (h\cdot f)+\wp'$ for all $f \in \mathcal{Q}_2$, where $h \in \mathcal{R}_2$), so that if $t_n : (\frac{1}{n!}\mathcal{R}_2)/\wp' \to (\frac{1}{n!}\mathcal{R}_2)/\wp'$ is the restriction of s to $(\frac{1}{n!}\mathcal{R}_2)/\wp'$ (so $i_n \circ t_n = t \circ i_n : (\frac{1}{n!}\mathcal{R}_2)/\wp' \to \mathcal{Q}_2/\wp'$) we note that, for all $\chi \in G$ and for all $f \in \mathcal{R}_2$, $(\theta_n \circ T_n(\chi + H_n))(\frac{f}{n!} + \wp') = \theta_n(\widehat{s}(\chi) + H_n)(\frac{f}{n!} + \wp') = (\widehat{i_n}(\widehat{s}(\chi)))(\frac{f}{n!} + \wp') = \chi(s \circ i_n(\frac{f}{n!} + \wp')) = \chi(i_n \circ t_n(\frac{f}{n!} + \wp')) = (\widehat{t_n} \circ \widehat{i_n}(\chi))(\frac{f}{n!} + \wp') = (\widehat{t_n} \circ \theta_n(\chi + H_n))(\frac{f}{n!} + \wp')$. So $(G/H_n, T_n) \cong (\widehat{(\frac{1}{n!}\mathcal{R}_2)/\wp'}, \widehat{t_n})$ for all $n \in \mathbf{N}$. Therefore $h(\widehat{t}) = \lim_{n\to\infty} h(T_n) = \lim_{n\to\infty} h(\widehat{t_n})$.

However, for all $n \in \mathbf{N}$, $\psi_n : \mathcal{R}_2/\wp' \to (\frac{1}{n!}\mathcal{R}_2)/\wp'$ given by $\psi_n(f + \wp') = \frac{f}{n!} + \wp'$ is a topological group isomorphism. Furthermore, for all $f \in \mathcal{R}_2$, $t_n \circ \psi_n(f + \wp') = t_n(\frac{f}{n!} + \wp') = t(\frac{f}{n!} + \wp' = \frac{h\cdot f}{n!} + \wp' = \psi_n((h \cdot f) + \wp') = \psi_n \circ t_1(f + \wp')$. So that, for all $n \in \mathbf{N}$, $(\mathcal{R}_2/\wp', t_1) \cong ((\frac{1}{n!}\mathcal{R}_2)/\wp', t_n)$ and , hence, $h(\widehat{t_1}) = h(\widehat{t_n})$. It follows that $h(\widehat{s}) = \lim_{n\to\infty} h(\widehat{t_n}) = h(\widehat{t_1})$. But $t_1 : \mathcal{R}_2/\wp' \to \mathcal{R}_2/\wp'$ is the restriction of $s : \mathcal{Q}_2/\wp' \to \mathcal{Q}_2/\wp'$ to $\mathcal{R}_2/\wp'$ which was our original system. We have thus reduced the problem to a shift commuting mixing map $\widehat{s}$ of $\mathcal{Q}_2/\wp'$ whose entropy we wish to show is infinite.

To see that $\widehat{t}$ is mixing on $\widehat{\mathcal{R}_d/\wp'}$ exactly when $\widehat{s}$ is mixing on $\widehat{\mathcal{Q}_d/\wp'}$ we use the well known fact (see, for example, Walters [64, Theorem 1.10]) that a continuous endomorphism of a compact abelian group is mixing if and only if the dual map has no finite orbits on the dual group. We then note that, for $f \in \mathcal{R}_2 \backslash \wp'$ (that is, the compliment of $\wp'$ in $\mathcal{R}_2$) and $m, n \in \mathbf{N}$, $t^n(f/m + \wp') = 0$ implies that $h^n \cdot f/m \in \wp'$

implies that $h^n \cdot f \in \wp'$ implies that $t^n(f+\wp') = 0$, where $f \in \mathcal{R}_2 \backslash \wp'$. So the existence of finite t-orbits in $\mathcal{R}_2$ and finite s-orbits in $\mathcal{Q}_2$ are equivalent, the converse being obvious. $\square$

Theorem 3.9 *Suppose $d \in \mathbf{N}$, $\wp$ is a zero characteristic prime ideal in $\mathcal{R}_d$ and the shift, σ, on*

$$\widehat{\mathcal{R}_d/\wp} = \{(x_{\mathbf{n}})_{\mathbf{n}\in\mathbf{Z}^d} \in \mathbf{S}^{\mathbf{Z}^d} : \sum_{\mathbf{n}\in\mathbf{Z}^d} c_f(\mathbf{n}) x_{\mathbf{n}} = 0 \ (\mathrm{mod}\ 1) \text{ for all } f \in \wp\}$$

is ergodic. Then there exists an integer $r = r(\wp) \in \{1, \cdots, d\}$, a primitive subgroup $\Gamma = \Gamma(\wp) \subset \mathbf{Z}^d$, and a finite set $Q = Q(\wp) \subset \mathbf{Z}^d$ such that $\Gamma \cong \mathbf{Z}^r$, $\mathbf{0} \in Q$, $Q \cap (Q + \mathbf{m}) = \emptyset$ whenever $\mathbf{0} \neq \mathbf{m} \in \Gamma$ and, if

$$\overline{\Gamma} = \Gamma + Q = \{\mathbf{m} + \mathbf{n} : \mathbf{m} \in \Gamma, \mathbf{n} \in Q\},$$

then the coordinate projection $\pi_{\overline{\Gamma}} : \widehat{\mathcal{Q}_d/\wp'} \to \widehat{\mathbf{Q}}^{\mathbf{Z}^d}$, which restricts any point $x \in \widehat{\mathcal{Q}_d/\wp'}$ to its coordinates in $\overline{\Gamma}$, is a topological group isomorphism; in particular, if $\{\mathbf{n}_1, \cdots, \mathbf{n}_r\}$ is a basis for Γ, then the $\mathbf{Z}^r$-action generated by $\{\sigma^{\mathbf{n}_1}, \cdots, \sigma^{\mathbf{n}_r}\}$ is isomorphic to the shift on $(\Sigma^Q)^{\mathbf{Z}^r} = (\widehat{\mathbf{Q}}^Q)^{\mathbf{Z}^r}$.

Proof. See Schmidt [60, Propositions 8.1 and 8.3].

Proof of Theorem 3.5. We may assume that T is a topological group <u>auto</u>morphism by considering the natural extension of (X, T) in the usual way. By Rokhlin [55, Section 3.3], this does not affect the entropy or mixing of T. By considering coordinatewise action of the completely positive entropy action α on the natural extension space we see that the completely positive entropy property of α is not affected and that T and α still commute.

We may thus consider the combined $\mathbf{Z}^3$-action β of α and T given by $\beta^{\mathbf{n}} = \alpha^{(n_1,n_2)} \circ T^{n_3}$ for all $\mathbf{n} = (n_1, n_2, n_3) \in \mathbf{Z}^3$. As described above we look at $M = \widehat{X}$ as an $\mathcal{R}_3$-module, where the action of $\mathcal{R}_3$ on M is determined by β. Now $\mathcal{R}_3$ is a Noetherian ring so that by Theorem 3.6, as an $\mathcal{R}_3$-module, M has an associated prime ideal, $\wp = \{f \in \mathcal{R}_3 : f \cdot m = 0 = 0_M\}$ for some $m \neq 0$ in M.

Let $\phi : \mathcal{R}_3 \to M$ be the map $f \mapsto f \cdot m$ for all $f \in \mathcal{R}_3$. Then $\ker\phi = \wp$ and $\mathcal{R}_3/\wp \cong \mathrm{im}\,\phi \subset M$. That is, $\mathcal{R}_3/\wp$ can be thought of as embedded in M. But, under the isomorphism Theorem identity of $f + \wp$ with $\phi(f) = f \cdot m$ for all $f \in \mathcal{R}_3$, $\mathbf{u^n}(f + \wp) = \mathbf{u^n}(f \cdot m) = (\mathbf{u^n} f)m = \mathbf{u^n} f + \wp$ for all $\mathbf{n} = (n_1, n_2, n_3) \in \mathbf{Z}^3$ (recall that $\mathbf{u^n} = u_1^{n_1} u_2^{n_2} u_3^{n_3}$). More generally, $g(f + \wp) = g(f \cdot m) = (gf)m = gf + \wp$ for all $f, g \in \mathcal{R}_3$. Hence, $\mathcal{R}_3/\wp$ can be thought of as an $\mathcal{R}_3$-submodule of M. In particular, $\mathcal{R}_3/\wp$ is $\widehat{\beta}$-invariant (recall that $\mathbf{u^n} \cdot m = \widehat{\beta}^{\mathbf{n}}(m)$ for all $\mathbf{n} \in \mathbf{Z}^3$ and $m \in M$).

Dual to this inclusion, ψ say, of $\mathcal{R}_3/\wp$ in M we have the surjection $\widehat{\psi} : X \to \widehat{\mathcal{R}_3/\wp}$. Furthermore, the dual of multiplication by $\mathbf{u^n}$ on $\mathcal{R}_3/\wp$ is the shift, σ, on $\widehat{\mathcal{R}_3/\wp} = \{(x_{\mathbf{n}})_{\mathbf{n} \in \mathbf{Z}^3} \in \mathbf{S}^{\mathbf{Z}^3} : \sum_{\mathbf{n} \in \mathbf{Z}^3} c_f(\mathbf{n}) x_(\mathbf{n}) = 0 \pmod 1 \text{ for all } f \in \wp\}$. Therefore, since entropy can only decrease on passing to factors, it is sufficient to show that $\sigma^{(0,0,1)}$ has infinite entropy on $\widehat{\mathcal{R}_3/\wp}$. We know that $h(\sigma^{(0,0,1)}) \neq 0$ since a factor of a mixing map is easily shown to be mixing. Also, completely positive entropy is easily shown to be preserved by passing to factors.

Suppose first that $\wp$ has positive characteristic. Since $h(\sigma^{(0,0,1)}) \neq 0$, $r = r(\wp)$ in Theorem 3.7 is equal to 2 or 3. In the latter case we have a shift on an infinite alphabet and in the former case we have the same or a two dimensional algebraic cellular automata (as in Theorem 3.4), each giving infinite entropy.

So suppose that $\wp$ has zero characteristic. By Theorem 3.8, we may consider ourselves to be in $\mathcal{Q}_3/\wp'$ and, by Theorem 3.9, we are looking at the restriction to $(\widehat{\mathbf{Q}}^Q)^\Gamma$ where $\Gamma \subset \mathbf{Z}^3$ is isomorphic to $\mathbf{Z}^r$ for $r = 1, 2$, or 3. If $r = 3$ we have a shift on an infinite alphabet. If $r = 1$ or 2 we have the same or a shift commuting automorphism, T, of $(\widehat{\mathbf{Q}}^Q)^{\mathbf{Z}^r}$. We give here a detailed account of the $r = 1$ case, noting that the $r = 2$ case is similarly dealt with but the alphabet becomes $\widehat{\mathbf{Q}}^{Q \times \mathbf{Z}}$ (that is, we exploit the identification $(\widehat{\mathbf{Q}}^Q)^{\mathbf{Z}^2} \cong (\widehat{\mathbf{Q}}^{Q \times \mathbf{Z}})^{\mathbf{Z}}$).

Thus, we wish to show that a mixing shift commuting automorphism, T of $(\widehat{\mathbf{Q}}^Q)^{\mathbf{Z}}$ has infinite entropy (see Remark 3.5). We have the obvious identification of $(\mathbf{Q}^Q)_{\mathbf{Z}}$ with $\mathbf{Q}^Q[u^{\pm 1}]$, under which the shift becomes multiplication by u^n, for all $n \in \mathbf{N}$ (with which T commutes).

Think of the typical element $v \in \mathbf{Q}^Q$ as a column vector $v = (v_1, \cdots, v_q)$, where $q = |Q|$. Thus $\mathbf{Q}^Q$ is a q-dimensional vector space over $\mathbf{Q}$. Let $\{e_1, \cdots, e_q\}$ be the standard orthonormal basis for $\mathbf{Q}^Q$. Now, for $f \in \mathbf{Q}^Q[u^{\pm 1}]$ and $n \in \mathbf{Z}$, let $v_f(n) \in \mathbf{Q}^Q$ be the coefficient of u^n in f and let $c_f(n,i)$ be the i'th entry of $v_f(n)$ (that is, $v_f(n) = \sum_{i=1}^{q} c_f(n,i) \cdot e_i$). For all but a finite number of values of $n \in \mathbf{Z}$ the $v_f(n)$, and hence $c_f(n,i)$ for $1 \leq i \leq q$, will be the zero element of $\mathbf{Q}^Q$, and $\mathbf{Q}$ respectively. So, for $f \in \mathbf{Q}^Q[u^{\pm 1}]$, $T(f) = T(\sum_{n\in\mathbf{Z}}(\sum_{i=1}^{q} c_f(n,i) \cdot e_i) \cdot u^n) = \sum_{n\in\mathbf{Z}} u^n \cdot T(\sum_{i=1}^{q} c_f(n,i) \cdot e_i) = \sum_{n\in\mathbf{Z}} u^n \cdot \sum_{i=1}^{q} c_f(n,i) \cdot T(e_i)$.

Thus, for $m \in \mathbf{Z}$ and $1 \leq j \leq q$, $c_{T(f)}(m,j) = \sum_{n\in\mathbf{Z}} \sum_{i=1}^{q} c_f(n,i) \cdot c_{T(e_i)}(m-n,j)$ and, hence, $v_{T(f)}(n) = \sum_{j=1}^{q} c_{T(f)}(m,j) \cdot e_j = \sum_{j=1}^{q} \sum_{n\in\mathbf{Z}} \sum_{i=1}^{q} c_f(n,i) \cdot c_{T(e_i)}(m-n,j) \cdot e_j = \sum_{n\in\mathbf{Z}} M(m-n) \cdot v_f(n)$, where $M(m-n) \in \mathbf{M}_q(\mathbf{Q})$ (the $q \times q$ matrices in $\mathbf{Q}$) is such that its (j,i)'th entry, $(M(m-n))_{(j,i)} = c_{T(e_i)}(m-n,j)$.

So, if $\{e'_i\}_{i\in\mathbf{Z}}$ is the 'standard orthonormal basis' (in the obvious sense) for the elements of $(\mathbf{Q}^Q)_{\mathbf{Z}} = \mathbf{Q}^Q[u^{\pm 1}]$ considered as bilaterally infinite column vectors whose entries lie in $\mathbf{Q}^Q$ and if $\mathbf{v}_f$ is $f \in \mathbf{Q}^Q[u^{\pm 1}]$ considered as an element of $(\mathbf{Q}^Q)_{\mathbf{Z}}$ then, $T(f) = \sum_{m\in\mathbf{Z}} v_{T(f)}(m) \cdot e'_m = \sum_{m\in\mathbf{Z}} \sum_{n\in\mathbf{Z}} M(m-n) \cdot v_f(n) \cdot e'_m = \mathcal{M} \cdot \mathbf{v}_f$, where $\mathcal{M} \in \mathbf{M}_{\pm\infty}(\mathbf{M}_q(\mathbf{Q}))$ (bi-laterally infinite matrices whose entries lie in $\mathbf{M}_q(\mathbf{Q})$) and the (n,m)'th entry, $\mathcal{M}_{(n,m)}$, of $\mathcal{M}$ is $M(m-n)$.

