Y. Hartman *et al.* (2022) "The Stabilized Automorphism Group of a Subshift,"
International Mathematics Research Notices, Vol. 2022, No. 21, pp. 17112–17186
Advance Access Publication August 6, 2021
https://doi.org/10.1093/imrn/rnab204

The Stabilized Automorphism Group of a Subshift

Yair Hartman[1], Bryna Kra[2,*], and Scott Schmieding[3]

[1]Ben-Gurion University of the Negev, 8410501, Israel, [2]Northwestern University, Evanston, IL 60208, USA, and [3]University of Denver, Denver, CO 80208, USA

[*]*Correspondence to be sent to: e-mail: kra@math.northwestern.edu*

For a mixing shift of finite type, the associated automorphism group has a rich algebraic structure, and yet we have few criteria to distinguish when two such groups are isomorphic. We introduce a stabilization of the automorphism group, study its algebraic properties, and use them to distinguish many of the stabilized automorphism groups. We also show that for a full shift, the subgroup of the stabilized automorphism group generated by elements of finite order is simple and that the stabilized automorphism group is an extension of a free abelian group of finite rank by this simple group.

1 Distinguishing Automorphism Groups

1.1 Automorphism groups and stabilized automorphism groups

Let (X,σ) be a shift over a finite alphabet $\mathcal{A}$, that is, $X \subset \mathcal{A}^{\mathbb{Z}}$ is closed and invariant under the left shift $\sigma\colon \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$. The automorphism group $\mathrm{Aut}(X,\sigma)$ of the shift is the collection of homeomorphisms $\phi\colon X \to X$ such that $\phi \circ \sigma = \sigma \circ \phi$. For many shifts with complicated dynamical behavior, including any mixing shift of finite type, the associated automorphism group is known to have a rich algebraic structure, for example, containing isomorphic copies of any finite group, the countably infinite direct sum of copies of $\mathbb{Z}$, and the free group on two generators (see [6, 11]). In contrast to

Received July 16, 2020; Revised March 9, 2021; Accepted July 8, 2021

shifts of finite type, numerous results show that for many zero entropy shifts, the automorphism group is more constrained (see, e.g., [8–10]).

In spite of much attention, several natural and simple to state questions remain open. Boyle *et al.* [6] raised the question of distinguishing (up to isomorphism) the automorphism groups of full shifts (X_n, σ_n) for various n (meaning $X_n = \mathcal{A}^{\mathbb{Z}}$ and the alphabet $\mathcal{A}$ has n symbols). They ask if the automorphism group of the full shift on 2 symbols is isomorphic to the automorphism group of the full shift on 3 symbols, and more generally, for which p and q the groups $\mathrm{Aut}(X_p, \sigma_p)$ and $\mathrm{Aut}(X_q, \sigma_q)$ are isomorphic as groups. For some choices of p and q, such as when $q = p^2$ for a prime p, one can show that the associated automorphism groups are not isomorphic (this was explicitly pointed out for 2 and 4 in [6], and we make note in Theorem 2.5 of the natural generalization using their method). But for general p and q, this problem remains open.

While many groups are known to embed into the automorphism group of a shift of finite type, the subgroup structure of the automorphism groups cannot be used to distinguish them, as shown by a result of Kim and Roush [16]. Namely, they showed that the automorphism group of any full shift can be embedded into the automorphism group of any other full shift (in fact, it can be embedded into the automorphism group of any mixing shift of finite type). Thus, any strategy for distinguishing two automorphism groups relying on finding some subgroup of one that does not lie in the other must fail.

Taking a new approach to this problem, we define a certain stabilization of the automorphism group and show that many of these stabilized groups can be distinguished (up to isomorphism) based only on the alphabet size. To simplify notation, we suppress the associated space in the notation for the automorphism group, writing $\mathrm{Aut}(\sigma_X)$ instead of $\mathrm{Aut}(X, \sigma_X)$. We make a slight abuse of notation for the full shift on n symbols, writing $\mathrm{Aut}(\sigma_n)$ for its automorphism group.

For a subshift (X, σ_X), we define the *stabilized automorphism group* $Aut^{(\infty)}(\sigma_X)$ to be

$$\mathrm{Aut}^{(\infty)}(\sigma_X) = \bigcup_{k=1}^{\infty} \mathrm{Aut}(\sigma_X^k).$$

Passing from the non-stabilized automorphism group to the stabilized setting offers certain advantages, and some of our results are analogous to what happens in the realm of algebraic K-theory. Given a ring $\mathcal{R}$, one defines the stabilized general linear group $GL(\mathcal{R})$ by taking the union of the finite general linear groups $GL_n(\mathcal{R})$. An important subgroup of $GL_n(\mathcal{R})$ is $E_n(\mathcal{R})$, the subgroup generated by elementary matrices (matrices that differ from the identity in at most one coordinate), and in 1950, Whitehead [38]

proved that the commutator of $GL(\mathcal{R})$ coincides with the stabilized subgroup of elementary matrices $E(\mathcal{R})$. One way to interpret this result is that, by stabilizing, a certain abstract subgroup that is defined group-theoretically (in this case the commutator) may be identified with a concrete naturally occurring subgroup: the group of stabilized elementary matrices. In the setting where (X, σ_X) is a shift of finite type, stabilizing produces analogous results. While the commutator of $\mathrm{Aut}(\sigma_X)$ is not very well understood, we prove in Theorem 3.14 that, at the stabilized level, the abelianization of $\mathrm{Aut}^{(\infty)}(\sigma_X)$ coincides with the abelianization of a certain explicit quotient of $\mathrm{Aut}^{(\infty)}(\sigma_X)$: the dimension representation (see Section 3.4 for definitions). Thus, in many cases (e.g., when (X, σ_X) is a full shift), the commutator subgroup of $\mathrm{Aut}^{(\infty)}(\sigma_X)$ coincides with a certain naturally occurring subgroup (the subgroup of stabilized inert automorphisms).

Illustrating the stronger tools available in the stabilized setting, we are able to distinguish many stabilized automorphism groups for which there are currently no techniques to distinguish the (non-stabilized) counterparts. In particular, in Section 3.5, we show that the stabilized automorphism groups of full shifts on alphabets with different numbers of prime factors cannot be isomorphic.

Theorem 1.1. Assume that (X_m, σ_m) and (X_n, σ_n) are the full shifts on m and n symbols for some integers $m, n \geq 2$, and assume that the stabilized automorphism group $\mathrm{Aut}^{(\infty)}(\sigma_m)$ on m symbols and the stabilized automorphism group $\mathrm{Aut}^{(\infty)}(\sigma_n)$ on n symbols are isomorphic. Then, m and n have the same number of distinct prime divisors.

In particular, this means that the stabilized automorphism groups on 2 symbols and 6 symbols are not isomorphic; the analog of this result for the (non-stabilized) automorphism groups on 2 and on 6 symbols remains open. However, our results do not distinguish the stabilized automorphism groups with 2 and 3 symbols or those with 6 and 12 symbols, and another method is needed to address this question (see Question 3.23).

After the results in this article were proven, the 3rd author [34] has proven a stronger result, showing that the stabilized groups $\mathrm{Aut}^{(\infty)}(\sigma_m)$ and $\mathrm{Aut}^{(\infty)}(\sigma_n)$ are isomorphic if and only if $m^k = n^j$ for some $k, j \geq 1$.

In Section 3, we prove various properties of the stabilized automorphism group and compare them with the (non-stabilized) automorphism group of the shift. It is easy to check that, as for the automorphism group, the stabilized automorphism group is countable. We also prove that, like the automorphism group, the stabilized

automorphism group is not finitely generated; in contrast, though, the proof is quite different from the proof for the non-stabilized case.

However, differences between the (non-stabilized) automorphism group and the stabilized group appear quickly. For example, while Ryan's [32, 33] theorem states that the center of the automorphism is exactly the powers of the shift, in Proposition 3.8, we show that the stabilized automorphism group has a trivial center.

A mixing shift of finite type (X_A, σ_A) has a dense set of periodic points, and as a result, the action of the automorphism group on X_A is far from minimal and has many invariant measures. However, it follows from a result of Boyle *et al.* [6] that the $\mathrm{Aut}^{(\infty)}(\sigma_A)$-action on the space X_A is minimal and uniquely ergodic. We discuss this in Section 3.3.

An important tool for studying $\mathrm{Aut}(\sigma_X)$ when (X, σ_X) is a shift of finite type is the dimension representation, a certain homomorphism from $\mathrm{Aut}(\sigma_X)$ to the group of automorphisms of an ordered abelian group associated with (X, σ_X). The kernel of this dimension representation, known as the subgroup of inert automorphisms, is a large, algebraically rich subgroup of $\mathrm{Aut}(\sigma_X)$; for example, in the case of a full shift, the automorphism group is an extension of a finitely generated free abelian group by the inert subgroup. However, in general the inert subgroup is not well understood. In Section 3, we show that the dimension representation extends naturally to a stabilized dimension representation and that the abelianization of the group $\mathrm{Aut}^{(\infty)}(\sigma_X)$ factors through this stabilized dimension representation. Similar to the non-stabilized group $\mathrm{Aut}(\sigma_X)$, the kernel of the stabilized dimension representation, which we refer to as the group of stabilized inerts, constitutes the core combinatorial part of $\mathrm{Aut}^{(\infty)}(\sigma_X)$. In the classical (non-stabilized) setting, the inert subgroup $\mathrm{Inert}(\sigma_X) \subset \mathrm{Aut}(\sigma_X)$ is residually finite, and hence (since $\mathrm{Inert}(\sigma_X)$ is infinite) is far from simple. In stark contrast to this, in Section 5, we prove the following theorem.

