ON THE AUTOMORPHISM GROUPS OF SHIFT SPACES

SUMADHU RUBAIYAT

Advisor: Professor Joshua Frisch

Department of Mathematics
University of California San Diego

In partial fulfillment of the requirements for the
Mathematics Honors Program

June 2025

Abstract

We prove that every normal subgroup of the automorphism group of the full shift either is a subgroup of the shifts or contains a free group on 2 generators, and by extension, a free group on any countable number of generators. Additionally, we prove that an automorphism of the full shift that maps every periodic point to a shift of itself is contained in the center.

Acknowledgments

I would like to express my deepest gratitude to Professor Joshua Frisch for his invaluable guidance throughout my thesis and for devoting countless hours to educate me on various mathematical subjects. I would also like to extend my gratitude to my collaborators and friends Ruoya Yan, Richard Li, and Fong Lok Heen for collaborating with me to both learn the preliminary content and prove the novel results. Finally, I would like to thank my friends and family for supporting me.

Contents

1. Introduction

We first cover some basic terms and intuition into symbolic dynamics. We heavily credit [2], the textbook I learned most of these terms from.

1.1. **Shift Spaces.** Let A be some finite set of symbols, $|A| \geq 2$. A is our alphabet. A bi-infinite sequence of symbols of A is $x = ...x_{-2}x_{-1}.x_0x_1x_2...$ for each $x_i \in A$. x_i is called the ith coordinate of x. For integers $m \leq n$, let $x_{[m,n]}$ be the block or word of symbols from coordinate m to coordinate n, namely $x_m x_{m+1}...x_n$.

Definition 1.1 (Full Shift)**.** The full A-shift, denoted $A^{\mathbb{Z}}$, is the set of all such bi-infinite sequences of symbols from A, i.e. $A^{\mathbb{Z}} = \{x = (x_i)_{i\in\mathbb{Z}} : x_i \in A \text{ for all } i \in \mathbb{Z}\}$. For $A = \{0, 1, ...n-1\}$, we can write $n^{\mathbb{Z}}$ instead.

Definition 1.2 (Shift Space)**.** Let F be some (finite or infinite) collection of blocks, called forbidden blocks, and define X_F to be the subset of bi-infinite sequences in $A^{\mathbb{Z}}$ which do not contain any block in F. Y is called a shift space of $A^{\mathbb{Z}}$ if $Y = X_F$ for some collection F of forbidden blocks.

Definition 1.3 (Subshift)**.** If a shift space P is a subset of a shift space Q, we say P is a subshift of Q.

That is, all shift spaces, by definition must be a subshift of the full shift on some alphabet.

Definition 1.4 (Language of Shift Space)**.** Let X be a subset of a full shift, and let $B_n(X)$ denote the set of all n-blocks that occur in points in X. The language of X is the collection

$$B(X) = \bigcup_{n=0}^{\infty} B_n(X).$$

Proposition 1.5. [2] *Let Y be a subshift of the full A-shift. Then $Y = X_{B(Y)^c}$.*

That is, the language of a shift space determines it. We can freely translate between the forbidden block formulation given by the definition and the language of the shift space. Another way to look at this is as follows:

Proposition 1.6. [2] *Let X be a subset of the full A-shift. Then X is a shift space if and only if whenever $x \in A^{\mathbb{Z}}$ and each $x_{[i,j]} \in B(X)$, then $x \in X$.*

Another way we can build shift spaces from other shift spaces without taking subshifts is looking at the higher block shift.

Definition 1.7 (Higher Block Shift)**.** Let X be a shift space over the alphabet A, and $A_X^{[N]} = B_N(X)$ be the collection of all allowed N-blocks in X. We can consider $A_X^{[N]}$ as an alphabet in its own right, and form the full shift $(A_X^{[N]})^{\mathbb{Z}}$. Define the N-th higher block code $\beta_N : X \to (A_X^{[N]})^{\mathbb{Z}}$ by

$$(\beta_N(x))_{[i]} = x_{[i,i+N-1]}.$$

Thus β_N replaces the i-th coordinate of x with the block of coordinates in x of length N starting at position i. This becomes clearer if we imagine the symbols in $A_X^{[N]}$ as written vertically. Then the image of $x = (x_i)_{i\in\mathbb{Z}}$ under β_4 has the form

$$\beta_4(x) = \cdots \begin{bmatrix} x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \end{bmatrix} \begin{bmatrix} x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{bmatrix} \begin{bmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \end{bmatrix} . \begin{bmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} \begin{bmatrix} x_4 \\ x_3 \\ x_2 \\ x_1 \end{bmatrix} \begin{bmatrix} x_5 \\ x_4 \\ x_3 \\ x_2 \end{bmatrix} \cdots \in (A_X^{[4]})^{\mathbb{Z}}.$$

Let X be a shift space. Then the N-th higher block shift $X^{[N]}$ or higher block presentation of X is the image $X^{[N]} = \beta_N(X)$ in the full shift over $A_X^{[N]}$.

Proposition 1.8. [2] *The higher block shifts of a shift space are also shift spaces.*

Definition 1.9 (Sliding Block Code)**.** A sliding block code is defined as a map $f : X \to Y$ on shift spaces X and Y over alphabets A and B respectively, where there exists a "looking window" radius r and block map $\Phi : A^{2r+1} \to B$ where $f(x) = y$ means for every coordinate i, $\Phi(x_{[i-r,i+r]}) = y_i$.

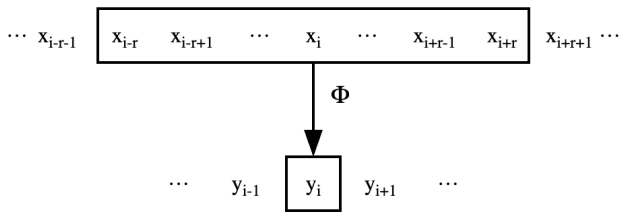

FIGURE 1. Sliding Block Codes [2]

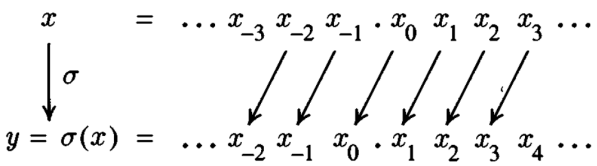

FIGURE 2. Shifts [2]

That is, the ith coordinate of $f(x)$ is determined by looking only at the r coordinates before and after the ith coordinate of x as shown in Figure 1.
An important class of sliding block codes is the shifts, denoted $\{\sigma_X^k : k \in \mathbb{Z}\}$ where $\sigma_X : X \to X$ which just moves everything over one spot as shown in Figure 2. We simply write σ when the metric space is clear.

Proposition 1.10. [2] *Let X and Y be shift spaces. A map $\phi\colon X \to Y$ is a sliding block code if and only if $\phi \circ \sigma_X = \sigma_Y \circ \phi$ and there exists $N \geq 0$ such that $\phi(x)_0$ depends only on $x_{[-N,N]}$.*

Definition 1.11 (Automorphism)**.** An automorphism is a sliding block code which is invertible.

That is, f is an automorphism of $A^{\mathbb{Z}}$ if and only if f is a sliding block code and there exists a sliding block code f^{-1} so that $f \circ f^{-1} = Id$.

Proposition 1.12. [2] *A sliding block code $\phi\colon X \to Y$ between shift spaces that is one-to-one (injective) and onto (surjective) has a sliding block inverse, and is therefore an automorphism.*

Definition 1.13 (Automorphism Group)**.** The set of automorphisms of X form a group, called Aut(X).

Note that for $|A| = n$, this group is isomorphic to $\mathrm{Aut}(n^{\mathbb{Z}})$, so we will be using $\mathrm{Aut}(A^{\mathbb{Z}})$ and $\mathrm{Aut}(n^{\mathbb{Z}})$ interchangeably.
The shifts $\{\sigma^n : n \in \mathbb{Z}\}$ are clearly a normal subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$.