Since $M(K) \in \mathbf{M}_q(\mathbf{Q})$ must clearly be the zero matrix for all but a finite number of values of $k \in \mathbf{Z}$, and since $\mathcal{M}_{(n+i,m+i)} = M((m+i)-(n+i)) = M(m-n) = \mathcal{M}_{(n,m)}$ for all $n, m, i \in \mathbf{Z}$, we have that, along any diagonal of $\mathcal{M}$, all entries (elements of $\mathbf{M}_q(\mathbf{Q})$) are the same and, for all but a finite number of those diagonals, these identical entries are all the zero vector in $\mathbf{M}_q(\mathbf{Q})$ (this is the band structure of the matrix B in [42]).

We now consider two possibilities. First, if there exists a non-zero $g \in \mathbf{Q}^Q[u^{\pm 1}] \cong (\mathbf{Q}^Q)_{\mathbf{Z}}$ (the direct sum of $\mathbf{Z}$ copies of $\mathbf{Q}^Q$) and some non-zero rational polynomial $h \in \mathbf{Q}[u]$ in T that annihilates g (that is, $\sum_{n\in\mathbf{Z}^+} c_h(n) \cdot T^n(g) = 0$, where $c_h(n) \in \mathbf{Q}$ for all $n \in \mathbf{Z}^+$ and there exists $m \in \mathbf{N}$ such that $c_h(m) \neq 0$ but $n > m$ implies that $c_h(n) = 0$) then the vector space $W \leq (\mathbf{Q}^Q)_{\mathbf{Z}}$ over $\mathbf{Q}$ spanned by $\{T^n(g)\}_{n\in\mathbf{Z}^+}$ is finite dimensional and there exist $l, r \in \mathbf{Z}$ such that $f \in W$ implies that $v_f(n) = 0$ in $\mathbf{Q}^Q$ for $n < l$ and $r < n$. Since W is clearly T-invariant and T commutes with the shift, σ, on $(\mathbf{Q}^Q)_{\mathbf{Z}}$, $\sigma^n(W)$ is T-invariant for all $n \in \mathbf{Z}$ and, for $k > r-l$, the set $\mathcal{W} = \{\sigma^{nk}(W) : n \in \mathbf{Z}\}$ is linearly independent over $\mathbf{Q}$ (that is, given a single vector from each of a finite number of elements of $\mathcal{W}$, no non-trivial linear combination in $\mathbf{Q}$ of this finite set of vectors is equal to zero). Also, for all $n \in \mathbf{N}$, $\bigoplus_{i=1}^{n} \sigma^{ik}(W)$ is clearly T-invariant.

Now, since $g \in W$, $n < l$ or $r < n$ implies that $v_g(n) = 0$ in $\mathbf{Q}^Q$ so that $\mathbf{v}_{T(g)} = \sum_{m \in \mathbf{Z}} \sum_{n=l}^{r} M(m-n) \cdot v_g(n) \cdot e'_m$ and, by T-invariance of W, $T(g)$ must be in W so that, for $m < l$ or $r < m$ $c_{T(g)}(m) = 0$ in $\mathbf{Q}^Q$ and, the coefficient of e'_m in the above summation must be zero in $\mathbf{Q}^Q$. That is, $\mathbf{v}_{T(g)} = \sum_{m=l}^{r} \sum_{n=l}^{r} M(m-n) \cdot v_g(n) \cdot e'_m$.

It follows that the projection $\pi_{\{l,\cdots,r\}} : W \to \prod_{n=l}^{r} \mathbf{Q}^Q$ gives an isomorphism of discrete groups between W and $V = \pi_{\{l,\cdots,r\}}(W)$ under which (W,T) is conjugate to (V,S), where the endomorphism S of V is given by the $(r-l+1) \times (r-l+1)$ matrix whose (n,m)'th entry is $M(m-n)$ (since both of the respective summations were from l to r, and since $M(m+l-1, n+l-1) = M(m,n)$ for all $1 \le m, n \le r-l+1$, there is no confusion here).

But the T-invariant W embeds in $(\mathbf{Q}^Q)_{\mathbf{Z}}$ and, hence, $(\widehat{V}, \widehat{S})$ can be thought as a factor of $(\widehat{(\mathbf{Q}^Q)_{\mathbf{Z}}}, \widehat{T})$. Similarly, for all $n \in \mathbf{N}$, $(\widehat{\prod_{i=1}^{n} V}, \widehat{\prod_{i=1}^{n} S})$ (where $\prod_{i=1}^{n} S$ is defined to act in the obvious coordinatewise manner on members of $\prod_{i=1}^{n} V$) can be thought of as a factor of $(\widehat{(\mathbf{Q}^Q)_{\mathbf{Z}}}, \widehat{T})$. This is by the aforementioned linear independence along with the obvious isomorphism which makes the restriction $T|_{\bigoplus_{i=1}^{n} \sigma^{ik}(W)}$ topological group conjugate to to $\prod_{i=1}^{n} S$ and the embedding of the T-invariant group $\bigoplus_{i=1}^{n} \sigma^{ik}(W)$ in $(\mathbf{Q}^Q)_{\mathbf{Z}}$.

But $\widehat{\prod_{i=1}^{n} V} = \prod_{i=1}^{n} \widehat{V}$ where $(\chi_1, \cdots, \chi_n) \in \prod_{i=1}^{n} \widehat{V}$ acts on $(g_1, \cdots, g_n) \in \prod_{i=1}^{n} V$ by $(\chi_1, \cdots, \chi_n)((g_1, \cdots, g_n)) = \sum_{i=1}^{n} \chi_i(g_i) \pmod 1$ (see, for example, Morris [43, Theorem 13]). So $\chi \in \widehat{\prod_{i=1}^{n} V}$ implies that $\chi = (\chi_1, \cdots, \chi_n)$ for some $\chi_1, \cdots, \chi_n \in \widehat{V}$ so that, for all $(g_1, \cdots, g_n) \in \prod_{i=1}^{n} V$,

$$(\widehat{\prod_{i=1}^{n} S}(\chi))(g_1, \cdots, g_n) = \chi(\prod_{i=1}^{n} S(g_1, \cdots, g_n)) = \chi(S(g_1), \cdots, S(g_n))$$

$$= (\chi_1(S(g_1)), \cdots, \chi_n(S(g_n))) = ((\widehat{S}(\chi_1))(g_1), \cdots, (\widehat{S}(\chi_n))(g_n))$$

$$= (\widehat{S}(\chi_1), \cdots, \widehat{S}(\chi_n))(g_1, \cdots, g_n) = ((\prod_{i=1}^{n} \widehat{S})((\chi_1, \cdots, \chi_n)))(g_1, \cdots, g_n)$$

$$= ((\prod_{i=1}^{n} \widehat{S})(\chi))(g_1, \cdots, g_n).$$

So $(\prod_{i=1}^n \widehat{V}, \prod_{i=1}^n \widehat{S}) \cong (\widehat{\prod_{i=1}^n V}, \widehat{\prod_{i=1}^n S})$ is a factor of $(\widehat{(\mathbf{Q}^Q)_{\mathbf{Z}}}, \widehat{T})$ and

$$h(\widehat{T}) \geq h(\prod_{i=1}^{n} \widehat{S}) = n \cdot h(\widehat{S})$$

(see, for example, Walters [64, Theorem 4.23]).

But $h(\widehat{S}) > 0$, since $(\widehat{V}, \widehat{S})$ is a non-trivial factor of $(\widehat{(\mathbf{Q}^Q)_{\mathbf{Z}}}, \widehat{T})$ where T, and hence $\widehat{S}$, is mixing. Thus, since $n \in \mathbf{Z}$ was arbitrary, $h(\widehat{T}) = \infty$.

The remaining possibility is the assumption that no non-zero $f \in (\mathbf{Q}^Q)_{\mathbf{Z}}$ is annihilated by any non-zero polynomial $h \in \mathbf{Q}[u]$ in T. Then fix non-zero $f \in (\mathbf{Q}^Q)_{\mathbf{Z}}$ and let $U \leq (\mathbf{Q}^Q)_{\mathbf{Z}}$ be that subspace of $(\mathbf{Q}^Q)_{\mathbf{Z}}$ over $\mathbf{Q}$ spanned by finite linear combinations, in $\mathbf{Q}$, of elements of $\{T^k(f)\}_{k \in \mathbf{Z}^+}$. Let $\theta : U \to (\mathbf{Q}^Q)_{\mathbf{Z}^+}$ be such that $\sum_{n \in \mathbf{Z}^+} q_n \cdot T^n(f) \mapsto (q_n)_{n \in \mathbf{Z}^+}$. Then θ is well-defined by our assumption, and clearly an isomorphism of discrete groups. Furthermore, $\theta \circ T \circ \theta^{-1}((q_n)_{n \in \mathbf{Z}^+}) = \theta \circ T(\sum_{n \in \mathbf{Z}^+} q_n \cdot T^n(f)) = \theta(\sum_{n \in \mathbf{Z}^+} q_n \cdot T^{n+1}(f)) = \theta(\sum_{n \in \mathbf{N}} q_{n-1} \cdot T^n(f)) = (q_{n-1})_{n \in \mathbf{Z}^+}$, where $q_{-1} = 0$. That is, the restriction of T to U (which is clearly T-invariant) is conjugate to the right-shift, σ_r, on $(\mathbf{Q}^Q)_{\mathbf{Z}^+}$. Thus, dual to the embedding of U in $(\mathbf{Q}^Q)_{\mathbf{Z}}$, we can think of $(\widehat{(\mathbf{Q}^Q)_{\mathbf{Z}^+}}, \widehat{\sigma_r}) = ((\Sigma^Q)^{\mathbf{Z}^+}, \sigma_l)$ (where σ_l is the left-shift on $(\Sigma^Q)^{\mathbf{Z}^+}$) as a factor of $((\Sigma^Q)^{\mathbf{Z}}, \widehat{T})$. But this factor is the left-shift on an infinite alphabet and therefore has infinite entropy so finally, again, $h(\widehat{T}) = \infty$. This completes the proof of Theorem 3.5. $\square$

Remark 3.5 A famous open problem of Lehmer [31] asks whether, when $\lambda_i \in \mathbf{C}$ for $i \in \{1, \cdots, n\}$ and $\Pi_{i=1}^n (x - \lambda_i)$ is a polynomial with only integer coefficients, the quantity $\Sigma_{|\lambda_i|>1} \log |\lambda_i|$ can be arbitrarily small and positive. By Lind [32, Theorem 2], a negative answer to Lehmer's problem would be enough to show that the entropy of a mixing automorphism of the infinite solenoid is infinite, shortening the proof of Theorem 3.5.

Chapter 4

Two dimensional subcellular automata

4.1 Generalisations of results on one dimensional cellular automata

Recall that, for $d, k \in \mathbf{N}$, $\mathcal{S} = \mathcal{S}(k) = \{0, \cdots, k-1\}$, $\Omega = \Omega_k(d) = \mathcal{S}^{\mathbf{Z}^d}$, and a d-dimensional cellular automaton (on Ω) is a continuous map T of (Ω, σ) (see Notation 1.1). A subshift (Σ, σ) is the restriction of σ to a closed σ-invariant subset Σ of Ω. When the meaning is clear we also denote the restriction by σ, otherwise we emphasize it by σ_Σ.

Definition 4.1 A *d-dimensional subcellular automaton* (of Σ) is a continuous map T of (Σ, σ).

Recall that a subshift of finite type is defined by what we can consider to be a set of allowed configurations $P \subset \mathcal{S}^F$ for some finite subset $F \subset \mathbf{Z}^d$ (see Definition 1.10). For $d = 1$ every subshift of finite type is topologically conjugate to a matrix subshift of finite type [1]; that is, a subshift of finite type on k symbols (this may differ from

[1]The same holds for $d > 1$ in some sense (see Miebach [39]) but the extension problem means this is rarely useful (see Markley and Paul [37]).

the alphabet size of the original system) that can be represented by a $k \times k$ matrix A of zeroes and ones. If A is irreducible (for all $1 \leq i, j \leq k$ there exists $n \in \mathbf{N}$ such that the (i,j)th entry of A^n is non-zero) we say that the matrix subshift of finite type is irreducible.

Hedlund [21] showed (the result was joint work of his, with Curtis and Linden) that, for $d = 1$ and given $k \in \mathbf{N}$, the set of cellular automata maps is equivalent to the set of maps f_∞ of (Ω, σ) determined by finite sets $E \subset \mathbf{Z}$ and maps $f : \mathcal{S}^E \to \mathcal{S}$ given by $(f_\infty(\mathbf{x}))_n = f(\pi_{E+n}(\mathbf{x})) = f(\pi_E(\sigma^n(\mathbf{x})))$ for all $n \in \mathbf{Z}$, $\mathbf{x} \in \Omega$, and for all such f and E.

Our use of projections in what follows is essentially equivalent to Hedlund's 'n-blocks'. Hedlund effectively always has $E = \{0, \cdots, m-1\} \subset \mathbf{Z}$ for some $m \in \mathbf{N}$ and implicitly generalizes to maps g_∞ of (Ω, σ), determined by arbitrary finite subsets $H = \{h_1, \cdots, h_q\}$ (where, initially, $h_1 = 0$) of $\mathbf{Z}$ and maps $g : \mathcal{S}^H \to \mathcal{S}$, by the implicit assumption that $E = \{0, 1, \cdots, h_q\}$ and the map f_∞ of (Ω, σ) is determined by $f : \mathcal{S}^E \to \mathcal{S}$ given by $f((x)) = g(\pi_H((x)))$ for all $(x) \in \mathcal{S}^E$: elements of $\mathcal{S}^M$, for proper subsets M of $\mathbf{Z}$ or $\mathbf{Z}^2$, will always be denoted by encasement in brackets. The case where $h_1 \neq 0$ is then dealt with by considering the action of $\sigma^n \circ f_\infty$ for suitable $n \in \mathbf{N}$. Our finite subsets of $\mathbf{Z}^2$ will always be arbitrary, unless stated otherwise.

We will write $\pi_M^{-1}((b))$ for $(b) \in \pi_M(\Sigma)$ when it is clear what the domain of π_M is. Otherwise, for $M \subset M' \subset \Sigma$ and $(b) \in \pi_M(\Sigma)$, $\pi_{M'}(\Sigma) \cap \pi_M^{-1}((b))$ emphasizes that π_M is the projection from $\pi_{M'}(\Sigma)$ to $\pi_M(\Sigma)$, whereas $\Sigma \cap \pi_M^{-1}((b))$ emphasizes that π_M is the projection from Σ to $\pi_M(\Sigma)$.

For $\mathbf{m} \in \mathbf{Z}^2$ and $M, N \subset \mathbf{Z}^2$ we denote $M + \mathbf{m} = \{\mathbf{n} + \mathbf{m} : \mathbf{n} \in M\}$ and $M + N = \{\mathbf{m} + \mathbf{n} : \mathbf{m} \in M, \mathbf{n} \in N\}$.

Note that, for $M \subset \mathbf{Z}^2$ and $\mathbf{n} \in \mathbf{Z}^2$, we denote by $\sigma^{\mathbf{n}}$ the map from $\mathcal{S}^{M+\mathbf{n}}$ to $\mathcal{S}^M$ given by $(\sigma^{\mathbf{n}}((b)))_{\mathbf{m}} = (b)_{\mathbf{m}+\mathbf{n}}$ for all $\mathbf{m} \in M$, for all $(b) \in \mathcal{S}^{M+\mathbf{n}}$. This abuse of notation causes no problems since we have $(\sigma^{\mathbf{n}}(\pi_{M+\mathbf{n}}(x)))_{\mathbf{m}} = (\pi_{M+\mathbf{n}}(x))_{\mathbf{m}+\mathbf{n}} = x_{\mathbf{m}+\mathbf{n}} = (\sigma^{\mathbf{n}}(x))_{\mathbf{m}} = (\pi_M(\sigma^{\mathbf{n}}(x)))_{\mathbf{m}}$ for all $\mathbf{m} \in M$, for all $x \in \Omega$. Thus, $\sigma^{\mathbf{n}} \circ \pi_{M+\mathbf{n}} = \pi_M \circ \sigma^{\mathbf{n}}$ for all $M \subset \mathbf{Z}^d, \mathbf{n} \in \mathbf{Z}^2$.

