Ergod. Th. & Dynam. Sys. (1990), **10**, 421–449
Printed in Great Britain

Automorphisms of one-sided subshifts of finite type

MIKE BOYLE

Department of Mathematics, University of Maryland, College Park, Maryland 20742, *USA*

JOHN FRANKS

Department of Mathematics, Northwestern University, Evanston, Illinois 60201, *USA*

AND

BRUCE KITCHENS

IBM Research, Thomas J. Watson Research Center, Yorktown Heights, New York 10598, *USA*

(*Received* 21 *March* 1988 *and revised* 13 *March* 1989)

Abstract. We prove that the automorphism group of a one-sided subshift of finite type is generated by elements of finite order. For one-sided full shifts we characterize the finite subgroups of the automorphism group. For one-sided subshifts of finite type we show that there are strong restrictions on the finite subgroups of the automorphism group.

1. *Introduction*

Let $\{0, \ldots, n-1\}$ be an n point space with the discrete topology. The space of one-sided sequences $\{0, \ldots, n-1\}^{\mathbb{N}} = X_{[n]}$ and the space of two-sided sequences $\{0, \ldots, n-1\}^{\mathbb{Z}} = \Sigma_{[n]}$ with the product topologies are Cantor sets. The shift transformation, σ, is defined on each by $(\sigma(x))_i = x_{i+1}$. In the case of $X_{[n]}$, σ is a continuous, onto, expanding map. In the case of $\Sigma_{[n]}$, σ is an expansive homeomorphism. The dynamical system $(X_{[n]}, \sigma)$ is the *one-sided n shift.* The dynamical system $(\Sigma_{[n]}, \sigma)$ is the (*two sided*) *n shift.* A continuous shift commuting map $\varphi: X_{[n]} \to X_{[n]}$ is a block map. That is, there is a k so that $\varphi(x)_i = \varphi([x_i, \ldots, x_{i+k}])$, where we use φ to denote both a map from $X_{[n]}$ to itself and a map from $\{0, \ldots, n-1\}^k$ to $\{0, \ldots, n-1\}$. In the two sided case there is a k so that $\varphi(x)_i = \varphi([x_{i-k}, \ldots, x_{i+k}])$. Observe that the only difference is that in the one-sided case the map is not allowed to have any 'memory'. This turns out to have very strong consequences. In both cases a homeomorphism that commutes with the shift is called an automorphism. The groups of automorphisms are denoted by Aut $(X_{[n]})$ and Aut $(\Sigma_{[n]})$, respectively. In a fundamental paper [H, 1969] Hedlund showed that Aut $(X_{[2]})$ is isomorphic to $\mathbb{Z}/2$, while Aut $(\Sigma_{[2]})$ contains every finite group. The primary purpose of this paper is to study the structure of Aut $(X_{[n]})$. We show that Aut $(X_{[n]})$ is generated by elements of finite order and characterize the finite subgroups. The first of these results is the one-sided analog of a well known question about the two-sided 2 shift: is Aut $(\Sigma_{[2]})$ generated by elements of finite order and the shift? One of our motivations was questions arising in complex dynamics. These were posed to us by C. McMullen. The results do turn out to have a nice application to the dynamics of the complex polynomials. This is shown in the work of P. Blanchard et al. [**BDK**] and J. Ashley [**A**].

A subshift of finite type is defined by a square, nonnegative integral matrix, **A**, or equivalently by a directed graph. The graph has $A(i,j)$ edges from vertex i to vertex j. Then the one-sided subshift of finite type defined by **A**, X_A, is the set of one-sided infinite walks on the edges of this graph. The two-sided subshift of finite type defined by **A**, Σ_A, is the set of two-sided infinite walks on the edges of this graph. If the matrix is **A**, the directed graph is G_A and the set of edges is E_A, then X_A is the set of $x \in (E_A)^{\mathbb{N}}$ such that the terminal vertex of x_i is the initial vertex of x_{i+1} for all i, and Σ_A is the set of all such $x \in (E_A)^{\mathbb{Z}}$. The shift map will map X_A and Σ_A, onto themselves. Again, an automorphism is a one-to-one and onto block map of X_A or Σ_A to itself. The group of automorphisms of X_A will be denoted by Aut (X_A) and the group of automorphism of Σ_A will be denoted by Aut (Σ_A). Here, we also show that Aut (X_A) is generated by elements of finite order and put strong restrictions on the finite groups that can occur as subgroups of Aut (X_A).

Our methods are an outgrowth of the methods used by R. F. Williams in [**W**]. In [**W**] Williams showed that any conjugacy of a one-sided subshift of finite type can be decomposed into a sequence of elementary conjugacies, introduced the use of the total amalgamation, and in a remarkable theorem (theorem G [**W**]) gave simple necessary and sufficient conditions for two one-sided subshifts of finite type to be conjugate.

This paper is organized as follows.

In § 2 we reprove Williams' classification Theorem 2.11 and examine carefully the structure of the elementary conjugacies. This allows us to show that every automorphism can be written as the composition of two basic types of finite order automorphisms 2.12.

In § 3 we characterize the finite subgroups of Aut $X_{[n]}$.

In § 4 we examine the finite subgroups of the automorphism group of irreducible one-sided subshifts of finite type.

In § 5 we go into a little of the algebraic structure of the automorphism groups of the full shifts.

In § 6 we make a few remarks about homeomorphisms that commute with more general expanding maps.

We have included an Appendix that contains some things we need about finite groups.

We would like to thank Jack Wagoner for many useful comments particularly concerning Theorem 2.12, to thank Bob Gilman for his help on group theory, to thank Curt McMullen and John Smillie for early discussions about these problems and to especially thank Don Coppersmith for discussions throughout the course of this work.

2. *Decomposition of automorphisms*

Given a matrix **A** with a repeated column we may form an *elementary amalgamation*, A_e, of **A** as follows. Suppose **A** has its rows and columns indexed by $\{1, \ldots, n\}$ and its jth column equal to its kth column. Let the rows and columns of A_e be indexed by the numbers 1 through n, except j and k, together with $\{j, k\}$. Then define A_e by

$$\left.\begin{array}{ll} \text{(i)} & A_e(i, i') = A(i, i') \\ \text{(ii)} & A_e(i, \{j, k\}) = A(i, j) = A(i, k) \\ \text{(iii)} & A_e(\{j, k\}, i) = A(j, i) + A(k, i) \\ \text{(iv)} & A_e(\{j, k\}, \{j, k\}) = A(j, j) + A(k, j) = A(j, k) + A(k, k). \end{array}\right\} \tag{2.1}$$

An alternative formulation of this is to let **R** be an $n \times (n-1)$ matrix with rows indexed by 1 through n and columns indexed by 1 through n, minus j and k, together with $\{j, k\}$. Let the ith column of **R** be equal to the ith column of **A** and the $\{j, k\}$th column of **R** be equal to the jth column of **A**. Then let **S** be an $(n-1) \times n$ matrix with the rows and columns indexed in the obvious way: let the ith column, $i \neq j$ or k be all zeros except for a 1 in the ith entry, and the jth and kth columns be all zeros except for a 1 in the $\{j, k\}$th place. Finally, observe that

$$A = RS \quad \text{and} \quad SR = A_e. \tag{2.2}$$

A third and simpler way to arrive at A_e is to add the jth row to the kth row and then delete the jth row and column. Then index the new rows and columns in the natural way.

A matrix such as the **S** just described is called a *subdivision matrix*. That is, a zero-one matrix with no rows all zero and exactly one 1 in each column.

In this terminology, given **A**, an $n \times (n-1)$ matrix **R**, and an $(n-1) \times n$ subdivision matrix **S** with $A = RS$, we say that $SR = A_e$ is an elementary amalgamation of **A**.

A *one-step amalgamation*, **B**, of **A** is defined by finding an $n \times (n-k)$ matrix **R**, $0 \leq k < n$, an $(n-k) \times n$ subdivision matrix **S** with $A = RS$ and letting $SR = B$. Notice that **B** can be obtained from **A** by a sequence of k elementary amalgamations.

A matrix that can be obtained from **A** by a sequence of elementary (or one-step) amalgamations is called an *amalgamation* of **A**.

We define the *total one-step amalgamation*, A_1, of **A** as follows. Suppose there are $n-k$, $0 \leq k < n$, distinct columns in **A**. Let **R** be an $n \times (n-k)$ matrix made up of the $(n-k)$ distinct columns of **A**. Notice that **R** is unique up to right multiplication by a permutation matrix. Any other one is **RP** for some $(n-k)$ permutation matrix **P**, i.e. we are allowed to rearrange the columns. Once **R** is fixed there is a unique $(n-k) \times n$ subdivision matrix **S** so that $A = RS$. Then $A_1 = SR$. If we change **R** by rearranging the columns, taking **RP** instead, then we must rearrange the rows of **S** appropriately, taking $P^{-1}S$. So $A_1 = P^{-1}SRP$. We could have proceeded the other way around, by first choosing an $(n-k) \times n$ subdivision matrix, **S**, whose ith and jth columns agree if and only if the ith and jth columns of **A** agree. We are free up to a rearrangement of the rows of **S**, any other one is **PS** for a permutation matrix **P**. Once **S** is fixed **R** is determined, and $A_1 = SR$. We have proved the following lemma.

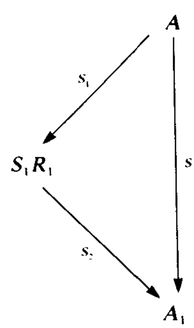
LEMMA 2.3. *Given a square nonnegative integer matrix* **A**, *the total one-step amalgamation*, A_1, *of* **A** *is uniquely determined up to conjugation by a permutation matrix.*

It now makes sense to speak of *the* total one-step amalgamations of a matrix. It is also clear that if we relabel the rows and columns of **A** we still have the same total one-step amalgamations, $(PAP^{-1})_1 = A_1$ when **P** is a permutation matrix. This leads to the following observation.

LEMMA 2.4. (Williams [W].) *Given A, R, S so that* $A_1 = SR$ *is a total one-step amalgamation of* **A** *and* R_1, S_1 *so that* S_1R_1 *is a one-step amalgamation of* **A** *there is a unique subdivision matrix* S_2 *so that* $S_2S_1 = S$. *And then*

$$A = RS = R_1S_1, \quad S_1R_1 = R_2S_2, \quad S_2R_2 = SR = A_1$$

where R_2 *is a uniquely determined matrix containing columns of* S_1R_1.

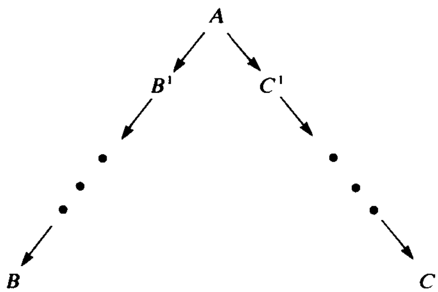


Proof. Notice that both S_1 and **S** have full rank so that both have right inverses. Also, if $\{1, \ldots, n\}$ indexes the vertices of **A**, then S_1 and **S** both define partitions of $\{1, \ldots, n\}$ and the partition defined by S_1 is a refinement of the one defined by **S**. Let S_2 be a matrix with rows indexed by the elements of the partition defined by **S**, columns indexed by the elements of the partition defined by S_1, and put a one in the *ij*th entry if the *j*th element of S_1's partition is contained in the *i*th element of the one defined by **S**. Clearly, S_2 is a subdivision matrix and $S = S_2S_1$. Now because S_1 has a right inverse we see that $A = RS = RS_2S_1 = R_1S_1$ implies that $R_1 = RS_2$. Let $R_2 = S_1R$ so that $S_1R_1 = S_1RS_2 = R_2S_2$ and $S_2R_2 = S_2S_1R = SR = A_1$. □

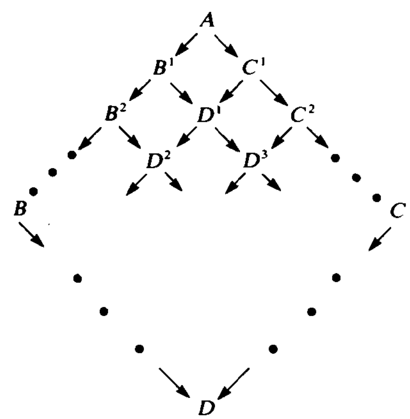
LEMMA 2.5 (Williams [W].) *If* **B** *and* **C** *are amalgamations of a common matrix* **A**, *then they have a common amalgamation* **D**.

https://doi.org/10.1017/S0143385700005678 Published online by Cambridge University Press

Proof. If we have the diagram



where each arrow represents a one-step amalgamation we can use Lemma 2.4 to complete it.