Definition 1.14 (Conjugate Shift Spaces)**.** Shift spaces X and Y are said to be conjugate if there exists an invertible sliding block code g so that g(X) = Y .

Proposition 1.15. [2] *The image of a shift space under a sliding block code is a shift space.*

Proposition 1.16. [2] *Let $\phi : X \to Y$ be a sliding block code. Then there exist a higher block shift $\widetilde{X}$ of X, an automorphism $\psi \in Aut(A^{\mathbb{Z}})$*

such that $\psi(X) = \widetilde{X}$, and a 1-block code $\widetilde{\phi} : \widetilde{X} \to Y$ so that $\phi = \widetilde{\phi} \circ \psi$; i.e., the following diagram commutes.

$$\begin{array}{ccc} X & \xrightarrow{\psi} & \widetilde{X} \\ & \searrow^{\phi} & \downarrow{\scriptstyle \widetilde{\phi}} \\ & & Y \end{array}$$

Proof. Suppose that ϕ is induced by a block map Φ and has looking window of size r. Let $\mathcal{A} = B_{2r+1}(X)$, and define $\psi : X \to \mathcal{A}^{\mathbb{Z}}$ by

$$\psi(x)_{[i]} = x_{[i-r,i+r]}.$$

Then $\psi = \sigma^{-m} \circ \beta_{2r+1}$. Thus $\widetilde{X} = \psi(X) = X^{[2r+1]}$ is a shift space, and since σ and β_{2r+1} are conjugacies, so is ψ. Put $\widetilde{\phi} = \phi \circ \psi^{-1}$. Note that $\widetilde{\phi}$ is a 1-block code. □

Then, we can understand the intuition behind automorphisms of the full shift by taking an Nth higher block shift for N being the looking window of the automorphism, so that these are just defined by renaming each symbol in the alphabet of the higher block shift by a bijection.

1.2. **Shift Space Properties.**

Definition 1.17 (Irreducible)**.** A shift space X is irreducible if for every ordered pair of blocks $u, v \in B(X)$ there exists $w \in B(X)$ such that $uwv \in B(X)$.

Definition 1.18 (Mixing)**.** A shift space X is mixing if for every ordered pair of blocks $u, v \in B(X)$, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, there exists $w \in B_n(X)$ with $uwv \in B(X)$.

Proposition 1.19. [2] *The mixing property is invariant under conjugacy.*

Definition 1.20 (Shift Space of finite type)**.** A shift space Y is said to be of finite type (SFT) if there exists a finite set F of forbidden blocks such that $\mathrm{Y} = X_F$.

Definition 1.21 (M-step SFT)**.** A SFT is M-step (or has memory M) if it can be described by a collection of forbidden blocks F where each block in F has length exactly $M + 1$.

Proposition 1.22. [2] *X is a SFT if and only if there exists an integer $M \geq 0$ such that X is M-step.*

Proposition 1.23. [2] *A shift space X is an M-step shift of finite type if and only if whenever $uv, vw \in B(X)$ and $|v| \geq M$, then $wvw \in B(X)$.*

Theorem 1.24. [2] *A conjugate shift space of an SFT is itself also an SFT.*

Proof. Suppose that X is a shift space that is conjugate to a shift of finite type Y. Let Φ be a block map that induces a conjugacy from X to Y, and Ψ be a block map that induces its inverse. The idea is to apply Proposition 1.23, observing that if two blocks in X overlap sufficiently, then their images under Φ will overlap enough to glue them together to form a block in Y. Applying Ψ to this block yields the original blocks in X glued along their overlap, but shortened at each end. To accommodate this shortening, we need to first extend the original blocks.
According to Proposition 1.23, our goal is to find an integer $M \geq 1$ such that if $v \in B(X)$ with $|v| \geq M$, and if $uv, vw \in B(X)$, then $uvw \in B(X)$.
Let $\phi : X \to Y$ be a conjugacy induced by a block map Φ, and $\psi = \phi^{-1} : Y \to X$ be its inverse, induced by Ψ. By increasing the window size if necessary, we can assume that ϕ and ψ have the same looking window, say l. Observe that since $\psi(\phi(x)) = x$ for all $x \in X$, the block

map $\Psi \circ \Phi : B_{4l+1}(X) \to B_1(X)$ merely selects the central symbol in a block.
Since Y has finite type, by Proposition 1.23 there is an $N \geq 1$ such that two blocks in Y that overlap in at least N places can be glued together along their overlap to form a block in Y.
Set $M = N + 4l$. To verify that this choice satisfies the conditions of Proposition 1.23, and thereby prove that X has finite type, let $uv, vw \in B(X)$ with $|v| \geq M$. By Proposition 1.5, there are words $s, t \in B_{2l}(X)$ such that $suv, vwt \in B(X)$. Since every $(4l+1)$-block in $suvwt$ is in $B(X)$ (although we do not know yet that $suvwt$ is itself in $B(X)$), the description above of the action of $\Psi \circ \Phi$ shows that $\Psi(\Phi(suvwt)) = uvw$. Now $\Phi(suv) = u'\Phi(v)$ and $\Phi(vwt) = \Phi(v)w'$, where $u', w' \in B(Y)$ and $|\Phi(v)| = |v| - 2l \geq N$. Hence $u'\Phi(v)$ and $\Phi(v)w'$ can be glued together to form $u'\Phi(v)w' \in B(Y)$. Then

$$uvw = \Psi(\Phi(suvwt)) = \Psi(u'\Phi(v)w') \in B(X),$$

proving that X has finite type. □

Definition 1.25 (Graph)**.** A graph G consists of a finite set $\mathcal{V} = \mathcal{V}(G)$ of vertices (or states) together with a finite set $\mathcal{E} = \mathcal{E}(G)$ of edges. Each edge $e \in \mathcal{E}(G)$ starts at a vertex denoted by $i(e) \in \mathcal{V}(G)$ and terminates at a vertex $t(e) \in \mathcal{V}(G)$ (which can be the same as $i(e)$). We shall usually shorten $\mathcal{V}(G)$ to $\mathcal{V}$ and $\mathcal{E}(G)$ to $\mathcal{E}$ when G is understood.

Definition 1.26 (Graph Homomorphism)**.** Let G and H be graphs. A graph homomorphism from G to H consists of a pair of maps $\partial\Phi : \mathcal{V}(G) \to \mathcal{V}(H)$ and $\Phi : \mathcal{E}(G) \to \mathcal{E}(H)$ such that $i(\Phi(e)) = \partial\Phi(i(e))$ and $t(\Phi(e)) = \partial\Phi(t(e))$ for all edges $e \in \mathcal{E}(G)$. In this case we write $(\partial\Phi, \Phi) : G \to H$.
A graph homomorphism $(\partial\Phi, \Phi)$ is a graph embedding if both $\partial\Phi$ and Φ are one-to-one. It is a graph isomorphism if both $\partial\Phi$ and Φ are one-to-one and onto, in which case we write $(\partial\Phi, \Phi) : G \cong H$. Two graphs G and H are graph isomorphic (written $G \cong H$) if there is a graph isomorphism between them.

This definition basically says that when two graphs are isomorphic you can obtain one from the other by renaming vertices and edges.

Definition 1.27 (Adjacency Matrix)**.** Let G be a graph with vertex set V. For vertices $I, J \in V$, let A_{IJ} denote the number of edges in G with initial state I and terminal state J. Then the adjacency matrix of G is $A = [A_{IJ}]$, and its formation from G is denoted by $A = A(G)$ or $A = A_G$.

Proposition 1.28. [2] *Let G be a graph with adjacency matrix A, and let $m \geq 0$. The number of paths of length m from I to J is $(A^m)_{IJ}$, the (I, J)th entry of A^m.*

Definition 1.29 (Edge Shift)**.** Let G be a graph with edge set E and adjacency matrix A. The edge shift X_G or X_A is the shift space over the alphabet $A = E$ specified by

$$X_G = X_A = \{\xi = (\xi_i)_{i\in\mathbb{Z}} \in E^{\mathbb{Z}} : t(\xi_i) = i(\xi_{i+1}) \text{ for all } i \in \mathbb{Z}\}.$$

According to this definition, a bi-infinite sequence of edges is in the edge shift of G exactly when the terminal state of each edge is the initial state of the next one; i.e., the sequence describes a bi-infinite walk or bi-infinite trip on G.