From now on, unless otherwise stated, we have the standing hypothesis that $d = 2$, $\mathcal{S} = \mathcal{S}(k)$, and $\Omega = \Omega_k(2)$, for some fixed $k \in \mathbf{N}$.

Thus, given a finite subset N of $\mathbf{Z}^2$ and a map $f : \mathcal{S}^N \to \mathcal{S} = \mathcal{S}^{\{\mathbf{0}\}}$ (where the superscript $\mathbf{0} = (0,0) \in \mathbf{Z}^2$ is usually taken for granted and omitted) then, for all $M \subset \mathbf{Z}^2$, we define $f^M : \mathcal{S}^{N+M} \to \mathcal{S}^M$ by $(f^M((x)))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}((x))))$ for all $\mathbf{m} \in M$, for all $(x) \in \mathcal{S}^{N+M}$. From now on, unless otherwise stated, N (or N' when referring to $d = 1$ analogues) and f will always signify a finite set of coordinates in $\mathbf{Z}^2$ and a function $f : \mathcal{S}^N \to \mathcal{S}$ (or $f : \mathcal{S}^{N'} \to \mathcal{S}$ respectively).

From now on Σ will always be a closed subset of Ω that is σ-invariant and $f^{\mathbf{Z}^2}$-invariant. Denote $f^\Sigma = f^{\mathbf{Z}^2}|_\Sigma$, thus $f^\Omega = f^{\mathbf{Z}^2}$ (this is our analogue of Hedlund's f_∞).The term *f^Σ-map* (or *f^Ω-map*) will indicate an arbitrary map of this form.

Now if $(b) = \pi_{N+M}(x)$ for some $x \in \Sigma$ and $M \subset \mathbf{Z}^2$ then $f^\Omega(x) = y$ for some $y \in \Sigma$ (by f^Ω-invariance of Σ). So, for all $\mathbf{m} \in M$, $(f^M((b)))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}((b))))$. But, for all $\mathbf{n} \in N$, $(\sigma^{\mathbf{m}}((b)))_{\mathbf{n}} = (b)_{\mathbf{n+m}}$, so $f(\pi_N(\sigma^{\mathbf{m}}((b)))) = f(\pi_{N+\mathbf{m}}((b))) = f(\pi_{N+\mathbf{m}}(x))$. But, for all $\mathbf{n} \in N$, $x_{\mathbf{n+m}} = (\sigma^{\mathbf{m}}(x))_{\mathbf{n}}$, so $f(\pi_{N+\mathbf{m}}(x)) = f(\pi_N(\sigma(x))) = (f^\Omega(x))_{\mathbf{m}} = y_{\mathbf{m}}$. So $f^M((b)) = \pi_M(y) \in \pi_M(\Sigma)$. We record this as a proposition.

Proposition 4.1 *$f^M(\pi_{M+N}(\Sigma)) = f^M_\Sigma(\pi_{M+N}(\Sigma)) \subset \pi_M(\Sigma)$ (so Σ is f^M-invariant in the sense in which we'd expect it to be).*

In particular, if $M = \{\mathbf{0}\}$, $f(\pi_N(\Sigma)) = f^{\{\mathbf{0}\}}(\pi_N(\Sigma)) \subset \pi_{\{\mathbf{0}\}}(\Sigma) = \mathcal{T}$ ($\mathcal{T}$ will always denote $\pi_{\{\mathbf{0}\}}(\Sigma)$). Denote $f^M|_{\pi_{N+M}(\Sigma)} : \pi_{N+M}(\Sigma) \to \pi_M(\Sigma)$ by f^M_Σ.

Proposition 4.2 *For all $z \in \Sigma$, $f^M_\Sigma(\pi_{M+N}(z)) = \pi_M(f^\Sigma(z))$.*

Proof. For all $z \in \Sigma$ and for all $\mathbf{m} \in M$, $(f^M_\Sigma(\pi_{M+N}(z)))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}(\pi_{M+N}(z))))$. On the other hand $(\sigma^{\mathbf{m}}(\pi_{M+N}(z)))_{\mathbf{n}} = (\pi_{M+N}(z))_{\mathbf{m+n}} = z_{\mathbf{m+n}} = (\sigma^{\mathbf{m}}(z))_{\mathbf{n}}$ for all $\mathbf{n} \in N$. So $\pi_N(\sigma^{\mathbf{m}}(\pi_{M+N}(z)))) = \pi_N(\sigma^{\mathbf{m}}(z))$, so that $(f^M_\Sigma(\pi_{M+N}(z)))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}(z))) = (f^\Sigma(z))_{\mathbf{m}}$. □

The proof of the following result, generalised to $d = 2$, is based on Hedlund's proof for $d = 1$. It shows that all of our results for maps of (Σ, σ) can be generalised to maps of general (Z, α) where Z is a compact, totally disconnected, metric space and $\alpha : Z \to Z$ is an expansive $\mathbf{Z}^2$-action by homeomorphisms of Z onto Z.

Theorem 4.1 *Let Z be a compact, totally disconnected, metric space and let $\alpha : Z \to Z$ be a $\mathbf{Z}^2$-action by homeomorphisms of Z onto Z. Then (Z, α) is expansive if and only if there exists $k \in \mathbf{N}$ and subshift (Σ, σ) of (Ω_k, σ) such that (Z, α) is topologically conjugate to (Σ, σ).*

Proof. Completely analogous to Hedlund [21, Theorem 2.1].

Hedlund's result for $d = 1$ that f_∞ is a cellular automaton of Ω (the <u>one</u> dimensional <u>full</u> shift) generalises to arbitrary <u>two</u> dimensional <u>sub</u>cellular automata.

Theorem 4.2 *Any f^Σ map is a subcellular automaton of Σ.*

Proof. Given $x, y \in \Sigma$ and $\epsilon > 0$ there exists finite $M_\epsilon \subset \mathbf{Z}^2$ such that $\rho(x, y) < \epsilon$ if and only if $\pi_{M_\epsilon}(x) = \pi_{M_\epsilon}(y)$. Similarly, there exists finite $M_\delta \subset \mathbf{Z}^2$ such that $M_\epsilon + N \subset M_\delta$ and corresponding $\delta > 0$ such that $\rho(x, y) < \delta$ if and only if $\pi_{M_\delta}(x) = \pi_{M_\delta}(y)$. So if $x, y \in \Sigma$ are such that $\rho(x, y) < \delta$ then $\pi_{M_\epsilon+N}(x) = \pi_{M_\epsilon+N}(y)$ and, thus, $f_\Sigma^{M_\epsilon}(\pi_{M_\epsilon+N}(x)) = f_\Sigma^{M_\epsilon}(\pi_{M_\epsilon+N}(y))$. So, by Proposition 4.2, $\pi_{M_\epsilon}(f^\Sigma(x)) = \pi_{M_\epsilon}(f^\Sigma(y))$. That is, $\rho(f^\Sigma(x), f^\Sigma(y)) < \epsilon$. So f^Σ is (uniformly) continuous.

Finally, for all $\mathbf{k}, \mathbf{m} \in \mathbf{Z}^2$ and $x \in \Sigma$, we have $(\sigma^{\mathbf{m}}(f^\Sigma(x)))_{\mathbf{k}} = (f^\Sigma(x))_{\mathbf{k+m}} = f(\pi_N(\sigma^{\mathbf{k+m}}(x))) = (f^\Sigma(\sigma^{\mathbf{m}}(x)))_{\mathbf{k}}$, so that $\sigma^{\mathbf{m}} \circ f^\Sigma = f^\Sigma \circ \sigma^{\mathbf{m}}$. □

Hedlund's result that, for given $n \in \mathbf{Z}$ and $N' \subset \mathbf{Z}$, $n \in N'$ if and only if there exists $f : \mathcal{S}^{N'} \to \mathcal{S}$ such that $f_\infty = \sigma^n$ generalizes to the two dimensional full shift, but only generalizes in one direction for subshifts.

Theorem 4.3 *For any $\mathbf{n} \in N$ there exists $f : \mathcal{S}^N \to \mathcal{S}$ such that $f^\Sigma = \sigma^{\mathbf{n}}$.*

Proof. Simply define $f : \mathcal{S}^N \to \mathcal{S}$ by $f((x)) = (x)_{\mathbf{n}}$ for all $(x) \in \mathcal{S}^N$ so that, for all $\mathbf{m} \in \mathbf{Z}^2$ and for all $(x) \in \Omega$, $(f^\Omega(x))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}(x))) = (\pi_N(\sigma^{\mathbf{m}}(x)))_{\mathbf{n}} = (\sigma^{\mathbf{m}}(x))_{\mathbf{n}} = \sigma^{\mathbf{m}+\mathbf{n}}(x) = (\sigma^{\mathbf{n}}(x))_{\mathbf{m}}$ so that $f^\Omega = \sigma^{\mathbf{n}}$ and, in particular, $f^\Sigma = (\sigma^{\mathbf{n}})|_\Sigma = \sigma_\Sigma^{\mathbf{m}} = \sigma^{\mathbf{m}}$ (by abuse of notation). □

The generalisation (to $d = 2$) of the proof of the converse for the full shift is straightforward and is omitted.

Counter-example. To see that the converse to Theorem 4.3 does not hold take any $\mathbf{p}, \mathbf{q} \in \mathbf{Z}^2$, put $N = \{\mathbf{p}\}$, and consider $\Sigma = \{x \in \Omega : x_{\mathbf{m}+\mathbf{q}} = x_{\mathbf{m}}$ for all $\mathbf{m} \in \mathbf{Z}^2\}$. By Theorem 4.3 $f^\Sigma = \sigma^{\mathbf{p}}$ for some $f : \mathcal{S}^N \to \mathcal{S}$. But $\sigma^{\mathbf{p}} = \sigma^{\mathbf{p}+n\mathbf{q}}$ for all $n \in \mathbf{Z}$ so, certainly, there exist $\mathbf{n} \in \mathbf{Z}^2$ such that $f^\Sigma = \sigma^{\mathbf{n}}$ and yet $\mathbf{n} \notin N$.

We now prove that the converse of Theorem 4.2 holds and hence that;

Theorem 4.4 *A map is an f^Σ map if and only if it is a subcellular automaton of Σ.*

Proof. One direction of proof is Theorem 4.2. For the other direction assume that T is a continuous map of (Σ, σ). For all $s \in \mathcal{S}$ put $U_s = \{x \in \Sigma : x_{\mathbf{0}} = s\}$. Now $\{U_s : s \in \mathcal{S}\}$ is a partition (allowing partitions to contain empty sets) of Σ and each U_s is open and closed in Σ.

If, for each s, we put $V_s = T^{-1}(U_s)$ then $\mathcal{P} = \{V_s : s \in \pi_{\mathbf{0}}(\Sigma)\}$ is also a partition of Σ into sets each of which is closed and open. Since $\mathcal{P}$ is a finite partition of closed sets there exists an $\epsilon > 0$ such that $s_1 \neq s_2$ in $\mathcal{S}$ implies that if, for $i = 1, 2$, $x_i \in V_{s_i}$ then $\rho(x_1, x_2) > \epsilon$ and there exists appropriate set $M_\epsilon \subset \mathbf{Z}^2$ such that $\rho(x_1, x_2) > \epsilon$ if and only if $\pi_{M_\epsilon}(x_1) \neq \pi_{M_\epsilon}(x_2)$. If we put $N = M_\epsilon$ then the map $f : \mathcal{S}^N \to \mathcal{S}$ defined by $f((w)) = s$ whenever $(w) \in \pi_N(V_s)$ is well-defined. Also, given $z \in \Sigma$, there exists $s \in \mathcal{S}$ such that $z \in V_s = T^{-1}(U_s)$, so that $T(z) \in U_s$ and $(T(z))_{\mathbf{0}} = s$. Since $z \in V_s$, $(f^\Sigma(z))_{\mathbf{0}} = f(\pi_N(z)) = s$, by definition of f. Now by the hypothesis $T \circ \sigma = \sigma \circ T$ and, by Theorem 4.2 $f^\Sigma \circ \sigma = \sigma \circ f^\Sigma$. So, for all $z \in \Sigma$ and for all $\mathbf{m} \in \mathbf{Z}^2$, there exists $s_{\mathbf{m}} \in \mathcal{S}$ such that $(T(z))_{\mathbf{m}} = (\sigma^{\mathbf{m}}(T(z)))_{\mathbf{0}} = (T(\sigma^{\mathbf{m}}(z)))_{\mathbf{0}} = (f^\Sigma(\sigma^{\mathbf{m}}(z)))_{\mathbf{0}} = (\sigma^{\mathbf{m}}(f^\Sigma(z)))_{\mathbf{0}} = (f^\Sigma(z))_{\mathbf{m}}$ so that $T(z) = f^\Sigma(z)$, for arbitrary $z \in \Sigma$. □

The following generalisation of another Hedlund result for <u>one</u>-dimensional <u>full</u>-shifts to an analogue for <u>two</u>-dimensional <u>sub</u>shifts concentrates on $\mathcal{T} = \pi_{\mathbf{0}}(\Sigma)$, as opposed to $\mathcal{S}$. The necessity of this is explained after the proof. Note that the g^M's and g^Σ are defined from $\mathcal{T}$ and $g : \mathcal{T}^N \to \mathcal{T}$ in the same way that the f^M's and f^Σ are defined from $\mathcal{S}$ and f respectively. Part (3)⇒(4) of the proof is significantly more involved than the equivalent part of the proof for the full-shift.

Theorem 4.5 *If $N = \{\mathbf{n}\}$ for some $\mathbf{n} \in \mathbf{Z}^2$ and $\mathcal{T} = \pi_{\mathbf{0}}(\Sigma)$ then $f(\mathcal{T}^N) \subset \mathcal{T}$. If, also, $g = f|_{\mathcal{T}^N}$ then $f^L_\Sigma = g^L_\Sigma$ for all $L \subset \mathbf{Z}^2$ and the following are equivalent:*

(1) $g : \mathcal{T}^N \to \mathcal{T}$ *is a bijection*

(2) $g^M : \mathcal{T}^{M+N} \to \mathcal{T}^M$ *is onto for all finite* $M \subset \mathbf{Z}^2$

(3) $|(g^M)^{-1}((b))| = 1$ *for all* $(b) \in \mathcal{T}^M$ *for all finite* $M \subset \mathbf{Z}^2$

(4) $f^\Sigma = g^\Sigma : \Sigma \to \Sigma$ *is onto*

(5) $f^\Sigma = g^\Sigma : \Sigma \to \Sigma$ *is a homeomorphism of* Σ

Proof. If $(t) \in \mathcal{T}^N$ then, since Σ is shift invariant, $\pi_N(z) = (t)$ for some $z \in \Sigma$. But Σ is f^Σ-invariant so $f((t)) = f(\pi_N(z)) = (f^\Sigma(z))_{\mathbf{0}} = \pi_{\mathbf{0}}(f^\Sigma(z)) \in \pi_{\mathbf{0}}(\Sigma) = \mathcal{T}$. That is $f(\mathcal{T}^N) \subset \mathcal{T}$.

Since $\mathcal{T} = \pi_{\mathbf{0}}(\Sigma)$ and Σ is shift invariant we have that $\Sigma \subset \mathcal{T}^{\mathbf{Z}^2}$ so that g is defined on Σ. For all $(c) \in \pi_L(\Sigma)$ and for all $\mathbf{m} \in L$, $(g^L_\Sigma((c)))_{\mathbf{m}} = g(\pi_N(\sigma^{\mathbf{m}}((c)))) = f(\pi_N(\sigma^{\mathbf{m}}((c)))) = (f^L_\Sigma((c)))_{\mathbf{m}}$ and, hence, $g^L_\Sigma = f^L_\Sigma$ and when $L = \mathbf{Z}^2$ we have $g^\Sigma = f^\Sigma$. We now show that (1), (2), (3), (4), and (5) are equivalent.