(2.6)

Each new arrow represents a new one-step amalgamation and each D^i is the total one-step amalgamation of the matrix directly above it. For example D^1 is the total one-step amalgamation of **A**. Each D^i is well-defined up to conjugation by a permutation matrix (2.3). □

Given a matrix **A** we can define, A_t, a *total amalgamation of A* to be a matrix that we arrive at by performing amalgamations until we cannot perform any more. We know that two matrices that differ by conjugation by a permutation matrix have the same total one-step amalgamation, up to permutation. This, together with Lemma 2.5 yields the following lemma.

LEMMA 2.7. (Williams [**W**].) *Given a matrix* **A** *the total amalgamation is well-defined up to conjugation by a permutation matrix.*

A square nonnegative integral matrix determines a directed graph and vice versa. For a matrix **A** let G_A denote the directed graph, V_A denote the vertices of G_A, E_A denote the edges of G_A, and $E_A(i, j)$ the edges from the vertex i to the vertex j.

Construction 2.8. Let **A** be an irreducible nonnegative integral matrix and **B** a one-step amalgamation of **A**. This means that we have two matrices **R** and **S**, with **S** a subdivision matrix so that **A** = **RS** and **B** = **SR**. We want to use these equations to define a graph homomorphism from G_A onto G_B, that defines a conjugacy from X_A to X_B with a two block inverse. **S** does two things for us, it defines an equivalence relation on the vertices of G_A, and defines a bijection between the equivalence classes and the vertices of G_B. For $i, j \in V_A$ we say $i \sim j$ if the ith and jth columns of **S** are the same. The equivalence class $[i]$ corresponds to $k \in V_B$ if $S(k, i) = 1$. We may think of the vertices of G_B as being labelled by the equivalence classes. In this notation $B([i], [j]) = \Sigma A(i', j)$, where the sum is over all $i' \in [i]$. The graph homomorphism will be φ. We start by defining it on V_A with $\varphi(i) = [i]$. Let $E_A(i, [j])$ be the union of all $E_A(i, j')$ for $j' \in [j]$, and $E_A([i], [j])$ be the obvious set of edges. For each pair of vertices $i, j \in V_A$, number the edges in $E_A(i, j)$ from 1 to $A(i, j)$. Define an equivalence relation on E_A by saying that two edges are related if they lie in the same $E_A(i, [j])$ and have the same number. Since $A(i, j')$ is the same for each $j' \in [j]$, the number of the edges in the equivalence class is the cardinality of $[j]$. Because we know that $B([i], [j]) = \Sigma A(i', j)$ where the sum is over all $i' \in [i]$, the number of equivalence classes in $E_A([i], [j])$ is $B([i], [j])$. This allows us to define a bijection between the equivalence classes in $E_A([i], [j])$ and the edges in $E_B([i], [j])$. This defines an onto graph homomorphism $\varphi : G_A \to G_B$ in the natural way.

We need to see that this defines the desired map from X_A to X_B. An edge $[e_1] \in E_B([j], [k])$ has cardinality of $[k]$ inverse images. All begin at the same $j' \in [j]$ and exactly one ends at each element of $[k]$. If we have an edge $[e_0] \in E_B([i], [j])$, its inverse images have the same properties so there will be exactly one element of $[e_0]$ that can precede any (in fact all) of the elements of $[e_1]$ in G_A. This shows that φ is onto and tells us how to define a two block inverse from X_B to X_A. Let $\varphi^{-1}([e_0], [e_1])$ be the unique element of $[e_0]$ that can precede the elements of $[e_1]$. Now, $\varphi^{-1} \circ \varphi$ is the identity on X_A.

We say that $\varphi : X_A \to X_B$ or $\varphi^{-1} : X_B \to X_A$ is a *one-step conjugacy*, $\varphi : X_A \to X_B$ is an *amalgamation*, and $\varphi^{-1} : X_B \to X_A$ is a *state splitting*. We say that φ *is compatible with S*, or *with the one-step amalgamation* $A = RS$, $SR = B$, for obvious reasons. If the one-step amalgamation $A = RS$, $SR = B$ is an elementary amalgamation we say that the map φ is an *elementary conjugacy*, and so forth.

We can go the other way. If $\varphi : X_A \to X_{A'}$ is a one-step amalgamation. We can get a one-step amalgamation $A = RS$, $SR = A'$ so that φ is compatible with this one-step amalgamation. If **B** is an amalgamation of **A** obtained by a sequence of one-step amalgamations, $A = R_1S_1$, $S_1R_1 = R_2S_2, \ldots, S_lR_l = B$. We can define a conjugacy $\varphi : X_A \to X_B$ that is *compatible with the amalgamation* by $\varphi = \varphi_l \circ \cdots \circ \varphi_1$ where each φ_i is compatible with S_i. Here φ is a one block map, but generally φ^{-1} will be an $l+1$ block map.

There are two kinds of arbitrary choices made in defining φ. The first is in the numbering of the edges in each $E_A(i, j)$. This numbering determines the equivalence relation on the edges. The second is in the correspondence between the equivalence classes in E_A and the edges in E_B. These two types of choices are reflected in the next lemmas, in Theorem 2.11 and later in Lemma 3.2.

LEMMA 2.9. *Suppose $A = RS$, $SR = B$ is a one-step amalgamation of* **A**, *with φ and $\varphi': X_A \to X_B$ two one-step amalgamations compatible with* **S**. *Then $\varphi = \kappa \circ \varphi' \circ \tau$ where $\kappa: X_B \to X_B$ and $\tau: X_A \to X_A$ are automorphisms defined by graph automorphisms of G_B and G_A, respectively, that fix the vertices.*

Proof. There are two types of choices available in defining a graph homomorphism compatible with **S**. The first is in the numbering of the edges in G_A. There is one numbering for φ and one for φ'. Define τ to be the graph automorphism of G_A that fixes the vertices and takes the numbering for φ to the one for φ'. The second choice available is in defining the correspondence between the equivalence classes of edges in G_A and the edges in G_B. Define κ to be the graph automorphism of G_B that fixes the vertices and changes the correspondence for $\varphi' \circ \tau$ to the correspondence for φ. □

LEMMA 2.10. *Given A, R, S so that $A_1 = SR$ is a total one-step amalgamation of A, R_1, S_1, R_2, S_2 so that $A = RS = R_1S_1$, $B = S_1R_1 = R_2S_2$ is a one-step amalgamation of A, $S_2R_2 = SR = A_1$, $S_2S_1 = S$, and $\varphi_1: X_A \to X_B$ compatible with S_1. There is a $\varphi_2: X_B \to X_{A_1}$ compatible with S_2 so that $\varphi_2 \circ \varphi_1$ is compatible with S. Moreover if we are also given φ compatible with S we may choose φ_2 so that $\varphi = \varphi_2 \circ \varphi_1 \circ \tau$ where $\tau: X_A \to X_A$ is defined by a simple graph automorphism of G_A.*

Proof. We have the diagram of Lemma 2.4 and φ_1 compatible with S_1. The matrices S, S_1, and S_2 define equivalence relations on V_A, V_A and V_B, respectively, which we will denote by $[\bullet]$, $[\bullet]_1$, $[\bullet]_2$. They also define correspondences between the equivalence classes and the vertices of V_{A_1}, V_B, and V_{A_1}, respectively. Notice that $[i] = \bigcup [i']_1$ where the union is over all $[i']_1$ in $[[i]_1]_2$. The map φ_1 comes from an equivalence relation $[\bullet]_1$ on $E_A(i, [j]_1)$, defined by a numbering of each element of $E_A(i, j')$, and a correspondence between the equivalence classes of $E_A([i]_1, [j]_1)$ and the edges in $E_B([i]_1, [j]_1)$.

Label an edge $[e]_1 \in E_B$ by (n, i) where n is the number of each $e' \in [e]_1$ in G_A and i is the beginning vertex in G_A of each $e' \in [e]_1$.

To define φ_2 first define an equivalence relation $[\bullet]_2$ on edges in G_B. Say $[e]_1$ is related to $[e']_1$ if $[e]_1, [e']_1$ are in the same $E_B([i]_1, [[j]_1]_2)$ and they have the same (n, i') label. Now make a one-to-one correspondence between $[\bullet]_2$ classes in $E_B([[i]_1]_2, [[j]_1]_2)$ and edges in

$$E_{A_1}([[i]_1]_2, [[j]_1]_2) = E_{A_1}([i], [j]).$$

The map φ_2 is now well-defined and is compatible with S_2. The map $\varphi_2 \circ \varphi_1$ is defined by the numbering of edges in G_A that defines φ_1 and is compatible with S.

The second assertion follows from Lemma 2.9. If φ is compatible with S, $\varphi = \kappa \circ \varphi_2 \circ \varphi_1 \circ \tau$. But $\kappa \circ \varphi_2$ is just another one-step amalgamation compatible with S_2. □

https://doi.org/10.1017/S0143385700005678 Published online by Cambridge University Press

For X_A we define the *k block presentation*, $X_{A^{[k]}}$ by the graph $G_A^{[k]}$. It has for vertices the allowable k blocks from X_A, and the number of edges from $[x_1, \ldots, x_k]$ to $[y_1, \ldots, y_k]$ is $A(x_k, y_k)$ if $x_{i+1} = y_i$ for $1 \le i < k$, and 0 otherwise.