Theorem 1.30. [2] *If G is a graph with adjacency matrix A, then the associated edge shift $X_G = X_A$ is a 1-step shift of finite type.*

Proof. Let $A = E$ be the alphabet of X_G. Consider the finite collection

$$F = \{ef : e, f \in A, t(e) \neq i(f)\}$$

of 2-blocks over A. According to Definition 1.29, a point $\xi \in A^{\mathbb{Z}}$ lies in X_G exactly when no block of F occurs in ξ. This means that $X_G = X_F$, so that X_G has finite type. Since all blocks in F have length 2, X_F is 1-step. □

Theorem 1.31. [2] *If X is an M-step shift of finite type, then there is a graph G such that $X^{[M+1]} = X_G$.*

Proof. First note that if $M = 0$, then X is a full shift, and we can take G to have a single vertex and one edge for each symbol appearing in X. Thus we may assume that $M \geq 1$. Define the vertex set of G to be $V = B_M(X)$, the allowed M-blocks in X. We define the edge set $\mathcal{E}$ as follows. Suppose that $I = a_1a_2 \dots a_M$ and $J = b_1b_2 \dots b_M$ are two vertices in G. If $a_2a_3 \dots a_M = b_1b_2 \dots b_{M-1}$, and if $a_1 \dots a_Mb_M$ $(= a_1b_1 \dots b_M)$ is in $B(X)$, then draw exactly one edge in G from I to J, named $a_1a_2 \dots a_Mb_M = a_1b_1b_2 \dots b_M$. Otherwise, there is no edge from I to J. From this construction, it is clear that a bi-infinite walk on G is precisely a sequence of $(M+1)$-blocks in $B_{M+1}(X)$ which overlap progressively. Hence $X_G = X^{[M+1]}$. □

Again, this intuitively links the notion of walks on graphs and shifts of finite type. Moreover, shifts of finite type directly encode a semblance of memory in terms of moving along the edges of a graph, contextualizing it within the vast amount of work done in theoretical computer science on computability of graph problems. Additionally, when we

dive into the topology of shift spaces of finite type, this can be visualized as a topology on the bi-infinite paths on a graph, but we will explore that further in Section 1.3 Dynamical Systems. Furthermore, we can use properties of graphs or their corresponding adjacency matrices to induce properties on their corresponding edge shifts of finite type.

Definition 1.32. A graph is essential if all vertices in the graph have at least one edge starting or terminating at it.

Definition 1.33. A graph G is irreducible if for every ordered pair of vertices I, J, there exists a path starting at I and ending at J in G.

Theorem 1.34. [2] *An essential graph is irreducible if and only if its edge shift is irreducible.*

Proof. Let G be an irreducible graph, and $\pi, \tau \in B(X_G)$. Suppose that π terminates at vertex I and τ starts at vertex J. By irreducibility of G, there is a path $\omega \in B(X_G)$ from I to J. Then $\pi\omega\tau$ is a path on G, so that $\pi\omega\tau \in B(X_G)$.
Conversely, suppose that G is essential, and that X_G is an irreducible shift. Let I and J be vertices of G. Since G is essential, there are edges e and f such that e terminates at I and f starts at J. By irreducibility of X_G, there is a block ω so that $e\omega f \in B(X_G)$. Then ω is a path in G from I to J, so that G is an irreducible graph. □

Definition 1.35. A matrix A is primitive if $A^N > 0$ for some $N \geq 1$. A graph is primitive if its adjacency matrix is primitive.

Proposition 1.36. [2] *If G is an essential graph, then the edge shift X_G is mixing if and only if G is primitive.*

Proposition 1.37. [2] *A shift of finite type is mixing if and only if it is conjugate to an edge shift X_G where G is primitive.*

1.3. **Dynamical Systems.** For the purposes of this paper, let us define the following metric on a shift space X:

Definition 1.38 (Distance of 2 points in a shift space)**.**

$$\rho(x,y) = \begin{cases} 2^{-k} & \text{if } x \neq y \text{ and } k = \max\{n \geq 0 : x_{[-n,n]} = y_{[-n,n]}\}, \\ 0 & \text{if } x = y. \end{cases}$$

Practically, this captures the notion that 2 points are close iff they agree on large central blocks.
This metric induces a topology on shift spaces.

Definition 1.39. The cylinder sets of a shift space X are $\{C_k^X(u) : k \in \mathbb{Z}, u \in B(X)\}$ with

$$C_k^X(u) = \{x \in X : x_{[k,k+|u|-1]} = u\}$$

Note that the cylinder sets are the open balls within this metric space, and thus the cylinder sets are an open basis on shift spaces. In other words, every open set within a shift space is either a union of cylinder sets or an intersection of finite cylinder sets.

Definition 1.40 (Continuity and Homeomorphisms)**.** Let (M, d_M) and (N, d_N) be metric spaces. A function $\phi\colon M \to N$ is:

- continuous if for every convergent sequence $x_n \to x$ in M, the image sequence converges as $\phi(x_n) \to \phi(x)$ in N;
- a homeomorphism if ϕ is continuous, bijective (one-to-one and onto), and its inverse ϕ^{-1} is continuous.

Consider $M = X$ and $N = Y$ are shift spaces and ϕ a sliding block code. If two points in X are close, they agree on a large central block, hence their images under ϕ also agree on a large (though slightly smaller) central block. Thus ϕ is continuous. Moreover, if ϕ is an automorphism, ϕ is a homeomorphism. The converse of this statement is known as the Curtis-Lyndon-Hedlund Theorem, and proved in Section 2.1.

Definition 1.41 (Dynamical System)**.** A *dynamical system* (M, ϕ) consists of a compact metric space M and a continuous map $\phi\colon M \to M$. We call (M, ϕ) an invertible dynamical system when ϕ is a homeomorphism.

If we let $M = X$ be a shift space and $\phi{=}\sigma_X$, this example is called a shift dynamical system. This is the object that we are the most interested in within the context of symbolic dynamics.

Definition 1.42 (Morphisms of Dynamical Systems)**.** Let (M, ϕ) and (N, ψ) be dynamical systems, and let $\theta\colon (M, \phi) \to (N, \psi)$ be a homomorphism. Then θ is called:

- An embedding if it is injective (one-to-one)
- A factor map if it is surjective (onto)
- A topological conjugacy if it is bijective (both one-to-one and onto) with continuous inverse

We write $\theta\colon (M,\phi) \cong (N,\psi)$ when θ is a topological conjugacy. Two dynamical systems are topologically conjugate if there exists a topological conjugacy between them.

Clearly, automorphisms are topological conjugacies within shift dynamical systems. Thus, our study of $\mathrm{Aut}(X)$ for shift spaces X can be rephrased as studying this function space of topological conjugacies of shift dynamical systems. Precisely, this is why the field is called Symbolic Dynamics.

1.4. **Outline.** Our novel contributions are proving:

Claim 1.43. *If N is a normal subgroup of $Aut(A^{\mathbb{Z}})$ either N is a subgroup of the shifts or it contains a free subgroup on two generators, hence the free subgroup on any countable number of generators.*

and in lieu of that, in Section 2 Periodic Points, we novelly prove:

Claim 1.44. *For any automorphism g that is not a shift, there exists p such that $g(p)$ is not a shift of p.*

In our relevant results, we will cover some known results we proved in pursuit of our primary claim.
The Curtis-Lyndon-Hedlund Theorem [2] states:

Claim 1.45. *The homomorphisms between shift dynamical systems are precisely the sliding block codes. That is, for any shift dynamical systems (X, σ_X) and (Y, σ_Y), $f : X \to Y$ is a homomorphism if and only if it is a sliding block code.*

This contextualizes our results about $\mathrm{Aut}(X)$ where X is an arbitrary shift space, within the broader study of topological conjugacies of dynamical systems.
The Kim-Rouch Embedding [6] asserts:

Claim 1.46. *For any valid alphabets A and B, there exists injective homomorphism $\phi : Aut(A^{\mathbb{Z}}) \to Aut(B^{\mathbb{Z}})$.*

This was a result we proved believing that our claim may be simpler to prove given a certain choice of alphabet, which is still an approach being considered to prove extensions of our claim.
The marker-subgroup construction [1] asserts:

Claim 1.47. *The group Aut(X) contains the free product of any finite number of 2-element groups. Thus it contains the free group on two generators, hence the free group on a countable number of generators.*

This result was pivotal to our novel result regarding normal subgroups containing a free group on two generators, hence the free group on a countable number of generators.