If (1) holds and M is a finite subset of $\mathbf{Z}^2$, and $(b) \in \mathcal{T}^M$ then take $(a) \in \mathcal{T}^{M+N}$ such that $(a)_{\mathbf{m}+\mathbf{n}} = g^{-1}((b)_{\mathbf{m}})$ for all $\mathbf{m} \in \mathbf{Z}^2$ and, clearly, $g^M((a)) = (b)$ so that (2) holds.

If (2) holds and M is a finite subset of $\mathbf{Z}^2$ and $(b) \in \mathcal{T}^M$. Since $|\mathcal{T}^N| = |\mathcal{T}| < \infty$ and g^M is onto it must also be a bijection so that (3) holds.

If (3) holds (so g^M is bijective for all finite $M \subset \mathbf{Z}^2$) and $z \in \Sigma$ then take a sequence $\{M_n\}_{n\in\mathbf{N}}$ of finite subsets of $\mathbf{Z}^2$ such that $M_n \subset M_{n+1}$ for all $n \in \mathbf{N}$ and $\cup_{n\in\mathbf{N}} M_n = \mathbf{Z}^2$. Now, for all $n \in \mathbf{N}$, let $(b_n) = \pi_{M_n}(z)$ and note that $\pi_{M_n}((b_{n+1})) = (b_n)$. Then, by (3) there exists a unique $(a_n) \in \mathcal{T}^{M_n+N}$ such that $g^{M_n}((a_n)) = (b_n)$.

Now, for all $\mathbf{m} \in M_n$ and for all $\mathbf{n} \in N$,

$$(\sigma^{\mathbf{m}}(\pi_{M_n+N}((a_{n+1}))))_{\mathbf{n}} = (\pi_{M_n+N}((a_{n+1})))_{\mathbf{n}+\mathbf{m}} = (a_{n+1})_{\mathbf{n}+\mathbf{m}} = (\sigma^{\mathbf{m}}(a_{n+1}))_{\mathbf{n}}$$

So $\pi_N(\sigma^{\mathbf{m}}(\pi_{M_n+N}((a_{n+1})))) = \pi_N(\sigma^{\mathbf{m}}((a_{n+1})))$. So, for all $\mathbf{m} \in M_n$,

$$(g^{M_n}(\pi_{M_n+N}((a_{n+1}))))_{\mathbf{m}} = g(\pi_N(\sigma^{\mathbf{m}}(\pi_{M_n+N}((a_{n+1}))))) = g(\pi_N(\sigma^{\mathbf{m}}((a_{n+1}))))$$

$$= (g^{M_{n+1}}((a_{n+1})))_{\mathbf{m}} = ((b_{n+1}))_{\mathbf{m}} = ((b_n))_{\mathbf{m}} = (g^{M_n}((a_n)))_{\mathbf{m}}$$

So $g^{M_n}(\pi_{M_n+N}((a_{n+1}))) = g^{M_n}((a_n))$ and, since g^{M_n} is bijective, $\pi_{M_n+N}((a_{n+1})) = ((a_n))$. Therefore, for all $n \in \mathbf{N}$, take $y_n \in \mathcal{T}^{\mathbf{Z}^2}$ such that $\pi_{M_n+N}(y_n) = (a_n)$ and see that $\{y_n\}_{n\in\mathbf{N}}$ is Cauchy, so $\lim_{n\to\infty} y_n = y$ for some $y \in \mathcal{T}^{\mathbf{Z}^2}$ such that $\pi_{M_n+N}(y) = \pi_{M_n+N}(y_n) = (a_n)$ for all $n \in \mathbf{N}$.

But, for all $\mathbf{m} \in \mathbf{Z}^2$, there exists $n \in \mathbf{N}$ such that $\mathbf{m} \in M_n$ so that, for all $\mathbf{n} \in N$, $(\sigma^{\mathbf{m}}(y))_{\mathbf{n}} = (y)_{\mathbf{m}+\mathbf{n}} = (\pi_{M_n+N}(y))_{\mathbf{m}+\mathbf{n}} = (\sigma^{\mathbf{m}}(\pi_{M-n+N}(y)))_{\mathbf{n}}$ and, putting $\Delta = \mathcal{T}^{\mathbf{Z}^2}$, $(g^{\Delta}(y))_{\mathbf{m}} = g(\pi_N(\sigma^{\mathbf{m}}(y))) = g(\pi_n(\sigma^{\mathbf{m}}(\pi_{M-n+N}(y)))) = (g^{M_n}(\pi_{M_n+N}(y)))_{\mathbf{m}} = (g^{M_n}((a_n)))_{\mathbf{m}} = (b_n)_{\mathbf{m}} = z_{\mathbf{m}}$. So $g^{\Delta}(y) = z$.

If $y \notin \Sigma$ then $(a_n) = \pi_{M_n+N}(y) \notin \pi_{M_n+N}(y)$ for some $n \in \mathbf{N}$. But $g^{M_n}((a_n)) = (b_n) \in \pi_{M_n}(z)$ and $|\pi_{M_n+N}(\Sigma)| = |\pi_{M_n}(\Sigma)| < \infty$ (by σ-invariance and $|N| = 1$) so, since g^{M_n} is a bijection, there exists $(a) \in \pi_{M_n+N}(\Sigma)$ such that $g^{M_n}((a)) \notin \pi_{M_n}(\Sigma)$. That is, $g^{M_n}(\pi_{M_n+N}(\Sigma) \not\subset \pi_{M_n}(\Sigma)$. But $g^{M_n}(\pi_{M_n+N}(\Sigma)) = g_{\Sigma}^{M_n}(\pi_{M_n+N}(\Sigma)) = f_{\Sigma}^{M_n}(\pi_{M_n+N}(\Sigma)) \subset \pi_{M_n}(\Sigma)$, so we must have $y \in \Sigma$. Hence $f^{\Sigma} = g^{\Sigma}$ is onto, so (4) holds.

Now suppose that (4) holds. We wish to show that f^{Σ} is injective. Suppose otherwise, then there are distinct $x, y \in \Sigma$ such that $f^{\Sigma}(x) = f^{\Sigma}(y)$. Now $x_{\mathbf{m}} \neq y_{\mathbf{m}}$ for some $\mathbf{m} \in \mathbf{Z}^2$ and so $(\sigma^{\mathbf{m}-\mathbf{n}}(x))_{\mathbf{n}} \neq (\sigma^{\mathbf{m}-\mathbf{n}}(y))_{\mathbf{n}}$ or, alternatively, $\pi_N(\sigma^{\mathbf{m}-\mathbf{n}}(x)) \neq \pi_N(\sigma^{\mathbf{m}-\mathbf{n}}(y))$. However, since $g(\pi_N(\sigma^{\mathbf{m}-\mathbf{n}}(x))) = f(\pi_N(\sigma^{\mathbf{m}-\mathbf{n}}(x))) = (f^{\Sigma}(x))_{\mathbf{m}-\mathbf{n}} = (f^{\Sigma}(y))_{\mathbf{m}-\mathbf{n}} = f(\pi_N(\sigma^{\mathbf{m}-\mathbf{n}}(y))) = g(\pi_N(\sigma^{\mathbf{m}-\mathbf{n}}(y)))$, $g : \mathcal{T}^N \to \mathcal{T}$ is not injective and so can't be surjective (since $|\mathcal{T}| < \infty$), so there must exist $t \in \mathcal{T}$ such that $g^{-1}(t) = \emptyset$. Select $z \in \Sigma$ such that $z_{\mathbf{0}} = t$. Now by (4) there exists $v \in \Sigma$ such that $f^{\Sigma}(v) = z$, so that $g(\pi_N(v)) = f(\pi_N(v)) = (f^{\Sigma}(v))_{\mathbf{0}} = z_{\mathbf{0}} = t$, contradicting surjectivity of g. So f^{Σ} is injective and (5) holds.

Finally, if (5) holds then certainly (4) holds and, by part of the proof of (4)$\Rightarrow$(5), g is surjective and hence bijective (since $|\mathcal{T}| < \infty$). So (1) holds. $\square$

To see why we had to replace $\mathcal{S}$, f, and f^M in the statement of the two-dimensional subshift analogue of the theorem for the one-dimensional full-shift by $\mathcal{T} = \pi_{\mathbf{0}}(\Sigma)$, $g = f|_{\pi_N}(\Sigma)$ and g^M respectively we have the following example.

Example 4.1 Consider $\mathcal{S} = \mathcal{S}_4 = \{0, 1, 2, 3\}$ (so $\Omega = \Omega_4$), $N = \{\mathbf{0}\}$, $f : \mathcal{S}^N \to \mathcal{S}$ such that $f((a_0)) = 1$, $f((a_1)) = 0$, and $f((a_2)) = 2 = f((a_3))$ (where $(a_i)_{\mathbf{0}} = i$ for $i = 1, 2, 3, 4$ and $(a_i) \in \mathcal{S}^N$) and $\Sigma = \{x \in \Omega : x_{\mathbf{m}} = 0 \text{ or } 1 \text{ for all } \mathbf{m} \in \mathbf{Z}^2\}$.

So $\mathcal{T} = \{0,1\}$ and $(f^\Omega(z))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}(z)))$ which equals either $f((a_0)) = 1$ or $f((a_1)) = 0$ for all $z \in \Sigma$ for all $\mathbf{m} \in \mathbf{Z}^2$, so that $f^\Omega(\Sigma) \subset \Sigma$. So, by the theorem, $f(\mathcal{T}^N) \subset \mathcal{T}$ (which is clear here anyway) and, clearly, $g = f|_{\mathcal{T}^N} : \mathcal{T}^N \to \mathcal{T}$ is a bijection so, by the theorem, f^Σ is a homeomorphism, so (5) in the theorem holds. But $f(\mathcal{S}^N) = \{f((a_i)) : i \in \mathcal{S}\} = \{0,1,2\} \neq \mathcal{S}$. That is, $f : \mathcal{S}^N \to \mathcal{S}$ is not bijective, so statement (1) in the theorem with $g : \mathcal{T}^N \to \mathcal{T}$ replaced by $f : \mathcal{S}^N \to \mathcal{S}$ does not hold.

If $|N| = 1$ and f^Ω is not onto then, with $\Sigma = \Omega$ in Theorem 4.5, we have that $f : \mathcal{S}^N \to \mathcal{S}$ is not onto and the two dimensional analogue of Hedlund's Remark 4.2 is that $f^\Omega(\Omega) = (f(\mathcal{S}^N))^{\mathbf{Z}^2} = \Omega_{|f(\mathcal{S}^N)|}$. So in Example 4.1 $f(\mathcal{S}^N) = \{0,1,2\}$ so that $f^\Omega(\Omega) = f^{\Omega_4}(\Omega_4) = \{0,1,2\}^{\mathbf{Z}^2} = \Omega_3$, whereas $\Sigma = \Omega_2$.

The two dimensional analogue of Hedlund's Remark 4.3 for the full-shift states that if $|N| = 1$ and f^Ω is not onto then there exists $x \in \Omega$ such that $\sigma^{\mathbf{m}}(x) = x$ for all $\mathbf{m} \in \mathbf{Z}^2$ and $(f^\Omega)^{-1}(x)$ is uncountable. However, for subshifts, the following example shows that $\{|f^\Sigma)^{-1}(z)| : z \in \Sigma\}$ can be bounded when f^Σ is not onto.

Example 4.2 Let $\mathcal{S} = \mathcal{S}_3$, $N = \{\mathbf{0}\}$, $f((a_0)) = 0$, and $f((a_1)) = 1 = f((a_2))$ (where $(a_i) \in \mathcal{S}^N$ are as in Example 4.1 for $i = 0,1,2$), and

$$\Sigma = \{x \in \Omega_3 : |\{\mathbf{m} \in \mathbf{Z}^2 : x_{\mathbf{m}} = 1 \text{ or } 2\}| \leq 1\}$$

(the complement is a countable union of open sets). Then $\pi_{\mathbf{0}}(\Sigma) = \mathcal{S}$, so $g = f$. Also,

$$f^\Omega(\Sigma) = \{x \in \Omega_3 : x_{\mathbf{m}} \neq 2 \text{ for all } \mathbf{m} \in \mathbf{Z}^2 \text{ and } |\{\mathbf{m} \in \mathbf{Z}^2 : x_{\mathbf{m}} = 1\}| \leq 1\} \subset \Sigma. \quad (5)$$

But $g = f$ is not onto so, by Theorem 4.5, f^Σ is not onto (this is also clear from (5)). Yet, for all $z \in \Sigma$, if $f^\Sigma(y) = z$ for $y \in \Sigma$ then $f(\pi_N((\sigma(y))) = (f^\Sigma(y))_{\mathbf{m}} = z_{\mathbf{m}} = 0$ for all but at most one $\mathbf{m}$, $\mathbf{m}_0$ say (when one exists), in $\mathbf{Z}^2$ at which $z_{\mathbf{m}_0} = 1$ (because if $z_{\mathbf{m}_0} = 2$ then $(f^\Sigma)^{-1}(z) = \emptyset$). So $\pi_N(\sigma^{\mathbf{m}_0}(y)) = 1$ or 2. That is, $y_{\mathbf{m}_0} = (\sigma^{\mathbf{m}_0}(y))_{\mathbf{0}} = 1$ or 2. For all other $\mathbf{m} \in \mathbf{Z}^2$ we have $y_{\mathbf{m}} = 0$. Thus

$$|(f^\Sigma)^{-1}(z)| = \begin{cases} 1 & \text{if } z_{\mathbf{m}} = 0 \text{ for all } \mathbf{m} \in \mathbf{Z}^2 \\ 0 & \text{if } z_{\mathbf{m}} = 2 \text{ for some } \mathbf{m} \in \mathbf{Z}^2 \\ 2 & \text{if } z_{\mathbf{m}} = 1 \text{ for some } \mathbf{m} \in \mathbf{Z}^2 \end{cases}$$

and, in particular, $\{|(f^{\Sigma}(z)| : z \in \Sigma\}$ is bounded.

Recall from Theorem 4.5 that $f(\mathcal{T}^N) \subset \mathcal{T}$ when $|N| = 1$.

Example 4.3 Now if $\mathcal{S} = \mathcal{S}_3 = \{0, 1, 2\}$ (so $\Omega = \Omega_3$), $N = \{(0,0),(1,0)\}$ (let the notation $(b) = (b_1, b_2) \in \mathcal{T}^N$ mean that $(b)_{(0,0)} = b_1$ and $(b)_{(1,0)} = b_2$), $\Sigma = \{z \in \Omega_3 : (x_{\mathbf{m}}, x_{\mathbf{m}+(1,0)}) = (0,0), (0,1)$, or $(1,0)$ for all $\mathbf{m} \in \mathbf{Z}^2\}$ (the complement is a countable union of open sets), and $f : \mathcal{S}^N \to \mathcal{S}$ is such that $f((0,0)) = 0$, $f((0,1)) = 1$, $f^{\Sigma}((1,0)) = 0$, and $f^{\Sigma}((1,1)) = 2$ then clearly $f^{\Omega}(\Sigma) \subset \Sigma$ and $\mathcal{T} = \pi_{\{\mathbf{0}\}}(\Sigma) = \{0,1\}$. But $(1,1) \in \mathcal{T}^N$ and yet $f((1,1)) = 2 \notin \mathcal{T}$. So, for $|N| > 1$, it is not generally true that $f(\mathcal{T}^N) \subset \mathcal{T}$.

However, though $(1,1) \in \mathcal{T}^N$, in this example $(1,1) \notin \pi_N(\Sigma)$. Here is our motivation for our next theorem (Theorem 4.6).

