Commun. Math. Phys. 118, 401–410 (1988)

Communications in Mathematical Physics

Ergodic Endomorphisms of Compact Abelian Groups*

M. Shirvani and T. D. Rogers
Department of Mathematics, University of Alberta, Edmonton, Alberta Canada, T6G 2G1

Abstract. We show that for a surjective endomorphism of a compact abelian group ergodicity is equivalent to a condition which implies r-mixing for all $r \geqq 1$, and we characterize such maps algebraically. This is then used in proving the ergodicity of an extensive class of endomorphisms of the binary sequence space. As a simple corollary it is found that one-dimensional linear cellular automata and the accumulator automata are r-mixing for all $r \geqq 1$.

1. Introduction

Let θ be a continuous automorphism of a compact abelian group G. The classical automorphism theorem of Halmos [4] states that θ is strongly mixing with respect to the normalized Haar measure on G if and only if it is ergodic. To explain our generalization, say θ is *completely mixing* in G if and only if the following holds:

Given any integer $r \geqq 1$, any $r+1$ measurable subsets $A_0, \ldots, A_r$ of G, and any r sequences $\{k_{in}\}$ of positive integers such that $\lim_{n \to \infty} k_{in} = \infty$ for all $1 \leqq i \leqq r$, we have

$$\lim_{n \to \infty} \mu(A_0 \cap \theta^{-k_{1n}}(A_1) \cap \cdots \cap \theta^{-k_{rn}}(A_n)) = \prod_{j=0}^{r} \mu(A_j).$$

In an arbitrary space the above property may well be stronger than the condition of r-mixing introduced by Rohlin [9], since the latter involves the extra assumption that $\lim_{n \to \infty} \min_{i \neq j} |k_{in} - k_{jn}| = \infty$. We prove the following generalization of the above result.

Theorem 1 (Endomorphism Theorem). *Let G be a compact abelian group with normalized Haar measure μ, and let θ be a continuous surjective endomorphism of G. Then θ is μ-invariant. Moreover, the following are equivalent:*

(i) *θ is completely mixing.*
(ii) *θ is r-mixing for all $r \geqq 1$.*

* This work was supported in part by grants from NSERC

(iii) θ *is ergodic.*

(iv) *The induced homomorphism* $\hat{\theta}$ *has no non-trivial finite orbits on the character group* $\hat{G}$.

(v) *For every* $n \geqq 1$ *the endomorphism* $I - \theta^n$ *of* G *is surjective, where* I *denotes the identity map on* G.

Rohlin [9] proves the equivalence of (ii), (iv) above by a different method. Note also that the bilateral shift endomorphism is completely mixing but not exact, so the conclusion of Theorem 1 cannot be much strengthened.

Our interest in the dynamics of endomorphisms arises from the study of generalized automata. Let $G = \mathbb{Z}_2^S = \prod_{i \in S} \mathbb{Z}_2$, where S is either $\mathbb{N}$ or $\mathbb{Z}$, and let θ be a continuous endomorphism of G. Then for each $i \in S$ there exists a finite subset $K_i \subset S$ such that $\theta(a)_i = \sum_{j \in K_i} a_j$ for all $a \in G$. Let $\rho(i) = \max\{j \in K_i\}$ and $\lambda(i) = \min\{j \in K_i\}$. Assume that ρ (and λ in the case $S = \mathbb{Z}$) is strictly increasing and has no fixed points. Then Theorems 2 and 3 combine to say that in this case θ is onto, completely mixing, has periodic points of all orders, and the set of periodic points of θ is dense in G. Furthermore, Theorem 4 states that in the case $G = \mathbb{Z}_2^{\mathbb{N}}$ the above maps are also strongly transitive (i.e. $\bigcup_{n=0}^{\infty} \theta^n(V) = G$ for every non-empty open subset V of G). As an immediate consequence of the above we have

Corollary 2. *One-dimensional cellular automata, and the accumulator automata* [1] *are completely mixing.*

The corollary may shed some light on the unpredictable space-time patterns produced by certain local automata. For example, some of Wolfram's class III automata [11] are clearly completely mixing. The corollary also strengthens a result due to Lind [6]. The accumulator automata $C: \mathbb{Z}_2^{\mathbb{N}} \to \mathbb{Z}_2^{\mathbb{N}}$ given by $(Cx)_i = x_{i+1} + \sum_{j=0}^{i} C_{ij} x_j$ were introduced in [1], where the algebraic structure of the set of periodic points associated with them were elucidated. The particular example of the twisted shift $\operatorname{map}(Tx)_i = x_0 + x_{i+1}$ was utilized in [12] as a symbolic dynamical system in the enumeration of the bifurcations of the stable periodic cycles associated with quadratic maps of the interval.