2. Periodic Points

Definition 2.1. A point x is periodic if $\sigma^n(x) = x$ for some n. We say the period of x is n.

Proposition 2.2. *Periodic points are dense in the full shift.*

Theorem 2.3. [2] *Let $\phi : X \to Y$ be a sliding block code. If $x \in X$ has period n under σ_X, then $\phi(x)$ has period n under σ_Y, and the least period of $\phi(x)$ divides the least period of x. Embeddings, and hence automorphisms, preserve the least period of a point.*

Proof. If x has period n, then $\sigma_X^n(x) = x$. Hence

$$\sigma_Y^n(\phi(x)) = \phi(\sigma_X^n(x)) = \phi(x),$$

so that $\phi(x)$ has period n. If x has least period n, then $\phi(x)$ has period n, and hence its least period divides n. If ϕ is one-to-one, then $\sigma_X^n(x) = x$ if and only if $\sigma_Y^n(\phi(x)) = \phi(x)$, so that x and $\phi(x)$ must have the same least period. □

Theorem 2.4. [2] *Let G be a graph with adjacency matrix A, and let $m \geq 0$. The number of cycles of length m in G is $\mathrm{tr}(A^m)$, the trace of A^m, and this equals the number of points in X_G with period m.*

Proof. The first part of this statement follows from the definition of cycle and the fact that the number of paths of length m from I to J is $(A^m)_{IJ}$, the (I, J)th entry of A^m. For the second part, note that if π is a cycle in G of length m, then π^∞ is a point of period m in X_G, while if $x \in X_G$ has period m, then $x_{[0,m-1]}$ must be a cycle in G of length m. This sets up a one-to-one correspondence between cycles in G of length m and points in X_G of period m. □

Definition 2.5 (Matrix Periodicity)**.** Let A be a nonnegative matrix. The period of a state I, denoted by $\mathrm{per}(I)$, is the greatest common divisor of those integers $n \geq 1$ for which $(A^n)_{II} > 0$. If no such integers exist, we define $\mathrm{per}(I) = \infty$. The period $\mathrm{per}(A)$ of the matrix A is the greatest common divisor of the numbers $\mathrm{per}(I)$ that are finite, or is ∞ if $\mathrm{per}(I) = \infty$ for all I. A matrix is aperiodic if it has period 1. The period $\mathrm{per}(G)$ of a graph G is the period of its adjacency matrix.

Theorem 2.6. [2] *If A is irreducible, then all states have the same period, and so $\mathrm{per}(A)$ is the period of any of its states.*

Proof. Let I be a state, and put $p = \mathrm{per}(I)$. If $p = \infty$, then $A = [0]$ since A is irreducible, and we are done. So we may assume that $p < \infty$. Let J be another state. Then there are $r, s \geq 1$ for which $(A^r)_{IJ} > 0$ and $(A^s)_{JI} > 0$. Let n be such that $(A^n)_{JJ} > 0$. Then

$$(A^{r+s})_{II} \geq (A^r)_{IJ}(A^s)_{JI} > 0,$$

and

$$(A^{r+n+s})_{II} \geq (A^r)_{IJ}(A^n)_{JJ}(A^s)_{JI} > 0.$$

Then p divides both $r+s$ and $r+n+s$, hence their difference n. This shows that p divides all n for which $(A^n)_{JJ} > 0$, so that $p = \text{per}(I)$ divides their greatest common divisor $\text{per}(J)$. Reversing the roles of I and J shows that $\text{per}(J)$ divides $\text{per}(I)$, proving that $\text{per}(I) = \text{per}(J)$. □

Definition 2.7 (Shift Space Periodicity)**.** Let X be a shift space. The period $\text{per}(X)$ of X is the greatest common divisor of integers $n \geq 1$ for which $p_n(X) > 0$, or is ∞ if no such integers exist.

Proposition 2.8. [2] *If G is a graph, then* $\text{per}(X_G) = \text{per}(G)$.

Proposition 2.9. [2] *Let A be a nonnegative matrix. The following are equivalent.*

(1) A is primitive.
(2) $A^N > 0$ for all sufficiently large N.
(3) A is irreducible and aperiodic.

Proposition 2.10. *A shift of finite type is mixing if and only if it is irreducible and* $\text{per}(X) = 1$*, i.e., the greatest common divisor of the periods of its periodic points is* 1.

A key insight is that periodic points of period greater than the looking window of a sliding block code can be used to infer its block map, and thus its action on the entirety of its domain.
Finally, we reach our first novel result.

Theorem 2.11. *For any automorphism g that is not a shift, there exists periodic point p such that $g(p)$ is not a shift of p.*

Proof. We do a proof by contrapositive. Suppose g maps periodic points p to shifts of p.
Let g have radius $r \geq 0$, with corresponding block map $G : A^{2r+1} \to A$. Without loss of generality, let $A = \{0, 1, ..., |A| - 1\}$.
Since g maps 0^∞ to itself, $G(0^{2r+1}) = 0$.
Note $g((0^{2r}1)^\infty) = \sigma^n((0^{2r}1)^\infty)$ for some $n \in \{-r, ..., r\}$. Looking at the symbol output at each coordinate $\{-r, ..., r\}$, we see that for words v of length $2r+1$ with all 0's except one 1, $G(v) = 1$ if the 1 is n to right of the center and $G(v) = 0$ otherwise. That is, $G(0^{r+n}10^{r-n}) = 1$ and $G(v) = 0$ for all other such v.

Let N be some integer such that $N \geq 4r+1$. Let w be an arbitrary word of length $2r+1$ that is not all zeroes, let $W = 10^N w 0^{2N}$, and let $p = W^\infty$. So,

- For $i \in \{-2N, ..., -1\}$, $p_i = 0$.
- For $i = 0$, $p_i = 1$.
- For $i \in \{1, ..., N\}$, $p_i = 0$.
- Finally, $p_{[N+1,N+2r+1]} = w$.

$$p = \ldots \overbrace{0 \ldots\ldots 0}^{2N} .1 \overbrace{0 \ldots 0}^{N} w ...$$

Since p has period $|W| = 3N + 2r + 2$, g maps p to $\sigma^m(p)$ for some $m \in \{-r, ..., 3N + r + 1\}$.

Claim 2.12. *In $g(p)$, there is exactly one 1 in the positions $\{-(3N + r + 1), ..., r\}$ such that at least $2N - 2r$ zeroes immediately precede it, namely the 1 at position $-m$.*

Proof. Since $g(p) = \sigma^m(p)$, the 1 shifted to position $-m$ indeed has $2N \geq 2N - 2r$ zeroes immediately preceding it. Any other 1 must be from w, which would be within $N + |w| = N + 2r + 1 \leq 2N - 2r$ to the right of another 1 not from w. □

Since $-n - r \geq -2r \geq -2N$ and $-n + r \leq 2r \leq N$, the block $p_{[-n-r,-n+r]}$ is all 0's, except one 1 exactly n from the right of the center, $-n$, i.e. $p_{[-n-r,-n+r]} = 0^{r+n}10^{r-n}$. Thus, $G(p_{[-n-r,-n+r]}) = G(0^{r+n}10^{r-n}) = 1$ and so $g(p)_{-n} = 1$.