THEOREM 2.11. (Williams [W].) *Let* **A** *and* **B** *be square, irreducible, nonnegative integral matrices that define one-sided subshifts of finite type X_A and X_B. Then X_A and X_B are topologically conjugate if and only if* **A** *and* **B** *have the same total amalgamations.*

Proof. If **A** and **B** have the same total amalgamations they are topologically conjugate. Let $\varphi: X_A \to X_B$ be a topological conjugacy, φ is a k block map for some k, and φ^{-1} is an l block map for some l. Define a matrix **C** to have states

$$\{([x_0, \ldots, x_{k-1}], [y_0, \ldots, y_{l-1}])\}$$

where there exists $x \in X_A$, $y \in X_B$ with $\varphi(x) = y$. Then $[x_0, \ldots, x_{k-1}]$ is a k block from X_A, $[y_0, \ldots, y_{l-1}]$ is an l block from X_B,

$$\varphi([x_0, \ldots, x_{k-1}]) = y_0 \quad \text{and} \quad \varphi^{-1}([y_0, y_{l-1}]) = x_0.$$

The transitions are the obvious ones obtained by overlapping. That is,

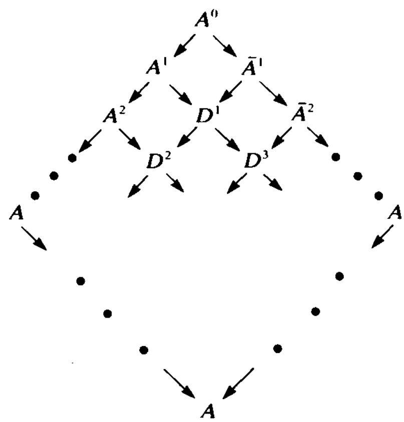
$$([x'_0, \ldots, x'_{k-1}], [y'_0, \ldots, y'_{l-1}])$$

can follow $([x_0, \ldots, x_{k-1}], [y_0, \ldots, y_{l-1}])$ when $x'_i = x_{i+1}$ for $0 \le i < k-1$ and $y'_i = y_{i+1}$ for $0 \le i < l-1$. We need to see that **A** is an amalgamation of **C**. Let $A^{[k]}$ be the k block presentation of **A** and we know **A** is an amalgamation of $A^{[k]}$. Define $A^{(k,r)}$, $0 < r \le l$ to have vertices $\{([x_0, \ldots, x_{k-1}], [y_0, \ldots, y_{r-1}])\}$ where there exists $x \in X_A$, $y \in X_B$ with $\varphi(x) = y$, so $[x_0, \ldots, x_{k-1}]$ is a k block in X_A, $[y_0, \ldots, y_{r-1}]$ is an r block in X_B, $\varphi([x_0, \ldots, x_{k-1}]) = y_0$ and $\varphi^{-1}([y_0, \ldots, y_{l-1}]) = x_0$. Define the obvious overlapping transitions for $A^{(k,r)}$. Notice $A^{[k]} = A^{(k,1)}$, $A^{(k,l)} = C$ and $A^{(k,r)}$ is a one-step amalgamation of $A^{(k,r+1)}$ for $1 < r < l$. This means **A** is an amalgamation of **C**. Similarly, **B** is an amalgamation of **C**. Then by Lemmas 2.5 and 2.7, **A** and **B** have the same total amalgamations. □

If φ is a graph automorphism we define the *first return map* on $E_A(i, j)$ in the obvious way. If G is a group of graph automorphisms we may speak of the *return maps* of G. We single out two special types of automorphisms. A graph automorphism is a *vertex* automorphism if the first return map on $E_A(i, j)$ is the identity for each pair of vertices i and j. A *vertex* automorphism of X_A is an automorphism defined by a vertex automorphism of G_A. A graph automorphism is *simple* if it fixes the vertices. An automorphism φ of X_A is *simple* if it is conjugate to an automorphism φ' of $X_{A'}$ where φ' is defined by a simple graph automorphism of $G_{A'}$ [N]. This idea is useful in understanding the action of automorphisms on the periodic points in two sided shifts [N], [**B**]. Any graph automorphism can be decomposed into a simple graph automorphism followed by a vertex graph automorphism.

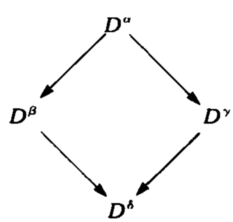
THEOREM 2.12. *The automorphism group of a one-sided subshift of finite type is generated by simple automorphisms and automorphisms defined by vertex automorphisms of the total amalgamation.*

Proof. Let X_A be the one-sided subshift of finite type, where **A** is totally amalgamated, and φ be an automorphism. Define $\mathbf{C} = \mathbf{A}_0$ as in the proof of Theorem 2.11. Complete the diagram as in (2.6).



(2.13)

We need to be slightly careful Examine a single one-step diamond.



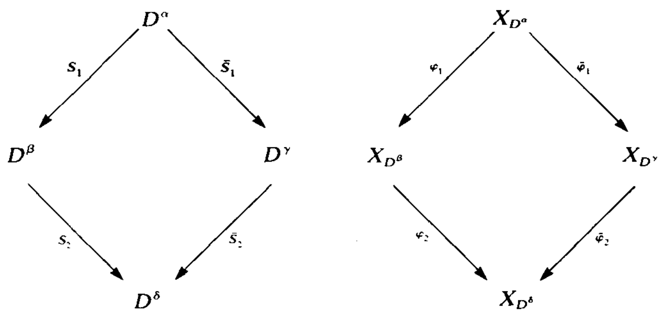
We make sure that D^δ is a total one-step amalgamation of D^α, $D^\alpha = RS$, $SR = D^\delta$ and that $S_2S_1 = \bar{S}_2\bar{S}_1 = S$. This is possible by Lemma 2.4. We want this to be true for all of the one-step diamonds in the diagram (2.13). The matrices down the lower left and right sides of diagram (2.13) are all **A** since they are amalgamations of **A** which is already a total amalgamation. We already have one-step conjugacies $\varphi_i : X_{A^i} \to X_{A^{i+1}}$ and $\bar{\varphi}_i : X_{\bar{A}^i} \to X_{\bar{A}^{i+1}}$ with the appropriate S's that are supplied by the original φ so that

$$\varphi = \bar{\varphi}_r \circ \cdots \circ \bar{\varphi}_0 \circ \varphi_0^{-1} \circ \cdots \circ \varphi_{r-1}^{-1} \circ \varphi_r^{-1}.$$

That is, if we go up the upper left hand side and down the upper right hand side we get φ.

Starting at the top of the diagram and working down we will apply Lemma 2.10 in each one-step diamond to choose compatible one-step conjugacies.

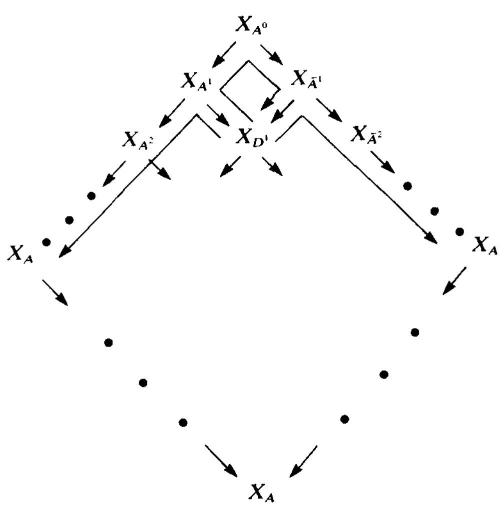
https://doi.org/10.1017/S0143385700005678 Published online by Cambridge University Press



(2.14)

At each stage we have φ_1 and $\bar{\varphi}_1$ defined and compatible with S_1 and $\bar{S}_1$, but φ_2 and $\bar{\varphi}_2$ not yet defined. By Lemma 2.10 we can choose φ_2 so that $\varphi_2 \circ \varphi_1$ is compatible with $S_2S_1 = \bar{S}_2\bar{S}_1$. Then we can choose $\bar{\varphi}_2$ so that $\bar{\varphi}_2 \circ \bar{\varphi}_1$ is compatible with S_2S_1 and so that $\varphi_2 \circ \varphi_1 \circ \tau = \bar{\varphi}_2 \circ \bar{\varphi}_1$ where τ is an automorphism of X_{D^α} that comes from a simple graph automorphism of D^α.

This gives the following diagram.



(2.15)

We have that

$$\bar{\varphi}_2 \circ \bar{\varphi}_1 \circ \varphi_1^{-1} \circ \varphi_2^{-1} = \varphi_2 \circ \varphi_1 \circ \tau \circ \varphi_1^{-1} \circ \varphi_2^{-1}.$$

Let ψ be the conjugacy that goes from X_{D^1} to X_{A^1} and down the left side to X_A. Let $\bar{\psi}$ be the conjugacy that goes from X_{D^1} to $X_{\bar{A}^1}$ and down the right side to X_A. Then

$$\begin{aligned}\varphi &= \bar{\psi} \circ \bar{\varphi}_2 \circ \bar{\varphi}_1 \circ \varphi_1^{-1} \circ \varphi_2^{-1} \circ \psi^{-1} \\ &= \bar{\psi} \circ \psi^{-1} \circ ((\psi \circ \varphi_2 \circ \varphi_1) \circ \tau \circ (\psi \circ \varphi_2 \circ \varphi_1)^{-1}).\end{aligned}$$

So $\bar{\psi} \circ \psi^{-1}$ is an automorphism of X_A, and φ is equal to $\bar{\psi} \circ \psi^{-1}$ preceded by a simple automorphism of X_A. We continue working down the diagram in this way until we get φ equal to an automorphism ξ preceded by a sequence of simple automorphisms, and ξ is the automorphism that is obtained by going down the lower left side of the diagram and up the lower right hand side. At each stage ξ is compatible with a graph automorphism of G_A, so ξ is defined by a graph automorphism of G_A. We know any graph automorphism can be decomposed into a vertex graph automorphism preceded by a simple graph automorphism. This means φ is equal to a vertex automorphism of X_A preceded by a sequence of simple automorphisms. □

The methods used in this proof are an outgrowth of the methods developed by R. F. Williams in [**W**]. In the two sided shift case things are much more complicated because both column and row amalgamations must be used. This means that there is no object equivalent to the total amalgamation. J. Wagoner in [**Wa1, Wa2, Wa3**] has developed a more general approach to use in the two sided setting.

COROLLARY 2.16. *The automorphism group of a one-sided subshift of finite type is generated by elements of finite order.*

LEMMA 2.17. *Let* **A** *be a square nonnegative integral matrix and* **B** *be an amalgamation of* **A** *then the largest entry in* **A** *is less than or equal to the largest entry of* **B**.

Proof. This follows immediately from equation (2.2) and the definition of amalgamation. □

COROLLARY 2.18. *Let X_A be a one-sided subshift of finite type with $A_t = A$ a zero-one matrix. Then the automorphism group of X_A is isomorphic to the group of graph automorphisms of G_A.*

Proof. This follows from Lemma 2.17 and Theorem 2.12 because in Diagram 2.13 all the matrices are zero-one so that there are no non-trivial simple automorphisms. □

Example 2.19. Let

$$A=\begin{bmatrix}0&1&1\\1&0&1\\1&1&0\end{bmatrix}$$

then Aut (X_A) is isomorphic to S_3.

For the Golden Mean,

$$A=\begin{bmatrix}1&1\\1&0\end{bmatrix}.$$

X_A has a trivial automorphism group. This has been shown by C. Jacobson and by W. Parry using different methods.

LEMMA 2.20. *Let $A\neq[n]$ be an irreducible matrix whose total amalgamation is $[n]$, then every entry of* **A** *is strictly less than n.*

Proof. Any matrix arrived at by an elementary state splitting has this property and then we apply Lemma 2.17. □

THEOREM 2.21 (Hedlund [H, Theorem 6.9].) Aut $(X_{[2]})$ *consists of two elements, the identity and the flip map.*

Proof. Lemma 2.20 tells us that any matrix that has [**2**] as its total amalgamation is either a zero-one matrix or [**2**]. This means the only simple automorphism of $X_{[2]}$ is the flip map. This is also the only graph automorphism of $G_{[2]}$, other than the identity. Theorem 2.12 tells us that these two maps generate Aut $(X_{[2]})$. □

Later we will need the following lemma.

LEMMA 2.22. *Suppose* **A** *is an irreducible matrix whose total one-step amalgamation is* $[n]$, *then* **A** *is an* $s\times s$, $s\le n$ *matrix with constant positive rows and column sum n. Moreover,* **A** *is* $n\times n$ *if and only if* **A** *is the matrix of all* 1's.

Proof. Think of G_A. Every vertex i precedes some vertex j. But any other vertex k has $A(i,j)=A(i,k)$. This says that the rows are constant and positive. Since the column sum is n, there must be n or less vertices. The second statement is clear. □

We say an automorphism φ of X_A *fixes vertices* if for any $x\in X_A$ and $i\in\mathbb{N}$, $(\varphi(x))_i$ and x_i have the same initial and terminal vertices.