The hypothesis that ρ (and λ) in Theorems 2 and 3 be order preserving may well be too strong, as is shown by the following:

Theorem 5. *Let* $G = \mathbb{Z}_2^S$, *and let* $\theta: G \to G$ *be defined by* $\theta(x)_i = x_{\rho(i)}$, *where* $\rho: S \to S$ *is injective and has no periodic points on* S. *Then* θ *is continuous, surjective, completely mixing, has points of all periods, and its set of periodic points is dense in* G.

Whether Theorems 2 and 3 can still be proved under the weakened hypothesis of Theorem 5 remains to be seen.

2. The Endomorphism Theorem

Let G be a compact abelian group (written additively) and let μ denote the normalized Haar measure on G. Let T be a continuous μ-invariant map of G into

itself. If T is completely mixing then it is in particular strongly mixing (the case $r=1$ of r-mixing). The latter property has many interesting consequences, among which are ergodicity, sensitive dependence to initial conditions (at all points of G), and the fact that the set of periodic points of T has measure zero in G (unless some iterate of T is the identity mapping on G). It is therefore of interest to determine conditions under which (algebraic) homomorphisms of G are completely mixing. Before stating these conditions, recall that the character group $\hat{G}$ of G consists of all continuous homomorphisms λ of G into the group of complex numbers of modulus one. Given a continuous endomorphism θ of G, the induced homomorphism $\hat{\theta}$ on $\hat{G}$ is defined by $\hat{\theta}(\lambda)(x)=\lambda(\theta(x))$ for all $x\in G$. We also write 1_G for the trivial character on G (i.e. $1_G(x)=1$ for all $x\in G$).

Proof of Theorem 1. The μ-invariance of θ is well-known ([8], I.7.2). The equivalence of (iv) and (v) is also easy to see. For, given any $n\geqq 1$, the set $H=\{x-\theta^n(x): x\in G\}$ is in fact a subgroup of G, and $\hat{\theta}^n(\lambda)=\lambda$ if and only if the restriction of λ to H is the trivial character 1_H. Moreover if $H\neq G$ then any non-trivial character of G/H gives rise to a character of G which is trivial on H. Thus $H\neq G$ is equivalent to the existence of non-trivial character λ of G such that $\hat{\theta}^n(\lambda)=\lambda$. This establishes the equivalence of (iv) and (v).

The implications (i)$\Rightarrow$(ii)$\Rightarrow$(iii) are trivial. The proof that (iii) implies (iv) is essentially Halmos' observation [3] that if $\hat{\theta}^n(\lambda)=\lambda$ and $\lambda\neq 1_G$, then $f=\sum_{i=0}^{n-1}\hat{\theta}^i(\lambda)$ is a non-constant function in $\mathscr{L}^2(G)$ such that $f\theta=f$. This implies that θ is not ergodic ([8], II.2.1).

It remains to prove that (iv) implies (i). Define the linear operator $U_\theta=U$ on $\mathscr{L}^2(G)$ by $U(f)=f\theta$ for all $f\in\mathscr{L}^2(G)$. Consider the equation

$$\lim_{n\to\infty}\langle f_0U^{k_1n}(f_1)\cdots U^{k_rn}(f_r),1_G\rangle=\prod_{j=0}^{r}\langle f_j,1_G\rangle \tag{1}$$

where $f_0,\ldots,f_r\in\mathscr{L}^2(G)$. Clearly θ is completely mixing if (1) holds when the f_i are the characteristic functions of the sets A_i. We claim that (1) is in fact true for all $f_i\in\mathscr{L}^2(G)$. It is sufficient to show that (1) holds when the f_i are linear combinations of characters, for then the fact that $\hat{G}$ is dense in $\mathscr{L}^2(G)$ ([7], 38D), together with some straightforward estimates, show that (1) holds for all $f_i\in\mathscr{L}^2(G)$.