Claim 2.13. *In $g(p)$, the 1 at position $-n$ has at least $2N - 2r$ zeroes immediately preceding it.*

Proof. Let $i \in \{-n - (2N - 2r), ..., -n - 1\}$. Call the relevant block $p_{[i-r,i+r]}$ the "window".
Note the window's lowest coordinate is at least $-n - (2N - 2r) - r = -2N - n + r \geq -2N$ and the highest coordinate is at most $(-n-1)+r \leq 2r - 1 \leq N$, so the window $p_{[i-r,i+r]}$ is contained in

$$\overbrace{0 \ldots\ldots 0}^{2N} .1 \overbrace{0 \ldots 0}^{N}$$

Then window $p_{[i-r,i+r]}$ is all 0's, except possibly one 1 at position 0¿i+n. Since G($p_{[i-r,i+r]}$)=1 iff $p_{i+n} = 1$, G($p_{[i-r,i+r]}$)=0. Thus, $g(p)_i = 0$.
□

Since $-n \in \{-(3N+r+1), ..., r\}$, Claims 2.12 and 2.13 together imply $n = m$.
Now consider $g(p)_{N+r+1}$. Note it is equal to $G(p_{[N+1,N+2r+1]}) = G(w)$. However, since $g(p) = \sigma^n(p)$, this symbol is also $p_{(N+r+1)+n}$, the symbol

n to the right of the center of w. Since $G(w)$ is the symbol n to the right of the center of w for arbitrary w (including if w is all zeroes), g is a shift; $g = \sigma^n$. $\square$

3. Relevant Results

3.1. **Curtis-Lyndon-Hedlund Theorem.** We heavily credit [2] in this section.

Lemma 3.1. [2] *If S is clopen in shift space X, S is the finite union of cylinder sets.*

Proof. Since S is open, it is the union of cylinder sets. Since S is a closed subset of compact space X, S is compact too. Since the aforementioned union of cylinder sets is an open cover of S, a finite subcollection of those cylinder sets cover S, so S is the finite union of cylinder sets. □

Theorem 3.2 (Curtis-Lyndon-Hedlund Theorem)**.** [2] *The homomorphisms between shift dynamical systems are precisely the sliding block codes. That is, for any shift dynamical systems (X, σ_X) and (Y, σ_Y), $f : X \to Y$ is a homomorphism iff it is a sliding block code.*

Proof. Without loss of generality, let the alphabet of Y be $\{0, ...n-1\}$.
($\Leftarrow$) Suppose f is a sliding block code with radius r. It is clear from the definition that it commutes with the shift.
Let b be an arbitrary symbol in Y's alphabet, and let $C_i(b) = \{y \in Y : y_i = b\}$. Since the open cylinders $C_i(b)$ form a subbasis of Y, it suffices to show $f^{-1}(C_i(b))$ is open. But $x \in X$ is in the inverse image iff f's block map maps $x_{[i-r,i+r]}$ to b, so the inverse image is the union of cylinder sets determining $[i-r, i+r]$, and is thus open.
($\Rightarrow$) Suppose f is a homomorphism.
For each symbol $b \in \{0, ..., n-1\}$, define $P_b = f^{-1}(C_0(b))$. Since f is continuous, P_b is open. Of course, for any $x \in X$, $f(x)_0$ is equal to exactly one element of $\{0, ..., n-1\}$, so the P_b's finitely partition X. Since the complement of each P_b is thus the (finite) union of other pre-images, each P_b is also closed.
Since P_b is clopen, Lemma 3.1 says it is the finite union of cylinder sets, which are finite intersections of open cylinders $C_i(b)$. Since membership in P_b is determined by a finite set of coordinates, there exists r_b such that membership in P_b is determined by the block at $[-r_b, r_b]$. Since there are finite P_b's, there exists r such that for $x \in X$, $x_{[-r,r]}$ determines which P_b it is in. In other words, there exists F such that $F(x_{[-r,r]}) = b$ implies $f(x)_0 = b$.
By shift-commutativity, F is a block code for sliding block code f. □

This extends any of our results from just being about $Aut(X)$ where X is an arbitrary shift space, to precisely stating something about the topological conjugacies of shift dynamical systems at large.

3.2. **Mutual Embedding of Full Shift Automorphism Groups.** In the following proof, we illustrate a conveyor belt construction that proves the automorphism group of any full shift can inject into the automorphism group of any other full shift.

Theorem 3.3. [6] *For any valid alphabets A and B, there exists injective homomorphism $\phi : Aut(A^{\mathbb{Z}}) \to Aut(B^{\mathbb{Z}})$.*

Proof. Without loss of generality, let $A = \{0, 1, 2, ..., |A| - 1\}$ and $B = \{0, 1, ..., |B| - 1\}$.
Fix some $c \in \mathbb{Z}$ where $2^c \geq |A|$. Consider the map $\gamma : A \to \{0, 1\}^{3c} \subseteq B^{3c}$ that maps symbols to their c-digit binary representation, then replaces each 0 with 000 and each 1 with 010. This is injective; γ gives every symbol in $|A|$ a length $3c$ representation in B^{3c}.
For any point $y \in B^{\mathbb{Z}}$, consider marking every symbol other than 0 or 1. Also, mark any 1, unless it is surrounded by two 0's.
Consider the unmarked blocks between marked symbols. Restrict our attention to the blocks of length $6c$, such that the first and second half represent symbols in A via γ. That is, consider such blocks w such that $w = \gamma(t_w)\gamma(b_w)$ for some $t_w, b_w \in A$. We call such blocks "valid" and call t_w the "top" and b_w the "bottom" symbol of w, writing

$$w = \begin{bmatrix} t_w \\ b_w \end{bmatrix}.$$

Consider any $g \in \mathrm{Aut}(A^{\mathbb{Z}})$, with radius $r \geq 0$ and block map $G : A^{2r+1} \to A$. Let $R = (6c - 1) + r(6c + 2) + 2$. We define the block map $G' : B^{2R+1} \to B$ by the following algorithm:

Let the input $I \in B^{2R+1}$ be indexed $-R$ to R.
Since we know their neighbors, we know whether entries $-(R-1)$ to $R-1$ are marked. "Valid" blocks are between marked symbols, so we can determine every "valid" block starting at $-(R-2)$ and ending at $R-2$.
If index 0 is not part of a "valid" block, return I_0.
We will defines points $t, b \in A^{\mathbb{Z}}$ from $-r$ to r. Initialize t_0, b_0 as the "top" and "bottom" symbols of the "valid" block in the middle (i.e. containing index 0), $\begin{bmatrix} t_0 \\ b_0 \end{bmatrix}$. We say this block is at position 0.

Initialize $p = 0$, $h = top$, and $d = right$.
For $i = 1, ..., r$:
Starting from the block in position p, moving in direction d, check if it's followed by 11, followed by another "valid" block.
If so, increment p (or if $d = left$, decrement p).
Else, flip h between top and $bottom$, and flip d between $left$ and $right$.
Set t_i as the element in A corresponding the top (or if $h = bottom$, bottom) of the "valid" block at position p.

In this way, we determine $t_1, ..., t_r$.
Do the same for $t_{-1}, ..., t_{-r}$ by starting instead with $h = top$ and $d = left$.
Do the same for $b_1, ..., b_r$ by starting instead with $h = bottom$ and $d = left$.
Do the same for $b_{-1}, ..., b_{-r}$ by starting instead with $h = bottom$ and $d = right$.
Thus, t and b are defined from $-r$ to r. Compute $G(t_{[-r,r]})$ and $G(b_{[-r,r]})$. Then, return the symbol at index 0 for if the "valid" block in the middle, $\begin{bmatrix} t_0 \\ b_0 \end{bmatrix}$, were replaced by

$$\begin{bmatrix} G(t_{[-r,r]}) \\ G(b_{[-r,r]}) \end{bmatrix}.$$

By inspection, this algorithm always halts.
We must also check it never attempts to check for a "valid" block outside of the radius it can see "valid" blocks, $[-(R-2), R-2]$. Since each "valid" block is length $6c$, the furthest right the rightmost symbol of the block at position 0 can be is position $6c-1$. Each relevant "valid" block is separated by 11, so they are each $6c+2$ apart. Relevant "valid" blocks have position at most p, so the furthest right the symbols of "valid" blocks can be is $(6c-1) + r(6c+2) \leq R-2$.
By symmetry, the furthest left possible "valid" block is within the radius, too. So, G' is a well-defined block code.