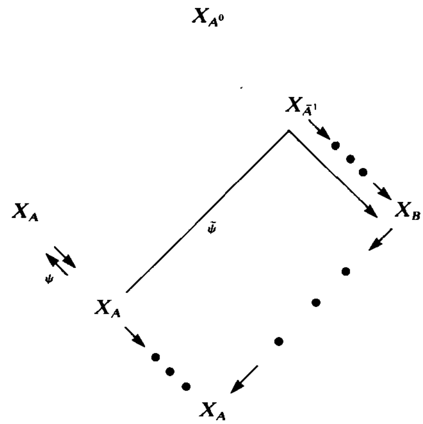
LEMMA 2.23. *Let* **A** *be totally amalgamated and* $\varphi\in$ Aut (X_A). *Then* φ *is a composition of simple automorphisms if and only if it fixes vertices.*

Proof. We make the following observations.
(i) The composition of automorphisms that fix vertices also fixes vertices.
(ii) If $\gamma: X_B\to X_A$ is a conjugacy that is defined by a graph homomorphism from G_B to G_A and τ is an automorphism of X_B that fixes vertices, then $\gamma\circ\tau\circ\gamma^{-1}$ is an automorphism of X_A that fixes vertices. To see this, let $y\in X_A$, and $x=\gamma^{-1}(y)$. The initial and terminal vertices of x_i determine the initial and terminal vertices of y_i. Since τ fixes vertices, $\gamma\circ\tau\circ\gamma^{-1}$ also fixes vertices.

Suppose φ is a simple automorphism of X_A. Then $\varphi=\zeta\circ\omega\circ\zeta^{-1}$, where $\zeta: X_B\to X_A$ is a conjugacy and ω is defined by a simple graph automorphism of X_B. We want to see that φ fixes vertices. We will use induction. Use the construction in the proof of theorem 2.12 to display the conjugacy $\zeta^{-1}: X_A\to X_B$ and define the maps around each one-step diamond. This means φ is obtained by going up the left side of the diamond to X_{A^0} down the right side to X_B, applying ω and then going back the same way to X_A. The induction is on the number of one-step conjugacies from X_{A^0} to X_B. The map φ fixes vertices if the number of these one-step conjugacies is zero because then $X_B=X_{A^0}$, the map from X_{A^0} to X_A is defined by a graph homomorphism, and we can apply observation (ii). Assume the claim is true when there are n of these one-step conjugacies. As in the proof of Theorem 2.12 we have

$$\zeta^{-1}=\bar{\psi}\circ\psi^{-1}\circ((\psi\circ\varphi_2\circ\varphi_1)\circ\tau\circ(\psi\circ\varphi_2\circ\varphi_1)^{-1}).$$

Let $\gamma=\psi\circ\varphi_2\circ\varphi_1$ and $\zeta_1^{-1}=\bar{\psi}\circ\psi^{-1}$. Then γ is compatible with the amalgamations from A^0 to **A** and so is defined by a graph homomorphism. We can apply observation (ii) to conclude that $\gamma\circ\tau\circ\gamma^{-1}$ fixes vertices. We have that $\zeta^{-1}=\zeta_1^{-1}\circ(\gamma\circ\tau\circ\gamma^{-1})$. If $\zeta_1\circ\omega\circ\zeta_1^{-1}$ fixes vertices, then by observation (i), φ fixes vertices. By the same construction we can work our way down the left hand side, picking off the upper left one-step diamonds, until we arrive at the following picture.



(2.24)

The maps are $\zeta_{n+1}^{-1} = \bar{\psi} \circ \psi^{-1}$, $\psi : X_A \to X_A$, and φ fixes vertices if $\zeta_{n+1} \circ \omega \circ \zeta_{n+1}^{-1}$ fixes vertices. The map ψ is defined by a graph automorphism of G_A, so we can apply the observations to reduce to considering $\bar{\psi}^{-1} \circ \omega \circ \bar{\psi}$. By the induction hypothesis, this map fixes vertices, so φ fixes vertices. Conversely, suppose φ is an automorphism that fixes vertices. Apply the proof of Theorem 2.12 to get $\varphi = \varphi_v \circ \varphi_s$ where φ_v is defined by a vertex automorphism of G_A and φ_s is a composition of simple automorphisms. Now φ_s fixes vertices. So $\varphi_v = \varphi \circ \varphi_s^{-1}$, also fixes vertices, which means it is the identity. □

Let Sim (X_A) denote the subgroup generated by the simple automorphisms of X_A.

There are two graphs associated to a directed graph, G_A, that will be useful. The first is the *vertex graph*, G_{A_V}. It has the same vertices as G_A, a single edge from vertex i to vertex j when $A(i,j) > 0$, and no edge from i to j when $A(i,j) = 0$. The *weighted vertex graph* G_{A_W} is the complete graph on the vertices of G_A with the weight $A(i,j)$ on the edge $E_{A_W}(i,j)$.

Let G_A be a directed graph and G_{A_W} be its weighted vertex graph. Let H be the group of graph automorphisms of G_{A_W} that preserve the weights on the edges. H is isomorphic to the group of permutation matrices that commute with A. There is an injective homomorphism of H into Aut (X_A). To see this, for each pair of vertices i and j in G_A number the edges $E_A(i,j)$ from 1 to $A(i,j)$. Then for ρ in H define $\bar{\rho}$ an automorphism of G_A that agrees with ρ on the vertices and preserves the edge labelling in G_A. So $\bar{\rho}$ defines an automorphism of X_A and we let $\bar{H}$ be the image of H in Aut (X_A).

THEOREM 2.25. Sim (X_A) *is a normal subgroup of* Aut (X_A), Aut (X_A)/Sim (X_A) *is a finite group isomorphic to the group of permutation matrices that commute with the total amalgamation of* A *and* Aut (X_A) *is a semi-direct product* Sim $(X_A) \rtimes$ Aut (X_A)/Sim (X_A).

Proof. Sim (X_A) is a normal subgroup because its generators are defined to be a conjugacy invariant set. All we need to see is that the subgroup $\bar{H}$ of Aut (X_A) that we just discussed is complementary to Sim (X_A). By Lemma 2.23 $\bar{H} \cap \text{Sim}(X_A) = \{e\}$ and by Theorem 2.12 any element of Aut (X_A) is a composition of an element of Sim (X_A) and an element of $\bar{H}$. □

Remark 2.26. From the proof of Lemma 2.23 we see that Sim (X_A), for A totally amalgamated, is generated by simple automorphisms of the form $\gamma \circ \tau \circ \gamma^{-1}$, where $\gamma : X_B \to X_A$ is a conjugacy defined by a graph homomorphism, and τ is defined by a simple graph automorphism of G_B. This follows because in the proof we could have continued until the map φ was decomposed into a composition of such maps.

Remark 2.27. Ulf Fiebig has shown by example that a nontrivial element of $\bar{H}$ ($\bar{H}$ as above with A totally amalgamated) can define a simple automorphism of the two sided shift.

3. *Finite subgroups of* Aut $(X_{[n]})$

We begin with two lemmas that apply to any X_A.

LEMMA 3.1. *Let G be a finite subgroup of* Aut (X_A). *Then X_A is conjugate to X_B where each element of G is defined by a graph automorphism of G_B.*

Proof. Let $\mathcal{P}_A$ be the time zero partition of X_A, consider $\mathcal{P}' = \bigvee g(\mathcal{P}_A)$, over all $g \in G$. It is a finite, open-closed partition of X_A. Clearly, if $P_i \in \mathcal{P}'$, then $g(P_i) = P_j$ for some j. For each $x \in X_A$, associate with it, its $(\mathcal{P}', \sigma)$ name. That is, $x' \in (\mathcal{P}')^{\mathbb{N}}$ where $(x')_n$ is the element of $\mathcal{P}'$ that contains $\sigma^n(x)$. There is a conjugacy between (X', σ), where X' is the set of names that arise in this way, and (X_A, σ). Now go to a higher block presentation of X' to get X_B a one step subshift of finite type. Each element of G induces an automorphism of X_B that is defined by a graph automorphism of G_B. □

The next lemma is crucial to the discussion that follows. Intuitively, it says that if G is a group of graph automorphisms with identity return maps, then it 'pushes down' to a conjugate G action on the total one-step amalgamation.

LEMMA 3.2. *Suppose G is a group of graph automorphisms of G_A, and every return map is the identity. Then there is an isomorphism $\psi : G \to G'$, where G' is a group of graph automorphisms of the total one-step amalgamation of* **A**, *and a graph homomorphism $\varphi : G_A \to G_{A_t}$, compatible with the amalgamation. Furthermore, the induced map, $\varphi : X_A \to X_{A_t}$, conjugates the G and G' actions: $\varphi \circ g = \psi(g) \circ \varphi$, for all $g \in G$.*

Proof. As in Construction 2.8, for each pair of vertices $i, j \in V_A$ we will number the edges $E_A(i, j)$ from 1 to $A(i, j)$. We want to do this so that the group G acting on G_A preserves the numbering of the edges. Observe that this is possible if and only if every return map is the identity. That is the hypothesis. Now we proceed exactly as in Construction 2.8 and define a graph homomorphism using this numbering. The equivalence relation on the vertices is clearly preserved by G, and we define G to act on V_{A_t} by $g([i]) = [g(i)]$.

https://doi.org/10.1017/S0143385700005678 Published online by Cambridge University Press

Now we consider the edges. Suppose $e, e' \in [e]$. Then $e \in E_A(i, j)$, $e' \in E_A(i, j')$ for some i and $j' \in [j]$, also the two have the same numbers. For

$$g \in G, \quad g(e) \in E_A(g(i), g(j)), \quad g(e') \in E_A(g(i), g(j')), \quad g(j') \in [g(j)],$$

and the numbers are unchanged. This means G preserves the equivalence relation on E_A. We define the action of G on the edges and so on G_{A_1} in the obvious way. This gives the desired result. □

LEMMA 3.3. *If G is a finite subgroup of* Aut $(X_{[n]})$ *then either:*

(i) *the composition factors of G are all isomorphic to subgroups of S_{n-1}; or*

(ii) *G is isomorphic to a subgroup G' of S_n and has a composition factor that cannot be embedded in S_{n-1}. In this case the action of G on $X_{[n]}$ is conjugate to the action of G' defined by its permutation of the symbols.*

Proof. Use Lemma 3.1 to get an X_A conjugate to $X_{[n]}$ with G acting as a group of graph automorphisms. Let

$$P_A = \{(i, j) \in V_A \times V_A : A(i, j) > 0\}.$$

For each $(i, j) \in P_A$ number the edges in $E_A(i, j)$ from 1 to $A(i, j)$. We know by Lemma 2.20 that either all $A(i, j) < n$ or we are done. We will think of E_A as a subset of $\{1, \ldots, n-1\} \times P_A$. Define a homomorphism $\nu_1 : G \to S_{P_A}$ in the natural way. Let $G_1 = \nu_1(G)$. Define another homomorphism $\varepsilon_1 : G \to S_{n-1}^{P_A} \rtimes G_1$ by $g(r, (i, j)) = (\gamma_{(i,j)}(r), \bar{g}(i, j))$ where $\gamma \in S_{n-1}^{P_A}$ so that $\gamma_{(i,j)}(r)$ agrees with g if $r \leq A(i, j)$, $\gamma_{(i,j)}(r) = r$ if $r > A(i, j)$, and $\bar{g} = \nu_1(g)$. This is an embedding. The projection map $\pi_1 : S_{n-1}^{P_A} \rtimes G_1 \to G_1$ gives $\nu_1 = \pi_1 \circ \varepsilon_1$. Let $K_1 = \ker \nu_1 \simeq \ker \pi_1 = (S_{n-1}^{P_A} \times \{1\}) \cap \varepsilon_1(G)$. Since K_1 is isomorphic to a subgroup of $S_{n-1}^{P_A}$, by Lemma A.10 it has all its composition factors isomorphic to subgroups of S_{n-1}. Now, we have

$$1 \to K_1 \to G \to G_1 \to 1.$$

Next we see that G_1 can act on G_A, by taking its action on P_A and preserving the edge numbering on G_A. By Lemma 3.2, G_1 induces a conjugate G_1 action on the total one-step amalgamation of G_A. As before, define a homomorphism $\nu_2 : G_1 \to S_{P_{A_1}}$, take $G_2 = \nu_2(G_1)$, and define the other homomorphisms $\varepsilon_2 : G_1 \to S_{n-1}^{P_{A_1}} \rtimes G_2$, and $\pi_2 : S_{n-1}^{P_{A_1}} \rtimes G_2 \to G_2$. Define $K_2 = \ker \nu_2$. Everything is done just as before. This gives

$$1 \to K_2 \to G_1 \to G_2 \to 1,$$

where $K_2 = \ker \nu_2$ has all of its composition groups isomorphic to subgroups of S_{n-1}. Continue in this manner until reaching a matrix B whose total one-step amalgamation is $[n]$. It is acted on by G_l with identity return maps and we have

$$G \xrightarrow{\nu_1} G_1 \xrightarrow{\nu_2} \cdots \xrightarrow{\nu_{l-1}} G_{l-1} \xrightarrow{\nu_l} G_l,$$

where each ν_i is onto and each K_i has all of its composition factors isomorphic to subgroups of S_{n-1}.