Note that if λ is a character then $U^n(\lambda)=\lambda\theta^n=\hat{\theta}^n(\lambda)$. Let $f_i=\sum_{j=0}^{n}c_{ij}\lambda_j$, where $\lambda_0=1_G$, the $c_{ij}\in\mathbb{C}$, and the $\lambda_j\in\hat{G}$. Then the left-hand side of (1) consists, apart from the term $c_{00}c_{10}\cdots c_{r0}=\prod_{j=0}^{r}\langle f_j,1_G\rangle$, of complex multiples of terms of the form $\langle\lambda_{i_0}\hat{\theta}^{k_1n}(\lambda_{i_1})\cdots\hat{\theta}^{k_rn}(\lambda_{i_r}),1_G\rangle$, where $0\leqq i_0,\ldots,i_r\leqq m$, and at least one $\lambda_{i_s}\neq 1_G$. An application of (the multiplicative version of) the $H-S$ Lemma (cf. Sect. 5) shows that for all sufficiently large n, $\lambda_{i_0}\hat{\theta}^{k_1n}(\lambda_{i_1})\cdots\hat{\theta}^{k_rn}(\lambda_{i_r})\neq 1_G$, whence the above inner product is zero. This establishes (1) for all linear combinations of characters, and hence concludes the proof of the theorem. □

In particular using (iv) of Theorem 1 we have

Corollary 1. *Let θ be a continuous surjective endomorphism of a compact abelian group. Then the ergodicity of any power of θ implies the ergodicity of all powers of θ.* □

The above is of course false for arbitrary ergodic maps T; more precisely, the ergodicity of T does not imply that of any of its iterates.

3. Complete Mixing and Strong Transitivity in $\mathbb{Z}_2^S$

Henceforth we confine ourselves to the case where G is a binary sequence space. To treat infinite and bi-finite sequences simultaneously we write $G = \mathbb{Z}_2^S = \prod_{i \in S} \mathbb{Z}_2$, where S is either $\mathbb{N} = \{0, 1, \ldots\}$ or $\mathbb{Z}$. In what follows θ denotes a continuous endomorphism of G.

It is easy to see that for each $i \in S$ there exists a *finite* subset $K_i \subseteq S$ such that $\theta(a)_i = \sum_{j \in K_i} a_j$ for all $a \in G$. Conversely, any choice of finite subsets K_i of S gives rise to a continuous homomorphism of G defined as in the above formula. Therefore, the dynamical properties of θ are determined solely by the collection of subsets $\{K_i : i \in S\}$. We begin with some elementary results.

Lemma 1. *Let $G = \mathbb{Z}_2^S$, and let θ be a continuous endomorphism of G. For any $n \geqq 1$ and any $i \in S$ write the i-th component of θ^n in the form*

$$\theta^n(x)_i = \sum_{j \in K(n,i)} x_j, \quad \text{all } x \in G.$$

Then for $n \geqq 2$ the sets $K(n, i)$ are defined recursively by

$$K(n, i) = \Delta_{j \in K(n-1,i)} K(1, j).$$

($A \Delta B = (A \setminus B) \cup (B \setminus A)$ is the symmetric difference of the sets A and B.)

Proof. By definition $\sum_{j \in K(n,i)} x_j = \theta^n(x)_i = \theta^{n-1}(\theta(x))_i = \sum_{j \in K(n-1,i)} \theta(x)_j = \sum_{j \in K(n-1,i)} \sum_{r \in K(1,j)} x_r$. The only terms x_r that survive in the last double sum are those for which r occurs an odd number of times in the various $K(1, j)$ for $j \in K(n-1, i)$. But this is merely another way of describing the symmetric difference of the $K(1, j)$. □

For example if $K(1, i) = \{0, i+1\}$ for all $i \in \mathbb{N}$, then $K(2, i) = K(1, 0) \Delta K(1, i+1) = \{0, 1\} \Delta \{0, i+2\} = \{1, i+2\}$, and more generally $K(n, i) = \{n-1, n+i\}$.

Lemma 2. *In the notation of Lemma 1 assume that θ is surjective, and that $K(1, i) \subseteq \{-i, \ldots, +i\}$ for all $i \in S$. Then θ is not ergodic.*

Proof. A trivial inductive argument shows that $K(n, i) \subseteq \{-i, \ldots, i\}$ for all i and n, and so $K(n, i) = K(m, i)$ for some $m > n$. In view of the definitions this means that $\theta^n(x)_i = \theta^{m+n}(x)_i$ for all $x \in G$, and since θ^n is surjective we get $y_i = \theta^m(y)_i$ for all $y \in G$. But then the i-th component of $I - \theta^m$ is identically zero, and the conclusion follows from Theorem 1. □

It is apparent from Lemma 2 that the maximum and minimum elements of

the sets $K(n, i)$ exert considerable influence over the dynamical properties of θ. Let

$$\rho(i) = \max\{j : j \in K(1, i)\},$$
$$\lambda(i) = \min\{j : j \in K(1, i)\},$$

for all $i \in S$. A case in which the ergodicity of θ can be asserted is when ρ (and λ when $S = \mathbb{Z}$) are both strictly increasing, i.e. $i < j$ implies that $\rho(i) < \rho(j)$.