Claim 3.4. *The points $t, b \in A^{\mathbb{Z}}$ are well-defined in their entirety, independent of G. Furthermore,*

$$\begin{bmatrix} G(t_{[-r,r]}) \\ G(b_{[-r,r]}) \end{bmatrix} = \begin{bmatrix} g(t)_0 \\ g(b)_0 \end{bmatrix}.$$

Proof. The algorithm defines t from $-r$ to r, but it does so independently from what G actually does, and it does so iteratively (so for any other, larger r', we have at each smaller index $i \in \{-r, ...r\}$ a consistent value for t_i). The same goes for b, so $t, b \in A^{\mathbb{Z}}$ are entirely well-defined, independent of G.
So, by definition, $G(t_{[-r,r]}) = g(t)_0$ and $G(b_{[-r,r]}) = g(b)_0$. □

Let $\mathbf{B}$ be the set of (not necessarily invertible) sliding block codes from $B^{\mathbb{Z}}$ to $B^{\mathbb{Z}}$. Define $\phi : \mathrm{Aut}(A^{\mathbb{Z}}) \to \mathbf{B}$ where $g \in \mathrm{Aut}(A^{\mathbb{Z}})$ is mapped to the sliding block code $\phi(g)$ corresponding to the block code $G' : B^{2R+1} \to B$ defined by the earlier algorithm.

Claim 3.5. *For any $f, g \in Aut(A^{\mathbb{Z}})$, $\phi(fg) = \phi(f)\phi(g)$.*

Proof. Since the algorithm only changes symbols in "valid" blocks, it suffices to show $\phi(fg)$ and $\phi(f)\phi(g)$ do the same thing to "valid" blocks. Let f have block code F with radius r_F, and g have block code G with radius r_G.
Let $\begin{bmatrix} t_0 \\ b_0 \end{bmatrix}$ be a "valid" block in some middle, as per the algorithm. Then $\phi(fg)$ replaces it with

$$\begin{bmatrix} fg(t)_0 \\ fg(b)_0 \end{bmatrix}.$$

Meanwhile, for $\phi(g)$, we consider each "valid" block at position p (that is, followed by $|p|$-many 11s and "valid" blocks, in the direction corresponding to the sign of p). Since the positive direction is rightward on top and leftward on bottom, it starts off being

$$\begin{bmatrix} t_p \\ b_{-p} \end{bmatrix},$$

and by the iterative definition of t and b, the "t" and "b" from here are actually $\sigma^p(t)$ and $\sigma^{-p}(b)$, so the $\phi(g)$ changes this "valid" block to

$$\begin{bmatrix} g(\sigma^p(t))_0 \\ g(\sigma^{-p}(b))_0 \end{bmatrix} = \begin{bmatrix} \sigma^p(g(t))_0 \\ \sigma^{-p}(g(b))_0 \end{bmatrix} = \begin{bmatrix} g(t)_p \\ g(b)_{-p} \end{bmatrix}.$$

Then, since each t_i is replaced by $g(t)_i$ and each b_i is replaced by $g(b)_i$ (for valid positions i, and thus for all $i \in \mathbb{Z}$ - for t, hitting the edge

just means reading the corresponding b entries instead, et cetera), after applying $\phi(f)$ we once again get the block

$$\begin{bmatrix} fg(t)_0 \\ fg(b)_0 \end{bmatrix}$$

replacing the "valid" block in the middle. □

Claim 3.6. *For the identity $e \in Aut(A^{\mathbb{Z}})$, $\phi(e)$ is the identity on $B^{\mathbb{Z}}$.*

Proof. As per usual, symbols outside of "valid" blocks are unchanged. As per the algorithm, for any "valid" block $\begin{bmatrix} t_0 \\ b_0 \end{bmatrix}$, since the G for e just returns the symbol in the middle,

$$\begin{bmatrix} G(t_{[-r,r]}) \\ G(b_{[-r,r]}) \end{bmatrix} = \begin{bmatrix} t_0 \\ b_0 \end{bmatrix}$$

and so the "valid" blocks remain the same too. □

Corollary 3.7. *For any $f \in Aut(A^{\mathbb{Z}})$, $\phi(f)$ is invertible. In fact, ϕ is a homomorphism from $Aut(A^{\mathbb{Z}})$ to $Aut(B^{\mathbb{Z}})$.*

Proof. By the last two claims,

$$\phi(f)\phi(f^{-1}) = \phi(ff^{-1}) = \phi(e) = e$$

and

$$\phi(f^{-1})\phi(f) = \phi(f^{-1}f) = \phi(e) = e,$$

so $\phi(f^{-1})$ is the inverse of $\phi(f)$.
Thus, the output of ϕ is always invertible; we may redefine ϕ to have the restricted codomain of $\mathrm{Aut}(B^{\mathbb{Z}})$.
Again using Claim 3.5, we see this map is a homomorphism. □

Claim 3.8. *The map ϕ is injective.*

Proof. Suppose $f, g \in \mathrm{Aut}(A^{\mathbb{Z}})$ are distinct; then there exists $x \in \mathrm{Aut}(A^{\mathbb{Z}})$ such that $f(x) \neq g(x)$.
Then, for the following point in $\mathrm{Aut}(B^{\mathbb{Z}})$,

$$\ldots \begin{bmatrix} x_{-2} \\ x_2 \end{bmatrix} 11 \begin{bmatrix} x_{-1} \\ x_1 \end{bmatrix} 11. \begin{bmatrix} x_0 \\ x_0 \end{bmatrix} 11 \begin{bmatrix} x_1 \\ x_{-1} \end{bmatrix} 11 \begin{bmatrix} x_2 \\ x_{-2} \end{bmatrix} \ldots$$

$\phi(f)$ maps it to

$$\ldots \begin{bmatrix} f(x)_{-2} \\ f(x)_2 \end{bmatrix} 11 \begin{bmatrix} f(x)_{-1} \\ f(x)_1 \end{bmatrix} 11. \begin{bmatrix} f(x)_0 \\ f(x)_0 \end{bmatrix} 11 \begin{bmatrix} f(x)_1 \\ f(x)_{-1} \end{bmatrix} 11 \begin{bmatrix} f(x)_2 \\ f(x)_{-2} \end{bmatrix} \ldots$$

whereas $\phi(g)$ maps it to

$$\ldots \begin{bmatrix} g(x)_{-2} \\ g(x)_2 \end{bmatrix} 11 \begin{bmatrix} g(x)_{-1} \\ g(x)_1 \end{bmatrix} 11. \begin{bmatrix} g(x)_0 \\ g(x)_0 \end{bmatrix} 11 \begin{bmatrix} g(x)_1 \\ g(x)_{-1} \end{bmatrix} 11 \begin{bmatrix} g(x)_2 \\ g(x)_{-2} \end{bmatrix} \ldots$$

so since $f(x)$ and $g(x)$ differ somewhere, so do these points.
So, $\phi(f) \neq \phi(g)$. □

Thus, we have found an injective homomorphism ϕ from arbitrary $\mathrm{Aut}(A^{\mathbb{Z}})$ to $\mathrm{Aut}(B^{\mathbb{Z}})$. □

3.3. **Markers and Subgroups.** We heavily credit [1] in this section. Consider a primitive matrix T≠[1] and its corresponding graph G and its corresponding mixing edge shift X_T.

Definition 3.9 (Overlapping blocks)**.** Two blocks overlap if an initial segment of one coincides with a terminal segment of the other. A collection of blocks in $B(X_T)$ has only trivial overlaps if distinct blocks do not overlap and each block overlaps itself only in the entire block.

