Expansive dynamics on zero-dimensional groups

BRUCE P. KITCHENS

*IBM T. J. Watson Research Center, Mathematical Sciences Department,
P.O. Box* 218, *Yorktown Heights, NY* 10598, *USA*

Abstract. If X is a compact, zero-dimensional group and T is an expansive, transitive automorphism then (X, T) is shown to be topologically conjugate to a full shift on finitely many symbols.

The problem of classifying such automorphisms up to simultaneous algebraic isomorphism and topological conjugacy is discussed but not solved. It is proved that for any entropy there are only finitely many such equivalence classes. When the entropy is $\log p$ for a prime p, there is only one equivalence class. All are then equivalent to $(\mathbb{Z}_p)^{\mathbb{Z}}$.

0. *Introduction*

Let X be a compact, zero-dimensional, topological group. If $T: X \to X$ is an expansive automorphism, theorem 1 shows that the dynamical system (X, T) is topologically conjugate to an automorphism of a finite group cross a full shift. This answers a question of Rufus Bowen.

The problem of determining when two such dynamical systems are simultaneously topologically conjugate and algebraically isomorphic is reduced to studying full shifts with a block wise multiplication. The structure of these is studied. Theorem 1 also shows that any such dynamical system is simultaneously topologically conjugate and algebraically isomorphic to a one step subshift of finite type whose alphabet is a finite group and that has a group operation inherited from this group. Theorem 2 shows that if the automorphism is transitive and (X, T) has topological entropy $\log p$ for some prime p then it can be recoded to be $(\mathbb{Z}_p)^{\mathbb{Z}}$.

Theorem 3 is analogous to R. F. Williams' theorem A in [**W**]. It says that any isomorphism between these groups can be decomposed into a sequence of elementary isomorphisms. The question of computing when two of these systems are simultaneously conjugate and isomorphic is not answered. Example 5 displays some of the difficulties that arise when this is attempted.

I would like to thank M. Boyle, D. Lind, P. Trow, S. Tuncel and especially D. Rudolph for their discussions on these subjects.

1. *Background*

Let X be a compact topological space and $T: X \to X$ be a homeomorphism. Then the pair (X, T) is a *topological dynamical system*. If $x \in X$ is a point whose forward

orbit under T is dense in X then we say x is a *forwardly transitive point* and that (X, T) is *transitive* or *irreducible*. If (X, T) and $(\bar{X}, \bar{T})$ are topological dynamical systems and there is a homeomorphism $\phi : X \to \bar{X}$ so that $\phi \circ T = \bar{T} \circ \phi$ then we say that (X, T) and $(\bar{X}, \bar{T})$ are *topologically conjugate*. The *topological entropy* (X, T) of a dynamical system is a non-negative real number that is an invariant of topological conjugacy. See [AM] for detailed discussion of these ideas.

Let S be a finite set with the discrete topology. The space $S^{\mathbb{Z}}$ with the product topology is a compact, zero-dimensional, metric space. The shift map $\sigma : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ defined by $(\sigma(x))_i = x_{i+1}$ is a homeomorphism. The dynamical system $(S^{\mathbb{Z}}, \sigma)$ or sometimes just $S^{\mathbb{Z}}$ or $\Sigma_{|S|}$ is called the *full shift on* $|S|$ *symbols* or the *full* $|S|$ *shift*.

If $\Lambda \subseteq S^{\mathbb{Z}}$ is a closed shift invariant set the dynamical system (Λ, σ) or just Λ is called a *subshift*. Define

$$L_\Lambda = \{i \in S : x_0 = i \quad \text{for some } x \in \Lambda\}.$$

This is the *symbol set* or *alphabet* of Λ. Define $\mathcal{W}(\Lambda, n) = \{[i_1, \dots, i_n] \in S^n : x_r = i_r, 1 \le r \le n \text{ for some } x \in \Lambda\}$. This is the set of n blocks or words of length n in Λ. The topological entropy of Λ, $h(\Lambda)$, is given by $\lim (1/n) \log |\mathcal{W}(\Lambda, n)|$. The *follower set* or *successor set* of a word $[i_1, \dots, i_n]$ in $\mathcal{W}(\Lambda, n)$ is denoted by $f([i_1, \dots, i_n])$ and is defined by

$$f([i_1, \dots, i_n]) = \{j \in L_\Lambda : [i_1, \dots, i_n, j] \in \mathcal{W}(\Lambda, n+1)\}.$$

We may think of f as a map $f : \mathcal{W}(\Lambda, n) \to \mathscr{P}(L_\Lambda)$ for each n. The predecessor sets, $p([i_1, \dots, i_n])$, are defined in the obvious manner. The *n block presentation* of Λ is denoted by $\Lambda^{[n]}$. It is a subshift of $(\mathcal{W}(\Lambda, n))^{\mathbb{Z}}$. A point in $\Lambda^{[n]}$ may be thought of as being labelled by $x_k = [x_k^1, \dots, x_k^n]$, $k \in \mathbb{Z}$ where each $x_k^i \in L_\Lambda$ for $1 \le i \le n$. Then $x \in (\mathcal{W}(\Lambda, n))^{\mathbb{Z}}$ is in $\Lambda^{[n]}$ if and only if

$$x_k^r = x_{k+j}^{r-j} \qquad \text{for all } k \in \mathbb{Z}, 1 < r \le n, 0 \le j < r \text{ and}$$
$$(\cdots x_{-1}^1 x_0^1 x_1^1 x_2^1 \cdots) \in \Lambda$$