Theorem 2. *Let $G = \mathbb{Z}_2^S$ and let θ be a continuous endomorphism of G. Assume that ρ (and λ in the case $S = \mathbb{Z}$) is strictly increasing and has no fixed points. Then θ is surjective and completely mixing.*

Proof. The following properties of the map ρ are trivial to verify: ρ is injective; $\rho^n(i) \neq i$ for all $n \geqq 1$ and all $i \in S$; if $j < \rho^n(j)$ for some $j \in S$ then $i < \rho^n(i)$ for all $i \geqq j$; if $\rho^n(j) < j$ for some $j \in S$ then $\rho^n(i) < i$ for all $i \leqq j$.

We treat the cases $S = \mathbb{N}$ and $S = \mathbb{Z}$ separately, beginning with the former. Here $0 < \rho^n(0)$, and so $i < \rho^n(i)$ for all $i \in S$. We first show that θ is surjective. This means that given $a \in G$ we have to solve the system of equations

$$\sum_{j \in K(1,i)} x_j = a_i, \quad \text{all} \quad i \in S, \tag{1}$$

for some $x \in G$. The solution may be found as follows: since $0 < \rho(0) < \rho(1) < \rho(2) < \cdots$, we begin by defining x_r arbitrarily for $0 \leqq r < \rho(0)$, use (1) to find $x_{\rho(0)}$, define x_r arbitrarily for $\rho(0) < r < \rho(1)$, use (1) to find $x_{\rho(1)}$, and so on.

The surjectivity of $I - \theta^n$ is just as easy. Given $a \in G$ we have to find $x \in G$ satisfying

$$x_i - \sum_{j \in K(n,i)} x_j = a_i, \quad \text{all} \quad i \in S. \tag{2}$$

By induction on n, the maximum element of $K(n, i)$ is $\rho^n(i) > i$. We may thus solve (2) exactly as we did (1), since (2) determines each $x_{\rho^n(i)}$ in terms of the x_j with $j < \rho^n(i)$. The ergodicity of θ now follows from Theorem 1.

In the case $S = \mathbb{Z}$ we still have to solve the systems (1) and (2) for any given $a \in G$. We indicate the solution of the more complicated system (2) only. Let $n \geqq 1$ be fixed.

Suppose first that $i < \lambda^n(i) \leqq \rho^n(i)$ for all $i \in S$. Then the left-hand side of (2) has the unique maximal subscript $\rho^n(i)$ and the unique minimal subscript i for all $i \in S$. Begin by defining the x_r arbitrarily for $0 \leqq r < \rho^n(0)$. For $i > 0$, use (2) to define $x_{\rho^n(i)}$ in terms of previously defined components (some of which may be arbitrary), and for $i < 0$, use (2) to define x_i (with no arbitrary choices).

The case where $\lambda^n(i) \leqq \rho^n(i) < i$ for all $i \in S$ can be treated analogously. We are left with the possibility that $i < \lambda^n(i) \leqq \rho^n(i)$ for some $i \in S$, and $\lambda^n(j) \leqq \rho^n(j) < j$ for some $j \in S$. It is then easy to see that there exist integers j_1 and j_2 such that $i < \lambda^n(i) \leqq \rho^n(i)$ for all $i \geqq j_1$, and $\lambda^n(i) \leqq \rho^n(i) < i$ for all $i \leqq j_2$. Moreover $j_2 = j_1$, or $j_2 = j_1 - 1$. We thus have $\cdots < \lambda^n(j_2 - 1) < \lambda^n(j_2) < j_2 \leqq j_1 < \rho^n(j_1) < \rho^n(j_1 + 1) < \cdots$ Define x_r arbitrarily for $\lambda^n(j_2) < r < \rho^n(j_1)$. For $i \geqq j_1$ the term $\rho^n(i)$ is the highest subscript occurring in (2), while for $i \leqq j_2$ the term $\lambda^n(i)$ is the lowest subscript occurring in (2). Therefore the system can be solved consistently, showing that $I - \theta^n$ is surjective. Similarly (1) may be solved along the same lines as above. The result follows. □

Corollary 2. *One-dimensional linear cellular automata, and the general accumulator maps of* [1] *are completely mixing.*

Proof. In the case of cellular automata $\rho(i) = i + r_1$ and $\lambda(i) = i + r_2$ where r_1 and r_2 are fixed non-zero integers. The accumulator maps are defined on $S = \mathbb{N}$ and have $\rho(i) = i + 1$. In each case the conditions of Theorem 2 are trivially verified. □

The above considerably strengthens Lind's result [6] for the map $\theta(x)_i = x_{i-1} + x_{i+1}$. The class III cellular automaton with code number 42 ([11], page 7) is the case $\theta(x)_i = x_{i-2} + x_{i-1} + x_i + x_{i+1} + x_{i+2}$ of Corollary 2.