Suppose $M \in B_m(X_T)$ and that $\mathcal{D} \subset B_k(X_T)$ is a collection of blocks with $M\mathcal{D}M = \{MDM : D \in \mathcal{D}\} \subset B_{2m+k}(X_T)$ such that for every $D \in \mathcal{D}$ the block M can overlap the concatenation MDM in only the initial and final segments of length m (this disallows even partial overlaps at the ends). Note Lemma 3.10 allows us an ample supply of blocks with trivial overlaps. Let π be an arbitrary permutation of $\mathcal{D}$. Define the action of a block map φ_π on $x \in X_T$ as follows. For each i, if $x[i, i+2m+k-1] = MDM$, define $(\varphi_\pi x)[i, i+2m+k-1] = M\pi(D)M$. Require φ_π to have no other action. Because the blocks from $M\mathcal{D}M$ cannot overlap except for the marker M, this is a well-defined σ-invariant map of finite order, so $\varphi_\pi \in Aut(X_T)$. The correspondence $\pi \leftrightarrow \varphi_\pi$ hence embeds the symmetric group sym($\mathcal{D}$) into Aut(X_T). We will show $|\mathcal{D}|$ can be made arbitrarily large by an appropriate choice of M. This implies by Cayley's Theorem that every finite group embeds into Aut(X_T).

Lemma 3.10. [1] *There is a collection* $M = \bigcup_{n=1}^{\infty} M_n \subset B(X_T)$ *such that* M_n *contains* n *blocks of equal length,* M *has only trivial overlaps, and*

$$M_M = \{MM' : M, M' \in M\} \subset B(X_T).$$

Proof. Since T is primitive and $T \neq [1]$ by our convention, there must be a loop $i_0 i_1 \cdots i_k i_0 \in B(X_T)$ of distinct symbols with $k \geq 1$. This is since the diagonal elements of T^N are non-zero for sufficiently large N, which means nodes of its corresponding graph have paths of length N to themselves.
Furthermore, one of these symbols, which we can assume is i_0, is followed by a symbol $j_1 \neq i_1$. Otherwise, G would have a cycle disconnected from the rest of G. This cycle is also not all of G since then T would not be an aperiodic.
First suppose $j_1 \neq i_0$. Choose a path of minimal length from j_1 to the loop, say $j_1 j_2 \cdots j_r i_s$. The case $r = 0$ is possible and corresponds to $j_1 = i_s$ for some $s \neq 0, 1$. Define $A = i_0 \cdots i_k$, $B = i_0 j_1 j_2 \cdots j_r i_s \cdots i_k \in B(X_T)$. For $1 \leq q \leq n$ define $M_{nq} = A^2 B^q A B^{n-q+1}$. Noting the positions of i_0 in these blocks, it follows from the above minimality of

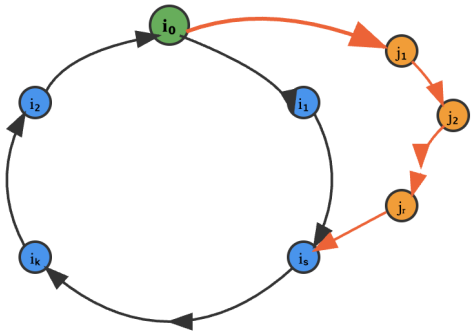

FIGURE 3. $j_1 \neq i_0$

paths that $M = \{M_{nq} : 1 \leq q \leq n, n \geq 1\}$ has only trivial overlaps, and that $MM \subset B(X_T)$ by construction. Since the lengths $|M_{nq}|$ are equal for $1 \leq q \leq n$, the collections $M_n = \{M_{nq} : 1 \leq q \leq n\}$ satisfy the conclusions.

The remaining possibility is for $j_1 = i_0$. In this case let $A = i_1 \cdots i_q i_0$, and put $M_{nq} = A^2 i_0^q A i_0^{n-q+1}$. Again noting the positions of i_0 in the M_{nq} shows that $M_n = \{M_{nq} : 1 \leq q \leq n\}$ for $n \geq 1$ satisfy the conclusions. □

Using this lemma, we can prove a wide variety of groups are contained in $\mathrm{Aut}(X_T)$.

Theorem 3.11. [1] *The group* $\mathrm{Aut}(X_T)$ *contains the free product of any finite number of* 2*-element groups. Thus it contains the free group on two generators, hence the free group on a countable number of generators.*

Proof. We embed the free product of three copies of $\mathbb{Z}/2\mathbb{Z}$, the generalization to more copies being routine. We first work on a special full shift, then carry this over to a general σ_T.
Note all full shifts embed into each other, so without loss of generality, let the alphabet be $\mathcal{L} = \{0, 1, 2, 3, *\}$. Define involutions φ_j for $j = 1, 2, 3$ as follows. All will be 2-block maps, and each will exchange three pairs of 2-blocks. Specifically, φ_j exchanges $s0$ with sj for $s \in \mathcal{L} \setminus \{0, j\}$. Thus each φ_j uses three markers for its definition, and has the important property that markers defining its action are not affected by it. It follows that each $\varphi_j \in \mathrm{Aut}(\mathcal{L}^{\mathbb{Z}})$. Let P be the free product of the 2-element groups $\{e, j\}$ for $j = 1, 2, 3$. Define a homomorphism from P to $\mathrm{Aut}(\mathcal{L}^{\mathbb{Z}})$ by mapping a reduced word $w = j_n \cdots j_1 \in P$ to $\psi = \varphi_{j_n} \cdots \varphi_{j_1}$. Since each $\varphi_j^2 = I$, the identity, this is well-defined. Consider the point $x = \cdots 0000 * 0000 \cdots$, with $x_0 = *$. Then $(\psi x)_n = j_n$, $(\varphi_{j_n}^{-1} \psi x)_{n-1} = j_{n-2}$ and so on. This means that inductively ψ determines the spelling of w, so this mapping embeds P into $\mathrm{Aut}(\mathcal{L}^{\mathbb{Z}})$. It is elementary group theory that P contains the free group F_2 of two generators. Moreover, all free groups on countable number of generators embed into F_2.
This idea generalizes to arbitrary X_T by using markers instead of symbols. If $\mathcal{L}_T$ is the alphabet for X_T, for each $a \in \{0, 1, 2, 3, *\}$ use Lemma 3.10 to construct a marker M_a over $\mathcal{L}_T$, all of equal length with only trivial overlaps, and beginning with and followed by i_0. Define involutions φ_j, $1 \leq j \leq 3$, to exchange $M_s M_0 i_0$ with $M_s M_j i_0$ for $s \in \mathcal{L} \setminus \{0, j\}$, and have no other effect. Since these markers have only trivial overlaps, the φ_j are well-defined. The argument that they generate the free product of three copies of $\mathbb{Z}/2\mathbb{Z}$ is exactly as before. □

4. Embedding Free Groups

Presently, many questions persist about the algebraic structure of automorphism groups of full shifts, $\mathrm{Aut}(A^{\mathbb{Z}})$. For example, the simple question of whether $\mathrm{Aut}(2^{\mathbb{Z}})$ and $\mathrm{Aut}(3^{\mathbb{Z}})$ are isomorphic remains unanswered [3].
One major result was Ryan's Theorem [8]:

Theorem 4.1. *The center of $Aut(A^{\mathbb{Z}})$ is just the shifts.*

Boyle, Lind and Rudolph [1] stated that Ryan's Theorem can be used to prove $\mathrm{Aut}(2^{\mathbb{Z}})$ and $\mathrm{Aut}(4^{\mathbb{Z}})$ are, in fact, not isomorphic.
More recently, Frisch, Schlank and Tamuz [3] proved

Theorem 4.2. *Every normal amenable subgroup of $Aut(A^{\mathbb{Z}})$ is a subgroup of the shifts.*

This is a generalization of Ryan's Theorem, as (essentially by definition) every shift is in the center, and since the center is necessarily abelian, it is amenable as well as normal in $\mathrm{Aut}(A^{\mathbb{Z}})$.
Our main result is a further strengthening of Ryan's Theorem: for normal subgroups that are not just a subgroup of the shifts, not only are they non-amenable, they in fact contain the free group on countable generators.
We now behold our ultimate novel result.