By Lemma 2.22 there are two cases:

(a) **B** is $s \times s$ for some $s < n$;

(b) **B** is the $n \times n$ matrix of all 1's.

In case (a), G_l is determined by its action on V_B and is isomorphic to a subgroup

https://doi.org/10.1017/S0143385700005678 Published online by Cambridge University Press

of S_{n-1}. Then by observation A.3, G has all its composition factors isomorphic to subgroups of S_{n-1}. In case (b), all the matrices from **A** down to **B** are zero-one matrices. This means that $K_i \simeq \{1\}$, for all i, and $G \simeq G_l$. But, G_l is determined by its action on V_B and so is isomorphic to a subgroup G' of S_n. Moreover, the action of G has been conjugated to the action defined by G''s permutations of the symbols. □

Definition 3.4. For convenience, we define the following groups: $Z_n^1 = S_n$, and

$$Z_n^{k+1} = S_n^{\{1,\dots,n\}^k} \rtimes Z_n^k \simeq (Z_n^k)^{\{1,\dots,n\}} \rtimes S_n,$$

as in discussion A.4.

Construction 3.5. Here we will describe a way of embedding certain finite groups into Aut $(X_{[n]})$. There are two ideas involved, one is the idea of a 'marker' and the other is the idea of 'carrying to the left'. Both ideas will become clear in the course of the discussion. Begin by numbering the symbols 0 through $n-1$. Consider Z_{n-1}^2. For (γ, g), in this group, define an automorphism by

$$((\gamma, g)(x))_i = \begin{cases} g(x_i) & \text{if } x_i \neq 0 \quad \text{and} \quad x_{i+1} = 0 \\ \gamma_{(x_{i+1})}(x_i) & \text{if } x_i, x_{i+1} \neq 0 \quad \text{and } x_{i+2} = 0 \\ x_i & \text{otherwise.} \end{cases}$$

This embeds Z_{n-1}^2 into Aut $(X_{[n]})$. In this case 0 is the marker and we carry once to the left unless blocked by a 0. We think of the symbols $1, \dots, n-1$, that have the possibility of being changed by (γ, g), as 'digits'. It is not hard to see that we can similarly embed the group Z_{n-1}^3. Simply use 0 as a marker and carry to the left twice unless blocked by a 0. A 0 stops the carry. We can keep this procedure up and we will be able to embed any Z_{n-1}^k.

For our purposes it simplifies things to see that the wreath products of S_{n-1} with itself, the W_{n-1}^k's of Definition A.7 can be embedded as a special case of this construction. Consider $W_{n-1}^2 = S_{n-1}^{S_{n-1}} \rtimes S_{n-1}$. We will consider an $(n-1)$-tuple of elements of $\{1, \dots, n-1\}$ with no repeats as an element of S_{n-1}. If $(x_1, \dots, x_{n-1}) \in \{0, \dots, n-1\}^{n-1}$ has no 0's and no repeats, we will say that it is an element of S_{n-1}. For $(\gamma, g) \in W_{n-1}^2$ we define an automorphism by

$$((\gamma, g)(x))_i = \begin{cases} g(x_i) & \text{if } x_i, x_{i+1}, \dots, x_{i+k} \neq 0 \text{ and } x_{i+k+1} = 0 \quad \text{for } 0 \le k \le n-2 \\ \gamma_{(x_{i+1},\dots,x_{i+n-1})}(x_i) & \text{if } (x_{i+1}, \dots, x_{i+n-1}) \in S_{n-1},\ x_{i+n} = 0, \quad \text{and } x_i \neq 0 \\ x_i & \text{otherwise.} \end{cases}$$

This is clearly a special case of the previous construction. We use induction to embed W_{n-1}^{k+1}. Let $(\gamma, g) \in W_{n-1}^{k+1} = W_{n-1}^k wr S_{n-1}$ act by using 0 as a marker, having g act as above on the $n-1$ symbols $(i_1, \dots, i_{n-1})$, preceding a 0, and $\gamma_{(i_1,\dots,i_{n-1})}$ act on the $(n-1)^k + 1$ symbols preceding $(i_1, \dots, i_{n-1}, 0)$ as it was defined to do above (it thinks of $(i_1, \dots, i_{n-1}, 0)$ as its marker). This allows us to embed all the W_{n-1}^k's in Aut $(X_{\{n\}})$.

Corollary 3.6. *$W_n^k \subseteq Z_n^l$ for some l.*

Example 3.7. The simplest example of this kind of construction can be found in

https://doi.org/10.1017/S0143385700005678 Published online by Cambridge University Press

[**H**, p. 335]. For $X_{[3]}$ define φ_0 by:

$$(\varphi_0(x))_i = \begin{cases} 1 & \text{if } x_i = 2 \quad \text{and } x_{i+1} = 0 \\ 2 & \text{if } x_i = 1 \quad \text{and } x_{i+1} = 0 \\ x_i & \text{otherwise.} \end{cases}$$

We can also define φ_1 and φ_2 in a similar manner but using 1 and 2 as markers, respectively.

THEOREM 3.8. *A finite group G is isomorphic to a subgroup of* Aut $(X_{[n]})$ *if and only if either*:

(i) *it is isomorphic to a subgroup G' of S_n that has a composition factor that cannot be embedded in S_{n-1}. In this case its action on $X_{[n]}$ must be conjugate to the action of G' defined by its permutation of the symbols*; *or*

(ii) *all its composition factors are isomorphic to subgroups of S_{n-1}.*

Proof. The only if part of the statement is Lemma 3.3. The converse follows from Construction 3.5 where we show how to embed W^k_{n-1} into Aut $(X_{[n]})$, for all k and from the characterization of the subgroups of the W^k_{n-1}'s in proposition A.11. □

COROLLARY 3.9. *If φ is an automorphism of the full n shift with finite order, and n is not prime. Then it has order $p_1^{e_1} \cdots p_l^{e_l}$ for primes $p_i < n$ and $e_i \in \mathbb{Z}^+$. Moreover, all of these orders occur.*

COROLLARY 3.10. *If φ is an automorphism of the full p shift with finite order, and p is prime. Then it has order $p_1^{e_1} \cdots p_l^{e_l}$ for primes $p_i < p$ and $e_i \in \mathbb{Z}^+$ or it has order p in which case it is conjugate to a rotation. Moreover, all of these orders occur.*

COROLLARY 3.11. *A finite group is isomorphic to a subgroup of* Aut $(X_{[3]})$ *if and only if it is $\mathbb{Z}/3$, S_3, or the order of every element is a power of* 2 (*it is a* 2-*group*).

An action of a group on a set is said to be *primitive* if there are no nontrivial invariant partitions of the set.

PROPOSITION 3.12. *Suppose G is a finite subgroup of* Aut $(X_{[n]})$ *and G's action on the fixed points* (*under the shift*) *of $X_{[n]}$ is primitive. Then G is isomorphic to a subgroup G' of S_n and the action of G is conjugate to the action of G' defined by its permutation of the symbols.*

Proof. Consider the proof of Lemma 3.3. We have that G_l is acting on a matrix **B** that is not $[n]$ but whose total one-step amalgamation is. There are two cases, (a) and (b). Suppose we are in case (a). Using **B** we can define a partition of the fixed points of $X_{[n]}$. Just partition the points according to the vertices of G_B where their loops occur. This partition is invariant under G_l. It must therefore be invariant under the entire action of G. This means that if G acts primitively on the fixed points, we must be in case (b). □

4. *Finite subgroups of* Aut (X_A)

In this section we generalize results of § 3 to arbitrary irreducible shifts of finite type, X_A. We let H denote the group of graph automorphisms of G_{A_W} that preserve the weights on edges. We say X_A is a *tower over the n shift* if $\mathbf{A}$ is a cyclic permutation matrix with one of the nonzero entries replaced by n. It is easy to verify for such $\mathbf{A}$ that $\mathrm{Aut}(X_A) \simeq \mathrm{Aut}(X_{[n]})$.

THEOREM 4.1. *Suppose $\mathbf{A}$ is a totally amalgamated irreducible matrix and X_A is not a tower over the n shift. Let M be the maximum entry of $\mathbf{A}$. Then a finite group embeds into $\mathrm{Sim}(X_A)$ if and only if all its composition factors are isomorphic to subgroups of S_M. Every finite subgroup of $\mathrm{Aut}(X_A)$ is isomorphic to an extension of such a group by a subgroup of H.*

Proof. To see the necessity we use the same proof as for Lemma 3.3. We display the group G as acting as a group of graph automorphisms and then start dividing out normal subroups which have composition factors that are isomorphic to subgroups of S_M. We do this until we arrive at

$$G \to G_1 \to \cdots \to G_l,$$

where G_l is a group of graph automorphisms of the total amalgamation of $\mathbf{A}$ with identity return maps, and the kernel of the map $G \to G_l$ is a subgroup of $\mathrm{Sim}(X_A)$ and has all its composition factors isomorphic to subgroups of S_M. The group G_l is isomorphic to a subgroup of H.

The required embeddings of finite groups will be done by cases below. □

Theorem 4.1 does not determine all the finite subgroups of $\mathrm{Aut}(X_A)$. Below, we will determine the cyclic subgroups. We say an irreducible matrix $\mathbf{A}$ is *atypical* of type (k, M, n) if $\mathbf{A}$ is $k \times k$, n divides k, and after conjugation by some permutation matrix $\mathbf{A}$ has the form

$$A(i,j) = \begin{cases} 0 & \text{if } j \neq i+1 \text{ modulo } k \\ M & \text{if } j = i+1 \text{ modulo } k \text{ and } n \text{ divides } i \\ 1 & \text{if } j = i+1 \text{ modulo } k \text{ and } n \text{ does not divide } i. \end{cases}$$

For example, a matrix atypical of type (k, M, n) with $k = n$ defines a tower over the M shift. A matrix is *typical* if it is not atypical.