Lemma 4.1 *(1) If $M_1 \subset M_2$, $((a)) \in \mathcal{S}^{M_2+N}$, and $\mathbf{m} \in M_1$ then*

$$\pi_N(\sigma^{\mathbf{m}}(\pi_{M_1+N}((a)))) = \pi_N(\sigma^{\mathbf{m}}((a))).$$

(2) For all $y \in \Omega$ and for all $\mathbf{m} \in M$,

$$\pi_N(\sigma^{\mathbf{m}}(\pi_{M+N}(y))) = \pi_N(\sigma^{\mathbf{m}}(y)).$$

(3) For all $(a) \in \mathcal{S}^{M+N}$ and for all $\mathbf{m} \in M$,

$$\pi_N(\sigma^{\mathbf{m}}(\pi_{\mathbf{m}+N}((a)))) = \pi_N(\sigma^{\mathbf{m}}((a))).$$

(4) For all $y \in \Omega$ and for all $\mathbf{m} \in \mathbf{Z}^2$,

$$\pi_N(\sigma^{\mathbf{m}}(\pi_{\mathbf{m}+N}(y))) = \pi_N(\sigma^{\mathbf{m}}(y)).$$

Proof. (1) For all $\mathbf{n} \in N$, $(\sigma^{\mathbf{m}}(\pi_{M_1+N}((a))))_{\mathbf{n}} = (\pi_{M_1+N}((a)))_{\mathbf{m}+\mathbf{n}} = (a)_{\mathbf{m}+\mathbf{n}} = (\sigma^{\mathbf{m}}((a)))_{\mathbf{n}}$.

(2) Put $M_1 = M$ and $M_2 = \mathbf{Z}^2$ in (1).

(3) Put $M_1 = \{\mathbf{m}\}$ and $M_2 = M$ in (1).

(4) Put $M = \mathbf{Z}^2$ in (3). $\square$

Recall from Proposition 4.1 that $f^M_{\Sigma}(\pi_{M+N}(\Sigma)) \subset \pi_M(\Sigma)$.

Theorem 4.6 *An f^Σ map is onto if and only if f^M_Σ is onto for all finite sets $M \subset \mathbf{Z}^2$.*

Proof. Suppose f^Σ is onto and M is a finite subset of $\mathbf{Z}^2$. Take $(b) \in \pi_M(\Sigma)$ and let $z \in \Sigma \cap (\pi_M)^{-1}((b))$. Then there exists $y \in \Sigma$ such that $f^\Sigma(y) = z$. Let $(a) = \pi_{M+N}(y)$. Then, for all $\mathbf{m} \in M$,

$$f^M((a))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}((a)))) = f(\pi_N(\sigma^{\mathbf{m}}(\pi_{M+N}(y))))$$

$$= f(\pi_N(\sigma^{\mathbf{m}}(y))) = (f^\Sigma(y))_{\mathbf{m}} = z_{\mathbf{m}} = (b)_{\mathbf{m}}.$$

So $f^M((a)) = (b)$ and f^M_Σ is onto.

Now suppose f^M_Σ is onto for all finite $M \in \mathbf{Z}^2$. Let $z \in \Sigma$ and take a sequence $\{M_k\}_{k\in\mathbf{N}}$ of finites sets $M_k \subset \mathbf{Z}^2$ such that $M_k \subset M_{k+1}$ for all $k \in \mathbf{N}$ and $\cup_{k\in\mathbf{N}} M_k = \mathbf{Z}^2$. Now, for all $k \in \mathbf{N}$, $(b_k) = \pi_{M_k}(z) \in \pi_{M_k}(\Sigma)$ so that there exists $(a_k) \in \pi_{M_k+N}(\Sigma)$ such that $f^{M_k}((a_k)) = (b_k)$. Select a corresponding $y_k \in \Sigma \cap (\pi_{M_k+N})^{-1}((a_k))$. Now, for all $k \in \mathbf{N}$ and for all $\mathbf{m} \in M_k$,

$$(f^\Sigma(y_k))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}(y_k))) = f(\pi_N(\sigma^{\mathbf{m}}(\pi_{M_k+N}(y_k))))$$

$$= f(\pi_N(\sigma^{\mathbf{m}}((a_k)))) = (f^{M_k}((a_k)))_{\mathbf{m}} = (b_k)_{\mathbf{m}} = z_{\mathbf{m}}.$$

So clearly $\lim_{k\to\infty} f^\Sigma(y_k) = z$. Take a convergent subsequence $\{y_{n_k}\}_{k\in\mathbf{N}}$ with limit $y \in \Sigma$ say. Then $f^\Sigma(y) = f^\Sigma(\lim_{k\to\infty} y_{n_k}) = \lim_{k\to\infty} f^\Sigma(y_{n_k}) = \lim_{k\to\infty} f^\Sigma(y_k) = z$ and f^Σ is onto. □

4.2 Permutative maps

We now generalise Hedlund's notion of permutative maps.

The points of N form a hull in $\mathbf{R}^2$, where we here allow a hull to be a line or a single point. We shall refer to the corner points of the hull formed by the points of N as the *corners of* N.

Definition 4.2 We say that a point $\mathbf{n} \in N$ (recall that $f : \mathcal{S}^N \to \mathcal{S}$) is a *corner point of* f if there is a line $\ell \subset \mathbf{R}^2$ through $\mathbf{n}$ such that $N \backslash \{\mathbf{n}\}$ lies completely in one of the two open half-planes into which ℓ divides $\mathbf{R}^2$.

Suppose that $\mathbf{n} \in \mathbf{Z}^2$ is given, then for all $s \in \mathcal{S}$ let $(s) \in \mathcal{S}^{\{\mathbf{n}\}}$ be such that $(s)_{\mathbf{n}} = s$ (it will be clear when, in the case of $N = \{\mathbf{n}\} \subset \mathbf{Z}^2$ being a singleton set, this abuse of notation is being used). For all $\mathbf{n} \in N$, we say that $f : \mathcal{S}^N \to \mathcal{S}$ is $\mathbf{n}$*-permutative* if, for all $(a) \in \mathcal{S}^{N \backslash \{\mathbf{n}\}}$, $f_{(a)} : \mathcal{S}^{\{\mathbf{n}\}} \to \mathcal{S}$ is a bijection, where $f_{(a)}((s)) = f((a_s))$, where $(a_s) \in \mathcal{S}^N$ is such that $(a_s)_{\mathbf{n}} = s$ and $\pi_{N \backslash \{\mathbf{n}\}}((a_s)) = (a)$. If $\mathbf{n}$ is a corner point of N we say that f is *corner* ($\mathbf{n}$-)*permutative*. We say that the corresponding (sub) cellular automaton (f^Σ) f^Ω is a *(corner)* ($\mathbf{n}$-)*permutative (sub) cellular automaton.*

This says that, for $f : \mathcal{S}^N \to \mathcal{S} = \{0, \cdots, k-1\}$ and $\mathbf{n} \in N$, then f is $\mathbf{n}$-permutative if and only if whenever $(b) \in \mathcal{S}^{N \backslash \{\mathbf{n}\}}$ and $S = \{(c_i) \in \mathcal{S}^N : 1 \leq i \leq k\}$ is the unique set of k distinct elements of $\mathcal{S}^N$ such that $\pi_{N \backslash \{\mathbf{n}\}}(S) = \{(b)\}$ then $|\{f((c_i)) : 1 \leq i \leq k\}| = k$.

Hedlund has the result that if, for the obvious one- dimensional full-shift analogue of permutative, $f : \mathcal{S}^{N'} \to \mathcal{S}$ is permutative at one of the two (or one if $|N'| = 1$) extreme values in N' then f_∞ is onto. We have the following two-dimensional version for the full-shift, the proof of which is rather more involved.

Theorem 4.7 *A corner permutative cellular automaton f^Ω of Ω is onto.*

Proof. If $|N| = 1$ then f^Ω is onto by Theorem 4.5. If $|N| > 1$ then, by Theorem 4.6, it is enough to show that $f^M : \mathcal{S}^{M+N} \to \mathcal{S}^M$ is onto for all finite sets $M \subset \mathbf{Z}^2$. Fix an arbitrarily chosen $M \subset \mathbf{Z}^2$. Let a (the) permutative corner point of f be $\mathbf{n} \in N$. Clearly there exists a line of irrational gradient $\ell \in \mathbf{R}^2$ through $\mathbf{0} = (0,0)$ such that one of the two closed half-planes into which $\ell + \mathbf{n}$ 'divides' $\mathbf{R}^2$ (that is, the two closed half-planes whose intersection is $\ell + \mathbf{n}$) contains all of N. Let this half plane be $\bar{H}$, let H be the open set $\bar{H} \backslash (\ell + \mathbf{n})$, and put $N_0 = N \backslash \{\mathbf{n}\} = N \cap H$ (since ℓ has irrational gradient). Number the points of M as $\mathbf{m}_1, \cdots, \mathbf{k}_{|M|}$ such that $\mathbf{m}_i + \mathbf{n} \in H + \mathbf{m}_j$ if and only if $1 \leq i < j \leq |M|$ (this can be done since ℓ has irrational gradient). Given $(b) \in \mathcal{S}^M$, we shall construct an element of $(f^M)^{-1}((b))$. First note that for $(a) \in \mathcal{S}^{M+N}$, for all $\mathbf{m} \in M$, $(f^M((a)))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}((a)))) = f(\pi_N(\sigma^{\mathbf{m}}(\pi_{\mathbf{m}+N}((a)))))$ (by Lemma 4.1), so that $\pi_{\mathbf{m}+N}((a))$ determines $(f^M((a)))_{\mathbf{m}}$. So if $\pi_{\mathbf{m}+N_0}((a))$ is determined then, by permutativity, there exists $s \in \mathcal{S}$ such that $(f((a)))_{\mathbf{m}} = (b)_{\mathbf{m}}$ if and only if $(a)_{\mathbf{m}+\mathbf{n}} = s$. Thus, by the construction of H, we are free to choose $(a)_{\mathbf{m}} \in \mathcal{S}$ for all $\mathbf{m} \in (\mathbf{m}_1 + H) \cap (M + N)$ so that $\pi_{\mathbf{m}_1+N_0}((a)) \subset \mathcal{S}^{\mathbf{m}_1+N_0}$ is determined. Hence, a unique $(a)_{\mathbf{m}_1+\mathbf{n}} \in \mathcal{S}$ such that $(f^M((c)))_{\mathbf{m}_1} = (b)_{\mathbf{m}_1}$, for all $(c) \in \mathcal{S}^{M+N}$ such that $\pi_{\mathbf{m}_1+N}((c)) = \pi_{\mathbf{m}_1+N}((a))$, is determined. Hence, $\pi_{(\mathbf{m}_1+\bar{H})\cap(M+N)}((a)))$ is determined. We proceed thus. Having determined $\pi_{(\mathbf{m}_i+\bar{H})\cap(M+N)}((a))$ for some $i \in \{1, \cdots, |M|-1\}$ we freely choose $(a)_{\mathbf{m}}$ for all $\mathbf{m} \in ((\mathbf{m}_{i+1}+H)\backslash(\mathbf{m}_i+\bar{H}))\cap(M+N)$ so that $\pi_{(\mathbf{m}_{i+1}+H)\cap(M+N)}((a))$ and, in particular, $\pi_{\mathbf{m}_{i+1}+N_0}((a))$ is determined and hence, by permutativity, unique $(a)_{\mathbf{m}_{i+1}+\mathbf{n}} \in \mathcal{S}$ such that $(f^M((c)))_{\mathbf{m}_{i+1}} = ((b))_{\mathbf{m}_{i+1}}$ for all $(c) \in \mathcal{S}^{M+N}$ such that $\pi_{\mathbf{m}_{i+1}+N}((c)) = \pi_{\mathbf{m}_{i+1}+N}((a))$ is determined.

Hence $\pi_{(\mathbf{m}_{i+1}+\bar{H})\cap(M+N)}((a)))$ is determined. Eventually $\pi_{(\mathbf{m}_{|M|}+\bar{H})\cap(M+N)}((a))) = \pi_{M+N}((a)) = (a)$ is determined and, by construction, $(f^M((a)))_{\mathbf{m}_i} = (b)_{\mathbf{m}_i}$ for $1 \leq i \leq |M|$ and hence $f^M((a)) = (b)$.

By arbitrary selection of $(b) \in \mathcal{S}^M$ and of the finite set $M \subset \mathbf{Z}^2$, f^Ω is onto by Theorem 4.6. □

The next two examples show that Theorem 4.6 cannot, in general, be extended to subshifts.

Example 4.4 Let $\mathcal{S} = \mathcal{S}_2$, so $\Omega = \Omega_2$, and $N = \{(0,1),(0,0),(1,0)\}$. Let $f : \mathcal{S}^N \to \mathcal{S}$ be such that $f((a)) = (a)_{(0,1)} + (a)_{(0,0)} + (a)_{(1,0)} \pmod 2$ for all $(a) \in \mathcal{S}^N$ and put $\Sigma = \{x \in \Omega : x_{\mathbf{m}+(0,1)} + x_{\mathbf{m}+(0,0)} + x_{\mathbf{m}+(1,0)} = 0 \pmod 2 \text{ for all } \mathbf{m} \in \mathbf{Z}^2\}$. Note that, for any fixed i, j in $\mathbf{Z}$, we can construct a point $z \in \Sigma$ by freely choosing either $z_{\mathbf{m}} = 0$ or $z_{\mathbf{m}} = 1$ for all $\mathbf{m} \in S_{ij} = \{(m,n) \in \mathbf{Z}^2 : n = j \text{ or } m = i, n \leq j\}$. The value of $z_{\mathbf{m}}$ for all $\mathbf{m} \in \mathbf{Z}^2 \backslash S_{ij}$ is then, clearly, uniquely determined. Since $|S_{ij}| = \infty$ we have that $|\Sigma| = 2^\infty$ is uncountable but, for all $z \in \Sigma$ and for all $\mathbf{m} \in \mathbf{Z}^2$, we have that $(f^\Sigma(z))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}(z))) = (\sigma^{\mathbf{m}}(z))_{(0,1)} + (\sigma^{\mathbf{m}}(z))_{(0,0)} + (\sigma^{\mathbf{m}}(z))_{(1,0)} = z_{\mathbf{m}+(0,1)} + z_{\mathbf{m}+(0,0)} + z_{\mathbf{m}+(1,0)} \pmod 2 = 0$, by the definition of Σ. But if $a \in \{0,1\}$ then $a + 0 \neq a + 1 \pmod 2$ and each point in N is a corner point of the hull of N so, certainly, f^Σ is corner $\mathbf{n}$-permutative for all $\mathbf{n} \in N$. But f^Σ maps an uncountable set to the single point $z_0 \in \Sigma$, where $(z_0)_{\mathbf{m}} = 0$ for all $\mathbf{m} \in \mathbf{Z}^2$.

The second example of a corner permutative subcellular automaton which is not onto is less trivial.