Theorem 1.2. For any $n \geq 2$, the group of stabilized inert automorphisms of the full shift (X_n, σ_n) is simple.

In some sense, the stabilized automorphism groups capture different information about the shift system than the non-stabilized automorphism groups. For example, the stabilized automorphism groups for the full shift on 2 symbols and on 4 symbols are isomorphic, whereas for the automorphism groups this is essentially the only case in which these groups can be distinguished. However, there is often an advantage in working with a stabilized object involving sufficiently high powers of the

transformation, rather than the original object. Examples of success in solving problems in the stabilized setting, but which are still open in the non-stabilized setting, are Wagoner's [36] Finite Order Generation Theorem for stabilized inert automorphisms, the classification [14, 39] of shifts of finite type up to topological conjugacy, and the characterization [7] of the existence of a closing factor map between equal entropy mixing shifts of finite. Some of these results, in turn, have shed light on problems in the non-stabilized setting, such as the use of shift equivalence to address the problem of classification of shifts of finite type up to conjugacy.

In this direction, we use our results on the stabilized automorphism group to address a question about the (non-stabilized) automorphism group. As part of our analysis in the stabilized setting, we make key use of a particularly important class of inert automorphisms, introduced by Nasu [28], called simple automorphisms. Wagoner [36] asked whether the group of inert automorphisms is always generated by simple automorphisms. Kim and Roush [17] answered Wagoner's question by constructing a particular shift of finite type that has an inert automorphism that is not a product of simple automorphisms. Our methods (together with the realization results in [19, 20]) also show that the same result holds for a wide class of shifts of finite type; for example, any shift of finite type having at least three fixed points and no points of least period two (we note this can also be deduced using some results from [3], though our methods are quite different). However, we do not know if this phenomena is even more general, and it is possible that the same result holds for any shift of finite type (including the full shift). A related problem is posed in Question 3.19.

In Section 4, we prove a stabilized version of the Kim–Roush Embedding Theorem; namely, we show the stabilized automorphism group of any full shift embeds into the stabilized automorphism group of any mixing shift of finite type. We use this to show that, unlike the classical automorphism group, the stabilized automorphism group of a mixing shift of finite type is never residually finite. We also prove along the way that the stabilized group contains divisible subgroups, highlighting another difference with the classical setting.

1.2 Guide to the paper

In Section 2, we give an overview of the tools we need from the classical setting of (non-stabilized) automorphism groups. Most of these results appear scattered throughout the literature, and we present them with the goal of generalizing and adapting these results for the setting of stabilized automorphisms. Along the way, in Theorem 2.5, we

write down the natural generalization of the observation made by Boyle *et al.* [6] that Ryan's theorem may be used to distinguish the automorphism groups of the full 2 shift and the full 4 shift.

In Section 3, we introduce the stabilized automorphism group. The basic properties are small variations on the classical setting, allowing us to set up and study the stabilized versions of the center, the dimension representation, and the inert subgroup. The innovations arise when we turn to studying the commutator subgroup of the stabilized automorphism group. The key ingredient used throughout this section that is not available in the classical setting is Wagoner's theorem, which shows that the stabilized inert automorphisms are generated by simple automorphisms. Our analysis in particular leads to Theorem 3.17, which, in conjunction with the constructions in [19, 20], gives a method to detect, in the classical non-stabilized setting, the difference between the subgroup of inerts and the subgroup generated by simple automorphisms. In Section 3.6, we study the abelianization of the stabilized automorphism group. Using our characterization of the commutator, we show how the abelianization can be used to distinguish many automorphism groups in the stabilized setting.

Section 4 continues the extension of various properties from the classical setting to the stabilized automorphism group. In particular, we prove a stabilized version of the Kim–Roush Embedding Theorem. The proof adapts the original construction used by Kim and Roush, with some necessary modifications.

The most difficult arguments of the paper are in Section 5, where we show that the group of stabilized inert automorphisms of a full shift is simple. For a given shift of finite type presented by a labeled graph Γ, the group of stabilized inerts contains a certain locally finite subgroup of stabilized simple graph automorphisms associated with the presenting graph Γ. In the case of a full shift, this locally finite subgroup turns out to be simple. By a result of Boyle, this locally finite subgroup, together with the shift, generates all of the stabilized inert subgroup. The key ingredient for us then is Lemma 5.2, which shows that any nontrivial normal subgroup of the stabilized inert automorphisms must have nontrivial intersection with the subgroup of stabilized simple graph automorphisms. The proof of Lemma 5.2 occupies the majority of the section.

2 Background and Notation

2.1 Symbolic dynamics

Assume that $\mathcal{A}$ is a finite set endowed with the discrete topology; we call $\mathcal{A}$ the *alphabet*. The space $\mathcal{A}^{\mathbb{Z}}$, endowed with the product topology, is a compact, metrizable space. An

element $x \in \mathcal{A}^{\mathbb{Z}}$ is a bi-infinite sequence over the alphabet $\mathcal{A}$, and we write $x = (x_i)_{i\in\mathbb{Z}}$ with each $x_i \in \mathcal{A}$. It is easy to check that the left shift $\sigma\colon \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ defined by $(\sigma x)_i := x_{i+1}$ is a homeomorphism of $\mathcal{A}^{\mathbb{Z}}$ to itself, and the dynamical system $(\mathcal{A}^{\mathbb{Z}}, \sigma)$ is called the *full $\mathcal{A}$-shift*. While the choice of symbols in the alphabet is irrelevant, we often want to distinguish different full shifts by the size of the alphabet $\mathcal{A}$, and so to emphasize the size of the alphabet, we write the full shift as (X_n, σ_n) when $|\mathcal{A}| = n$.

A *subshift* $X \subset \mathcal{A}^{\mathbb{Z}}$ is a closed, σ-invariant set X, and we use the shorthand *shift* to refer to a subshift. We write (X, σ_X) for this system.

If $w = w_1 \dots w_n \in \mathcal{A}^n$, then we call w a *word of length n*. If w is a word of length n, then the set $[w]$ defined by

$$[w] = \{x \in \mathcal{A}^{\mathbb{Z}}\colon x_i = w_i \text{ for } i = 1, \dots n\}$$

is the *cylinder set determined by w*. If (X, σ_X) is a subshift, then the *language $\mathcal{L}(X)$ of X* is defined by

$$\mathcal{L}(X) = \{w \in \bigcup_{n=1}^{\infty} \mathcal{A}^n\colon [w] \cap X \neq \emptyset\}.$$

The collection of sets $\left\{\sigma_X^k([w])\colon w \in \mathcal{L}(X) \text{ and } k \in \mathbb{Z}\right\}$ generate the topology of the space X.

If $x \in X$ and $k, m \in \mathbb{Z}$ with $m > k$, then $x_{[k,m]}$ denotes the word $x_k x_{k+1} \dots x_m$ of consecutive entries in x. Analogously, $x_{(-\infty,m]}$ denotes the infinite word $\dots x_{m-1} x_m$, and we similarly define $x_{[k,\infty)}$.

A shift (X, σ_X) is *irreducible* if for all words $u, v \in \mathcal{L}(X)$, there exists some $w \in \mathcal{L}(X)$ such that $uwv \in \mathcal{L}(X)$, and the shift is *mixing* if for all $u, v \in \mathcal{L}(X)$, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, there is a word $w \in \mathcal{L}(X)$ of length n such that $uwv \in \mathcal{L}(X)$. Irreducibility of the shift (X, σ_X) is equivalent to the system (X, σ_X) being *transitive*: there exists some $x \in X$ such that the orbit closure $\overline{\{\sigma_X^n x\}_{n\in\mathbb{N}}}$ is all of X.

Two systems (X, σ_X) and (Y, σ_Y) are *(topologically) conjugate* if there exists a homeomorphism $h\colon X \to Y$ such that $h \circ \sigma_X = \sigma_Y \circ h$ and we refer to the map h as a *conjugacy*. It follows from the Curtis–Hedlund–Lyndon theorem [11] that any such conjugacy is given by a *sliding block code*, meaning there exists some radius $r \in \mathbb{N}$ such that for all $x \in X$, the value $h(x)_i$ only depends on the entries $x_{i-r} \dots x_i \dots x_{i+r}$. For example, the shift σ_X is given by a sliding block code with $r = 1$.

A *shift of finite type* is a subshift whose language consists of all words (over some finite alphabet) which do not contain some given finite list of words. Alternatively,

a shift of finite type can be defined by a $\kappa \times \kappa$ adjacency matrix $A = (a_{i,j})$ over $\mathbb{Z}_+$ as follows. Given A, we define Γ_A to be a graph with κ vertices and $a_{i,j}$ edges between vertices i and j. Labeling the set of edges, the associated shift of finite type, which we denote by (X_A, σ_A), consists of bi-infinite walks through edges in Γ_A. Any shift of finite type (X, σ_X) is conjugate to a shift of finite type (X_A, σ_A) for some $\mathbb{Z}$-matrix A. We use Γ_n to denote the graph consisting of one vertex with n edges.

A shift of finite type (X, σ_X) is mixing if and only if it is conjugate to a shift of finite type (X_A, σ_A) for which the $\mathbb{Z}_+$-matrix A is *primitive*, meaning there exists J such that every entry of A^J is positive. A shift of finite type (X, σ_X) is irreducible if and only if it is conjugate to some (X_A, σ_A) for which A is an irreducible matrix, meaning that for any entry $A_{i,j}$ in A there exists J such that $A^J_{i,j}$ is positive.