PROPOSITION 4.2. *Suppose A is a typical totally amalgamated irreducible matrix with maximum entry M. If a finite group G has all its composition factors isomorphic to subgroups of S_M, then G is isomorphic to a subgroup of $\mathrm{Sim}(X_A)$, and $H \oplus G$ is isomorphic to a subgroup of $\mathrm{Aut}(X_A)$. The group $\mathbb{Z}/n$ embeds into $\mathrm{Aut}(X_A)$ if and only if $n = pq$ where p is the order of an element of H and $q = p_1^{e_1} \cdots p_r^{e_r}$ where $p_1, \ldots, p_r$ are the primes less than or equal to M.*

By Corollary 3.6 we may assume the group G is in Z_M^k, for some k in $\mathbb{N}$. G is a group of permutations on the set $\{1, \ldots, M\}^k$; we write an element of this set as a word $w = w_1 \cdots w_k$ on symbols $\{1, \ldots, M\}$. Given g in G and $1 \leq j \leq k$, there is a function $g_j : \{1, \ldots, M\}^{k-j+1} \to \{1, \ldots, M\}$ such that for all w, $(gw)_j = g_j(w_j \cdots w_k)$. We choose a numbering of the edges in G_A and define $\bar{H}$ as in Theorem 2.25. We let π_V denote the projection of G_A onto its vertex graph G_{A_V}.

Case I. G_{A_V} is not cyclic.

Choose j, j' such that $A(j, j') = M$. Choose an edge a from j to j'. If $j \neq j'$, then choose a path $U = U_1 \cdots U_{l-1}$ of minimal length from j' to j (now aU is a simple cycle). If $j = j'$, then below U is the empty word. Choose a word W beginning at j', of minimal positive length n such that U_n and W_n do not have the same terminal vertex. Because G_{A_V} is not cyclic, W exists with $1 \leq n < l$.

Now, given $g \in G$, we define $\bar{g}: X_A \to X_A$. Suppose $x \in X_A$, $1 \leq j \leq k$ and for some i and r

$$x_i \cdots x_{i+r} = a_j U^{(j)} a_{j+1} U^{(j+1)} \cdots a_k U^{(k)} a_{k+1} W', \tag{4.3}$$

where the a_t are symbols, the $U^{(t)}$ are words of length $l-1$, W' is a word whose length equals that of W, and for some $h \in H$

$$(\pi_V \circ h)(x_i \cdots x_{i+r}) = \pi_V((aU)^k a W).$$

Let $\eta(a)$ denote the numbering of an edge a. Then we define $(\bar{g}x)_i$ to be the unique edge a whose initial and terminal vertices agree with x_i and whose numbering is $\eta(a) = g_j(\eta(a_j) \cdots \eta(a_k))$. Otherwise $(\bar{g}x)_i = x_i$. Distinct words of the form (4.3) can overlap in at most l symbols. Therefore the map $g \mapsto \bar{g}$ is a well-defined isomorphism onto some subgroup $\bar{G}$ of Aut (X_A). By Lemma 2.23, $\bar{G} \subseteq$ Sim (X_A). By construction, the actions of $\bar{H}$ and $\bar{G}$ commute, so $\bar{H} \oplus \bar{G} \subseteq$ Aut (X_A). This proves sufficiency of the condition for embedding $\mathbb{Z}/n$ into Aut (X_A), and necessity follows from Theorem 4.1.

Case II. G_{A_V} is cyclic.

Suppose G_A has L vertices. Number these so that $A(i, j) > 0$ if and only if $j = i+1$ modulo L and also $A(L, 1) = M$. Because **A** is typical, there exists n with $1 \leq n < L$ such that $H \simeq \mathbb{Z}/n$. Let $L = nr$, so $A(i, j) = M$ if r divides i and $j = i+1$ modulo L. Because **A** is typical, there exists t such that $1 \leq t < r$ and $A(i, j) > 1$ if r divides $i - t$ and $j = i+1$ modulo L. We consider paths in G_A of the special form

$$a_j V^{(j)} a_{j+1} V^{(j+1)} \cdots a_k U, \tag{4.4}$$

where $1 \leq j \leq k$, each a_t is a symbol whose initial vertex i is divisible by r, each $V^{(t)}$ is a path of length $r-1$ all of whose edges are numbered 1, and U is a word of length less than r with an edge which is not numbered 1. Words of the form (4.4) replace the words (4.3) in Case I, and then the arguments of Case I (in a more transparent form) go through. □

We now turn to the 'atypical' shifts. We will only outline the proofs for this rather special but somewhat intricate case.

PROPOSITION 4.5. *Suppose* $\mathbf{A} = M\mathbf{P}$ *where* $M \in \mathbb{N}$ *and* $\mathbf{P}$ *is a cyclic permutation matrix of order* $k > 1$.

(1) *If* G *is a finite group with all composition factors isomorphic to subgroups of* S_M, *then* G *is isomorphic to a subgroup of* Sim (X_A).

(2) $\mathbb{Z}/n$ *embeds into* Aut (X_A) *if and only if* n *has one of the following forms*:

 (i) $n = rq$, *where* $q \mid k$ *and* $r = p_1^{e_1} \cdots p_r^{e_r}$, $p_1, \ldots, p_r$ *are the primes less than or equal to* $M-1$;

https://doi.org/10.1017/S0143385700005678 Published online by Cambridge University Press

(ii) $n = rq$, *where* $q | k$, $q \neq k$ *and* $r = p_1^{e_1} \cdots p_r^{e_r}$, $p_1 \cdots, p_r$ *are the primes less than or equal to* M;

(iii) $n = Mk$.

Proof. Constructions for (1), (2i) and (2ii) are easy variations on Theorem 4.2. To check necessity of the conditions on n in (2), consider a vertex automorphism R of X_A of order k. Verify Cent $(R) \simeq$ Aut $(X_M) \oplus \mathbb{Z}/k$, where Cent (R) is the centralizer of R in Aut (X_A). Reduce to the case M prime and k relatively prime to $M!$. Then any element of order k in Aut (X_A) is conjugate to R. Therefore a cyclic group with order divisible by k is conjugate to one in Cent (R), and a cyclic group of order divisible by Mk has order equal to Mk since any finite subgroup of Aut (X_M) of order divisible by M is isomorphic to $\mathbb{Z}/M$. □

PROPOSITION 4.6. *Suppose A is atypical of type* (k, M, n). *Let* **P** *be a cyclic permutation matrix of order* k/n. *Then* Aut $(X_A) \simeq$ Aut (X_{MP}).

Proof. Exercise. □

5. *More algebraic structure*

PROPOSITION 5.1. *If* $n > 2$, Aut $(X_{[n]})$ *is not finitely generated.*

Proof. We will define a homomorphism from Aut $(X_{[n]})$ onto a direct sum of k copies of $\mathbb{Z}/2$, for every k. This will mean that Aut $(X_{[n]})$ must have at least k generators and so is not finitely generated.

Number the symbols 0 through $n-1$. Each automorphism defines a permutation on the points of $X_{[n]}$ fixed by the shift. Map the automorphism to the sign of this permutation. This maps Aut $(X_{[n]})$ onto $\mathbb{Z}/2$. It is onto because the automorphism that sends the symbol 0 to 1, 1 to 0, and fixes the other symbols, has sign one.

For the next step, send an automorphism to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ by sending it to the sign of its permutation on the (shift) fixed points on the first coordinate, and to the sign of its permutation of the (shift) orbits of period two on the second coordinate. To see this is onto, observe that the automorphism previously described goes to $(1, x)$ for some x. Now take the automorphism that uses 2 for a marker and interchanges 0 and 1 when they immediately precede a 2. Otherwise, it is the identity. This gets sent to $(0, 1)$, so the map is onto.

At each successive stage do the same, working up in the periods of (shift) periodic points. At the nth stage the map that uses $n-1$ 2's as a marker, permutes 0 and 1 when they precede it, and is the identity otherwise, gets mapped to $(0, \ldots, 0, 1)$. □

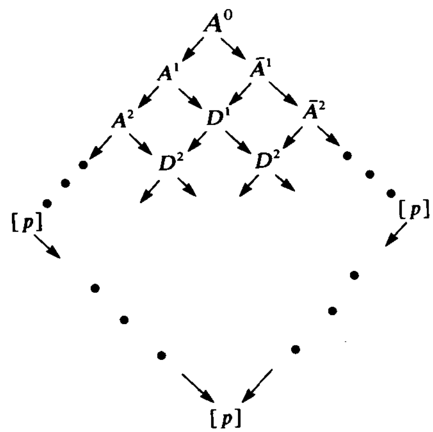
LEMMA 5.2. *If* $\mathbf{A} \neq [n]$, $\mathbf{A}_t = [n]$ *and* G *is a group of graph automorphisms of* G_A *containing a simple subgroup that cannot be embedded in* S_{n-1}, *then* **A** *is a zero-one matrix.*

Proof. Since G contains a simple subgroup that cannot be embedded in S_{n-1}, by Corollary A.14 G cannot be embedded in any W_{n-1}^k. Then we go back to the proof of Lemma 3.3. It means that when we push down to the matrix **B**, we are in case (b). So, **B** and **A** are zero-one matrices. □

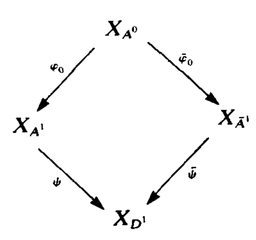
https://doi.org/10.1017/S0143385700005678 Published online by Cambridge University Press

PROPOSITION 5.3. *If φ is an automorphism of the one sided p shift, for p prime, that commutes with a rotation then it is a power of that rotation.*

Proof. Begin as in the proof of Theorem 2.12, building a matrix diamond that displays φ.



As in that proof we already have one-step conjugacies $\varphi_i : X_{A^i} \to X_{A^{i+1}}$ and $\bar{\varphi}_i : X_{\bar{A}^i} \to X_{\bar{A}^{i+1}}$. By the definition of these, ρ defines a graph automorphism of each G_{A^i} and $G_{\bar{A}^i}$ that commutes with each φ_i and $\bar{\varphi}_i$. Since ρ generates a simple subgroup of S_p Lemma 5.2 says that each A^i and $\bar{A}^i$ is either a zero-one matrix or $[p]$. If A^0 is $[p]$ then A^1, $\bar{A}^1$, and D^1 are all $[p]$. This means we can choose $\psi : G_{A^1} \to G_{D^1}$ and $\bar{\psi} : G_{\bar{A}^1} \to G_{D^1}$ so that $\psi \circ \varphi_0 = \bar{\psi} \circ \bar{\varphi}_0$. Then both ψ and $\bar{\psi}$ will induce the same action of ρ on G_{D^1}. We can summarize this by saying that the entire little diamond



commutes with ρ.

If A^0 is zero-one then by Lemma 3.2 there is a map $\gamma : G_{A^0} \to G_{D^1}$ that induces a ρ action on G_{D^1}. By Lemma 2.10 we may choose a map $\psi : G_{A^1} \to G_{D^1}$ so that $\gamma = \psi \circ \varphi_0$. The map ψ will commute with ρ since both γ and φ_0 do. We may do the same for $G_{\bar{A}^1}$ with $\psi \circ \varphi_0 = \bar{\psi} \circ \bar{\varphi}_0$. This again results in a small diamond that commutes with ρ.

We may work our way down the diagram defining the maps so that ρ acts on every graph and commutes with every map. Each matrix that occurs in the diagram is either a zero-one matrix or the matrix $[p]$. Since there are no simple graph automorphisms of graphs defined by zero-one matrices, we see from the proof of Theorem 2.12 that φ is defined by a graph automorphism of $G_{[p]}$ that commutes with ρ, a rotation of this graph. The only permutations in S_p that commute with a cyclic permutation of order p are powers of that rotation. □

Observation 5.4. For n not prime, the centralizer of a rotation is infinite in Aut $(X_{[n]})$.