$\Lambda^{[n]}$ is just a relabelling of Λ so that $(\Lambda^{[n]}, \sigma)$ and (Λ, σ) are naturally topologically conjugate. If (Λ, σ) and $(\bar{\Lambda}, \bar{\sigma})$ are subshifts then a map $\phi : \Lambda \to \bar{\Lambda}$, such that $\phi \circ \sigma = \bar{\sigma} \circ \phi$, is continuous if and only if there is a k and l so that

$$(\phi(x))_n = \phi([x_{n-k}, \dots, x_{n+l}]) \qquad \text{for all } n \in \mathbb{Z}.$$

Here we abuse notation by thinking of ϕ as a map from Λ to $\bar{\Lambda}$ and from $\mathcal{W}(\Lambda, k+l+1)$ to $L_{\bar{\Lambda}}$. We say ϕ is a $k+l+1$ *block map* with *memory* k and *anticipation* l. A special class of the subshifts are the subshifts of finite type. There are several characterizations. The one we will use here is to say that a subshift Λ is a *subshift of finite type* if there exists an N so that if $n \ge N$ and $[i_1, \dots, i_n] \in \mathcal{W}(\Lambda, n)$ then $f([i_1, \dots, i_n]) = f([i_{n-N+1}, \dots, i_n])$. This means that a fixed finite amount of the past determines the future. In this case we say that Λ is an N *step subshift of finite type*. If we consider the N block presentation of Λ we have a *one step subshift of finite type*. In $\Lambda^{[N]}$ we have a transition rule given by a matrix A. Let $L_A = \mathcal{W}(\Lambda, N) = \mathcal{W}(\Lambda^{[N]}, 1)$ so A is indexed by $L_A \times L_A$. Then for $i = [i_1, \dots, i_N]$,

$j = [j_1, \ldots, j_N] \in L_A$ we say

$$A_{ij} = \begin{cases} 1 & \text{if } [i_1, \ldots, i_N, j_N] \in \mathcal{W}(\Lambda, N+1) \\ & \text{and } i_{k+1} = j_k \text{ for } 1 \le k < N \\ 0 & \text{otherwise.} \end{cases}$$

$\Lambda^{[N]}$ is denoted by (Σ_A, σ) or Σ_A and consists of all points $x \in (L_A)^{\mathbb{Z}}$ so that $A_{x_k x_{k+1}} = 1$ for all $k \in \mathbb{Z}$. We say A is the *transition matrix*. A subshift of finite type Σ_A is irreducible if the transition matrix, A, is irreducible. That is, for each pair $i, j \in L_A$ there is an n so that $(A^n)_{ij} > 0$. It is aperiodic if there is an n so that $A^n > 0$. The topological entropy of a subshift of finite type is $h(A) = \log \lambda$ where λ is the spectral radius of A. For a detailed discussion of subshifts and subshifts of finite type see [**AM**].

We will also assume that the reader is familiar with the basic ideas about finite groups and topological groups. See [**Ro**] and [**P**] for these discussions.
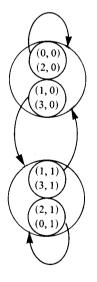
2. Subshifts as groups

Let Λ be a subshift. Further, suppose that it is a topological group and that the shift is a group automorphism.

Examples. (1) $\Sigma_2 = \{0, 1\}^{\mathbb{Z}}$ with coordinate by coordinate addition modulo 2. This may be more succinctly written as $(\mathbb{Z}_2)^{\mathbb{Z}}$.

(2) Let G be any finite group and then consider $(G)^{\mathbb{Z}}$. The group operation is given by coordinate by coordinate addition in G.

(3) Define $\Sigma_A \subseteq (\mathbb{Z}_4 \oplus \mathbb{Z}_2)^{\mathbb{Z}}$ by

This means

$$f((0, 0)) = f((2, 0)) = f((1, 1)) = f((3, 1)) = \{(0, 0), (2, 0), (1, 0), (3, 0)\}$$
$$f((1, 0)) = f((3, 0)) = f((2, 1)) = f((0, 1)) = \{(1, 1), (3, 1), (2, 1), (0, 1)\}.$$

The group operation is given by coordinate by coordinate addition in $\mathbb{Z}_4 \oplus \mathbb{Z}_2$. The

thing that must be checked is that when two points that lie in Σ_A are added together, they result in a point that also lies in Σ_A. Since Σ_A is presented as a one step subshift of finite type and the group operation is defined coordinate by coordinate we need only to check that if $[i_1, i_2]$ and $[j_1, j_2]$ are A-admissible 2 blocks then their product is an A-admissible 2 block. This condition is met.

We now make the following observation.