Write $P_n = \{x \in G : \theta^n(x) = x\}$ for $n \geqq 1$. If θ is a linear map then each P_n is a subspace of G(regarded as a vector space over the field of two elements). In particular the cardinality of P_n is either a finite power of 2 or that of the continuum. As has already been remarked, the fact that the maps θ of Theorem 2 are strongly mixing implies that $P(G) = \bigcup_{n=0}^{\infty} P_n$ has measure zero in G. There are, nonetheless, many periodic points.

Theorem 3. *Let $G = \mathbb{Z}_2^S$ and let θ be a continuous endomorphism of G. Assume that ρ (and λ in the case $S = \mathbb{Z}$) is strictly increasing and has no fixed points. Then θ has periodic points of all orders, and the set of periodic points of θ is dense in G.*

Proof. Clearly we have $\theta^n(x) = x$ if and only if $(I - \theta^n)(x) = 0$. To show the existence of points of period exactly n we need a closer look at the proof of the surjectivity of the maps $I - \theta^n$ given in Theorem 2. For example in the case $S = \mathbb{N}$ a point of period dividing n is a solution of $x_i + \sum_{j \in K(n,i)} x_j = 0$ for all $i \in S$. In particular if d is a proper divisor of n then $x_{\rho^d(0)}$ is uniquely determined by the x_j, $0 \leqq j < \rho^d(0)$ (which have been chosen arbitrarily). However for any choice of the components a_j, $0 \leqq j < \rho^d(0)$, we can find $x, y \in P_n$ with $x_j = y_j = a_j$ for $0 \leqq j < \rho^d(0)$, $x_{\rho^d(0)} = 0$, and $y_{\rho^d(0)} = 1$, so at most one of x or y can have period d. This plainly establishes the existence of points of period exactly n. Similarly given any $m \geqq 1$ there exists n such that $\rho^n(0) > m$. Thus given any $a \in G$ one can find $x \in P_n$ such that $x_i = a_i$ for $0 \leqq i \leqq m < \rho^n(0)$. This proves that the set of periodic points is dense in G. The proof of the (entirely analogous) case $S = \mathbb{Z}$ is left to the reader. □

A well-known consequence of the ergodicity of the maps θ is that they are all *topologically transitive*, i.e., for any non-empty open set V, the set $\bigcup_{n=0}^{\infty} \theta^n(V)$ is dense in G. Following [2] we say θ is *strongly transitive* if $\bigcup_{n=0}^{\infty} \theta^n(V) = G$ for all non-empty open subsets V of G. In this direction we have

Theorem 4. *Let $G = \mathbb{Z}_2^{\mathbb{N}}$, and let θ be a continuous endomorphism of G such that ρ is strictly increasing and has no fixed points. Then θ is strongly transitive.*

Proof. We have to prove that given any $a, b \in G$ (possibly $a = b$) and any neighbourhood V of a, there exists an integer m and an element $x \in V$ such that $\theta^m(x) = b$. A fundamental system of open neighbourhoods of the identity is given by the

cylinder sets $V_n = \{x \in G : x_i = 0 \text{ for } 0 \leqq i \leqq n\}$ for all $n \geqq 0$. Thus given $a, b \in G$ and $n \geqq 0$ we have to find $m \geqq 1$ and $x \in G$ such that $\theta^m(x) = b$ and $x_i = a_i$ for $0 \leqq i \leqq n$. Choose any m such that $\rho^m(0) > n$. Set $x_i = a_i$ for $0 \leqq i \leqq n$, and use the equations $\sum_{j \in K(m,i)} x_j = b_i$ to determine the $x_{\rho^m(i)}$ for all $i \geqq 0$ (other components of x may be chosen at will). □

The result, of course, does not extend to the case $S = \mathbb{Z}$. Indeed, even the bi-infinite shift map $\sigma(x)_i = x_{i+1}$ does not possess strong transitivity, since from almost no neighbourhood of $\overline{1}$ (all 1's) can one reach $\overline{10}$ (alternate 1's and 0's) under any iterate of σ.

4. Other Examples

Unfortunately the condition that ρ (and λ) be strictly increasing is not always necessary for the truth of Theorems 2 and 3, as the following result shows

Theorem 5. *Let $G = \mathbb{Z}_2^S$, and let $\theta : G \to G$ be defined by $\theta(x)_i = x_{\rho(i)}$, where ρ is injective and has no periodic points on S. Then θ is continuous, surjective, completely mixing, has points of all periods, and the set of periodic points of θ is dense in G.*

Proof. The surjectivity of θ is trivial since given $a \in G$ one simply defines $x \in G$ by $x_{\rho(i)} = a_i$ for all $i \in S$, and x_j is arbitrary if $j \notin \rho(S)$. The definition is consistent since ρ is injective.