Standing assumption. Unless otherwise noted, we always assume that any shift of finite type (X, σ_X) has positive entropy $h_{\text{top}}(\sigma_X)$: in terms of the language, this means that

$$h_{\text{top}}(\sigma_X) = \lim_{n\to\infty} \frac{\log |\{w \in \mathcal{L}(X) \colon |w| = n\}|}{n} > 0.$$

In terms of a matrix presentation, if A is an irreducible matrix and (X, σ_X) is conjugate to (X_A, σ_A), then $h(\sigma_X) = h(\sigma_A) = \log \lambda_A$ where λ_A is the Perron–Frobenius eigenvalue of the matrix A.

2.2 Automorphism groups

Given a compact space X, let Homeo(X) denote the group of all homeomorphisms from X to itself (with group operation given by composition). It is obvious that for a shift system (X, σ_X) one has $\sigma_X \in \text{Homeo}(X)$, and the centralizer of σ_X in Homeo(X) is called the *automorphism group of the subshift* (X, σ_X). As we consider various shift spaces, we denote the group (under composition) of all automorphisms of a subshift (X, σ_X) by $\text{Aut}(X, \sigma_X)$, and when the shift is clear from the context, we write this as $\text{Aut}(\sigma_X)$. In a slight abuse of notation, we denote the automorphism group of the full shift on n letters by $\text{Aut}(\sigma_n)$.

A topological conjugacy $h \colon (X, \sigma_X) \to (Y, \sigma_Y)$ between shift spaces (X, σ_X) and (Y, σ_Y) induces an isomorphism $h_* \colon \text{Aut}(X, \sigma_X) \to \text{Aut}(Y, \sigma_Y)$ defined by

$$h_*(\phi) = h \circ \phi \circ h^{-1}.$$

For any subshift (X, σ_X), the subgroup $\langle \sigma_X \rangle$ generated by the shift always lies, by definition, in the center $Z(\mathrm{Aut}(\sigma_X))$ of the automorphism group $\mathrm{Aut}(\sigma_X)$; when X is infinite, the subgroup generated by σ_X is isomorphic to $\mathbb{Z}$. For an irreducible shift of finite type, this subgroup is the whole center.

Theorem 2.1 (Ryan [32, 33]). If (X, σ_X) is an infinite irreducible shift of finite type, then $Z(\mathrm{Aut}(\sigma_X)) = \langle \sigma_X \rangle$.

As observed in [6], this has an immediate application to distinguishing automorphism groups of full shifts, using arithmetic properties of the size of the alphabet. A general result along these lines is given in Theorem 2.5, but we briefly recall the following corollary, which can be proven by elementary means.

Corollary 2.2. For any prime p, $\mathrm{Aut}(\sigma_p)$ is not isomorphic to $\mathrm{Aut}(\sigma_{p^p})$.

Proof. Fix a prime p. It is easy to check that $\sigma_{p^p} \in \mathrm{Aut}(\sigma_{p^p})$ has a pth root, meaning there exists $\phi \in \mathrm{Aut}(\sigma_{p^p})$ such that $\phi^p = \sigma_{p^p}$ (e.g., one can construct such an ϕ using the fact that (X_{p^p}, σ_{p^p}) and (X_p, σ_p^p) are topologically conjugate).

If $\mathrm{Aut}(\sigma_p)$ and $\mathrm{Aut}(\sigma_{p^p})$ are isomorphic, then any isomorphism maps the center isomorphically onto the center. By Ryan's theorem, this means that $\sigma_p \in \mathrm{Aut}(\sigma_p)$ is mapped to $\sigma_{p^p}^{\pm 1} \in \mathrm{Aut}(\sigma_{p^p})$. Since σ_{p^p} has a pth root, this implies either σ_p or σ_p^{-1} has a pth root. However, we claim that neither σ_p nor σ_p^{-1} does. Indeed, suppose there exists $\psi \in \mathrm{Aut}(\sigma_p)$ such that $\psi^p = \sigma_p$ or $\psi^p = \sigma_p^{-1}$; we suppose $\psi^p = \sigma_p$, as the other case is similar. The system (X_p, σ_p) has $p^p - p$ points of least period p, and hence $p^{p-1} - 1$ orbits of length p. Since p does not divide $p^{p-1} - 1$, there exist some $1 \leq i < p$, $0 \leq j < p$, such that $\psi^i(x) = \sigma_p^j(x)$ for some period p point x. But this implies

$$\sigma_p^i(x) = \psi^{pi}(x) = \sigma_p^{pj}(x) = x,$$

which, since $i < p$, is a contradiction. ∎

2.3 The dimension representation

Krieger [21, 22] defined a *dimension triple* $(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$ associated with a shift of finite type (X_A, σ_A), where $\mathcal{G}_A$ is an abelian group, $\mathcal{G}_A^+$ is a positive cone in $\mathcal{G}_A$ (meaning it is a subsemigroup of $\mathcal{G}_A$ containing 0 that generates $\mathcal{G}_A$), and δ_A is a group automorphism of the pair $(\mathcal{G}_A, \mathcal{G}_A^+)$. A conjugacy between shifts of finite type induces a corresponding

isomorphism of their respective dimension triples; since each element of $\mathrm{Aut}(\sigma_A)$ is a conjugacy from (X_A, σ_A) to itself, this gives rise to the *dimension representation*

$$\pi_A : \mathrm{Aut}(\sigma_A) \to \mathrm{Aut}(\mathcal{G}_A).$$

To define this representation precisely in the manner suitable for our purposes, we briefly outline two definitions of the dimension triple $(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$; the 1st is an intrinsic definition given by Krieger and the 2nd is more algebraic. These two definitions produce isomorphic objects and this is described in [25, Section 7.5]; our presentation closely follows the one given there.

Assume that A is an irreducible $\kappa \times \kappa$ matrix with entries in $\mathbb{Z}_+$, and let (X_A, σ_A) denote the associated shift of finite type. We further assume that (X_A, σ_A) has positive topological entropy $h_{\mathrm{top}}(\sigma_A) > 0$, and note that $h_{\mathrm{top}}(\sigma_A) = \log \lambda_A$ where λ_A denotes the Perron–Frobenius eigenvalue of A. The *eventual range* $\mathcal{R}(A)$ *of* A is the subspace of $\mathbb{Q}^\kappa$ defined by

$$\mathcal{R}(A) = \bigcap_{j=1}^{\infty} \mathbb{Q}^\kappa A^j$$

(throughout, we assume the matrices act on row vectors). The *dimension triple* $(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$ *associated with* A consists of the abelian group $\mathcal{G}_A$, the semigroup $\mathcal{G}_A^+ \subset \mathcal{G}_A$, and the automorphism δ_A of $\mathcal{G}_A$, where

(i) $\mathcal{G}_A = \{x \in \mathcal{R}(A) : xA^j \in \mathbb{Z}^\kappa \text{ for some } j \geq 0\}$,
(ii) $\mathcal{G}_A^+ = \{x \in \mathcal{R}(A) : xA^j \in (\mathbb{Z}_+)^\kappa \text{ for some } j \geq 0\}$,
(iii) $\delta_A(x) = xA$.

When $A = (n)$, we usually simply write $(\mathcal{G}_n, \mathcal{G}_n^+, \delta_n)$ instead of $(\mathcal{G}_{(n)}, \mathcal{G}_{(n)}^+, \delta_{(n)})$.

We now describe the intrinsic definition of the dimension triple. An *m-ray* is defined to be a subset of X_A of the form

$$R(x, m) = \{y \in X_A : y_{(-\infty, m]} = x_{(-\infty, m]}\}$$

for some $x \in X_A$ and $m \in \mathbb{Z}$, and an *m-beam* is a finite union of m-rays. A *ray* is defined to be an m-ray for some $m \in \mathbb{Z}$, and a *beam* is an m-beam for some $m \in \mathbb{Z}$. Note that if U is an m-beam for some $m \in \mathbb{Z}$, then U is also an n-beam for any $n \geq m$. Recall that Γ_A denotes the graph associated with the edge shift of finite type (X_A, σ_A). Given an m-beam

$$U = \bigcup_{i=1}^{j} R(x^{(i)}, m),$$

let $v_{U,m} \in \mathbb{Z}^\kappa$ denote the vector whose Jth component is the cardinality of the set

$$\{x^{(i)} \in U\colon \text{ the edge corresponding to } x_m^{(i)} \text{ ends at state } J\}.$$

Beams U and V are said to be *equivalent* if there exists some $m \in \mathbb{Z}$ such that $v_{U,m} = v_{V,m}$, and we use $[U]$ to denote the equivalence class of a beam U. Since A is irreducible and $0 < h_{\text{top}}(\sigma_A) = \log \lambda_A$, given beams U, V, there exist beams U', V' such that

$$[U] = [U'],\ [V] = [V'],\ \text{and}\ \ U' \cap V' = \emptyset.$$

Let D_A^+ denote the abelian semigroup whose elements are equivalence classes of beams endowed with the operation defined by

$$[U] + [V] = [U' \cup V'].$$

Letting D_A denote the group completion of D_A^+ (thus, elements of D_A are formal differences $[U] - [V]$), the map $d_A\colon D_A \to D_A$ induced by

$$d_A([U]) = [\sigma_A(U)]$$

is a group automorphism of D_A. This defines Krieger's dimension triple (D_A, D_A^+, d_A).

An automorphism $\phi \in \text{Aut}(X_A, \sigma_A)$ induces an automorphism

$$\phi_*\colon (D_A, D_A^+, d_A) \to (D_A, D_A^+, d_A)$$

by setting

$$\phi_*([U]) = [\phi(U)], \qquad [U] \in D_A^+.$$

Here, by a *morphism of a triple*, we mean a morphism preserving all the relevant data given by the group, the subsemigroup, and the group automorphism associated with D_A or $\mathcal{G}_A$. For example, an automorphism $\Phi \in \text{Aut}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$ is a group automorphism $\Phi\colon \mathcal{G}_A \to \mathcal{G}_A$ taking $\mathcal{G}_A^+$ onto $\mathcal{G}_A^+$ such that $\Phi \circ \delta_A = \delta_A \circ \Phi$.