PROPOSITION 1. *If Λ is a subshift that is also a group, with σ an automorphism then there is a k, an l, and a function $\alpha: \mathcal{W}(\Lambda, k+l+1) \times \mathcal{W}(\Lambda, k+l+1) \to L_\Lambda$ so that*

$$(xy)_n = \alpha([x_{n-k}, \ldots, x_{n+l}], [y_{n-k}, \ldots, y_{n+l}])$$

for all $n \in \mathbb{Z}$ where xy is the product of x and y in Λ.

Proof. We may consider multiplication as a continuous shift commuting map $\alpha: \Lambda \times \Lambda \to \Lambda$. If $i \in L_\Lambda$ we consider $[i]_0 = \{x \in \Lambda: x_0 = i\}$ and then, since $\Lambda \times \Lambda$ and Λ are zero-dimensional, $\alpha^{-1}([k]_0) \subseteq \Lambda \times \Lambda$ is open and closed. This means it is a finite union of cylinders. This is true for each $i \in L_\Lambda$ which is finite so there is a k and l such that

$$(xy)_0 = \alpha([x_{-k}, \ldots, x_l], [y_{-k}, \ldots, y_l]).$$

Since the shift is an automorphism, α is shift commuting and we have the desired result. $\square$

We say that Λ has $k+l+1$ *block multiplication* with *memory k* and *anticipation l* in this case. Notice that in this terminology all three examples have 1 block multiplication with no memory or anticipation.

Suppose X and $\bar{X}$ are two topological groups $T: X \to X$ and $\bar{T}: \bar{X} \to \bar{X}$ are continuous automorphisms. We will say (X, T) and $(\bar{X}, \bar{T})$ are *conjugate* if there is a $\phi: X \to \bar{X}$ satisfying the usual conditions for topological conjugacy. If ϕ is also a group isomorphism we will say that (X, T) and $(\bar{X}, \bar{T})$ are *isomorphic.*

The motivation for this work was a question raised by Rufus Bowen, namely: What subshifts can support a group structure that makes the shift an automorphism?

3. *Zero dimensional groups*

We will now consider topological groups that are both zero dimensional or totally disconnected and compact. These are the profinite groups. Let X be a topological group and T an automorphism. We say T is *expansive* if there exists an open neighbourhood, $\mathcal{U}$, of the identity such that for each $x, y \in X$ with $x \neq y$ there exists an $n \in \mathbb{Z}$ so that $T^n x \notin (T^n y) \mathcal{U}$. The following theorem is a standard theorem about topological groups [P, p. 79].

THEOREM. *If X is a compact, zero dimensional, topological group then every open neighbourhood of the identity contains an open normal subgroup.*

We will use this to prove a proposition that is motivated by a theorem of W. Reddy [R].

PROPOSITION 2. *Suppose X is a compact, zero dimensional, topological group and T is an expansive automorphism, then (X, T) is isomorphic to a subshift (Λ, σ) with a 1 block group operation.*

Proof. Let (X, T) be as stated and $\mathcal{U}$ be an open normal subgroup so that for any $x, y \in X$, $x \neq y$, there is an $n \in \mathbb{Z}$ such that $T^n x \notin (T^n y)\mathcal{U}$. We may choose a neighbourhood of the identity that does this because T is expansive, and we may choose it to be a normal subgroup by the previous theorem. Let $\mathcal{P}$ be the finite, open-closed partition of X that is composed of the cosets of $\mathcal{U}$. It is finite, hence open and closed because X is compact. Let $\hat{G}$ denote the finite group $X/\mathcal{U}$ and think of it as the labels for the elements of $\mathcal{P}$. Define Λ a subshift of $(\hat{G})^{\mathbb{Z}}$ to be the set of all $(\mathcal{P}, T)$ names of points in X. To every $x \in X$ we associate a sequence $\bar{x} \in (\hat{G})^{\mathbb{Z}}$ by $(\bar{x})_n$, $n \in \mathbb{Z}$ is the element of $\hat{G}$ that labels the element of the partition $\mathcal{P}$ that contains $T^n x$. This sequence is the $(\mathcal{P}, T)$ name of x. Each element of X has a unique $(\mathcal{P}, T)$ name and the set of all names forms a subshift. Clearly, (X, T) is conjugate to (Λ, σ). Since, $\mathcal{U}$ was a normal subgroup, the group operation on Λ is 1 block. It is given by coordinate by coordinate multiplication in $\hat{G}$. It is now clear that (X, T) is isomorphic to (Λ, σ). $\square$

We will now examine these types of subshifts a little more carefully.

PROPOSITION 3. *Suppose (Λ, σ) is a subshift with a 1 block group operation. Then*:
    (i) *L_Λ is a finite group*;
    (ii) *$f([e]^n)$ is normal in L_Λ, where $[e]^n$ is the word consisting of n e's, and e is the identity element of L_Λ*;
    (iii) *$f(u)$, where $u \in \mathcal{W}(\Lambda, n)$, is a coset of $f([e]^n)$.*