Example 4.5 Let $\mathcal{S} = \mathcal{S}_4$, so $\Omega = \Omega_4$, and $N = \{(0,1),(0,0),(1,0)\}$. Let $f : \mathcal{S}^N \to \mathcal{S}$ be such that $f((a)) = (a)_{(0,1)} + (a)_{(0,0)} + (a)_{(1,0)} \pmod 4$ for all $(a) \in \mathcal{S}^N$ and put $\Sigma = \{x \in \Omega : x_{\mathbf{m}+(0,1)} + x_{\mathbf{m}+(0,0)} + x_{\mathbf{m}+(1,0)} = 0 \text{ or } 2 \pmod 4 \text{ for all } \mathbf{m} \in \mathbf{Z}^2\}$. Note that, for any fixed i,j in $\mathbf{Z}$, we can construct a point $z \in \Sigma$ by freely choosing $z_{\mathbf{m}} \in \{0,1,2,3\}$ for all $\mathbf{m} \in S_{ij} = \{(m,n) \in \mathbf{Z}^2 : n = j \text{ or } m = i, n \leq j\}$. In this case we still have some freedom of choice of $z_{\mathbf{m}}$ for all $\mathbf{m} \in \mathbf{Z}^2 \backslash S_{ij}$, since the definition of Σ is less restrictive than that in Example 4.4. Since $|S_{ij}| = \infty$ we have that $|\Sigma| = 4^{\infty}$ is uncountable. For all $z \in \Sigma$ and for all $\mathbf{m} \in \mathbf{Z}^2$, we have that $(f^{\Sigma}(z))_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}(z))) = (\sigma^{\mathbf{m}}(z))_{(0,1)} + (\sigma^{\mathbf{m}}(z))_{(0,0)} + (\sigma^{\mathbf{m}}(z))_{(1,0)} \pmod 4 = z_{\mathbf{m}+(0,1)} + z_{\mathbf{m}+(0,0)} + z_{\mathbf{m}+(1,0)} \pmod 4 = 0$ or 2, by the definition of Σ (clearly then, $f^{\Sigma}(\Sigma) \subset \Sigma$). But if $a,b,c \in \{0,1,2,3\}$ then $b \neq c$ implies that $a+b \neq a+c \pmod 4$ and each point in N is a corner point of the hull of N so, certainly, f^{Σ} is corner $\mathbf{n}$-permutative for all $\mathbf{n} \in N$. But f^{Σ} maps Σ into $\{z \in \Sigma : z_{\mathbf{m}} = 0 \text{ or } 2 \text{ for all } \mathbf{m} \in \mathbf{Z}^2\}$ so that f^{Σ} is not onto since Σ clearly contains uncountably many points z such that $z_{\mathbf{m}} = 1$ or 3 for some $\mathbf{m} \in \mathbf{Z}^2$.

The next chapter continues our interest in subcellular automata with respect to some measure theoretic considerations.

Chapter 5

Corner permutative subcellular automata and entropy preservation

We retain the notations and standing hypotheses of the previous chapter.

5.1 Background

This section merely recalls the notation, established concepts, and results mentioned in Sections 1.3, 1.4, and 1.5 of the introduction.

For a compact set X and a continuous Z^d-action α of X, $M(X)$ and $M(X, \alpha)$ denote the set of Borel probability measures of X and the set of α-invariant Borel probability measures of X respectively. Topological entropy $h(\alpha)$ (Definition 1.4) and measure theoretic entropy (Definition 1.8) are related by the variational principle that $h(\alpha) = \sup\{h_\mu(\alpha) : \mu \in M(X, \alpha)\}$. For $h \in [0, h(\alpha)]$ we put

$$M^h(X, \alpha) = \{\mu \in M(X, \alpha) : h_\mu(\alpha) = h\}$$

and we reserve $M^*(X, \alpha)$ to denote $M^{h(\alpha)}(X, \alpha)$ (which may be empty). If $h(\alpha) < \infty$ and $|M^*(X, \alpha)| = 1$ we say that (X, α) is intrinsically ergodic.

For $d = 1$ we have that an irreducible subshift of finite type is intrinsically ergodic and that Parry measure (equidistributed Bernoulli measure in the case of the full shift) is the unique maximal measure [49].

Coven and Paul have shown [14] that if $d = 1$ and $T : (X, \alpha) \to (X', \alpha')$ is a continuous surjective map (recall that this means that $T \circ \alpha = \alpha' \circ T$) of intrinsically ergodic systems, with unique maximal measures μ, ν respectively, then $\hat{T} : M(X, \alpha) \to M(X', \alpha')$ defined by $(\hat{T}(\lambda))(B) = \lambda(T^{-1}(B))$ for all $\lambda \in M(X, \alpha)$ and for all $B \in \mathcal{B}(X')$ (the Borel σ-algebra of X') is surjective and $\hat{T}(\mu) = \nu$.

For $d = 1$ a matrix subshift of finite type (Σ, σ) is irreducible if and only if (Σ, σ) is transitive (Definition 1.11) and the set $\{z \in \Sigma : |\mathcal{O}_\sigma(z)| < \infty\}$ is dense in Σ where $\mathcal{O}_\sigma(z)$ is the σ-orbit of $z \in \Sigma$. This well-known fact is mentioned in, for example, Markley and Paul [37, Section 5]. Note that transitive and dense are topological properties. Since every subshift of finite type is topologically conjugate to a matrix subshift of finite type we conclude that, for $d = 1$, a subshift (Σ, σ) of finite type is intrinsically ergodic if it is transitive and has a dense set of points whose σ-orbit is finite.

For $d = 2$ however Burton and Steif exhibit [8] an example, called the iceberg model, which is transitive, has a dense set of points whose σ-orbit is finite, and yet is not intrinsically ergodic. Furthermore, the iceberg model has exactly two maximal measures, and there is a surjective subcellular automaton map of (Σ, σ) which permutes these two maximal measures.

The goal of this chapter is to extend Coven and Paul's result to general subshifts (not necessarily of finite type and not necessarily intrinsically ergodic), for the class of two dimensional corner permutative subcellular automata. That is, for subcellular automata T of (Σ, σ), we aim to show that $\hat{T}(M^*(\Sigma, \sigma)) \subset M^*(\Sigma, \sigma)$, with equality when T is onto. In fact, we'll show that $\hat{T}(M^h(\Sigma, \sigma)) \subset M^h(\Sigma, \sigma)$, with equality when T is onto, for all $h \in [0, h(\alpha)]$. The result has also been proved, by Newton and Parry [44], (for Lebesgue spaces in general) for $d = 1$, T onto, and T countable to one almost everywhere. Our proof of the entropy preservation of T (that is, that $\hat{T}(M^h(\Sigma, \sigma)) \subset M^h(\Sigma, \sigma))$ is for $d = 2$, doesn't require that T is onto, and nor that T is countable to one anywhere. Our stronger result (that is, that $\hat{T}(M^h(\Sigma, \sigma)) =$

$M^h(\Sigma,\sigma)$), again for $d = 2$, does require that T is onto, but again doesn't require that T is countable to one anywhere.

5.2 Preliminaries.

(i) If T is a map of (X,α) (α a $\mathbf{Z}^d$-action) then, for all $\mathbf{n} \in \mathbf{Z}^d$, $T^{-1} \circ \alpha^{\mathbf{n}} = \alpha^{\mathbf{n}} \circ T^{-1}$ on subsets of X (proof trivial).

(ii) For a family $\{\mathcal{P}_i : i \in I\}$, for some indexing set I, of finite partitions of X, $T^{-1}(\bigvee_{i\in I} \mathcal{P}_i) = \bigvee_{i\in I} T^{-1}(\mathcal{P}_i)$ (follows immediately from $T^{-1}(\cap_{i\in I} A_i) = \cap_{i\in I} T^{-1}(A_i)$ for $A_i \subset X$ for $i \in I$).

5.3 A maximal measure of a compact space is continuous

Recall that a continuous measure is one which has value zero on points.

Theorem 5.1 *If X is a compact metric space and α is a continuous $\mathbf{Z}^d$-action of X such that $0 < h(\alpha) < \infty$ then $\mu \in M^*(X,\alpha)$ implies that μ is continuous.*

Proof. Suppose $0 < h(\alpha) < \infty$, $\mu \in M^*(X,\alpha)$, and that there exists $x \in X$ such that $\mu(x) = \delta > 0$. Since μ is α-invariant and $\mu(X) = 1 < \infty$ we must have $|\mathcal{O}(x)| = |\mathcal{O}_\alpha(x)| = n \in \mathbf{N}$. Define $\nu \in M(X,\alpha)$ by $\nu(D) = \mu(D\backslash\mathcal{O}(x))/\mu(X\backslash\mathcal{O}(x))$ for all $D \in \mathcal{B}(X)$.

Given a finite Borel partition $\mathcal{P}$ of X put $\mathcal{P}_m = \bigvee_{\mathbf{m}\in B(m)} \alpha^{\mathbf{m}}(\mathcal{P})$ for all $m \in \mathbf{N}$, where $B(m)$ is the d-dimensional ball of radius m and centre $\mathbf{0} = (0,\cdots,0) \in \mathbf{Z}^d$.

Note that, for any $y \in X$, there exists a sequence $\{E_n(y)\}_{n\in\mathbf{N}} \subset \mathcal{B}(X)$ such that $y \in E_n(y) \in \mathcal{P}_n$ for all $n \in \mathbf{N}$. So $\mu(E_n(y)) > \mu(y) = \delta$ for all $n \in N$ and for all $y \in \mathcal{O}(x)$. If, for $E \in \mathcal{B}(X)$, $E \cap \mathcal{O}(x) = \emptyset$ then $\nu(E) = \mu(E)/\mu(X\backslash\mathcal{O}(x)) = K\mu(E)$, where $\infty > K = 1/\mu(X\backslash\mathcal{O}(x)) > 1$ (for if $\mu(\mathcal{O}(x)) = 1$ we'd have that $h(\alpha) = 0$).

For all $n \in \mathbf{N}$ let $\mathcal{Q}_n = \{E_n(y) : y \in \mathcal{O}(x)\}$, then

$$H_\nu(\mathcal{P}_n) = -\sum_{E\in\mathcal{Q}_n} \nu(E)\log\nu(E) - \sum_{E\in\mathcal{P}_n\backslash\mathcal{Q}_n} \nu(E)\log\nu(E)$$

$$= -\sum_{E\in\mathcal{Q}_n} \nu(E)\log\nu(E) - \sum_{E\in\mathcal{P}_n\setminus\mathcal{Q}_n} K\mu(E)(\log K + \log\mu(E))$$

$$= KH_\mu(\mathcal{P}_n) + \sum_{E\in\mathcal{Q}_n} (K\mu(E)\log\mu(E) - \nu(E)\log\nu(E)) - \sum_{E\in\mathcal{P}_n\setminus\mathcal{Q}_n} K\mu(E)\log K$$

giving $h_\nu(\alpha,\mathcal{P}) = Kh_\mu(\alpha,\mathcal{P})$ since the finite sum is obviously bounded for all $n \in \mathbf{N}$ and $-\sum_{E\in\mathcal{P}_n\setminus\mathcal{Q}_n} K\mu(E)\log K \leq \mu(X\setminus\mathcal{O}(x))K\log K$ is also bounded. But $\mathcal{P}$ was arbitrary, so $h_\nu(\alpha) = Kh_\mu(\alpha) > h_\mu(\alpha)$, contradicting the maximality of μ. □

5.4 Entropy reduction without surjectivity

The following Theorem is a straightforward generalisation to $d = 2$ of a result for $d = 1$ in Coven and Paul's paper [14], but we eliminate the unnecessary condition that T is onto.

Theorem 5.2 *Let α,γ be continuous $\mathbf{Z}^2$-actions of compact metric spaces X, Y respectively. If $T : (X,\alpha) \to (Y,\gamma)$ is continuous then $\hat{T} : M(X,\alpha) \to M(Y,\gamma)$ is entropy reducing (that is, $h_{\hat{T}(\mu)}(\gamma) \leq h_\mu(\alpha)$ for all $\mu \in M(X,\alpha)$).*

Proof. If $\mathcal{P}$ is a finite Borel partition of Y then $T^{-1}(\mathcal{P})$ is a finite Borel partition of X and $H_\mu(T^{-1}(\mathcal{P})) = H_{\hat{T}(\mu)}(\mathcal{P})$ (by definition of $\hat{T}$). Furthermore $T^{-1}(\bigvee_{\mathbf{m}\in Q_n}\alpha^{\mathbf{m}}(\mathcal{P}) = \bigvee_{\mathbf{m}\in Q_n}\gamma^{\mathbf{m}}(T^{-1}(\mathcal{P}))$, by preliminaries (i) and (ii). The result follows. □

Remark 5.1 Surjectivity of T is not necessary. By definition of $\hat{T}$, $T : (X,\mathcal{B}(X),\mu) \to (Y,\mathcal{B}(Y),\hat{T}(\mu))$ is onto (mod 0) anyway, since $(\hat{T}(\mu))(T(X)) = \mu(T^{-1}(T(X))) = \mu(X) = 1$.

5.5 A result on allowable partition grouping

The next theorem we prove allows certain numbers of atoms of each of a sequence of partitions to be grouped together to form single atoms without affecting entropy values.

Lemma 5.1 *If $l \in \mathbf{N}$, $\alpha_j, x_j \in \mathbf{R}^+$ for $j \in \{1,\cdots,l\}$, and $\sum_{j=1}^l \alpha_j = 1$ then $\sum_{j=1}^l \alpha_j x_j \log x_j \geq (\sum_{j=1}^l \alpha_j x_j)\log(\sum_{j=1}^l \alpha_j x_j)$.*

Proof. See Walters [64, Theorem 4.2].

Theorem 5.3 *Let $a, d, k, l \in \mathbf{N}$ be fixed. If $\{\mathcal{P}_n\}_{n\in\mathbf{N}}$ is a sequence of measurable partitions of probability space $(X, \mathcal{B}, \mu)$ then the value, if it exists (allowed to be infinite), of $\lim_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{P}_n)$ is equal to $\lim_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{Q}_n)$ where, for all $n \in \mathbf{N}$, $\mathcal{Q}_n$ is a measurable partition of $(X, \mathcal{B}, \mu)$ and each atom of $\mathcal{Q}_n$ is a union of, up to, $lk^{n^{d-1}}$ atoms of $\mathcal{P}_n$.*

Proof. Assume $\lim_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{P}_n)$ exists and that $\mathcal{Q}_n$ is as described for each $n \in \mathbf{N}$. Clearly $\mathcal{P}_n \geq \mathcal{Q}_n$ for all $n \in \mathbf{N}$, so that

$$\lim_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{P}_n) \geq \limsup_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{Q}_n) \in [0, \infty].$$

Also, for all $n \in \mathbf{N}$, $\mathcal{P}_n = \mathbf{E}_1 \cup \cdots \cup \mathbf{E}_m$ and $\mathcal{Q}_n = \{F_1, \cdots, F_m\}$ for some $m = m(n) \in \mathbf{N}$ where, for all $i \in \{1, \cdots, m\}$, there exists $k_i \in \{1, \cdots, lk^{n^{d-1}}\}$ such that, for all $j \in \{1, \ldots, k_i\}$, there exists $E_{ij} = E_{ij}(n) \in \mathcal{B}$ such that $\mathbf{E}_i = \{E_{i1}, \cdots, E_{ik_i}\}$ and $F_i = \cup_{j=1}^{k_i} E_{ij}$. For all $i \in \{1, \cdots, m\}$, put $m_{ij} = \mu(E_{ij})$ for all $j \in \{1, \cdots, k_i\}$.

Now, for all $i \in \{1, \cdots, m\}$, we apply Lemma 5.1, with $l = k_i$, $\alpha_i = 1/l = 1/k_i$, and $x_j = lm_{ij} = k_i m_{ij}$ for all $j \in \{1, \cdots, k_i\}$, to get

$$H_i = (\sum_{j=1}^{k_i} m_{ij}) log(\sum_{j=1}^{k_i} m_{ij}) \leq \sum_{j=1}^{k_i} m_{ij} \log(k_i m_{ij})$$

for all $i \in \{1, \cdots, m\}$, so that

$$H_\mu(\mathcal{Q}_n) = -\sum_{i=1}^{m} H_i \geq -\sum_{i=1}^{m}\sum_{j=1}^{k_i} m_{ij}(\log m_{ij} + \log k_i) \geq H_\mu(\mathcal{P}_n) - \log(lk^{n^{d-1}}),$$

since $-\log k_i \geq -\log(lk^{n^{d-1}})$ for all $i \in \{1, \cdots, m\}$ and since $\sum_{i=1}^m \sum_{j=1}^{k_i} m_{ij} = 1$. So

$$\liminf_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{Q}_n) \geq \lim_{n\to\infty} \frac{1}{an^d}(H_\mu(\mathcal{P}_n) - \log(lk^{n^{d-1}})) = \lim_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{P}_n). \text{ Hence}$$

$$\lim_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{P}_n) \geq \limsup_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{Q}_n) \geq \liminf_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{Q}_n) \geq \lim_{n\to\infty} \frac{1}{an^d} H_\mu(\mathcal{P}_n).$$

□

5.6 Entropy preservation by corner permutative subcellular automata

We need two further theorems before proving proving that corner permutative subcellular automata are entropy preserving, the first is the $\mathbf{Z}^2$ analogue of the Kolmogorov-Sinai Theorem. This is well-known (see Conze [13, p. 18] or Katznelson and Weiss' paper [26, p. 170]).