The relation between these two definitions is settled by the following.

Proposition 2.3 (see [25, Theorem 7.5.13]). Assume (X_A, σ_A) is a shift of finite type and A is $\kappa \times \kappa$. The map $\theta\colon D_A^+ \to \mathcal{G}_A^+$ induced by the map

$$\theta([U]) = \delta_A^{-\kappa-n}(v_{U,n}A^\kappa),$$

where U is an n-beam, is a semigroup isomorphism, and its completion is a group isomorphism $\theta\colon D_A \to \mathcal{G}_A$ such that

$$\theta \circ d_A = \delta_A \circ \theta.$$

In other words, this proposition means that θ induces an isomorphism of triples

$$\theta\colon (D_A, D_A^+, d_A) \to (\mathcal{G}_A, \mathcal{G}_A^+, \delta_A).$$

For $\phi \in \mathrm{Aut}(\sigma_A)$, let $S_\phi\colon (\mathcal{G}_A, \mathcal{G}_A^+, \delta_A) \to (\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$ denote the automorphism of the dimension triple such that the diagram

$$\begin{array}{ccc} D_A & \xrightarrow{\theta} & \mathcal{G}_A \\ {\scriptstyle \phi_*}\downarrow & & \downarrow{\scriptstyle S_\phi} \\ D_A & \xrightarrow{\theta} & \mathcal{G}_A \end{array}$$

commutes. We can now define the dimension representation

$$\pi_A\colon \mathrm{Aut}(\sigma_A) \to \mathrm{Aut}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$$

by setting $\pi_A(\phi) = S_\phi$.

2.4 An application of the dimension representation

As usual, $\omega(n)$ denotes the number of distinct prime divisors of n (counted without multiplicity).

The following result appears implicitly in [6].

Proposition 2.4. For a full shift (X_n, σ_n), we have

$$\mathrm{Aut}(\mathcal{G}_n, \mathcal{G}_n^+, \delta_n) \cong \mathbb{Z}^{\omega(n)}.$$

Moreover, the dimension representation $\pi_n\colon \mathrm{Aut}(\sigma_n) \to \mathrm{Aut}(\mathcal{G}_n, \mathcal{G}_n^+, \delta_n)$ is surjective.

In the proof and in the sequel, if $H \subset \mathbb{R}$ is a subgroup and $n \geq 1$, we use the notation $\mathfrak{m}_n$ to refer to the map from H to itself given by $a \mapsto n \cdot a$.

Proof. For a full shift (X_n, σ_n), it follows quickly from Proposition 2.3 that there is an isomorphism of triples

$$(\mathcal{G}_n, \mathcal{G}_n^+, \delta_n) \cong (\mathbb{Z}[\tfrac{1}{n}], \mathbb{Z}_+[\tfrac{1}{n}], \mathfrak{m}_n).$$

Then, it is straightforward to check that

$$\mathrm{Aut}(\mathbb{Z}[\tfrac{1}{n}], \mathbb{Z}_+[\tfrac{1}{n}], \mathfrak{m}_n) \cong \mathbb{Z}^{\omega(n)}$$

is generated by the maps $\{\mathfrak{m}_p : p \text{is a prime dividing } n\}$.

For the 2nd part, we write the prime factorization of n as $n = \prod_{i=1}^{\omega(n)} p_i^{a_i}$ with p_i prime. There exists a conjugacy $h : (X_n, \sigma_n) \to \left(\prod_{i=1}^{\omega(n)} X_{p_i}, \prod_{i=1}^{\omega(n)} \sigma_{p_i}^{a_i}\right)$ and we let $h_* : \mathrm{Aut}(\sigma_n) \to \mathrm{Aut}(\prod_{i=1}^{\omega(n)} \sigma_{p_i}^{a_i})$ denote the induced isomorphism of automorphism groups. For each i, let ϕ_i denote the automorphism of $\left(\prod_{i=1}^{\omega(n)} X_{p_i}, \prod_{i=1}^{\omega(n)} \sigma_{p_i}^{a_i}\right)$ that acts by σ_{p_i} in the ith coordinate and the identity in the other coordinates. Then, the images of the automorphisms $h_*^{-1}(\phi_i)$ under the map π_n generate $\mathrm{Aut}(\mathcal{G}_n, \mathcal{G}_n^+, \delta_n)$. ■

For $a \in \mathbb{N}$, let $\mathfrak{R}(a) = \{k \in \mathbb{N} : a^{1/k} \in \mathbb{N}\}$ denote the non-negative integral roots of a. To the authors' knowledge, the only known method for distinguishing automorphism groups of full shifts relies on Ryan's [32] theorem, which characterizes the center of the group of $\mathrm{Aut}(\sigma_A)$. This technique was explicitly mentioned in [6] for the full shifts on 2 and 4 symbols. The following result, a natural generalization of this, is not altogether new; we include it since it could not be found explicitly in the literature. Our argument uses the dimension representation; an alternative proof may be given using [24, Theorem 8].

Theorem 2.5. Let $m, n \geq 2$, and suppose $\mathrm{Aut}(\sigma_m) \cong \mathrm{Aut}(\sigma_n)$. Then, $\mathfrak{R}(m) = \mathfrak{R}(n)$. In particular, for any prime p and $k \geq 2$, $\mathrm{Aut}(\sigma_p)$ and $\mathrm{Aut}(\sigma_{p^k})$ are not isomorphic.

Proof. Let $k \in \mathfrak{R}(m)$, so there exists $a \in \mathbb{N}$ such that $a^k = m$. Then, (X_m, σ_m) is topologically conjugate to (X_a, σ_a^k), and in particular, there exists $\phi \in \mathrm{Aut}(\sigma_m)$ such that $\phi^k = \sigma_m$. Suppose $\Psi : \mathrm{Aut}(\sigma_m) \to \mathrm{Aut}(\sigma_n)$ is an isomorphism, and let $\phi' = \Psi(\phi)$. By Ryan's theorem (Theorem 2.1), $\Psi(\sigma_m) = \sigma_n^{\pm 1}$, so $(\phi')^k = \sigma_n^{\pm 1}$. Applying the dimension representation, we have the equality

$$k(\pi_n(\phi')) = \pi_n((\phi')^k) = \pi_n(\sigma_n^{\pm 1}) = \pm \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_r \end{pmatrix} \in \mathbb{Z}^{\omega(n)}.$$

Since $\pi_n(\phi') \in \mathbb{Z}^{\omega(n)}$, each v_i must be divisible by k. Let $w_i = \frac{v_i}{k}$. Writing $n = \prod_{i=1}^{\omega(n)} p_i^{v_i}$ for some primes p_i, it follows from Proposition 2.4 that $n = \left(\prod_{i=1}^{\omega(n)} p_i^{w_i}\right)^k$ so $k \in \mathfrak{R}(n)$. Thus, $\mathfrak{R}(m) \subset \mathfrak{R}(n)$, and the same argument shows $\mathfrak{R}(n) \subset \mathfrak{R}(m)$. Thus, $\mathfrak{R}(m) = \mathfrak{R}(n)$. ■

In particular, it follows that the group $\mathrm{Aut}(\sigma_9)$ is not isomorphic to the group $\mathrm{Aut}(\sigma_{27})$, as $\mathfrak{R}(9) \neq \mathfrak{R}(27)$.

2.5 Inert and simple automorphisms

An automorphism $\phi \in \mathrm{Aut}(\sigma_A)$ is said to be *inert* if it lies in the kernel of the dimension representation, and we denote the subgroup of inert automorphisms by $\mathrm{Inert}(\sigma_A)$. A particularly important collection of inert automorphisms is the class of simple automorphisms, first introduced by Nasu [28]. We recall the definition.

If Γ is a directed graph, we call a graph automorphism of Γ that fixes every vertex a *simple graph symmetry* of the graph Γ. We use the term graph symmetry instead of graph automorphism to avoid confusion between automorphisms of a graph and automorphisms of a shift.

Let (X_A, σ_A) be a shift of finite type presented by a matrix A over $\mathbb{Z}_+$ with associated directed labeled graph Γ_A, and suppose τ is a simple graph symmetry of Γ_A. Then, τ induces an automorphism $\tilde{\tau} \in \mathrm{Aut}(\sigma_A)$ given by a 1-block code, and any automorphism in $\mathrm{Aut}(\sigma_A)$, which is induced by such a graph symmetry is called a *simple graph automorphism*. An automorphism $\phi \in \mathrm{Aut}(\sigma_A)$ is called *simple* if there exists a shift of finite type (X_B, σ_B), a conjugacy $h\colon (X_A, \sigma_A) \to (X_B, \sigma_B)$, and a simple graph automorphism $\tilde{\tau} \in \mathrm{Aut}(X_B, \sigma_B)$ such that

$$\phi = h_*^{-1}(\tilde{\tau}) = h^{-1} \circ \tilde{\tau} \circ h.$$

Note that, by construction, any simple automorphism is of finite order. It is straightforward to check that the subgroup of $\mathrm{Aut}(\sigma_A)$ generated by simple automorphisms forms a normal subgroup contained in $\mathrm{Inert}(\sigma_A)$, and we denote this subgroup by $\mathrm{Simp}(\sigma_A)$.