Proof. Statement (i) is clear. It is also clear that $[e]^n \in \mathcal{W}(\Lambda, n)$ because any word $u \in \mathcal{W}(\Lambda, n)$ raised to some power will be $[e]^n$. Statement (ii) follows because if $g \in f([e]^n)$ and $h \in L_\Lambda$ then there is a word $[h_1, \ldots, h_n]$ so that $[h_1, \ldots, h_n, h] \in \mathcal{W}(\Lambda, n+1)$. Then

$$[h_1, \ldots, h_n, h][e, \ldots, e, g][h_1, \ldots, h_n, h]^{-1}$$
$$= [h_1, \ldots, h_n, h][e, \ldots, e, g][h_1^{-1}, \ldots, h_n^{-1}, h^{-1}]$$
$$= [e, \ldots, e, hgh^{-1}] \in \mathcal{W}(\Lambda, n+1)$$

so that

$$hgh^{-1} \in f([e]^n).$$

Statement (iii) follows because if $[g_1, \ldots, g_n] \in \mathcal{W}(\Lambda, n)$ and $g \in f([g_1, \ldots, g_n])$ then we see that $g(f([e]^n)) \subseteq f([g_1, \ldots, g_n])$. Conversely, if $h \in f([g_1, \ldots, g_n])$ then $[g_1, \ldots, g_n, g]^{-1}[g_1, \ldots, g_n, h] = [e, \ldots, e, g^{-1}h]$ so that $g^{-1}h \in f([e]^n)$ and $g(f([e]^n)) = f([g_1, \ldots, g_n])$. $\square$

PROPOSITION 4. *Suppose X is a compact, zero-dimensional, topological group and T is an expansive automorphism, then (X, T) is isomorphic to a one step subshift of finite type (Σ_A, σ) with a one block group operation.*

Proof. Notice that $f([e]^{n+1}) \subseteq f([e]^n) \subseteq \cdots \subseteq f(e) \subseteq L_\Lambda$. Since L_Λ is finite and each $f([e]^k)$ is a normal subgroup there is an N so that $f([e]^n) = f([e]^N)$ for all $n \geq N$.

Furthermore, if $[g_1, \ldots, g_N] \in \mathcal{W}(\Lambda, N)$, $[h_1, \ldots, h_m, g_1, \ldots, g_N] \in \mathcal{W}(\Lambda, N+m)$ then $f([h_1, \ldots, h_m, g_1, \ldots, g_N]) = f([g_1, \ldots, g_N])$. This follows because $f([h_1, \ldots, h_m, g_1, \ldots, g_N]) \subset f([g_1, \ldots, g_N])$ and both are cosets of $f([e]^N)$. This says Λ is an N step subshift of finite type. Let Σ_A be the N block presentation of Λ and carry the one block group operation on Λ over to a one block group operation on Σ_A in the obvious way. □

4. *Structure and isomorphism*

Here, we will examine carefully the structure of subshifts of finite type that have a group structure which makes the shift an automorphism. First, assume Σ_A is a subshift of finite type with one block multiplication. Then by proposition 3 we see that $f(e)$ and $p(e)$ are normal subgroups of L_A, $f(g)$ and $p(g)$ are cosets of $f(e)$ and $p(e)$ respectively, and so $f(gh) = f(g)f(h)$. This means that $f: L_A \to L_A/f(e)$ is a group homomorphism. It has kernel $p(e)$ so that $L_A/p(e)$ is isomorphic to $L_A/f(e)$. This leads to the following observation.

PROPOSITION 5. Σ_A, *a one step subshift of finite type, has a one block group operation if and only if* $f: L_A \to L_A/f(e)$ *is an onto group homomorphism. Furthermore, it is transitive if and only if* $f^k(e) = L_A$ *for some* k *where* f^k *is defined inductively by* $f^{n+1}(g) = \bigcup f(h)$ *with* $h \in f^n(g)$.

Proof. We have already seen that the 'only if' part of the first assertion follows from proposition 3. The 'if' direction is also clear.

Notice that any one step subshift of finite type with a one step group operation has a fixed point of all e's, the identity element of L_A. This is because any point will have finite order. This means that transitivity will always imply aperiodicity. This proves the 'only if' direction of the second assertion. For the converse consider a set of paths

$$\{[e, g_1^i, \ldots, g_k^i] \in \mathcal{W}(\Sigma_A, k+1): 1 \le i \le |L_A| \text{ and } \{g_k^1, \ldots, g_k^{|L_A|}\} = L_A\}.$$

Let g be any element of L_A and $[g, h_1, \ldots, h_k]$ any element of $\mathcal{W}(\Sigma_A, k+1)$. Then multiplying through the chosen set gives

$$\{[h, h_1 g_1^i, \ldots, h_k g_k^i] \in \mathcal{W}(\Sigma_A, k+1) \text{ and } \{h_k g_k^1, \ldots, h_k g_k^{|L_A|}\} = L_A\}. \quad □$$

Everything that we have said so far about the structure of Σ_A is true whether it is irreducible or not. We will see that in fact there are no interesting differences.

THEOREM 1. *Suppose X is a compact, zero dimensional, topological group and T is an expansive automorphism. Then:*

　(i) (X, T) *is isomorphic to* (Σ_A, σ) *a one step subshift of finite type with a one block group operation;*

　(ii) (X, T) *is isomorphic to* $(F, \tau) \times (\Sigma_n, \sigma)$ *where F is a finite finite group, τ is an automorphism, Σ_n is a full n shift with a k block group operation, and the group operation on $F \times \Sigma_n$ is given as an extension of Σ_n by F;*

　(iii) *If (X, T) has zero entropy then $n = 1$, i.e. the full shift is trivial.*

　(iv) *If (X, T) is irreducible then $F = \{e\}$, i.e. the finite group is trivial.*

Proof. Part (i) is proposition 4. We will start here and prove part (ii).