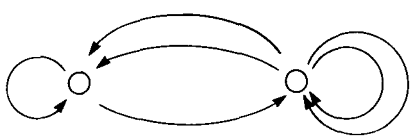
Proof. Suppose $n = k \times l$. Define ψ_1 as follows:

$$(\psi_1(x))_i = \begin{cases} x_i + k \text{ modulo } n & \text{if } x_i - x_{i+1} = 0 \text{ modulo } k \\ x_i & \text{otherwise.} \end{cases}$$

This commutes with the usual rotation. We can define ψ_t, for $t > 1$, similarly by considering the sum $x_i + x_{i+t}$ instead of the sum $x_i + x_{i+1}$. □

Next we will discuss some of the algebraic structure of Aut $(X_{[3]})$. Some of the ideas come from Hedlund's proof [H] that the only automorphisms of the one sided two shift are the identity and the flip (Theorem 2.21).

For $i = 0, 1, 2$ let G_i be the subgroup of Aut $(X_{[3]})$ made up of the automorphisms that always fix the symbol i. That is, $\varphi \in G_i$ when $(\varphi(x))_t = i$ if and only if $x_t = i$, for all t and x. If $i \neq j$, $G_i \cap G_j = \{1\}$. By Theorem 2.12 the simple automorphisms generate Aut $(X_{[3]})$ and every simple automorphism is obtained from a simple graph automorphism. $\langle G_0, G_1, G_2 \rangle$ contains the simple automorphisms obtained from graph automorphisms of $G_{[3]}$. The simple automorphisms obtained from any other graph must lie completely inside one G_i. This follows because if we split [3] into a two by two matrix we will have the following picture.



The two single edges will have the same label, say i. And, the sets of parallel edges will each have the other two labels. Any simple automorphism obtained from a graph automorphism of this graph will be an element of G_i. The same will be true of any automorphism coming from a split of this graph. This means $\langle G_0, G_1, G_2 \rangle =$ Aut $(X_{[3]})$. It is not a free product, but it is close. Let π : Aut $(X_{[3]}) \to$ {permutations of the fixed points} be the homomorphism defined by restriction. Let $F = \ker \pi$, and $F_i = F \cap G_i$. So the F_i are isomorphic and Aut $(X_{[3]}) \simeq F \rtimes S_3$. We want to prove that F is the free product of the F_i.

We say that the *coding length* of an automorphism, φ, is the minimal number l so that $[x_0, \ldots, x_{l-1}]$ determines $(\varphi(x))_0$, for all x. Observe that an automorphism is *left permutive*, which means that if φ is the automorphism of coding length l then

$$(\varphi([i, x_1, \ldots, x_{l-1}]))_0 = (\varphi([j, x_1, \ldots, x_{l-1}]))_0 \quad \text{if and only if } i = j.$$

Otherwise, φ could not be one-to-one. Let $w = [w_0, \ldots, w_{n-1}]$ be a word of length $n \geq l$. We will denote by $\varphi(w)$ the $n - l + 1$ block that is the image of w.

LEMMA 5.5. *If $\varphi \in G_0$ and has coding length $l > 1$, then for any word w of length $l-1$ $\varphi(w1) = \varphi(w2)$.*

Proof. Let $\mathcal{M} = \{m \in \mathbb{N}: m \geq l-1$ and $\exists$ words w_1, w_2 of length m, with $\varphi(1w_1) = \varphi(2w_2)\}$. $\mathcal{M}$ contains $l-1$ because we know we can find a word w of length $l-1$ beginning with either a 1 or 2, and symbols a and b so that $\varphi(wa) \neq \varphi(wb)$, and neither are 0. This is because φ is in G_0, and $(\varphi(w))_0 = 0$ if and only if $w_0 = 0$. Suppose $w_0 = 1$, then let $\bar{w}$ be the same word as w except beginning with a 2. Then since φ is left permutive $\varphi(wa) = \varphi(\bar{w}b)$ and $l-1$ is in $\mathcal{M}$. Let M be the largest element of $\mathcal{M}$. This must exist or by compactness φ is not one-to-one. Let w_1 and w_2 be two words of length M so that $\varphi(1w_1) = \varphi(2w_2)$. By the maximality of M, $\varphi(11w_1) \neq \varphi(22w_2)$. Since $\varphi(01w_1) = \varphi(02w_2)$, and φ is left permutive, $\varphi(a1w_1) = \varphi(a2w_2)$ for $a = 0, 1, 2$. By repeating this reasoning we see that for any word ν of length $l-1$, $\varphi(\nu 1 w_1) = \varphi(\nu 2 w_2)$. □

LEMMA 5.6. *Let $a_n \cdots a_1 = a$ be a word on $\{0, 1, 2\}$ with no symbol occurring next to itself. For each t let φ_{a_t} be an element of G_{a_t} with coding length $l_t > 1$. Then $\varphi_a = \varphi_{a_n} \circ \cdots \circ \varphi_{a_1}$ has coding length $L = l_1 + \sum_{t=2}^{n} (l_t - 1)$ (i.e. the maximal possible).*

Proof. We prove this by induction on n in the following proposition: there is a word w of length $L-1$ and symbols α, β such that $a_n \neq \varphi(w\alpha) \neq \varphi(w\beta) \neq a_n$. For $n = 1$ this is immediate. Now we induct. Suppose the assertion is true for $n-1$. Let $\Phi = \varphi_{a_{n-1}} \circ \cdots \circ \varphi_{a_1}$. We have a word w of length $L-1$ and symbols α and β so that $\Phi(w\alpha) = a_n$, $\Phi(w\beta) = b$, $a_n \neq b$, and neither are a_{n-1}. By Lemma 5.5 we can also choose a word ν of length $l_n - 1$, such that $\varphi_{a_n}(\nu a_n)$, $\varphi_{a_n}(\nu b)$ are distinct and not a_n. Because Φ is left permutive we may choose a word u so that $\Phi(uw\alpha) = \nu a_n$, and $\Phi(uw\beta) = \nu b$. This means $\varphi_{a_n} \circ \Phi(uw\alpha)$, $\varphi_{a_n} \circ \Phi(uw\beta)$ are distinct symbols with neither equal to a_n. □

The next proposition follows immediately from the previous lemma.

PROPOSITION 5.7. *F is the free product of F_0, F_1, and F_2.*

PROPOSITION 5.8. Aut $(X_{[3]})$ *is isomorphic to a subgroup of* Aut $(X_{[n]})$ *for all $n > 2$.*

Proof. Recall the notation from the preceding discussion about Aut $(X_{[3]})$ and the G_i's. There is one simple automorphism in G_i that comes from the graph of [3]. It has order two. Every other simple automorphism in G_i comes from an automorphism of a different graph and must have order two. Let $\varphi \in F_0$ be a simple automorphism. It has order two and all such automorphisms generate F_0. Define $\pi_0: X_{[n]} \to X_{[3]}$ by:

$$(\pi_0(x))_i = \begin{cases} 1 & \text{if } x_i = 1 \\ 2 & \text{if } x_i = 2 \\ 0 & \text{otherwise.} \end{cases}$$

Define $\hat{\varphi}: X_{[n]} \to X_{[n]}$ by:

$$(\hat{\varphi}(x))_i = \begin{cases} x_i & \text{if } x_i \neq 1, 2 \\ (\varphi \circ \pi_0(x))_i & \text{if } x_i = 1, 2. \end{cases}$$

This defines an order two automorphism of $X_{[n]}$ and we have the following commutative diagram:

$$\begin{array}{ccc} X_{[n]} & \xrightarrow{\hat{\varphi}} & X_{[n]} \\ \downarrow{\scriptstyle \pi_0} & & \downarrow{\scriptstyle \pi_0} \\ X_{[3]} & \xrightarrow{\varphi} & X_{[3]} \end{array}$$

Do this for every simple automorphism in F_0 and let $\hat{F}_0$ be the group they generate in Aut $(X_{[n]})$. We have a set of generators for F_0, one for $\hat{F}_0$, and a bijection between them. It is easy to see that a word on these generators in F_0 is the identity if and only if the corresponding word is the identity in $\hat{F}_0$. This means the two are isomorphic.

Make the same construction to get $\hat{F}_1$, and $\hat{F}_2$. Observe that the products of the $\hat{F}_i$'s is free by looking at the restriction of the automorphisms to the copy of $X_{[3]}$ sitting in the natural way inside $X_{[n]}$.

Finally, embed S_3 into Aut $(X_{[n]})$ by letting it act on the symbols 0, 1, and 2 while fixing the others. This gives the same relations with the $\hat{F}_i$'s in Aut $(X_{[n]})$ as it gives with the F_i's in Aut $(X_{[3]})$. Then Aut $(X_{[3]}) \simeq (\hat{F}_0 * \hat{F}_1 * \hat{F}_3) \rtimes S_3$ is a subgroup of Aut $(X_{[n]})$. □

COROLLARY 5.9. Aut $(X_{[n]})$ *for* $n>2$ *contains free groups.*

6. *Expanding maps*

Here we give a simple proof of a general constraint on the finite groups of homeomorphisms that commute with some expanding maps.

Observation 6.1. Suppose $f: X \to X$ is a continuous expanding map of a compact space to itself with cardinality $f^{-1}(x) \le d$ for some d and all x. Let G be a finite group of homeomorphisms of X that commute with f. Suppose $x \in X$ is an f periodic point whose inverse images are dense in X. Then there are $r \in \mathbb{N}$ points with the same f period as x for some r, and G is isomorphic to an extension of K by L where K is a subgroup of W_d^k for some k, and L is a subgroup of S_r.

Proof. Let f and x be as stated. Since f is expanding and X is compact there can only be finitely many periodic points for f of any period. Let r be the number of points with the same period as x. Since $\bigcup_{n=0}^{\infty} f^{-n}(x)$ is dense in X, G acts faithfully on $\bigcup_{n=0}^{l} f^{-n}(x)$ for some l. Let

$$G_1 = \{g \in G: g(y) = y, \ \forall y \in G(x)\}.$$

G_1 is normal in $G = G_0$, the cardinality of $G(x)$ is less than or equal to r, so G_0/G_1 is isomorphic to a subgroup of S_r. Next let

$$G_2 = \{g \in G_1: g(y) = y, \ \forall y \in f^{-1}(G(x))\}.$$

Now G_1/G_2 is isomorphic to a subgroup of $S_d^{f^{-1}(G(x))}$ since G_1 fixes all elements of $G(x)$ and the cardinality of $f^{-1}(y)$ is less than or equal to d. We continue back on each level until we reach $f^{-l}(G(x))$. This gives

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{l+1} \supseteq G_{l+2} = \{1\}.$$

Then by observation A.3 and Propositions A.5 and A.11, $G_1 = K$ is isomorphic to a subgroup of W_d^k, for some k, and the conclusion follows. □

COROLLARY 6.2. *Suppose $f: X \to X$ is a continuous expanding map of a compact space to itself with cardinality $f^{-1}(x) \le d$ for some d and all x. Let φ be a homeomorphism of X of finite order that commutes with f. Suppose $x \in X$ is an f periodic point whose inverse images are dense in X. Then there are $r \in \mathbb{N}$ points with the same f period as x for some r, and φ has order $sp_1^{e_1} \cdots p_l^{e_l}$, where s is the order of a permutation on r symbols, primes $p_i \le d$, and $e_i \in \mathbb{Z}^+$.*

Remark 6.3. There are some expanding maps where there are no restrictions on the order of automorphisms that commute with the map. To see this let $y^{(n)}$ be the point in the 2 shift made up be repeating the word 01^n forever. Let Y be the subshift that is the closure of the orbits of all these points. The orbit of $y^{(n)}$ is an isolated set of cardinality $n+1$. There is an automorphism that is the shift on the orbit of $y^{(n)}$ and is the identity everywhere else.

Appendix: *Group theory*

We will review some things about group theory. The discussion will include composition series, extensions, wreath products, and some facts about wreath products of permutation groups. The terminology and notation will follow that which is used in Rotman, [**R**]. We would like to thank Bob Gilman for his help on this section and, in particular, for supplying Lemmas A.9, A.10, and Proposition A.11.