There exist irreducible shifts of finite type (X_A, σ_A) for which $\mathrm{Simp}(\sigma_A)$ is a proper subgroup of $\mathrm{Inert}(\sigma_A)$; see [17]. In general, the difference between $\mathrm{Simp}(\sigma_A)$ and $\mathrm{Inert}(\sigma_A)$ for an irreducible shift of finite type is not well understood; for example, it is not known whether for a full shift (X_n, σ_n) the groups $\mathrm{Simp}(\sigma_n)$ and $\mathrm{Inert}(\sigma_n)$ agree.

However, Wagoner [36] showed that, upon passing to sufficiently large powers of the shift, inert automorphisms can be written as products of simple automorphisms (an alternate proof was given by Boyle [2]).

Theorem 2.6 (Wagoner [36]). If ϕ is an inert automorphism of a mixing shift of finite type (X_A, σ_A), then there exists M such that for all $m \geq M$, ϕ can be written as a product of simple automorphisms lying in $\mathrm{Aut}(X_A, \sigma_A^m)$.

3 The Stabilized Automorphism Group

3.1 1st properties

For a subshift (X, σ_X), let $\mathrm{Aut}^{(k)}(\sigma_X)$ denote the centralizer of σ_X^k in the group $\mathrm{Homeo}(X)$. Thus, $\mathrm{Aut}^{(k)}(\sigma_X)$ is precisely $\mathrm{Aut}(X, \sigma_X^k)$ and $\mathrm{Aut}^{(k)}(\sigma_X)$ is a subgroup of $\mathrm{Aut}^{(km)}(\sigma_X)$ for all $k, m \geq 1$.

Definition 3.1. If (X, σ_X) is a subshift, define the *stabilized automorphism group* $Aut^{(\infty)}(\sigma_X)$ to be

$$\mathrm{Aut}^{(\infty)}(\sigma_X) = \bigcup_{k=1}^{\infty} \mathrm{Aut}^{(k)}(\sigma_X),$$

where the union is taken in $\mathrm{Homeo}(X)$.

For the full shift (X_n, σ_n) on n symbols, we denote the stabilized automorphism group by $\mathrm{Aut}^{(\infty)}(\sigma_n)$.

It is straightforward to verify the following.

Lemma 3.2 (Stabilized Curtis–Lyndon–Hedlund theorem). Let (X, σ_X) be a shift with alphabet $\mathcal{A}$, and let $\phi \in \mathrm{Aut}^{(k)}(\sigma_X)$. Then, there exists a non-negative integer r and k block maps $\beta_i \colon \mathcal{A}^{2r+1} \to \mathcal{A}$ for $i = 0, 1, \ldots, k-1$ such that

$$\phi(x)_z = \beta_{z \bmod k}(x_{z-r}, \ldots, x_z, \ldots, x_{z+r}).$$

Note that, the case that all β_i are identical yields an element that commutes with σ_X.

One concludes, either from the definition or using Lemma 3.2 that $\mathrm{Aut}^{(\infty)}(\sigma_X)$ is a countable group that contains the automorphism group $\mathrm{Aut}(\sigma_X)$.

For some subshifts, nothing new arises in the stabilized automorphism group.

Example 3.3. Let (X, σ_X) be a minimal shift associated with an irrational rotation: for example, such a shift can be defined by fixing an irrational $\alpha \in (0, 1)$, considering

$$T(x) = x + \alpha \pmod 1,$$

and using the coding of the orbit of 0 defined by setting the n^{th} entry to be 0 if $T^n(x) \in [0, \alpha)$ and 1 if $T^n(x) \in [\alpha, 1)$. This gives rise to a Sturmian shift (see, e.g., [31, Chapter 6] for background on Sturmian shifts), and $\mathrm{Aut}(\sigma_X) \cong \mathbb{Z}$ is generated by the shift σ_X (see [30]).

The system (X, σ_X) has a single pair of asymptotic orbits $\mathcal{O}_1, \mathcal{O}_2$, and for each $k \geq 1$ the system (X, σ_X^k), then has k pairs of asymptotic orbits given by the collection $\{\sigma_X^i(\mathcal{O}_1), \sigma_X^i(\mathcal{O}_2)\}_{i=0}^{k-1}$. Using [10, Lemma 2.3], it follows that any automorphism in $\mathrm{Aut}(\sigma_X^k)$ is of the form σ_X^j for some $j \in \mathbb{Z}$, and hence

$$\mathrm{Aut}(\sigma_X^k) = \langle \sigma_X \rangle \cong \mathbb{Z}.$$

Thus, in this case, we have that $\mathrm{Aut}^{(\infty)}(\sigma_X) = \mathrm{Aut}(\sigma_X) \cong \mathbb{Z}$.

However, for a shift of finite type, each inclusion in the definition of the stabilized automorphism group is strict.

Lemma 3.4. If (X_A, σ_A) is an infinite irreducible shift of finite type, then for any $k \in \mathbb{N}$ and any $m \geq 2$, the subgroup $\mathrm{Aut}^{(k)}(\sigma_A)$ is a proper subgroup of $\mathrm{Aut}^{(km)}(\sigma_A)$.

Proof. By Ryan's theorem (Theorem 2.1), the center of $\mathrm{Aut}^{(km)}(\sigma_A) = \mathrm{Aut}(\sigma_A^{km})$ is exactly $\langle \sigma_A^{km} \rangle$. Thus, there exists some $\phi \in \mathrm{Aut}^{(km)}(\sigma_A)$ such that ϕ does not commute with σ_A^k. ■

In Proposition 3.8, we make further use of Ryan's theorem and prove a stronger result, showing that for an irreducible shift of finite type (X, σ_A), we have that $\mathrm{Aut}(\sigma_A)$ is not abstractly isomorphic to $\mathrm{Aut}^{\infty}(\sigma_A)$.

The following proposition follows immediately from the definition of the stabilized automorphism group.

Proposition 3.5. For any shift (X, σ_X) and $k \geq 1$, $\mathrm{Aut}^{(\infty)}(\sigma_X^k) = \mathrm{Aut}^{(\infty)}(\sigma_X)$.

It is well known that if two shifts are conjugate, then their automorphism groups are isomorphic, and the same holds true for their stabilized automorphism groups. In fact, a stronger result holds in the stabilized setting, and to make this precise, we define a weaker notion that suffices for the associated groups to be isomorphic.

Recall that (X, σ_X) and (Y, σ_Y) are *eventually conjugate* if there exists some $K \in \mathbb{N}$ such that for all $k \geq K$, (X, σ_X^k) and (Y, σ_Y^k) are conjugate. We define a weaker notion: we say that the systems (X, σ_X) and (Y, σ_Y) are *rationally conjugate* if there exist $j, k \geq 1$ such that the systems (X, σ_X^j) and (Y, σ_Y^k) are conjugate. For example, the systems (X_2, σ_2) and (X_4, σ_4) are rationally conjugate but are not eventually conjugate.

Proposition 3.6. If the systems (X, σ_X) and (Y, σ_Y) are rationally conjugate, then $\mathrm{Aut}^{(\infty)}(\sigma_X)$ and $\mathrm{Aut}^{(\infty)}(\sigma_Y)$ are isomorphic.

Proof. If $h\colon (X, \sigma_X^j) \to (Y, \sigma_Y^k)$ is a conjugacy, then h_* gives rise to an isomorphism

$$h_*\colon \mathrm{Aut}^{(\infty)}(\sigma_X^j) \to \mathrm{Aut}^{(\infty)}(\sigma_Y^k).$$

By Proposition 3.5, this implies $\mathrm{Aut}^{(\infty)}(\sigma_X)$ and $\mathrm{Aut}^{(\infty)}(\sigma_Y)$ are isomorphic. ■

In particular, since (X_4, σ_4) is conjugate to (X_2, σ_2^2), it follows that $\mathrm{Aut}^{(\infty)}(\sigma_2)$ and $\mathrm{Aut}^{(\infty)}(\sigma_4)$ are isomorphic, in contrast to the non-stabilized setting, where $\mathrm{Aut}(\sigma_2)$ and $\mathrm{Aut}(\sigma_4)$ are not isomorphic (see Theorem 2.5).

Recall that two matrices A and B with entries in $\mathbb{Z}_+$ are said to be *shift equivalent* (over $\mathbb{Z}_+$) if there exists an integer $m \geq 1$ and matrices R and S over $\mathbb{Z}_+$ such that

$$AR = RB,\ SA = BS,\ A^m = RS,\ \text{and } B^m = SR.$$

If A and B are irreducible $\mathbb{Z}_+$-matrices which are shift equivalent, then the systems $(X_A, \sigma_A), (X_B, \sigma_B)$ are eventually conjugate, and Kim and Roush [14] showed the converse holds. We use this to show the following proposition.

Proposition 3.7. Suppose (X_A, σ_A) and (X_B, σ_B) are irreducible shifts of finite type defined by $\mathbb{Z}_+$-matrices A, B. If A and B are shift equivalent, then $\mathrm{Aut}^{(\infty)}(\sigma_A)$ and $\mathrm{Aut}^{(\infty)}(\sigma_B)$ are isomorphic.

Proof. By Kim and Roush [14, 15], matrices A and B are shift equivalent if and only if the systems (X_A, σ_A) and (X_B, σ_B) are eventually conjugate. The result then follows from Proposition 3.6. ■

3.2 The center

Ryan's theorem (Theorem 2.1) shows that for any irreducible shift of finite type, the center is exactly the powers of the shift. In contrast, the center is trivial in the stabilized automorphism group.

Proposition 3.8. Suppose (X_A, σ_A) is an infinite irreducible shift of finite type. Then, the center $Z(\mathrm{Aut}^{(\infty)}(\sigma_A))$ of $\mathrm{Aut}^{(\infty)}(\sigma_A)$ is trivial, and the group $\mathrm{Aut}^{(\infty)}(\sigma_A)$ is not finitely generated.