Take (Σ_A, σ) as stated. Let $H = p(e) \cap f(e)$, it is a normal subgroup of L_A.

Step 1. Assume $H = \{e\}$. Then we can define a new isomorphic subshift $\Sigma_{\bar{A}}$ by letting $L_{\bar{A}} = L_A/f(e))$ and defining transitions by saying:

$$g(f(e)) \to h(f(e)) \quad \text{if and only if there is a } g' \in g(f(e)) \text{ with } f(g') = h(f(e)).$$

Notice that this g' will be unique by the assumption that $H = \{e\}$. This is crucial, it gives a one block isomorphism $\phi : \Sigma_A \to \Sigma_{\bar{A}}$ by $\phi(g) = g(f(e))$. The inverse, ϕ^{-1}, is a two block map defined by $\phi^{-1}([g(f(e)), h(f(e))]) = g'$ where g' is the unique element of $g(f(e))$ with $f(g') = h(f(e))$. The group operation on $\Sigma_{\bar{A}}$ is the natural one block operation from $L_{\bar{A}}$.

Step 2. This is the more difficult part. Here we have that H is bigger than just $\{e\}$. Let $L_A/H = \hat{G}$ and recall from the theory of group extensions (see [**Ro**] for example) that L_A can be written as an extension of $\hat{G}$ by H by considering the short exact sequence

$$1 \to H \to G \to \hat{G} \to 1,$$

and choosing a section $\sigma : \hat{G} \to G$ which produces a function $\rho : \hat{G} \times \hat{G} \to H$ satisfying

$$\sigma(gg') = \sigma(g)\sigma(g')\rho(g, g').$$

Then $G \simeq \hat{G} \times H$ where the multiplication is given by

$$(g, h)(g', h') = (gg', \rho(g, g')\sigma^{-1}(g')h\sigma(g')h').$$

Here, define a subshift of finite type $\Sigma_{\hat{A}}$ by $L_{\hat{A}} = \hat{G} = L_A/H$ and transitions $gH \to hH$ if and only if $hH \subseteq f(gH)$. Give $\Sigma_{\hat{A}}$ a one block group operation from $L_{\hat{A}}$. Now Σ_A is isomorphic to $\Sigma_{\hat{A}} \times \Sigma_{|H|}$. Where $\Sigma_{|H|}$ is the full $|H|$ shift and $\Sigma_{\hat{A}} \times \Sigma_{|H|}$ has a one block multiplication that comes from considering it as a subshift of $(\hat{G} \times H)^{\mathbf{Z}}$ with the multiplication given by the isomorphism $G \simeq \hat{G} \times H$. Notice that $\Sigma_{\hat{A}}$ by itself has a one block multiplication that agrees with the multiplication in $\Sigma_{\hat{A}} \times \Sigma_{|H|}$, but $\Sigma_{|H|}$ by itself does not unless $\hat{G} \times H$ is a direct product, $\hat{G} \oplus H$.

Step 3. Start with Σ_A and apply step two to get Σ_A isomorphic to $\Sigma_{\hat{A}} \times \Sigma_{|H|}$. By the construction in step 2 we have that in $\Sigma_{\hat{A}}$, $H = \{e\}$. Now either $f(e) = \{e\}$ or we may apply step 1 to get $\Sigma_{\hat{A}}$ isomorphic to $\Sigma_{\bar{A}}$. When $f(e) = \{e\}$, $\Sigma_{\hat{A}}$ is a finite group. If we have applied step 1, Σ_A is isomorphic to $\Sigma_{\bar{A}} \times \Sigma_{|H|}$ where the multiplication is given by tracing back through $\Sigma_{\hat{A}} \times \Sigma_{|H|}$. The multiplication on $\Sigma_{\bar{A}} \times \Sigma_{|H|}$ will be two block multiplication with no memory and anticipation one.

Step 4. Notice that in $\Sigma_{\bar{A}} \times \Sigma_{|H|}$, $\Sigma_{\bar{A}}$ has one block multiplication that agrees with the multiplication in $\Sigma_{\bar{A}} \times \Sigma_{|H|}$. This means we may proceed to work on $\Sigma_{\bar{A}}$ just as we did on Σ_A. Since $|L_{\bar{A}}| \cdot |H| < |L_A|$ we will eventually end up with a $\Sigma_{\bar{A}}$ that has $f(e) = \{e\}$. Notice that every time we apply step two and then step one the length of multiplication goes up by one block of anticipation.