Theorem 4.3. *If N is a normal subgroup of $Aut(A^{\mathbb{Z}})$, either N is a subgroup of the shifts or it contains a free subgroup on two generators, hence the free group on a countable number of generators.*

Proof. Let $g \in N$ not be a shift. Then there exists blocks u, v such that $|u| = |v|$ and $g(u^\infty) = v^\infty$ and v^∞ is not a shift of u^∞. Let $n = |u|$.
Let r be the looking window of g and G:$A^{2r+1} \to A$ be its block map.
Let $s \in A$ such that $u \neq s$ (in case $|u| = 1$). Let $M \geq 2(r + 2n)$.
Let X be the subshift of $A^{\mathbb{Z}}$ where the only legal blocks of length $nM+1$ are those found in $(su^M)^\infty$ and u^∞. Let $Y = g(X)$.
Let $c = 2\lceil r/n \rceil$. Note g$((su^M)^\infty)$=$\sigma^r((bv^{M-c})^\infty)$ for some $|b| = cn+1$.
Then Y precisely includes the points only consisting of blocks of length $nM + 1$ found in v^∞ and $(bv^{M-c})^\infty$.
Consider $H = \{a \in \mathrm{Aut}(A^{\mathbb{Z}}) : a|_X = id, a(Y) = Y\}$, $\hat{H} = \{a \in \mathrm{Aut}(A^{\mathbb{Z}}) : a(Y) = Y\}$.
For any $a \in H$, consider arbitrary $y \in Y$. Since $a(y) \in Y$, we have $g^{-1}a(y) \in X$. Thus, $a^{-1}g^{-1}a(y) = g^{-1}a(y)$. Thus, $ga^{-1}g^{-1}a(y) = gg^{-1}a(y) = a(y)$. In other words, $ga^{-1}g^{-1}a$ and a are the same when restricted to Y.

Thus, the map $\varphi : H \to \hat{H}$ such that $\varphi(a) = ga^{-1}g^{-1}a$ is well defined and makes the following diagram commute:

$$\begin{array}{ccc} H & \xrightarrow{\text{restrict}} & \hat{H}|_Y \\ {\scriptstyle\varphi}\downarrow & \searrow^{\varphi} & \uparrow{\scriptstyle\text{restrict}} \\ N \supset [g{:}H] & \xhookrightarrow{\text{inclusion}} & \hat{H} \end{array}$$

(Note φ is not necessarily a homomorphism.)

Claim 4.4. *X is a mixing subshift of finite type of $A^{\mathbb{Z}}$.*

Proof. It is a shift space of finite type since there are a finite number of blocks of length $nM + 1$. To illustrate that it is mixing, let p, q be blocks that appear in points of X. Then,
for $l \geq M^2n^2$ there exists a block $w = (u^M a)^{l \bmod Mn}\, u^{(\lfloor \frac{l}{Mn} \rfloor - (l \bmod Mn))\cdot M}$ in the language of X of length l so that

$$\ldots uuuu\, p\, w\, q\, uuuu \ldots$$

is a point. To make the construction perfectly clear, the point is

$$\ldots uuuu\, p\, \overbrace{u^M a u^M a \ldots u^M a}^{l \bmod Mn} \quad \overbrace{u^M \ldots u^M}^{\lfloor \frac{l}{Mn} \rfloor - (l \bmod Mn)} \quad q\, uuuu \ldots$$

Note that $\lfloor \frac{l}{Mn} \rfloor - (l \bmod Mn) \geq Mn - (Mn - 1) = 1$, so there are atleast M u's at the end of w, and the point is in fact in X. The length of w is l due to the calculation shown below:

$$|w| = |u^M a| \cdot (l \bmod Mn) + |u^M| \cdot (\lfloor \frac{l}{Mn} \rfloor - (l \bmod Mn))$$

$$= (Mn + 1) \cdot (l \bmod Mn) + Mn \cdot (\lfloor \frac{l}{Mn} \rfloor - (l \bmod Mn))$$

$$= Mn \cdot (l \bmod Mn) + (l \bmod Mn) + Mn \cdot \lfloor \frac{l}{Mn} \rfloor - Mn \cdot (l \bmod Mn)$$

$$= ((l \bmod Mn) + Mn \cdot \lfloor \frac{l}{Mn} \rfloor) + (Mn \cdot (l \bmod Mn) - Mn \cdot (l \bmod Mn))$$

$$= l + 0 = l.$$

□

Note $\hat{H}|_Y = \mathrm{Aut}(Y)$. Since $Y = g(X)$, g is an automorphism, and X is a mixing subshift of finite type, $\mathrm{Aut}(Y)$ is mixing subshift of finite type by 1.19 and 1.24. Additionally, by Theorem 3.11 [1], $\mathrm{Aut}(Y)$ contains the free group on two generators, hence the free group on a countable number of generators. Thus $\hat{H}|_Y$ contains the free group

on two generators, hence the free group on a countable number of generators.

Claim 4.5. *The restriction map from H to $\hat{H}|_Y$ are surjective.*

Proof. Note that for every $\hat{a} \in \mathrm{Aut}(Y) = \hat{H}|_Y$, $\hat{a}$ can be extended to X by defining it on looking window at least nM, noting that if we ever see u^M, we act as the identity. Seeing a copy of u^M implies the point is not in Y since u is not a shift of v, so the largest block in Y that does not contain a copy of v is size

$$2n + |b| - 2 = 2n + cn + 1 - 2 = 2n + 2\lceil r/n \rceil \cdot n - 1,$$

and since $\lceil r/n \rceil \leq r/n + 1$,

$$2n + 2\lceil r/n \rceil \cdot n - 1 \leq 2n + 2(r+n) - 1 \leq 2(r+2n) - 1 < nM = |u^M|.$$

Thus, we have found an automorphism $a \in H$ which extend $\hat{a}$ to act as the identity on X, so the map is surjective. □

Let $\langle a, b \rangle$ be a free group in $\hat{H}|_Y$. Let α, β be a choice of preimage of a and b in H. We claim that $\varphi(\alpha)$ and $\varphi(\beta)$ have no relations in $[g{:}H]$. $\varphi(\alpha)$ and $\varphi(\beta)$ in $[g{:}H] \subset \hat{H}$ must map to a free group in $\hat{H}|_Y$. But this implies that they have no relations in $[g{:}H]$, as desired.
Since $[g{:}H] \subset N$, $\varphi(\alpha)$ and $\varphi(\beta)$ have no relations in N. Thus, Ncontains the free group on two generators, hence the free group on a countable number of generators.

□

References

[1] Mike Boyle, Douglas Lind, and Daniel Rudolph, *The automorphism group of a shift of finite type*, Transactions of the American Mathematical Society **306** (1988), no. 1, 71–114.

[2] Douglas A. and Marcus Lind Brian, *An Introduction to Symbolic Dynamics and Coding*, Cambridge University Press, USA, 1995.

[3] JOSHUA and SCHLANK FRISCH TOMER and TAMUZ, *Normal amenable subgroups of the automorphism group of the full shift*, Ergodic Theory and Dynamical Systems **39** (2017), no. 5, 1290–1298, DOI 10.1017/etds.2017.72.

[4] Scott Schmieding, *Symbolic Dynamics and Subshifts of Finite Type*, 2018. Accessed: 2025-05-30.

[5] Yair Hartman and Bryna Kra and Scott Schmieding, *The stabilized automorphism group of a subshift*, 2020.

[6] K. H. Kim and F. W. Roush, *On the Automorphism Groups of Subshifts*, Pure Mathematics and Applications, Series B **1** (1990), no. 4, 203–230.

[7] J. Patrick Ryan, *The shift and commutativity*, Mathematical Systems Theory **6** (1972), no. 2, 82–85, DOI 10.1007/BF01706077.

[8] ———, *The shift and commutativity II*, Mathematical Systems Theory **8** (1974), no. 3, 249–250, DOI 10.1007/BF01762673.