Clearly $K(n, i) = \{\rho^n(i)\}$, so surjectivity of $I - \theta^n$ amounts to the solution, for x, of the system

$$x_i - x_{\rho^n(i)} = a_i, \quad \text{all} \quad i \in S, \tag{1}$$

where $a \in G$ is given. Let n be fixed, and define an equivalence relation $\sim_n$ on S by: $i \sim_n j$ if either $i = \rho^{rn}(j)$ or $j = \rho^{rn}(i)$ for some $r \geqq 0$ (the transitivity of $\sim$ depends upon the injectivity of ρ). Consider an equivalence class $[i_0]_n$, where $i_0 \in S$. Then the relation $\prec$, where $j \prec k$ if and only if $j = \rho^n(k)$, induces a strict total order on $[i_0]_n$ (anti-symmetry follows from the fact that ρ has no periodic points, so $j = \rho^n(k)$ and $k = \rho^n(j)$ cannot hold simultaneously). We may therefore write $[i_0]_n = \{\ldots, i_{-2}, i_{-1}, i_0, i_1, i_2, \ldots\}$, where $\rho^n(i_k) = i_{k+1}$ for all integers k. The subsystem of (1) indexed by the elements of $[i_0]_n$ thus has the form

$$\begin{aligned} &\vdots \\ x_{i_{-1}} - x_{i_0} &= a_{i_{-1}} \\ x_{i_0} - x_{i_1} &= a_{i_0} \\ &\vdots \end{aligned}$$

One may choose x_{i_0} arbitrarily, and solve the system by forward/backward substitution. Of course the subsystems indexed by different equivalence classes are disjoint, so the above method of solution is consistent. This establishes the ergodicity of θ.

The existence of periodic points is the case $a = 0$ of the above construction,

and is clearly equivalent to the conditions $x_r = x_i$ for all $r \in [i]_n$. To show the existence of points of period exactly n we need merely observe that if d is a proper divisor of n then $[i]_n$ is a proper subset of $[i]_d$ (for example $\rho^d(i) \in [i]_d \setminus [i]_n$). Consider the n distinct equivalence classes $[i]_n, [\rho(i)]_n, \ldots, [\rho^{n-1}(i)]_n$. By assigning values of 0 or 1 to the components of x on the above classes (with an appropriate definition elsewhere) we obtain 2^n vectors x satisfying $\theta^n(x) = x$. If d is a divisor of n then $\sim_d$ partitions $\{i, \rho(i), \ldots, \rho^{n-1}(i)\}$ into d equivalence classes, whereby one obtains only 2^d points whose period divides d. But $\sum_{\substack{d \mid n \\ d \neq n}} 2^d \leqq \sum_{i=1}^{n-1} 2^i = 2^n - 2$, so there is at least one point whose period is exactly n.

To show that the set of periodic points is dense in G, let J be any finite subset of S. If $i \in J$ then $\rho^n(i) \notin J$ for *all* sufficiently large n (for if $\rho^n(i) \in J$ for an infinity of values of n then $\rho^n(i) = \rho^m(i)$ for some $n \neq m$, which is impossible). Since J is finite it follows that $J \cap \rho^n(J) = \varnothing$ for all sufficiently large n. This means that the classes $[i]_n$, for $i \in J$, are all distinct, and so the components of x indexed by them can be assigned arbitrary values. In other words, given any $y \in G$ and any finite J there exists $x \in P_n$ such that $x_i = y_i$ for all $i \in J$, as required. □

Observe that the conditions on ρ in the above theorem cannot be relaxed. For example if $\rho(i) = \rho(j)$ for some $i \neq j$ then $(\theta x)_i = (\theta x)_j$ for all $x \in G$, so θ is not surjective, while if $\rho^n(i) = i$ for some $n \geqq 1$ then $I - \theta^n$ is not surjective.

Finally, we observe that the maps in Theorem 5 are not in general strongly transitive, even when $S = \mathbb{N}$. For example consider the map ρ on $\mathbb{N}$ given by $\cdots \to 8 \to 6 \to 4 \to 2 \to 0 \to 1 \to 3 \to 5 \to \cdots$ Let $b_i = 1$ for all $i \in \mathbb{N}$. Then no $x \in G$ such that $x_0 = 0$ can map to b under any iterate of θ, for given any n we have $\theta^n(x)_{2n} = x_{\rho^n(2n)} = x_0 = 0 \neq b_{2n}$. Hence from almost no neighbourhood of the identity can one reach b. The problem of relaxing the conditions on ρ (and λ) in Theorem 2 and 3 still remains.