To prove part (iii) notice that if $|f(e)| > 1$ then $h(\Sigma_A) > 0$. This means that when $h(X) = 0$, $|f(e)| = 0$ and Σ_A consists of a finite number of periodic orbits.
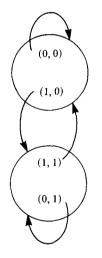
To prove part (iv) just observe that if $F \neq \{e\}$ then $(F, \tau) \times (\Sigma_n, \sigma)$ cannot be irreducible. $\square$

Example 4. Consider Σ_A the subshift defined as example three. Here $L_A = \mathbb{Z}_4 \oplus \mathbb{Z}_2$, $f(e) = \mathbb{Z}_4 \oplus \{0\}$, $p(e) = \{(0, 0), (2, 0), (1, 1), (3, 1)\}$ and $H = \{(0, 0), (2, 0)\} \approx \mathbb{Z}_2$. First we observe that Σ_A is not isomorphic to $(G)^{\mathbb{Z}}$ for any finite group G. Suppose it were, then since it is commutative and has entropy log 4 it would have to be isomorphic to either $(\mathbb{Z}_4)^{\mathbb{Z}}$ or $(\mathbb{Z}_2 \oplus \mathbb{Z}_2)^{\mathbb{Z}}$. But Σ_A has four fixed points $(0, 0)^{\mathbb{Z}}$, $(2, 0)^{\mathbb{Z}}$, $(0, 1)^{\mathbb{Z}}$, and $(2, 1)^{\mathbb{Z}}$ which have orders as group elements of one, two, two, and two, respectively. This means Σ_A is not isomorphic to $(\mathbb{Z}_4)^{\mathbb{Z}}$ because the fixed point $(1)^{\mathbb{Z}}$ has order four. Similarly, Σ_A is not isomorphic to $(\mathbb{Z}_2 \oplus \mathbb{Z}_2)^{\mathbb{Z}}$ because Σ_A contains the point $\dots (1, 1)(1, 0)(1, 1)(1, 0) \dots$, which has order four. There is no point of order four in $(\mathbb{Z}_2 \oplus \mathbb{Z}_2)^{\mathbb{Z}}$.

Now let us apply the construction of the proof of theorem 1. We think of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ as an extension of $H \approx \mathbb{Z}_2$ by $\hat{G} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$ producing the function

$$\rho : (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \times (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \to \mathbb{Z}_2$$

$$\rho((n, m), (n', m')) = \begin{cases} 1 & \text{if } n = n' = 1, \\ 0 & \text{otherwise.} \end{cases}$$

This gives $\Sigma_{\hat{A}}$ defined by

This, by step one of the proof is isomorphic to $(\mathbb{Z}_2)^{\mathbb{Z}}$. The final result is that Σ_A is isomorphic to the full four shift with alphabet $L_4 = \{(0, 0)(1, 0)(0, 1)(1, 1)\}$ and two block multiplication given by

$$[(x_0^1, x_0^2), (x_1^1, x_1^2)][(y_0^1, y_0^2), (y_1^1, y_1^2)] = \begin{cases} (x_0^1 + y_0^1, x_0^2 + y_0^2 + 1) \\ \quad \text{when } [x_0^1, x_1^1], [y_0^1, y_1^1] \in \{[0, 1], [1, 0]\} \\ (x_0^1 + y_0^1, x_0^2 + y_0^2) \\ \quad \text{otherwise.} \end{cases}$$

The main remaining problem is to compute whether or not two specified subshifts with group structures are isomorphic. At this point we do not have a method to do this. The next results are partial results in this direction.

PROPOSITION 7. *If G and H are two finite groups then $(G)^{\mathbf{Z}}$ and $(H)^{\mathbf{Z}}$ are isomorphic if and only if G and H are isomorphic.* ☐

Proof. Let $\phi : (G)^{\mathbf{Z}} \to (H)^{\mathbf{Z}}$ be an isomorphism. Then $\phi :$ Fix $(G) \to$ Fix (H) is a finite group isomorphism where Fix $(G) = \{x \in G^{\mathbf{Z}}, \sigma(x) = x\}$. But Fix (G) is isomorphic to G. ☐

THEOREM 2. *Suppose X is a compact, zero-dimensional, topological group, and T is an expansive transitive automorphism. Let $h(X, T) = \log N$, and $N = p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition of N. Then (X, T) is isomorphic to the full N shift with an at most $e_1 + \cdots + e_r$ block group operation that has zero memory.*

Proof. Begin with (X, T) as stated and apply theorem 1(i) to get (Σ_A, σ) with L_A a finite group. Consider H as in the proof of theorem 1(ii). By applying step one if need be we may assume $|H| > 1$ in Σ_A, unless $h(X, T) = 0$ which is trivial. Since H is a normal subgroup, its order divides $p_1^{e_1} \cdots p_r^{e_r}$. Apply step two to get Σ_A isomorphic to $\Sigma_{\hat{A}} \times \Sigma_{|H|}$. Then use step one to reduce $\Sigma_{\hat{A}}$ to $\Sigma_{\bar{A}}$. Notice Σ_A is isomorphic to $\Sigma_{\bar{A}} \times \Sigma_{|H|}$ with the appropriate group operation. The operation is two block with zero memory. Also $h(\Sigma_{\bar{A}}) = \log \bar{N}$, $\bar{N} \cdot |H| = p_1^{e_1} \cdots p_r^{e_r}$. In $\Sigma_{\bar{A}}$, we again have $|H| > 1$, unless $\Sigma_{\bar{A}}$ is a single fixed point. Proceed by taking out this new H. The resulting subshift will have a three block group operation with no memory. We continue until Σ_A is isomorphic to a full shift with a k block operation that has no memory. Observe that $k \le e_1 + \cdots + e_r$, since there is no non-trivial reduction, $|H| > 1$, at each step. ☐