Theorem 5.4 *If the finite measurable partition ξ of a probability space $(X, \mathcal{B}, \mu)$ has $\bigvee_{\mathbf{n}\in\mathbf{Z}^2} \alpha^{\mathbf{n}}(\mathcal{A}) = \mathcal{B}$ for a $\mathbf{Z}^2$-action α of X by measure preserving transformations, where $\mathcal{A} = \mathcal{A}(\xi)$ is the sub-algebra of $\mathcal{B}$ generated by ξ, then $h_\mu(\alpha) = h_\mu(\alpha, \xi)$.*

Given $M \subset \mathbf{Z}^2$ let $\mathcal{P}_M$ be the partition of Σ given by $\mathcal{P}_M = \{E_{(b)} : (b) \in \pi_M(\Sigma)\}$, where $E_{(b)} = \{z \in \Sigma : \pi_M(z) = (b)\}$ for all $(b) \in \pi_M(\Sigma)$.

Proposition 5.1 *With the convention just given, $\mathcal{P}_{M+N} \geq (f^\Sigma)^{-1}(\mathcal{P}_M)$.*

Proof. If $E \in \mathcal{P}_{M+N}$ then there exists $(a) \in \pi_{M+N}(\Sigma)$ such that, for all $y \in E$, $\pi_{M+N}(y) = (a)$. So, for all $y \in E$ and for all $\mathbf{m} \in M$, $(f^\Sigma(y))_{\mathbf{m}} = (f^M(\pi_{M+N}(y)))_{\mathbf{m}} = (f^M((a)))_{\mathbf{m}}$, by Proposition 4.1 part (2). So, for all $y \in E$, $\pi_M(f^\Sigma(y)) = f^M((a))$, so that $f^\Sigma(y) \in F = F_{f^M((a))} = \{z \in \Sigma : \pi_M(z) = f^M((a))\} \in \mathcal{P}_M$. So $y \in (f^\Sigma)^{-1}(F)$ and, hence, $E \subset (f^\Sigma)^{-1}(F)$. □

Proposition 5.2 greatly simplifies Theorem 5.5.

Proposition 5.2 *If $N \subset P \subset \mathbf{Z}^2$ and $g : \mathcal{S}^P \to \mathcal{S}$ is such that $g((a)) = f(\pi_N((a)))$ for all $(a) \in \pi_P(\Sigma)$ then $f^\Sigma = g^\Sigma$.*

Proof. For all $x \in \Sigma$ and for all $\mathbf{m} \in \mathbf{Z}^2$,

$$(g^\Sigma(x))_{\mathbf{m}} = g(\pi_P(\sigma^{\mathbf{m}}(x))) = f(\pi_N(\pi_P(\sigma^{\mathbf{m}}(x)))) = f(\pi_N(\sigma^{\mathbf{m}}(x))) = (f^\Sigma(x))_{\mathbf{m}}. \quad \square$$

Theorem 5.5 *If $T = f^\Sigma$ is a corner $\mathbf{n}$-permutative sub-cellular automaton then there exist $k, l \in \mathbf{N}$, $\mathbf{l} \in \mathbf{Z}^2$ and a sequence $\{M_n\}_{n\in\mathbf{N}}$ of finite subsets of $\mathbf{Z}^2$ such that $\cup_{n\in\mathbf{N}}(M_n + n\mathbf{l}) = \mathbf{Z}^2$ and, for all $n \in \mathbf{N}$, $M_n \subset (M_{n+1} + \mathbf{l})$ and each atom of $T^{-1}(\mathcal{P}_{M_n})$ is a union of, at most, lk^n atoms of $\mathcal{P}_{M_{n+1}+\mathbf{n}}$.*

Proof. Using Proposition 5.2 we may assume that N's hull $H(N)$ is a triangle, that $N = \mathbf{Z}^2 \cap H(N)$, that all three corners of $H(N)$ are points of $\mathbf{Z}^2$, and that f is still corner $\mathbf{n}$-permutative (that is,f is still permutative at $\mathbf{n}$ and $\mathbf{n}$ is still a corner).

Consider the sequence $\{M_n\}_{n\in\mathbf{N}}$ defined by $M_1 = N - \mathbf{n}$ and $M_{n+1} = M_n + N - \mathbf{n}$ for all $n \in \mathbf{N}$. Note that the sequence $\{H(M_n)\}_{n\in\mathbf{N}}$ consists of mutually similar triangles with common corner points $\mathbf{0}$ shared by mutually corresponding corners under the similarity. So clearly there exists $\mathbf{l} \in \mathbf{Q}^2$ such that $H(M_n + n\mathbf{l}) \subset H(M_{n+1} + (n+1)\mathbf{l})$ for all $n \in \mathbf{N}$ and, assuming without loss of generality that N is large enough that $\mathbf{l}$ may be taken to be in $\mathbf{Z}^2$, that $\bigcup_{n\in\mathbf{N}}(M_n + n\mathbf{l}) = \mathbf{Z}^2$.

Suppose $y \in T(\Sigma)$, so $y = T(x)$ for some $x \in \Sigma$. For all $\mathbf{m} \in \mathbf{Z}^2$ we require $y_{\mathbf{m}} = f(\pi_N(\sigma^{\mathbf{m}}(x))) = f(\pi_N(\sigma^{\mathbf{m}}(\pi_{\mathbf{m}+N}(x))))$ (using Proposition 4.1, part (4)). That is, $\pi_{\mathbf{m}+N}(x)$ determines $y_{\mathbf{m}}$ so, by $\mathbf{n}$-permutativity, $y_{\mathbf{m}}$ and $\pi_{\mathbf{m}+N_0}(x)$ uniquely determines $x_{\mathbf{m}+\mathbf{n}}$.

Let $n \in \mathbf{N}$ and let ℓ_1 be the bi-laterally infinite extension of the side of $H(M_n)$ which is opposite $\mathbf{n}$. Clearly, there exists a unique ordered set, $\{\ell_i : 2 \le i \le m\}$, of lines parallel to ℓ_1 in $\mathbf{R}^2$ for some $m \in \mathbf{N}$ such that $\cup_{i=1}^m A_i = M_n$, and $1 \le i < j \le m$ implies that $\ell_i \cap \ell_j = \emptyset$ and that ℓ_i is closer to ℓ_1 than ℓ_j is, where, for $1 \le i \le m$, $A_i = \ell_i \cap M_n$ is non-empty.

By the proceeding two paragraphs we see that $\pi_{A_1}(y)$ and $\pi_{A_1+N_0}(x)$ uniquely determine $\pi_{A_1+\mathbf{n}}(x)$ and hence $\pi_{(A_1+N_0)\cup(A_1+\mathbf{n})}$ (note that, since A_1 is in the side of $H(M_n)$ which is opposite $\mathbf{n}$, if $\mathbf{m}_1 \ne \mathbf{m}_2$ are in A_1 then $\mathbf{m}_1 \notin (\mathbf{m}_2 + N_0 - \mathbf{n})$, so that the determination of $x_{\mathbf{m}_2+\mathbf{n}}$ is independant of $x_{\mathbf{m}_1+\mathbf{n}}$). Similarly, for $1 \le i \le m$, $\pi_{A_i}(y)$ and $\pi_{A_i+N_0}(x)$ uniquely determine $\pi_{A_i+\mathbf{n}}(x)$ and hence $\pi_{A_i+N_0}(x) = \pi_{(A_i+N_0)\cup(A_i+\mathbf{n})}(x)$. But, by construction, $A_i + N_0 \subset \cup_{j=1}^{i-1}(A_j + N)$ for $2 \le i \le m$, so that $\pi_{A_i}(y)$ and $\pi_{\cup_{j=1}^{i-1}(A_j+N)}(x)$ uniquely determine $\pi_{A_i+\mathbf{n}}(x)$ and hence uniquely determines $\pi_{A_i+N}(x) = \pi_{(A_i+N_0)\cup(A_i+\mathbf{n})}(x)$. It clearly follows that $\pi_{M_n}(y) = \pi_{\cup_{i=1}^m A_i}(y)$ and $\pi_{A_1+N_0}(x)$ uniquely determine $\pi_{M_{n+1}+\mathbf{n}}(x) = \pi_{M_n+N}(x) = \pi_{(\cup_{i=1}^m A_i)+N}(x)$.

So if $E = E_{(b)} \in \mathcal{P}_{M_n}$ for some $(b) \in \pi_{M_n}(\Sigma)$ and if $x \in T^{-1}(E)$ then $T(x) = y$ for some $y \in \Sigma$ such that $\pi_{M_n}(y) = (b)$, so that $\pi_{M_{n+1}+\mathbf{n}}(x)$ is uniquely determined by $\pi_{A_1+N_0}(x)$. But, by construction, $A_1 + (N_0 - \mathbf{n})$ lies inside of $M_{n+1} \backslash M_n$ which, in turn, lies inside of the union of $n+1$ translates of $H(N)$ and n translates of some half revolution rotation of $H(N)$. So $\pi_{M_{n+1}+\mathbf{n}}(x)$ is uniquely determined by $\pi_{(M_{n+1}\setminus M_n)+\mathbf{n}}(x)$ which gives, at most, $\mathcal{S}^{(2n+1)|N|} = lk^n$ possibilities for $\pi_{M_{n+1}+\mathbf{n}}(x)$, where $l = \mathcal{S}^{|N|}$ and $k = \mathcal{S}^{2|N|}$. So x is in one of, at most, lk^n atoms of $\mathcal{P}_{M_{n+1}+\mathbf{n}} = \mathcal{P}_{M_n+N}$. By Proposition 5.1 the result follows. $\square$

We now come to the main result of the chapter.

Theorem 5.6 *If a map T is a corner $\mathbf{n}$-permutative subcellular automaton of (Σ, σ) then $\hat{T}(M^h(\Sigma,\sigma)) \subset M^h(\Sigma,\sigma)$ for all $h \in [0, h(\sigma)]$. That is, $\hat{T}$ is entropy preserving.*

Proof. By Theorem 5.4, with $\xi = \{E_i : i \in \pi_{\mathbf{0}}(\Sigma)\}$ where $E_i = \{z \in \Sigma : z_{\mathbf{0}} = i\}$ for $i \in \pi_{\mathbf{0}}(\Sigma)$, we need only show that $h_{\hat{T}(\mu)}(\sigma,\xi) = h_\mu(\sigma,\xi)$. Furthermore, by taking $\{M_n\}_{n\in\mathbf{N}}$ and $\mathbf{l}$ as in Theorem 5.5 and noting that $\bigvee_{\mathbf{m}\in M} \sigma^{\mathbf{m}}(\xi) = \mathcal{P}_M$ for $M \subset \mathbf{Z}^2$, we need only show that

$$\lim_{n\to\infty} \frac{1}{|M_n + n\mathbf{l}|} H_\mu(\mathcal{P}_{M_n+n\mathbf{l}}) = \lim_{n\to\infty} \frac{1}{|M_n + n\mathbf{l}|} H_{\hat{T}(\mu)}(\mathcal{P}_{M_n+n\mathbf{l}}).$$

By shift invariance of $|\cdot|, \mu$ and $\hat{T}(\mu)$, we require that

$$\lim_{n\to\infty} \frac{1}{|M_n|} H_\mu(\mathcal{P}_{M_n}) = \lim_{n\to\infty} \frac{1}{|M_n|} H_{\hat{T}(\mu)}(\mathcal{P}_{M_n})$$

and, by preliminaries that

$$\lim_{n\to\infty} \frac{1}{|M_n|} H_\mu(\mathcal{P}_{M_n}) = \lim_{n\to\infty} \frac{1}{|M_n|} H_\mu(T^{-1}(\mathcal{P}_{M_n})).$$

Since clearly $\lim_{n\to\infty} |M_n|/|M_{n+1}| = 1$ we need only show that

$$\lim_{n\to\infty} \frac{1}{|M_n|} H_\mu(\mathcal{P}_{M_{n+1}}) = \lim_{n\to\infty} \frac{1}{|M_n|} H_\mu(T^{-1}(\mathcal{P}_{M_n}))$$

and, by shift invariance of μ, that

$$\lim_{n\to\infty} \frac{1}{|M_n|} H_\mu(\mathcal{P}_{M_{n+1}+\mathbf{n}}) = \lim_{n\to\infty} \frac{1}{|M_n|} H_\mu(T^{-1}(\mathcal{P}_{M_n})).$$

Since the hull of M_n is made up n^2 translates of the hulls of N and L (where L is a half rotation of N about $\mathbf{n}$ say) for all $n \in \mathbf{N}$, and by the conclusion of Theorem 5.5, the result follows from Theorem 5.3. $\square$

The containment, $\hat{T}(M^h(\Sigma,\sigma)) \subset M^h(\Sigma,\sigma)$, can be replaced by equality when T is onto. We first need:

Lemma 5.2 *If $T : (X_1, S_1) \to (X_2, S_2)$ (where $S_i : X_i \to X_i$ is a homeomorphism for $i = 1, 2$) is continuous and onto then $\hat{T} : M(X_1, S_1) \to M(X_2, S_2)$ is onto.*

Proof. Proved by Goodwyn in [18]. Proof outlined in Coven and Paul [14].

Theorem 5.7 *If map T is a surjective corner $\mathbf{n}$-permutative subcellular automaton of (Σ, σ) then $\hat{T}(M^h(\Sigma, \sigma)) = M^h(\Sigma, \sigma)$ for all $h \in [0, h(\sigma)]$.*

Proof. Since σ is the two dimensional shift we may clearly put $X_1 = X_2 = \Sigma$ and $S_1 = S_2 = \sigma^{(1,0)}$ in Lemma 5.2 to get that $\hat{T}$ is onto. Thus, given $h \in [0, h(\sigma)]$ and $\mu \in M^h(\Sigma, \sigma)$ there exists $\nu \in M(\Sigma, \sigma)$ such that $\hat{T}(\nu) = \mu$. Clearly, $\nu \in M^{h'}(\Sigma, \sigma)$ for some $h' \in [0, h(\sigma)]$ and, by Theorem 5.6, $\mu = \hat{T}(\nu) \in M^{h'}(\Sigma, \sigma)$ so, clearly, $h' = h_\mu(\sigma) = h$ and $\mu = \hat{T}(\nu) \in \hat{T}(M^{h'}(\Sigma, \sigma)) = \hat{T}(M^h(\Sigma, \sigma))$. Since μ was an arbitrary element of $M^h(\Sigma, \sigma)$ we have that $M^h(\Sigma, \sigma) \subset (\hat{T}(M^h(\Sigma, \sigma))$. Thus, by Theorem 5.6, $M^h(\Sigma, \sigma) = (\hat{T}(M^h(\Sigma, \sigma))$. But h was arbitrarily chosen from $[0, h(\sigma)]$. $\square$

5.7 Shereshevsky's conjecture revisited

Recall Definition 4.2.