Proof. Suppose $\phi \in Z(\mathrm{Aut}^{(\infty)}(\sigma_A))$, and choose $k \geq 1$ such that $\phi \in \mathrm{Aut}^{(k)}(\sigma_A)$. Then, $\phi \in Z(\mathrm{Aut}^{(k)}(\sigma_A))$, so by Ryan's theorem, we have $\phi = \sigma_A^{km}$ for some $m \in \mathbb{Z}$. However, if $\sigma_A^{km} = \phi \in Z(\mathrm{Aut}^{(\infty)}(\sigma_A))$, then $\sigma_A^{km} \in Z(\mathrm{Aut}^{(2km)}(\sigma_A)) = \langle \sigma_A^{2km} \rangle$, so $m = 0$.

For any irreducible shift of finite type (X_A, σ_A), any finitely generated subgroup of $\mathrm{Aut}^{(\infty)}(\sigma_A)$ has nontrivial centralizer (as each finitely generated subgroup is included in $\mathrm{Aut}^{(k)}(\sigma_A)$ for some k, for which σ_A^k would be in the centralizer). By the previous part, it follows that for any infinite irreducible shift of finite type, the group $\mathrm{Aut}^{(\infty)}(\sigma_A)$ is not finitely generated. ■

3.3 The $\mathrm{Aut}^{(\infty)}(\sigma_A)$-action on X_A

Let (X_A, σ_A) be a mixing shift of finite type, and let $P(X_A)$ denote the set of σ_A-periodic points in X_A. Then, both $\mathrm{Aut}(\sigma_A)$ and $\mathrm{Aut}^{(\infty)}(\sigma_A)$ act on the set $P(X_A)$. While the action of $\mathrm{Aut}(\sigma_A)$ on $P(X_A)$ is far from transitive (since any $\phi \in \mathrm{Aut}(\sigma_A)$ must preserve the order of a σ_A-periodic point), it follows from [5, Theorem 3.6] that $\mathrm{Aut}^{(\infty)}(\sigma_A)$ acts highly transitively on the σ_A-periodic points of X_A (recall an action of a group G on a countable set X is said to be highly transitive if for all $k \geq 1$ it is transitive on the set of ordered k-tuples of distinct elements in X).

It is straightforward to check that the action of $\mathrm{Aut}(\sigma_A)$ on X_A is not minimal, since there are periodic points. Similarly, there are many $\mathrm{Aut}(\sigma_A)$-invariant probability measures, including atomic measures supported on periodic points, and the measure of maximal entropy. However, the minimal components and $\mathrm{Aut}(\sigma_A)$-invariant measures are essentially classified in [6, Sections 9 and 10]. Using this, we deduce the following proposition.

Proposition 3.9. If (X_A, σ_A) is a mixing shift of finite type, then $\mathrm{Aut}^{(\infty)}(\sigma_A)$ acts highly transitively on the set of σ_A-periodic points in X_A, and the action of $\mathrm{Aut}^{(\infty)}(\sigma_A)$ on X_A is minimal and uniquely ergodic. Moreover, the unique $\mathrm{Aut}^{(\infty)}(\sigma_A)$-invariant probability measure is given by the measure of maximal entropy for the system (X_A, σ_A).

Proof. For the full shift on (X_n, σ_n) is easy to see that $\mathrm{Aut}^{(\infty)}(\sigma_n)$ acts highly transitively on the set of periodic points of σ_n: any permutation of fixed points σ_n^m may be implemented by a simple graph automorphism. Then, the minimality, the unique ergodicity, and the claim regarding the measure of maximal entropy follow from [6, Theorem 9.2 and Corollary 10.2].

For the general case of a mixing shift of finite type (X_A, σ_A), to apply this same result it suffices to show that $\mathrm{Aut}^{(\infty)}(\sigma_A)$ acts highly transitively on the set of periodic

points of σ_A. Suppose $Q = \{x_1, \ldots, x_l\}$ is a set of σ_A-periodic points and τ is some permutation of the set Q. Let y_1, y_2 be a pair of σ_A-periodic points not contained in Q and choose m large enough that the set of fixed points of σ_A^m contains $Q \cup \{y_1, y_2\}$. If τ is an even permutation, then it follows from [19, Main Theorem] that there exists $\alpha_\tau \in \mathrm{Inert}(\sigma_A)$ such that α_τ acts on Q via τ. If τ is odd, define τ' to be the permutation of $Q \cup \{y_1, y_2\}$, which acts by τ on Q and by an involution on $\{y_1, y_2\}$. Then, τ' is an even permutation, so again [19, Main Theorem] implies there exists some $\alpha_{\tau'}$ such that the action of $\alpha_{\tau'}$ on Q is given by τ'. It follows that $\mathrm{Aut}^{(\infty)}(\sigma_A)$ acts highly transitively on the σ_A-periodic points of X_A. The statement now follows in the same way as for the full shift. ■

3.4 The stabilized dimension representation

Let A be a $\mathbb{Z}_+$-matrix, and recall we have defined the dimension representation

$$\pi_A : \mathrm{Aut}(\sigma_A) \to \mathrm{Aut}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A).$$

For any $k \geq 1$, we also have a homomorphism

$$\pi_A^{(k)} : \mathrm{Aut}(\sigma_A^k) \to \mathrm{Aut}(\mathcal{G}_{A^k}, \mathcal{G}_{A^k}^+, \delta_{A^k}).$$

Note that in general, we have $(\mathcal{G}_A, \mathcal{G}_A^+) = (\mathcal{G}_{A^k}, \mathcal{G}_{A^k}^+)$ for all $k \in \mathbb{N}$, and $\delta_{A^k} = \delta_A^k$. However, the dimension triples $(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$ and $(\mathcal{G}_{A^k}, \mathcal{G}_{A^k}^+, \delta_{A^k})$ are *not* isomorphic, as there is no isomorphism that intertwines the maps δ_A and δ_{A^k}. For each $k \geq 1$ the map $\pi_A^{(k)} : \mathrm{Aut}^{(k)}(\sigma_A) \to \mathrm{Aut}(\mathcal{G}_{A^k}, \mathcal{G}_{A^k}^+, \delta_{A^k})$ sends σ_A^k to $\delta_{A^k} = \delta_A^k$, and the image of $\pi_A^{(k)}$ lands in the centralizer of δ_A^k, so in fact, we have a homomorphism

$$\pi_A^{(k)} : \mathrm{Aut}^{(k)}(\sigma_A) \to \mathrm{Aut}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A^k).$$

It follows from the definitions that for all $k \geq 1$, $\mathrm{Aut}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$ can be viewed naturally as a subgroup of $\mathrm{Aut}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A^k)$, and we can define the *stabilized group of automorphisms of the dimension triple* by setting

$$\mathrm{Aut}^{(\infty)}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A) = \bigcup_{k=1}^{\infty} \mathrm{Aut}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A^k).$$

Equivalently, $\mathrm{Aut}^{(\infty)}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$ is the union of the centralizers of δ_A^k in the group of automorphisms of the pair $(\mathcal{G}_A, \mathcal{G}_A^+)$, that is, all automorphisms of the group $\mathcal{G}_A$, which preserve $\mathcal{G}_A^+$.

Furthermore, as remarked in [6, p. 87], for $k \geq 1$, the restriction of the map

$$\pi_A^{(k)} : \mathrm{Aut}^{(k)}(\sigma_A) \to \mathrm{Aut}(\mathcal{G}_{A^k}, \mathcal{G}_{A^k}^+, \delta_A^k) = \mathrm{Aut}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A^k)$$

to $\mathrm{Aut}(\sigma_A) \subset \mathrm{Aut}(\sigma_A^k)$ coincides with the map $\pi_A : \mathrm{Aut}(\sigma_A) \to \mathrm{Aut}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$. We can thus define the *stabilized dimension representation*

$$\pi_A^{(\infty)} : \mathrm{Aut}^{(\infty)}(\sigma_A) \to \mathrm{Aut}^{(\infty)}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A).$$

In what follows, we use the shorthand notation $\mathrm{Aut}^{(\infty)}(\mathcal{G}_A)$ to refer to the group $\mathrm{Aut}^{(\infty)}(\mathcal{G}_A, \mathcal{G}_A^+, \delta_A)$.

Example 3.10. Consider the case of the full 3-shift, presented via the matrix $A = (3)$. For all $k \in \mathbb{N}$, we have $\mathcal{G}_3 = \mathcal{G}_{3^k} = \mathbb{Z}[\frac{1}{3}]$. In this case, $\mathrm{Aut}(\mathcal{G}_{3^k}) = \mathrm{Aut}(\mathcal{G}_3) \cong \mathbb{Z}$ for any k, and

$$\pi_3^{(k)} : \mathrm{Aut}^{(k)}(\sigma_3) \to \mathrm{Aut}(\mathcal{G}_3) \cong \mathbb{Z}$$

with $\pi_3^{(k)}(\sigma_3) = \delta_3$.

Recall $\omega(n)$ denotes the number of distinct prime factors of n, and the maps $\mathfrak{m}_p$ are defined by $\mathfrak{m}_p(x) = p \cdot x$.

Proposition 3.11. For the full shift (X_n, σ_n), we have

$$\mathrm{Aut}^{(\infty)}(\mathcal{G}_n) \cong \mathrm{Aut}(\mathcal{G}_n, \mathcal{G}_n^+, \delta_n) \cong \mathbb{Z}^{\omega(n)}$$

is generated by the maps $\{\mathfrak{m}_p : p \text{is a prime dividing } n\}$.