COROLLARY. *If X is a compact, zero-dimensional, topological group, T is an expansive, transitive automorphism, and $H(X, T) = \log p$ for a prime p, then (X, T) is isomorphic to $(\mathbb{Z}_p)^{\mathbf{Z}}$.*

Proof. Theorem 2 shows that (X, T) is isomorphic to $(G)^{\mathbf{Z}}$ for some G. But G has order p and is therefore isomorphic to $\mathbb{Z}_p$. ☐

Here we will follow the lead of R. F. Williams [W] and define four elementary isomorphisms between subshifts of finite type with one block multiplication. Then we will show that any isomorphism can be decomposed into a finite sequence of these.

Given Σ_A, $f(e)$, $p(e)$ and $H = p(e) \cap f(e)$ as before we obtain a new subshift of finite type with a one block group operation, $\Sigma_{\bar{A}}$, by *state splitting* as follows. Choose S a normal subgroup of $f(e)$ and then define

$$L_{\bar{A}} = \{(g, hS): hS \subseteq f(g)\} \subseteq L_A \oplus L_A / S$$

and transitions $(g, hS) \to (g', h'S)$ if and only if $g' \in hS$. Multiplication is defined by multiplication in $L_A \oplus L_A / S$. The map $\phi : \Sigma_A \to \Sigma_{\bar{A}}$ is a two block map

$$[g, h] \to (g, hS),$$

ϕ^{-1} is a one block map $(g, hS) \to g$, and ϕ is a group isomorphism of Σ_A and $\Sigma_{\bar{A}}$.

As an example consider the subshift $(\mathbb{Z}_4)^{\mathbf{Z}}$, let $S = \{0, 2\}$. Notice that if $S = \{0\}$ we get the usual two block presentation and if $S = f(e)$ nothing happens.

The inverse operation to state splitting is *amalgamation*. We obtain a new subshift $\Sigma_{\bar{A}}$ from Σ_A by choosing $\mathscr{A} \subseteq G$ such that:

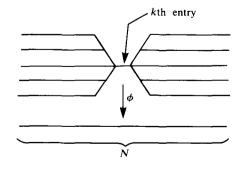(i) $\mathscr{A}$ is a normal subgroup of $f(e)$;

(ii) $\mathscr{A} \cap p(e) = \{e\}$; this insures that the elements of $\mathscr{A}$ have disjoint successors. Then define $L_{\bar{A}} = L_A/\mathscr{A}$ with transitions $g\mathscr{A} \to g'\mathscr{A}$ if and only if there exists an element $h \in g\mathscr{A}$ with $g'\mathscr{A} \subseteq f(h)$. This element $h \in g\mathscr{A}$ will be unique because of (ii). Here $\phi : \Sigma_A \to \Sigma_{\bar{A}}$ is a one block map given by $g \to g\mathscr{A}$, $\phi^{-1} : \Sigma_{\bar{A}} \to \Sigma_A$ is a two block map given by $[g\mathscr{A}, g'\mathscr{A}] \to h$ where h is the unique element in $g\mathscr{A}$ with $g'\mathscr{A} \subseteq f(h)$ and ϕ is a group isomorphism of Σ_A and $\Sigma_{\bar{A}}$.
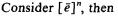
Both of these operations may also be performed when the roles of $f(e)$ and $p(e)$ are reversed. We will say that the splitting we have defined is a *state splitting by successors* and when the roles of f and p are reversed as a *state splitting by predecessors*. The same is true for amalgamations, the operation described is an *amalgamation by common predecessor and disjoint successors*, when the roles of $f(e)$ and $p(e)$ are reversed we have an *amalgamation by common successor and disjoint predecessors*. These four operations will be collectively referred to as the *elementary isomorphisms*. Then we have the following theorem which is analogous to the R. F. Williams theorem A in [**W**].

THEOREM 3. *Two subshifts of finite type with one block group operations are isomorphic if and only if it is possible to go from one of them to the other by a finite sequence of elementary isomorphisms.*

Proof. The fact that when the two are related by a finite sequence of elementary isomorphisms they are isomorphic, is clear. To see the converse, let $\phi : \Sigma_A \to \Sigma_{\bar{A}}$ be an isomorphism. By going to a higher block presentation for Σ_A we may assume ϕ is a one block map. This means that $\phi : L_A \to L_{\bar{A}}$ is an onto group homomorphism, $\phi^{-1}(\bar{e})$ is a normal subgroup of L_A, $\phi^{-1}(\bar{g})$ is a coset for any $\bar{g} \in L_{\bar{A}}$ and that $L_A/\phi^{-1}(e) \simeq L_{\bar{A}}$. All of this is true when we consider $\phi : \mathscr{W}(\Sigma_A, n) \to \mathscr{W}(\Sigma_{\bar{A}}, n)$ by which we mean that ϕ is viewed as a map on the n block level. This says that combinatorially the inverse image of any block of length n looks like the inverse image of $[\bar{e}]^n$. Since ϕ is a conjugacy there is an N and k so that all inverse images of any block of length N from $\Sigma_{\bar{A}}$ agree in the kth position.