5. The Homomorphism-Separation Lemma

Here we prove the following purely algebraic result, needed for the proof of Theorem 1:

The H-S Lemma. *Let M be an additive abelian group, and let ψ be an endomorphism of M such that*

$$\psi, \text{ and } 1 - \psi^n \text{ for all } n \geqq 1, \text{ are } 1-1 \text{ maps of } M. \tag{1}$$

Let $\{k_{1n}\}, \ldots, \{k_{rn}\}$ be sequences of positive integers satisfying $\lim_{n \to \infty} k_{in} = \infty$ for $1 \leqq i \leqq r$. If $x_0, \ldots, x_r$ are elements of M such that

$$x_0 = \sum_{i=1}^{r} \psi^{k_{in}}(x_i), \quad \text{for all} \quad n, \tag{2}$$

then $x_0 = \cdots = x_r$.

Proof. The subring $R = \mathbb{Z}[\psi]$ of End (M) generated by ψ is Noetherian. Replacing M by its R-submodule generated by the x_i we may assume that M is a finitely

generated left R-module. Also observe that if M is the direct sum $M_1 \oplus \cdots \oplus M_k$ of its R-submodules M_i and if each $x_i = \sum_{j=1}^{k} y_{ij}$, where the $y_{ij} \in M_j$, then (2) its equivalent to the k systems $y_{0j} = \sum_{i=1}^{r} \psi^{k_{in}}(y_{ij}) = 0$, $1 \leqq j \leqq k$, and also the restriction of ψ to each M_j also satisfies (1). Since $x_0 = \cdots = x_r = 0$ if and only if all the $y_{ij} = 0$, it is sufficient to assume from the beginning that all the $x_i \in M_j$.

We prove the lemma in a series of steps.

1. Consider the special case where M has a countable basis $u_1, u_2, \ldots$ over some field F, and ψ is the F-linear one-sided shift map $\psi(u_i) = u_{i+1}$ for all i. Clearly for all sufficiently large n the right-hand side of (2) cannot contain any of the u_i involved in x_0. This implies that $x_0 = 0$, and simple induction on r concludes the proof in this case.

2. Now consider the case where $\operatorname{char} R = 0$, M has no R-torsion (i.e. if $0 \neq x \in M$ and $0 \neq r \in R$ then $rx \neq 0$), and let $S = R \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $N = M \otimes_{\mathbb{Z}} \mathbb{Q}$ has no S-torsion, and ψ extends naturally to an endomorphism, still denoted by ψ, of N. Since S is a principal ideal domain ([5], Theorem 2.15) we can write $N = Sy_1 \oplus \cdots \oplus Sy_m$, where each Sy_i is a free cyclic S-module ([5], Theorem 3.10). Consider one of the summand, Sy_j say. Since this module has no S-torsion it follows that $y_j, \psi(y_j), \psi^2(y_j), \ldots$ form a $\mathbb{Q}$-basis of Sy_j, and clearly ψ acts as the shift map relative to this basis. An application of Step 1. concludes this case.

3. Now assume merely that M has no $\mathbb{Z}$-torsion (i.e. if $0 \neq x \in M$ and $n > 0$ is an integer then $nx \neq 0$). As in Step 2. Let $N = M \otimes_{\mathbb{Z}} \mathbb{Q}$ and $S = R \otimes_{\mathbb{Z}} \mathbb{Q}$. Then N is a direct sum of free cyclic modules of the form Sy, and the R-torsion submodule T of N. In view of Step 2 we may assume that $x_0, \ldots, x_r \in T$, and that in fact they generate T as S-module.