Proof. The statement follows immediately from Proposition 2.4, and the fact that the maps $\mathfrak{m}_p$ generate $\mathrm{Aut}(\mathbb{Z}[\frac{1}{n}], \mathbb{Z}_+[\frac{1}{n}], \delta_n) \cong \mathbb{Z}^{\omega(n)}$. ■

For an example where the stabilized group of automorphisms of the dimension group is non-abelian; see Example 3.24.

In the case of a full shift (X_n, σ_n), the classical dimension representation

$$\pi_n : \mathrm{Aut}(\sigma_n) \to \mathrm{Aut}(\mathcal{G}_n)$$

is surjective (see Proposition 2.4). However, in the general setting of mixing shifts of finite type, the dimension representation need not be surjective: Kim *et al.* [18] give an example of a mixing shift of finite type for which the dimension representation is not surjective, and in the general setting of mixing shifts of finite type, the question of when the dimension representation is surjective remains open. In the stabilized setting, however, the question has a satisfying answer, as shown in [6] (our terminology is different, but this is an immediate translation of their result).

Theorem 3.12 (Boyle *et al.* [6, Theorem 6.8]). For any mixing shift of finite type (X_A, σ_A), the stabilized dimension representation

$$\pi_A^{(\infty)} \colon \mathrm{Aut}^{(\infty)}(\sigma_A) \to \mathrm{Aut}^{(\infty)}(\mathcal{G}_A)$$

is surjective.

As in the standard setting, we define the *group of stabilized inert automorphisms* to be the kernel of $\pi_A^{(\infty)}$, and we denote this group by

$$\mathrm{Inert}^{(\infty)}(\sigma_A) = \ker \pi_A^{(\infty)}.$$

It follows immediately from the definitions that

$$\mathrm{Inert}^{(\infty)}(\sigma_A) = \bigcup_{k=1}^{\infty} \mathrm{Inert}(\sigma_A^k).$$

Similarly, we define the simple automorphisms in the stabilized automorphism group to be the union of the simple automorphisms at each of the finite levels.

We show later that one of the many differences between stabilized and standard automorphism groups lies in the structure of their corresponding inert subgroups. In particular, in Section 5, we prove that, in the case of a full shift, $\mathrm{Inert}^{(\infty)}(\sigma_n)$ is always simple. This is in stark contrast to the classical inert subgroup $\mathrm{Inert}(\sigma_n)$, which is residually finite. Using the stabilized version of the Kim–Roush embedding proved in Section 4, it follows that for any mixing shift of finite type (X_A, σ_A), $\mathrm{Inert}^{(\infty)}(\sigma_A)$ always contains an infinite simple group; in particular, $\mathrm{Inert}^{(\infty)}(\sigma_A)$ is never residually finite (Section 4.2). We note that, as a consequence, $\mathrm{Inert}^{(\infty)}(\sigma_A)$ and $\mathrm{Inert}(\sigma_A)$ are not isomorphic as groups (in fact, it follows that $\mathrm{Inert}^{(\infty)}(\sigma_A)$ does not even embed into $\mathrm{Inert}(\sigma_A)$).

Rewriting Wagoner's theorem (Theorem 2.6) in our terminology, we have the following theorem.

Theorem 3.13 (Wagoner (Theorem 2.6 rephrased)). If (X_A, σ_A) is a mixing shift of finite type, then $\mathrm{Inert}^{(\infty)}(\sigma_A)$ is generated by simple automorphisms in $\mathrm{Aut}^{(\infty)}(\sigma_A)$.

3.5 The commutator subgroup

For a group G, we write $[g,h] = g^{-1}h^{-1}gh$ for the commutator of the elements $g, h \in G$ and for subgroups $H_1, H_2 \subset G$, we let $[H_1, H_2]$ denote the group generated by all commutators $[h_1, h_2]$ with $h_1 \in H_1$ and $h_2 \in H_2$. The goal of this section is to prove the following theorem.

Theorem 3.14. Let (X_A, σ_A) be a mixing shift of finite type. Then, we have

$$\mathrm{Inert}^{(\infty)}(\sigma_A) \subseteq [\mathrm{Aut}^{(\infty)}(\sigma_A), \mathrm{Aut}^{(\infty)}(\sigma_A)].$$

If $\mathrm{Aut}^{(\infty)}(\mathcal{G}_A)$ is abelian, then equality holds. In particular, for a full shift on n letters we have

$$\mathrm{Inert}^{(\infty)}(\sigma_n) = [\mathrm{Aut}^{(\infty)}(\sigma_n), \mathrm{Aut}^{(\infty)}(\sigma_n)].$$

Note that, in the case where $\mathrm{Aut}^{(\infty)}(\mathcal{G}_A)$ is torsion-free (e.g., a full shift), Wagoner's theorem as phrased in Theorem 3.13 characterizes the dynamical object given by the group of stabilized inert automorphisms via an abstract property of the group: the subgroup generated by the elements of finite order. Theorem 3.14 gives a general relation between an abstract group property, this time the commutator and the dimension representation of the symbolic system.

The following lemma is the technical tool needed for the proof of Theorem 3.14.

Lemma 3.15. Let (X_A, σ_A) be a shift of finite type, and let τ be a simple graph symmetry of the graph Γ_A, which permutes two distinct edges e and f between the vertices i and j. Let $\tilde{\tau}$ denote the automorphism of (X_A, σ_A) induced by τ. Then, we have $\tilde{\tau}$ lies in $[\mathrm{Aut}(\sigma_A^2), \mathrm{Aut}(\sigma_A^2)]$.

Proof. We consider (X_A, σ_A^2) as a shift on the alphabet $\begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$ where $a_0 a_1$ is an admissible word in X_A. Define the zero-block code ϕ_0 in $\mathrm{Aut}(\sigma_A^2)$ by

$$\phi_0 : \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \mapsto \begin{pmatrix} \tau(a_0) \\ a_1 \end{pmatrix}.$$

Note that since τ is a simple graph automorphism, it follows that ϕ_0 is an automorphism of (X_A, σ_A^2). Then, in $\mathrm{Aut}(\sigma_A^2)$, we have

$$\tilde{\tau} = \phi_0 \sigma_A \phi_0^{-1} \sigma_A^{-1}. \tag{1}$$

■

For a set X, let $\mathrm{Sym}(X)$ denote the group of all permutations of the set X.

Theorem 3.16. Let (X_A, σ_A) be a shift of finite type, and let $\phi \in \mathrm{Aut}(\sigma_A)$ be a simple automorphism. Then, we have $\phi \in [\mathrm{Aut}(\sigma_A^2), \mathrm{Aut}(\sigma_A^2)]$.

Proof. Since ϕ is simple, there exists some shift of finite type (X_B, σ_B) and a conjugacy $h\colon (X_A, \sigma_A) \to (X_B, \sigma_B)$ such that $h_*(\phi)$ is a simple graph automorphism. Set $\tilde{\tau} = h_*(\phi)$. Since h also induces an isomorphism between $\mathrm{Aut}(\sigma_A^2)$ and $\mathrm{Aut}(\sigma_B^2)$, it suffices to show that $\tilde{\tau} \in [\mathrm{Aut}(\sigma_B^2), \mathrm{Aut}(\sigma_B^2)]$.

Let $E_{i,j}$ denote the set of edges between vertices i, j in the graph Γ_B. There exist permutations $\tau_{i,j} \in \mathrm{Sym}(E_{i,j})$ such that $\tilde{\tau}$ is induced by the simple graph symmetry $\prod_{i,j} \tau_{i,j}$. For each pair i, j, the permutation $\tau_{i,j}$ is given by a product of transpositions in $\mathrm{Sym}(E_{i,j})$. By Lemma 3.15, the automorphism induced by each of these transpositions lies in $[\mathrm{Aut}(\sigma_B^2), \mathrm{Aut}(\sigma_B^2)]$, so $\tilde{\tau}$ lies in $[\mathrm{Aut}(\sigma_B^2), \mathrm{Aut}(\sigma_B^2)]$ as well. ■

We now use Theorem 3.16 to complete the proof of Theorem 3.14.

Proof of Theorem 3.14. Theorem 3.16 implies that any simple automorphism lies in the commutator. By Theorem 3.13, the group $\mathrm{Inert}^{(\infty)}(\sigma_A)$ is generated by simple automorphisms, proving the 1st part.

To check the 2nd statement, when $\mathrm{Aut}^{(\infty)}(\mathcal{G}_A)$ is abelian, the dimension representation

$$\pi_A^{(\infty)}\colon \mathrm{Aut}^{(\infty)}(\sigma_A) \to \mathrm{Aut}^{(\infty)}(\mathcal{G}_A)$$

factors through the abelianization of $\mathrm{Aut}^{(\infty)}(\sigma_A)$. Thus,

$$[\mathrm{Aut}^{(\infty)}(\sigma_A), \mathrm{Aut}^{(\infty)}(\sigma_A)] \subseteq \mathrm{Inert}^{(\infty)}(\sigma_A).$$

The statement about full shifts follows from Proposition 3.11. ■

As a 2nd corollary of Theorem 3.16, we can in some cases show that, in the non-stabilized automorphism group $\mathrm{Aut}(\sigma_A)$, a particular inert automorphism can not lie in the subgroup generated by simple automorphisms. Such results can also be deduced from [3, Theorem 2], where the possible actions of simple automorphisms on finite subsystems of the shift were classified. Together with the powerful realization result in [19, 20], this provides a large class of examples where the answer to Wagoner's Question 3.17 is no.