Pictorially

Consider $[\bar{e}]^n$, then

$$\phi^{-1}([\bar{e}]^n) = \{[g_1', \ldots, g_N'], \ldots, [g_1^r, \ldots, g_N^r]\};$$

assume $g_i^1 = e$ for $i = 1, \ldots, N$ and then $g_k^i = e$ for $i = 1, \ldots, r$. Notice that the set $\mathcal{A} = \{g_{k+1}^1, \ldots, g_{k+1}^r\}$ (disregard repeats) forms a normal subgroup of $f(e)$. Also note that $\mathcal{A} \cap p(e) = \{e\}$ otherwise there would be a block $[e, g_j^i, e]$ mapping to $[\bar{e}, \bar{e}, \bar{e}]$ with $g_j^i \neq e$. $\mathcal{A}$ meets the two conditions for an amalgamation. We can form $\Sigma_{\hat{A}}$ by amalgamating in Σ_A by $\mathcal{A}$ and still have that $\phi : \Sigma_{\hat{A}} \to \Sigma_{\bar{A}}$ is a one block map. Now notice that all the inverse images of any block of length N in $L_{\bar{A}}$, agree in the k and $k+1$ entries. We continue in the same way from the $(k+1)$st to the Nth entry. Then go back and make amalgamations using the predecessors working down from the $(k-1)$st entry to the first entry. When we are done we have a new subshift Σ_B with a one block map $\phi : \Sigma_B \to \Sigma_{\bar{A}}$. Notice now that each block of length N in $\Sigma_{\bar{A}}$ has exactly one preimage. This means the N-block presentation of Σ_B and the N block presentation of $\Sigma_{\bar{A}}$ are identical. $\qquad\square$
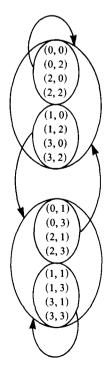
Example 5. Let $L_A = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$,
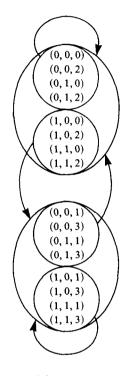
$$f(e) = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \{0\},$$

and

$$f((0, 0, n)) = f((2, 1, n)) = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \{0\},$$
$$f((1, 0, n)) = f((3, 1, n)) = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \{1\},$$
$$f((2, 0, n)) = f((0, 1, n)) = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \{2\},$$
$$f((3, 0, n)) = f((1, 1, n)) = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \{3\}.$$

Then Σ_A is an irreducible one step subshift of finite type with a one block group operation. Define one amalgamation by $\mathcal{A}_1 = \{(0, 0, 0), (0, 1, 0)\}$. This results in Σ_{A_1} which after relabelling has $L_{A_1} = \mathbb{Z}_4 \oplus \mathbb{Z}_4$ and is described by

Here $f(e_1) = \mathbb{Z}_4 \oplus 2\mathbb{Z}_4$, $p(e_1) = 2\mathbb{Z}_4 \oplus \mathbb{Z}_4$, $H_1 = 2\mathbb{Z}_4 \oplus 2\mathbb{Z}_4$ and it is not possible to make any further amalgamations. We may, however, proceed as in the proof of theorem 1 to get the full eight shift with a two block multiplication. We may define a different amalgamation on Σ_A by taking $\mathcal{A}_2 = \{(0, 0, 0), (2, 0, 0)\}$. This results in Σ_{A_2} which after relabelling has $L_{A_2} = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$ and can be described by

Here $f(e_2) = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus 2\mathbb{Z}_4$, $p(e_2) = \{0\} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$, and $H_2 = \{0\} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$. Another amalgamation can now be made by taking $\mathcal{A}_3 = \{(0, 0, 0), (1, 0, 0)\}$. The result is $(\mathbb{Z}_2 \oplus \mathbb{Z}_4)^{\mathbb{Z}}$.

We have produced five representations of $(\mathbb{Z}_2 \oplus \mathbb{Z}_4)^{\mathbb{Z}}$. This illustrates the problem of computing when two such groups are isomorphic. The situation is similar to the general topological conjugacy problem for subshifts of finite type [W]. There we also know that any topological conjugacy can be decomposed into a sequence of elementary conjugacies but we do not know if it is even possible to compute when two are conjugate. Here there may be another approach. It may be possible to develop a cohomology using the multiplication functions. We know that we get at least one representative function from each conjugacy class by considering functions with no memory and a bounded anticipation (theorem 2).

REFERENCES

[AM]   R. L. Adler & B. Marcus. *Topological Entropy and the Equivalence of Dynamical Systems.* Mem. Amer. Math. Soc. 219 (1979).

[P]   L. Pontrjagin. *Topological Groups.* Princeton University Press, 1946.
[R]   W. L. Reddy. Lifting expansive homeomorphisms to symbolic flows. *Math. Sys. Theory* **2** (1968) 91–92.
[Ro]   J. Rotman. *The Theory of Groups, an Introduction.* Allyn and Bacon, Inc., 1973.
[W]   R. F. Williams. Classification of subshifts of finite type. *Ann. of Math.* **98** (1973) 120–153; Errata, *Ann. of Math.* **99** (1974), 380–381.