Since S is a principal ideal domain and T is finitely S-generated, there exists a non-zero polynomial $g(\psi) \in \mathbb{Q}[\psi]$ such that $g(\psi)x = 0$ for all $x \in T$, whence $g(\psi) = 0$. Thus for some integer n and rational numbers q_i we have $\psi^n = \sum_{0 \leqq i < n} q_i \psi^i$, and therefore T has finite $\mathbb{Q}$-dimension. In particular the injective maps ψ and $1 - \psi^n$ are invertible. Put $V = T \otimes_{\mathbb{Q}} F$, where F denotes the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, and consider an ψ-composition series $\{0\} = V_0 \subset V_1 \subset \cdots \subset V_m = V$ of V. Since the map induced by ψ on each factor V_i / V_{i-1} also satisfies (1) we may assume (by induction on $\dim_F V$) that $V = V_1$. But now the absolute irreducibility of the action of ψ on V (and Schur's Lemma) implies that $\dim_F V = 1$, say $V = Fu$. We have $x_i = \lambda_i u$ and $\psi(u) = \alpha u$, where the λ_i and α belong to F. By (1) we know that α is not a root of unity. Clearly (2) is equivalent to $\lambda_0 = \sum_{i=1}^{r} \lambda_i \alpha^{k_{in}}$ for all n, which implies that $\lambda_0 = 0$. (For example it is well-known ([10], IV.3, Theorem 8) that one can find a valuation $\|$ on the algebraic number field $\mathbb{Q}(\lambda_0, \ldots, \lambda_r, \alpha)$ such that $|\alpha| < 1$, whence $\lambda_0 = 0$ follows upon letting $n \to \infty$.)

4. Now consider the case where M is a torsion group. Then we can write $M = \oplus M_p$, where the sum ranges over all primes p and $M_p = \{x \in M : p^e x = 0 \text{ for some } e \geqq 0\}$. Since only a finite number of the M_p can be non-zero we may assume that $M = M_p$.

Consider first the case where $px = 0$ for all $x \in M$. Then M is a finitely generated

module over $R' = \mathbb{Z}_p[\psi]$. Since R' is a principal ideal domain we have $M = R'y_1 \oplus \cdots \oplus R'y_m \oplus T$, where the $R'y_i$ are free cyclic R'-modules and T is the R'-torsion submodule of M. Observe that $T = \{0\}$, for if $x \in T$ then by definition $g(\psi)x = 0$ for some $0 \neq g(\psi) \in \mathbb{Z}_p[\psi]$, whence $(1 - \psi^n)x = 0$ for some $n \geqq 1$. In view of (1) this implies $x = 0$, as claimed. As in Step 2 the action of ψ on each $R'y_j$ is like the shift map, and so the conclusion $x_i = 0$ follows from Step 1.

In general there exists $e \geqq 1$ such that $p^e x = 0$ for all $x \in M$. As M is a torsion group the map induced by ψ on each R'-module $p^i M/p^{i+1}M$ also satisfies (1). By the previous paragraph we find that $x_0, \ldots, x_r$ belong to every $p^i M$, and in particular to $p^e M = \{0\}$, as required.

5. Finally in the case of an arbitrary group M let $T = \{x \in M : nx = 0 \text{ for some } n > 0\}$. Then T is a submodule of M, and the map induced by ψ on the $\mathbb{Z}$-torsion-free module M/T satisfies (1). An application of Step 3 to M/T shows that all the $x_i \in T$, and proof is concluded by an application of Step 4 to T.

References

1. Allison, B. N., Pounder, J. R., Rogers, T. D.: Algebraic structure of automata with spatial memory. University of Alberta preprint (August 1987)
2. Coven, E. M., Mulvey, I.: Transitivity and the centre for maps of the circle. Ergod. Theory Dynam. Syst. **6**, 1–8 (1986)
3. Halmos, P. R.: On automorphisms of compact groups. Bull AMS **49**, 619–624 (1943)
4. Halmos, P. R.: Lectures on ergodic theory. New York: Chelsea 1956
5. Jacobson, N.: Basic algebra I. San Francisco: Freeman 1980
6. Lind, D. A.: Ergodic theory and cellular automata, in: Cellular automata. Proceedings of an Interdisciplinary Workshop. Farmer, D., Toffoli, T., Wolfram, S. (eds.). Amsterdam: North-Holland 1984
7. Loomis, L. H.: An introduction to abstract harmonic analysis. Princeton, NJ: Van Nostrand 1953
8. Mañé, R.: Ergodic theory and differentiable dynamics. Berlin, Heidelberg, New York: Springer 1987
9. Rohlin, V. A.: On endomorphisms of compact commutative groups. Izv. Akad. Nauk SSSR. Ser. Mat. **13**, 329–340 (1949)
10. Weil, A.: Basic number theory. Berlin, Heidelberg, New York: Springer 1974
11. Wolfram, S. A.: Universality and complexity in cellular automata. In Cellular automata. Proceedings of an Interdisciplinary Workshop. Farmer, D., Toffoli, T., Wolfram, S. (eds.). Amsterdam: North-Holland 1984
12. Weiss, A., Rogers, T. D.: The number of orientation reversing cycles in the quadratic map. Can. Math. Soc. Conf. Proc. 8 (1987)

Communicated by J.-P. Eckmann

Received January 19, 1988