Definition 5.1 We say that a corner point $\mathbf{n} \in N$ is a *shadowed corner point*, or *s.c.p., of f* if there is a line $\ell' \subset \mathbf{R}^2$ <u>through</u> $\mathbf{n}$ such that $(N \cup \{\mathbf{0}\}) \backslash \{\mathbf{n}\}$, where $\mathbf{0} = (0, 0) \in \mathbf{Z}^2$, lies completely in one of the two <u>open</u> half-planes into which ℓ' divides $\mathbf{R}^2$.

We omit 'of f' from these definitions when the defining function from $\mathcal{S}^N$ to $\mathcal{S}$ is obvious.

We say that a cellular automaton f^Ω is *shadowed corner permutative at* $\mathbf{n}$ if $\mathbf{n}$ is a s.c.p. of f and f^Ω is corner $\mathbf{n}$-permutative.

Observation 5.1 Since N is finite we may clearly assume that the lines ℓ and ℓ' in definition 5.1 are of rational gradient.

Observation 5.2 If $\mathbf{0}$ is in the hull $H(N)$ of N then every corner point, except $\mathbf{0}$ if $\mathbf{0}$ itself is a corner point, of f is a s.c.p. of f.

If $\mathbf{0} \notin H(N)$ then, assuming the points of N not to be co-linear, there is a unique pair of distinct lines, ℓ_1 and ℓ_2, each through $\mathbf{0}$, and having non-empty intersection with $H(N)$ (indeed, non-empty intersection with the set of corner points of N), but such that one of the two open half-planes into which ℓ_i (for i=1,2) divides $\mathbf{R}^2$ contains no points of N.

Let $\mathbf{n}_1$ and $\mathbf{n}_2$ be that unique pair of corner points of f, lying on ℓ_1 and ℓ_2 respectively, whose distance from $\mathbf{0}$ is greater than that for any other points of N lying on ℓ_1 and ℓ_2 respectively. Then $\mathbf{n}_1$ and $\mathbf{n}_2$ are s.c.p's. Corner points other than $\mathbf{n}_1$ and $\mathbf{n}_2$, of f are s.c.p's of f if and only if they do not lie in the closed triangle in $\mathbf{R}^2$ with vertices at $\mathbf{0}$, $\mathbf{n}_1$, and $\mathbf{n}_2$.

In other words, imagine a light emitted from $\mathbf{0}$ and s.c.p's as being those corner points of f that are shadowed by either the interior or the boundary of the hull $H(N)$ of N. If $\mathbf{0}$ is a corner point of f then all corner points, except $\mathbf{0}$, of f are s.c.p's. If $\mathbf{0}$ lies on an edge, but is not a corner point, of the hull of N, or if $\mathbf{0}$ lies in the interior of the hull of N, then every corner point of f is a s.c.p. of f. If $\mathbf{0}$ lies on the line projected by an edge of the hull of N, but not on that edge, then the corner point on that edge furthest from $\mathbf{0}$ is a s.c.p., but the corner point on that edge closest to $\mathbf{0}$ is not a s.c.p.

Theorem 5.8 *A shadowed corner permutative cellular automaton must have infinite entropy.*

Proof. Let the metric, ρ, on $\Omega = \mathcal{S}^{\mathbf{Z}^2}$ be such that $\rho((x_{\mathbf{n}}),(y_{\mathbf{n}})) = 2^{-r}$ if $(x_{\mathbf{n}}) \neq (y_{\mathbf{n}})$, where $r = \min\{|\mathbf{n}| : x_{\mathbf{n}} \neq y_{\mathbf{n}}\}$, and 0 otherwise (this gives the product topology on Ω). Thus, given $\epsilon > 0$ there exists minimal $R_\epsilon \in [0,\infty)$ such that points in Ω are ϵ-close if and only if they agree at all $\mathbf{Z}^2$-coordinates in $C(R_\epsilon)$, the closed circle in $\mathbf{R}^2$ of centre $\mathbf{0}$ and radius R_ϵ. Furthermore, $R_\epsilon \to \infty$ as $\epsilon \to 0$.

Let ϵ, and hence $R = R_\epsilon$, be given and let ℓ be the line of rational gradient (observation 5.1) for the permutative s.c.p., $\mathbf{m} \in N$ say, of f. Let $\ell' \subset \mathbf{R}^2$ be that unique line through $\mathbf{0}$ and parallel to ℓ. Put $L_R = \ell' \cap C(R) \cap \mathbf{Z}^2$.

For all $n \in \mathbf{N}$ let $S_n = \{(x_{\mathbf{n}}) \in \Omega : x_{\mathbf{n}} = 0$ if $\mathbf{n} \notin L_R + i \cdot \mathbf{m}$ for some $i \in \{0, \cdots, n-1\}\}$. Clearly, if $(x_{\mathbf{n}}) \neq (y_{\mathbf{n}})$ in S_n then there is a minimal value of i in $\{0, \cdots, n-1\}$ for which $x_{\mathbf{l}+i\cdot\mathbf{m}} \neq y_{\mathbf{l}+i\cdot\mathbf{m}}$ for some $\mathbf{l} \in L_R$. If $i = 0$ then clearly $\rho((x_{\mathbf{n}}), (y_{\mathbf{n}})) > \epsilon$. If $i \geq 1$ then, by the construction of S_n, $i-1$ is the minimal element of $\{0, \cdots, n-2\}$ such that $(f^\Omega((x_{\mathbf{n}})))_{\mathbf{l}+(i-1)\cdot\mathbf{m}} \neq (f^\Omega((y_{\mathbf{n}})))_{\mathbf{l}+(i-1)\cdot\mathbf{m}}$, for some $\mathbf{l} \in L_R$, and we inductively see that $((f^\Omega)^i((x_{\mathbf{n}})))_{\mathbf{l}} \neq ((f^\Omega)^i((y_{\mathbf{n}})))_{\mathbf{l}}$, so that $\rho((f^\Omega)^i((x_{\mathbf{n}})), (f^\Omega)^i((y_{\mathbf{n}}))) \geq \epsilon$. Thus, S_n is (n, ρ, ϵ)-separated. But $|S_n| = s^{|L_R| \cdot n}$, where $s = |\mathcal{S}|$, so that

$$h(f^\Omega) \geq \lim_{\epsilon \to 0} \limsup_{n \to \infty} \frac{|L_R| \cdot n \cdot \log s}{n} = \lim_{\epsilon \to 0} |L_R| \cdot \log s = \infty$$

since $|L_R| \to \infty$ as $R = R_\epsilon \to \infty$ as $\epsilon \to 0$. $\square$

Remark 5.2 Theorem 3.4 follows as a Corollary from this result, since any algebraic cellular automata is $\mathbf{n}$-permutative for all non-redundant $\mathbf{n} \in N$.

Bibliography

[1] M. F. Atiyah & I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Mass., (1969).

[2] V. I. Arnold & A. Avez, *Ergodic Problems in Classical Mechanics*, Addison-Wesley, Reading, Mass., (1989).

[3] D. Z. Arov, *Calculations of entropy for a class of group endomorphisms*, Zap. Meh. Mat. Fak. Har'kov Mat. Obšč **4** 30 48-69 (1964).

[4] H. Bass, *The degree of polynomial growth of finitely generated nilpotent groups*, Proc. London Math. Soc. **25**, 603–614 (1972).

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

[6] V. Bergelson & J. Rosenblatt, *Mixing actions of groups*, Illinois J. of Math. **32** (1), 65–80 (1988).

[7] R. Bowen, *Topological entropy and axiom A*, Proc. Symp. in Pure Math. **16**, 23–42 (1970).

[8] R. Burton & J. Steif, *Non-uniqueness of measures of maximal entropy for subshifts of finite type*, Erg. Th. & Dyn. Sys. **14**, 213–235 (1994).

[9] R. Burton & J. Steif, *New results on measures of maximal entropy*, Israel J. of Math. **89**, 275–300 (1995).

[10] R. Burton & J. Steif, *Some 2-d symbolic systems: entropy and mixing*, Erg. Th. of Z^d-actions, Cambridge University Press, Pollicott & Schmidt (eds), 297–306 (1996).

[11] V. Chothi, G. Everest, & T. Ward, *S-integer dynamical systems: periodic points*, J. reine angew. Math. **489** 99–132 (1997).

[12] J. Conze, *Points périodiques et entropie topologique*, C. R. Acad. Sc. Paris T **267** 149–152 (1968).

[13] J. Conze, *Entropie d'un groupe abélien de transformations*, Z. Wahr. verw. Geb. **25** 11–30 (1972).

[14] E.M. Coven & M.E. Paul, *Endomorphisms of irreducible subshifts of finite type*, Math. Sys. Th. **8** 167–175 (1975).

[15] S. A. Elsanousi, *A variational principal for the pressure of a continuous Z^2-action on a compact metric space*, Amer. J. Math. **99** 77–106 (1977).

[16] J. Feldman, *Ergodic theory of continuous group actions*, Soc. Math. de France, Astérisque **49** 61–74 (1977).

[17] T. N. T. Goodman, *Relating topological entropy and measure entropy*, Bull. London Math. Soc. **3** 176–180 (1971).

[18] L. W. Goodwyn, *Topological entropy and expansive cascades*, Univ. of Maryland Dissertation (1968).

[19] M. Gromov, *Groups of polynomial growth and expanding maps*, Publ. Math. I.H.E.S. **53**, 53–73 (1981).

[20] P.R. Halmos, *On automorphisms of compact groups*, Bull. Amer. Math. Soc. **49** 619-624 (1943).

[21] G.A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Sys. Th. **3** 320–375 (1969).

[22] E. Hemmingsen & W. Reddy, *Expansive homeomorphisms on homeogeneous spaces*, Fund. Math. **64** 203–207 (1969).

[23] E. Hewitt & K.A. Ross, *Abstract Harmonic Analysis I*, Springer, Berlin (1963).

[24] P. J. Higgins, *An Introduction to Topological Groups*, Cambridge University Press (1974).

[25] S. A. Juzvinskiĭ, *Calculation of the entropy of a group-endomorphism*, Sibirsk. Mat. Ž. **8** 230–239 (1967).

[26] Y. Katznelson & B. Weiss, *Commuting measure-preserving transformations*, Isreal J. of Math. **12** 161–173 (1972).

[27] H. Keynes & J. Robertson, *Generators for topological entropy and expansiveness*, Math. Systems Theory **3** 51–59 (1969).

[28] J. C. Kieffer, *A Generalized Shannon-McMillan theorem for the action of an amenable group on a probability space*, The Annals of Prob. **3** (6) 1031–1037 (1975).

[29] S. Lang, *Algebra*, (2nd edition), Addison-Wesley, Reading, Mass., (1984).

[30] F. Ledrappier, *Un champ markovien peut* ê*tre d'entropie nulle et melangeant*, C. R. Acad. Sc. Paris Ser. A **287** 561–562 (1978).

[31] D. H. Lehmer, *Factorization of cyclotomic polynomials*, Ann. of Math. **34** 461–479 (1933).

[32] D. Lind, *Ergodic automorphisms of the infinite torus are Bernoulli*, Ann. of Math. **34** 461–479 (1933).

[33] D. Lind & B. Marcus, *Symbolic Dynamics and Coding*, Cambridge University Press, (1995).

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

[35] R. Mañé, *Expansive homeomorphisms and topological dimension*, Trans. Amer. Math. Soc. **252** 313–319 (1979).

[36] N. Markley, *Homeomorphisms of the circle without periodic points*, Proc. London Math. Soc. **20** (3) 688–698 (1970).

[37] N. Markley & M. Paul, *Matrix subshifts for* $\mathbf{Z}^v$ *symbolic dynamics*, Proc. London Math. Soc. **20** (3) 688–698 (1970).

[38] H. Matsumura, *Commutative Algebra*, Benjamin, New York, (1970).

[39] J. Miebach, *A representation for* Z^d *subshifts of finite type*, in 'Topology, Measure and Fractals', Akademie Verlag, Berlin, Mathl. Res. **66** 208–213 (1992).

[40] M. Misiurewicz, *Diffeomorphisms without any measure with maximal entropy*, Bull. Acad. Pol. Sci. **21** 903–910 (1973).

[41] M. Misiurewicz, *A short proof of the variational principle for a* $\mathbf{Z}_+^d$*-action on a compact space*, Astérisque **40** 147–157 (1975).

[42] G. Morris & T. Ward, *Entropy bounds for endomorphisms commuting with K-actions*, Israel J. of Math., to appear.

[43] S.A. Morris, *Pontryagin Duality and the Structure of Locally Compact Abelian Groups*, London Math. Soc. Lecture Note 29, Cambridge University Press, Cambridge (1977).

[44] D. Newton & W. Parry, *On a factor automorphism of a normal dynamical system*, Ann. Math. Statist. **37** 1528–1533 (1966).

[45] T. O'Brien, *Expansive homeomorphisms on compact manifolds*, Proc. Amer. Math. Soc. **24** 767–771 (1970).

[46] J. M. Ollagnier, *Ergodic theory and statistical mechanics*, Lecture Notes in Math. **1115** Springer-Verlag, Berlin, (1985).

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

[48] J.C. Oxtoby, *Measure and Category*, Grad. Texts in Math., Springer, New York (1970).

[49] W. Parry, *Intrinsic Markov chains*, Trans. Amer. Math. Soc. **112** 55–66 (1964).

[50] A. L. T. Paterson, *Amenability*, A.M.S. surveys and monographs number 29, Providence, Rhode Island (1988).

[51] W. Reddy, *The existence of expansive homeomorphisms on manifolds*, Duke Math. J. **32** 627–632 (1965).

[52] W. Reddy, *Pointwise expansive homeomorphisms*, J. London Math. Soc. **2** (2) 232–236 (1970).

[53] V.A. Rokhlin, *The entropy of an automorphism of a compact commutative group*, Teor. Verojatnost i Primenen. **6** 351–352 (1961).

[54] V.A. Rokhlin, *On the fundamental ideas of measure theory*, Amer. Math. Soc. Transl. **1** (10) 1–54 (1962).

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

[56] V.A. Rokhlin, *Metric properties of endomorphisms of compact commutative group*, Amer. Math. Transl. Ser. **64** 244–252 (1967).

[57] D.J. Rudolph, *An isomorphism theory for Bernoulli free* $\mathbf{Z}$*-skew-compact group actions*, Advances in Math. **47** 241–257 (1983).

[58] K. Schmidt, *Asymptotic properties of unitary representations and mixing*, Proc. of London Math. Soc. **48** (3) 445–460 (1984).

[59] K. Schmidt, *Algebraic Ideas in Ergodic Theory*, C.B.M.S. Series Math. 76, A. M. S., Providence, Rhode Island (1989).

[60] K. Schmidt, *Dynamical Systems of Algebraic Origin*, Progress in Math. 128, Birkhäuser, Basel (1995).

[61] M. Shereshevsky, *Expansiveness, entropy, and polynomial growth for groups acting on subshifts by automorphisms*, Indag. Math. N.S. **4** (2) 203–210 (1993).

[62] Ja. G. Sinaĭ, *On the concept of entropy for a dynamical system*, Dokl. Akad. Nauk. SSSR **124** 768–771 (1959).

[63] P. Walters, *A variational principle for the pressure of continuous transformations*, Amer. J. of Math. **97** (4) 937–971 (1976).

[64] P. Walters, *An Introduction to Ergodic Theory*, Grad. Texts in Math., Springer, New York (1982).

[65] T. Ward & Q. Zhang, *The Abramov-Rokhlin entropy addition formula for amenable group actions*, Mh. Math. **114** 317–329 (1992).

[66] D. Witte, *Arithmetic groups of higher Q-rank cannot act on 1-manifolds*, Proc. Amer. Math. Soc. **122** (2) 333–340 (1994).

[67] J. Wolf, *Growth of finitely generated solvable groups and curvature of Riemannian manifolds*, J. Diff. Geom. **2** 421–446 (1968).

Appendix A

"A note on mixing properties of invertible extensions"

Appendix B

"Entropy bounds for endomorphisms commuting with K actions"