Let G be a finite group. A *normal series* is a chain

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_l = \{1\}$$

where G_{i+1} is normal in G_i. Another normal series

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_k = \{1\}$$

is a *refinement* if $G_0, \ldots, G_l$ is a sublist of $H_0, \ldots, H_k$. The *factor groups* of a normal series are the quotient groups

$$G_0/G_1, \ldots, G_{l-1}/G_l.$$

Two normal series are *equivalent* if there is a one-to-one correspondence between the factor groups so that the corresponding groups are isomorphic.

A *composition series* is a normal series where G_{i+1} is a maximal normal subgroup of G_i for each i. A normal series is a composition series if and only if each factor group is a simple group. The factor groups of a composition series are called *composition factors* of G.

THEOREM A.1. (Schreier, 1926.) *Any two normal series of an arbitrary group have refinements that are equivalent.*

THEOREM A.2 (Jordan–Hölder.) *Any two composition series of a finite group are equivalent.*

https://doi.org/10.1017/S0143385700005678 Published online by Cambridge University Press

For groups G, K, and Q, we say that G is an *extension* of K by Q if there is a short exact sequence

$$1 \to \mathrm{K} \to \mathrm{G} \xrightarrow{\pi} \mathrm{Q} \to 1.$$

The group G is a *semi-direct product* of K by Q, denoted $K \rtimes Q$, if the sequence splits. That is, there is a homomorphism $\zeta: Q \to G$ so that $\pi \circ \zeta$ is the identity on Q. Another way to say this is that G contains copies of K and Q with K normal in G, $KQ = G$, and $K \cap Q = \{1\}$.

Observation A.3. If G is an extension of K by Q then the composition factors of G are the union of the composition factors for Q and the ones for K.

Proof. Let

$$K = K_0 \supseteq \cdots \supseteq K_l = \{1\}$$

and

$$Q = Q_0 \supseteq \cdots \supseteq Q_k = \{1\}$$

be composition series for K and Q with

$$1 \to K \to G \xrightarrow{\pi} Q \to 1.$$

Then $\pi^{-1}(Q_{i+1})$ is normal in $\pi^{-1}(Q_i)$ for each i and

$$\pi^{-1}(Q_{i+1})/\pi^{-1}(Q_i) \simeq Q_{i+1}/Q_i.$$

This means

$$G = \pi^{-1}(Q_0) \supseteq \cdots \supseteq \pi^{-1}(Q_k) = K_0 \supseteq K_1 \cdots \supseteq K_l = \{1\}$$

is a composition series for G with the desired properties. □

Discussion A.4. Given two groups K and Q and a homomorphism $\theta: Q \to \mathrm{Aut}\,(K)$ we can define the semi-direct product of K by Q realizing θ by $G = K \times Q$ where the multiplication is given by: $(k, q)(l, r) = (\theta_r(k)l, qr)$. Given a group Q that acts on a set A and another group L, there is a natural homomorphism $\theta: Q \to \mathrm{Aut}\,(L^A)$ defined by $(\theta_q(\gamma))_a = \gamma_{q(a)}$. We will denote this by $\theta_q(\gamma) = \gamma^q$. Given Q acting on A and L another group we can form the semi-direct product $G = L^A \rtimes Q$ of L^A by Q realizing this homomorphism. The group G is the set $L^A \times Q$ with multiplication $(\gamma, q)(\delta, r) = (\gamma^r\delta, qr)$. This construction will play an important role in §§ 3 and 4. There is some conflict of terminology between this construction (using Q, A, and L) and the special case of it that follows, see [**Ha**] versus [**R**].

Given two finite groups, L and Q, Q naturally acts on itself by left multiplication $\theta_r(q) = rq$ so we can form the special semi-direct product just described $L\,wr\,Q = L^Q \rtimes Q$. This will be called the *wreath product* of L by Q.

Theorem A.5. (Kaloujnine & Krasner, 1951.) *If K and Q are finite groups then $K\,wr\,Q$ contains an isomorphic copy of every extension of K by Q.*

Theorem A.6. *If p is a prime, then a Sylow p-subgroup of S_{p^n} is the wreath product of $\mathbb{Z}/p$ with itself n times, where the product is $V_p^1 = \mathbb{Z}/p$ and $V_p^{k+1} = V_p^k\,wr\,\mathbb{Z}/p$.*

Next we want to examine a special wreath product that we will make use of in §§ 3 and 4.

Definition A.7. Let $W_n^1 = S_n$ and $W_n^{k+1} = W_n^k \text{ wr } S_n$.

LEMMA A.8. *For $n \neq 4$ the group W_n^k has all of its composition factors isomorphic to either $\mathbb{Z}/2$ or A_n. The group W_4^k has all its composition factors isomorphic to either $\mathbb{Z}/2$ or $\mathbb{Z}/3$.*

Proof. We prove this by induction on k. It is true when $k=1$. The product $(W_n^k)^{S_n}$ has its composition factors as desired by Observation A.3. Again applying Observation A.3 to $(W_n^k)^{S_n} \rtimes S_n$ we see that W_n^{k+1} has its composition factors as desired. □

For a group G and a subgroup H of G we let $[G:H]$ denote the index of H in G, that, is, the cardinality of G/H.

LEMMA A.9. *If G is a subgroup of S_n and H is a normal subgroup of G so that G/H is simple then G/H is isomorphic to a subgroup of S_n.*

Proof. We prove this by induction on the order of G. Take the case $\{1\} \neq G$, there is a subgroup $L \subseteq G$ so that $1 < [G:L] \leq n$. This follows because for each $i = 1, \ldots, n$, if $G_i = \{g \in G: g(i) = i\}$, $[G:G_i]$ is equal to the size of the orbit of i under G. There must be an i so that this is not 1, take this G_i to be L. Consider HL. If $HL = G$ then $G/H \simeq L/(L \cap H)$ and we apply the induction hypothesis to L. Otherwise $HL \neq G$ and we consider the action of H on the coset space G/HL. This maps G into $S_{G/HL}$, where $1 < [G:HL] \leq n$. The map has kernel H since G/H is simple. It embeds G/H into $S_{G/HL}$. □

LEMMA A.10. *If G has all its composition factors isomorphic to subgroups of S_n, so does every subgroup of G.*

Proof. Let H be a subgroup of G. Then intersect a composition series of G with H.

$$H_0 = H \cap G_0 \supseteq H_1 = H \cap G_1 \supseteq \cdots \supseteq H_l = H \cap G_l.$$

Extend this to a composition series for H giving

$$H_i \supseteq K_1^i \supseteq \cdots K_{l_i}^i \supseteq H_{i+1}.$$

There is a natural map $H_i/H_{i+1} \to H_i/K_1^i$, where $H_i/H_{i+1} \subseteq S_n$ and H_i/K_1^i is simple. We can apply Lemma A.9. Similarly, $K_1^i/H_{i+1} \subseteq H_i/H_{i+1}$ and there is a natural map $K_1^i/H_{i+1} \to K_1^i/K_2^i$. We are again in a position to apply Lemma A.9 and we can continue. □

PROPOSITION A.11. *A finite group G is a subgroup of W_n^k, for some k, if and only if all its composition factors are isomorphic to subgroups of S_n.*

Proof. If G is a subset of W_n^k Lemmas A.8 and A.10 tell us that G satisfies the required condition. Conversely, suppose G satisfies the condition and

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_l = \{1\}$$

is a composition series for G. Then G_{l-1} is isomorphic to a subgroup of S_n. We know that G_{l-2} is isomorphic to an extension of G_{l-1} by G_{l-2}/G_{l-1}. By the theorem of Kaloujnine & Krasner (A.5) we know that G_{l-2} is isomorphic to a subgroup of

G_{l-1} *wr* (G_{l-2}/G_{l-1}) which is a subgroup of W_n^1 *wr* $S_n = W_n^2$. We continue until we get G to be isomorphic to a subgroup of W_n^l. □

COROLLARY A.12. *Every element of* W_n^k *has order* $p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ *where* $p_1, \ldots, p_r$ *are the primes less than or equal to n.*

Proof. We induct on k. This is clear in S_n. Let $(\gamma, g) \in W_n^k$. This has powers $(\gamma, g)^t = (\gamma^{g^{t-1}}\gamma^{g^{t-2}}\cdots\gamma, g^t)$. If t is the order of g then $\gamma^{g^t} = \gamma$ and $(\gamma, g)^{st} = ((\gamma^{g^{t-1}}\cdots\gamma)^s, 1)$. Since $(\gamma^{g^{t-1}}\cdots\gamma)$ is in W_n^{k-1} it has order s with the right prime decomposition. The order of (γ, g) divides st. □

COROLLARY A.13. *A finite group* G *is a subgroup of* W_2^k *for some* k *if and only if every element has order* 2^l *for some* l *(it is a* 2*-group).*

Proof. If $G \subseteq W_2^k$ then the condition on the orders is Corollary A.12. If G is finite and every element has order 2^l for some l then Cauchy's theorem says that G has order 2^r for some r. This means G is isomorphic to a subgroup of S_{2^r} and is contained in a Sylow 2-subgroup $\hat{G}$. By the theorem describing the Sylow p-subgroups of S_{p^k} in terms of wreath products (A.6), we see that $\hat{G} \simeq V_2^r \simeq W_2^r$. □

COROLLARY A.14. *If* G *is a finite group that contains a simple subgroup* H *that cannot be embedded in* S_n *then* G *is not isomorphic to a subgroup of* W_n^k *for any* k.

Proof. We see that

$$G \supseteq H \supseteq \{1\}$$

is a normal series and by Schreier's Theorem (A.1) can be extended to a composition series. This means H is a composition factor of G. By Proposition A.11 G cannot be a subgroup of W_n^k.

COROLLARY A.15. *The condition on orders of Corollary* A.12 *does not guarantee that a finite group is a subgroup of* W_n^k, *for some* k, *in general. This is in contrast to Corollary* A.13 *when* $n = 2$.

Proof. The group A_6 consists of elements of order 5, 2×2, 3, 2, and 1 but cannot be embedded in S_5 or by Corollary A.14, in W_5^k for any k. □

REFERENCES

[A] J. Ashley. Marker automorphisms of the one-sided d-shift. *Ergod. Th. & Dynam. Sys.* to appear.

[BDK] P. Blanchard, R. Devaney & L. Keen. The dynamics of complex polynomials and automorphisms of the shift, preprint.

[B] M. Boyle. Nasu's simple automorphisms, *Dynamical Systems – Maryland 1986–1987. Proceedings of a Special Year*, ed. J. Alexander, Springer Lecture Notes 1342. Springer-Verlag: New York, 1988.

[Ha] M. Hall, Jr. *The Theory of Groups*, Chelsea Pub. Co.: New York, 1976.

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

[N] M. Nasu. Topological conjugacy for sofic systems and extensions of automorphisms of finite subsystems of topological Markov chains. *Dynamical Systems – Maryland 1986–1987, Proceedings of a Special Year*, ed. J. Alexander, Springer Lecture Notes 1342, Springer-Verlag: New York, 1988.

[R] J. J. Rotman. *An Introduction to the Theory of Groups.* 3rd ed., Allyn and Bacon, Inc.: Boston, 1984.

[Wa1] J. Wagoner. Markov partitions and K_2. *Pub. Math. IHES* No. 65 (1987), 91-129.

[Wa2] J. Wagoner. Triangle identities and symmetries of a subshift of finite type. *Pacific J. Math.*, to appear.

[Wa3] J. Wagoner. Eventual finite order generation for the kernel of the dimension group representation. *Trans. of AMS* **317** (1) (1990), 331-350.

[W] R. F. Williams. Classification of subshifts of finite type. *Ann. of Math.* **98** (1973), 120-153; erratum **99** (1974), 380-381.