Theorem 3.17. Let (X_A, σ_A) be a shift of finite type, and suppose there exists odd $k \in \mathbb{N}$ such that X_A has no σ_A-periodic points of least period $2k$, and further assume that there are at least three distinct orbits of least period k. Then, the group generated by simple automorphisms is a proper subgroup of $\mathrm{Inert}(\sigma_A)$.

Proof. By [19, 20, Main Theorem], there exists $\phi \in \mathrm{Inert}(\sigma_A)$ such that the action of ϕ on the σ_A-orbits of length k consists of a 3-cycle. We show that ϕ cannot be written as a product of commutators in $\mathrm{Aut}(\sigma_A^2)$ of the form given in (1). By Theorem 3.16, it follows that $\phi \notin \mathrm{Simp}(\sigma_A)$.

Suppose $\gamma \in \mathrm{Aut}(\sigma_A^2)$. Since k is odd, σ_A^2 maps length k σ_A-orbits to themselves. Furthermore, since there are no σ_A-periodic points of least period $2k$, it follows that $\mathrm{Aut}(\sigma_A^2)$ induces a well-defined action on the set of σ_A-orbits of length k. Since σ_A acts trivially on the set of σ_A-orbits of length k, the commutator $\gamma\sigma_A\gamma^{-1}\sigma_A^{-1}$ acts trivially on the set of length k σ_A-orbits. Thus, since ϕ acts nontrivially on the σ_A-orbits of length k, ϕ cannot be written as a product of such commutators. ■

For a concrete example of the phenomena exhibited in this corollary, consider the primitive matrix

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}. \tag{2}$$

Since the system (X_A, σ_A) has three fixed points and no points of least period 2, by Theorem 3.17, $\mathrm{Inert}(\sigma_A) \neq \mathrm{Simp}(\sigma_A)$.

Remark 3.18. Considering the matrix A in (2), it can be shown using [4, Theorem 1] that there exists a product of finite order inert automorphisms in $\mathrm{Aut}(\sigma_A)$ whose action

on the set of fixed points in (X_A, σ_A) is a 3-cycle. Letting $\mathrm{Fin}(\sigma_A)$ denote the subgroup of $\mathrm{Inert}(\sigma_A)$ generated by elements of finite order, in light of Theorem 3.17, for this matrix A we have the following proper containments:

$$\mathrm{Simp}(\sigma_A) \subsetneq \mathrm{Fin}(\sigma_A) \subsetneq \mathrm{Inert}(\sigma_A).$$

In general, we do not know if $\mathrm{Simp}(\sigma_A)$ is always finite index in $\mathrm{Inert}(\sigma_A)$. Based on Theorems 3.16 and 3.17, as a way to approach this question, we ask the following.

Question 3.19. Assume (X_A, σ_A) is a shift of finite type. Is

$$\mathrm{Inert}(\sigma_A) \cap [\mathrm{Aut}(\sigma_A^2), \mathrm{Aut}(\sigma_A^2)]$$

finite index in $\mathrm{Inert}(\sigma_A)$?

3.6 The abelianization of $\mathrm{Aut}^{(\infty)}(\sigma_A)$ and Theorem 1.1

For a group G, we let G_{ab} denote its abelianization. We write Ab_{σ_A} for the abelianization map $\mathrm{Aut}^{(\infty)}(\sigma_A) \to \left(\mathrm{Aut}^{(\infty)}(\sigma_A)\right)_{\mathrm{ab}}$, and $\mathrm{Ab}_{\mathcal{G}_A}$ for the abelianization map $\mathrm{Aut}^{(\infty)}(\mathcal{G}_A) \to \left(\mathrm{Aut}^{(\infty)}(\mathcal{G}_A)\right)_{\mathrm{ab}}$. With the previous results in hand, we can now show that the abelianization of $\mathrm{Aut}^{(\infty)}(\sigma_A)$ for a general mixing shift of finite type (X_A, σ_A) coincides with the abelianization of its dimension representation.

Theorem 3.20. Suppose (X_A, σ_A) is a mixing shift of finite type. Then, we have an isomorphism of the abelianizations:

$$\mathrm{Aut}^{(\infty)}(\sigma_A)_{\mathrm{ab}} \cong \mathrm{Aut}^{(\infty)}(\mathcal{G}_A)_{\mathrm{ab}}.$$

Proof. Consider the following diagram:

$$\begin{array}{ccc} \mathrm{Aut}^{(\infty)}(\sigma_A) & \xrightarrow{\pi_A^{(\infty)}} & \mathrm{Aut}^{(\infty)}(\mathcal{G}_A) \\ \downarrow{\scriptstyle \mathrm{Ab}_{\sigma_A}} & \swarrow{\scriptstyle f} & \downarrow{\scriptstyle \mathrm{Ab}_{\mathcal{G}_A}} \\ \left(\mathrm{Aut}^{(\infty)}(\sigma_A)\right)_{\mathrm{ab}} & \xleftarrow{\overline{g}} & \left(\mathrm{Aut}^{(\infty)}(\mathcal{G}_A)\right)_{\mathrm{ab}} \end{array} \quad . \tag{3}$$

By Theorem 3.14, $\mathrm{Inert}^{(\infty)}(\sigma_A) \subset [\mathrm{Aut}^{(\infty)}(\sigma_A), \mathrm{Aut}^{(\infty)}(\sigma_A)]$, and by Theorem 3.12, the map $\pi_A^{(\infty)}$ is surjective, so the map f is well defined. Since f factors through the abelianization

of $\mathrm{Aut}^{(\infty)}(\mathcal{G}_A)$, the map g exists. Moreover, since Ab_{σ_A} is surjective, f is surjective, and hence g is surjective.

We claim that the map g is also injective. Suppose $a \in \ker g$. Since the map $\mathrm{Ab}_{\mathcal{G}_A}$ is surjective, we can find $b \in \mathrm{Aut}^{(\infty)}(\mathcal{G}_A)$ such that $\mathrm{Ab}_{\mathcal{G}_A}(b) = a$, and hence $f(b) = \mathrm{Id}$. By Theorem 3.12, $\pi_A^{(\infty)}$ is surjective, so there exists $c \in \mathrm{Aut}^{(\infty)}(\sigma_A)$ such that $\pi_A^{(\infty)}(c) = b$. Then, c lies in the kernel of the map Ab_{σ_A}, which implies that c is a commutator. Thus, $\pi_A^{(\infty)}(c) = b$ is also a commutator, and hence $a = \mathrm{Ab}_{\mathcal{G}_A}(b) = \mathrm{Id}$. ■

Corollary 3.21. If $n \geq 2$, then we have $\mathrm{Aut}^{(\infty)}(\sigma_n)_{\mathrm{ab}} \cong \mathbb{Z}^{\omega(n)}$.

Proof. This follows immediately from Theorem 3.20 and Proposition 3.11. ■

This allows us to complete the proof of Theorem 1.1, via the following theorem.

Theorem 3.22. If $\mathrm{Aut}^{(\infty)}(\sigma_n)$ and $\mathrm{Aut}^{(\infty)}(\sigma_m)$ are isomorphic, then $\omega(n) = \omega(m)$.

Proof. If $\mathrm{Aut}^{(\infty)}(\sigma_n)$ and $\mathrm{Aut}^{(\infty)}(\sigma_m)$ are isomorphic, then their abelianizations are isomorphic. The result then follows from Corollary 3.21. ■

Toward a converse of Theorem 3.22, observe that by Proposition 3.5, if m, n satisfy $m^k = n^j$ for some k and j, then $\mathrm{Aut}^{(\infty)}(\sigma_m) \cong \mathrm{Aut}^{(\infty)}(\sigma_n)$.

In general, we ask the following question.

Question 3.23. For integers $m, n \geq 2$, when are $\mathrm{Aut}^{(\infty)}(\sigma_m)$ and $\mathrm{Aut}^{(\infty)}(\sigma_n)$ isomorphic?

We end this section with an example showing how Theorem 3.20 can be used to compute the abelianization $\mathrm{Aut}^{(\infty)}(\sigma_A)_{\mathrm{ab}}$ of the stabilized automorphism group. In the example, $\mathrm{Aut}^{(\infty)}(\sigma_A)_{\mathrm{ab}}$ has nontrivial torsion, and it follows (by Corollary 3.21) that $\mathrm{Aut}^{(\infty)}(\sigma_A)$ is not isomorphic to $\mathrm{Aut}^{(\infty)}(\sigma_n)$ for any $n \in \mathbb{N}$.

Example 3.24. Consider the matrix

$$A = \begin{pmatrix} 5 & 2 & 2 \\ 4 & 1 & 4 \\ 0 & 6 & 3 \end{pmatrix}$$

(this matrix appears in [6, Example 6.7]). By Theorem 3.20, in order to compute $\mathrm{Aut}^{(\infty)}(\sigma_A)_{\mathrm{ab}}$, it suffices to compute the abelianization of the stabilized automorphism group of the dimension group.

As shown in [6], the matrix A has eigenvalues $-3, 3, 9$ and can be conjugated over $\mathbb{Z}[\frac{1}{3}]$ to a diagonal matrix. For any k, A^{2k}, then has eigenvalues $9^k, 9^k, 81^k$, and can be conjugated over $\mathbb{Z}[\frac{1}{3}]$ to the matrix $U_{2k} = \begin{pmatrix} 81^k & 0 & 0 \\ 0 & 9^k & 0 \\ 0 & 0 & 9^k \end{pmatrix}$. It follows that $\mathrm{Aut}(\mathcal{G}_{A^{2k}}) = \mathrm{Aut}(\mathcal{G}_{A^{2(k+1)}}) \cong GL_1(\mathbb{Z}[\frac{1}{3}]) \oplus \mathrm{GL}_2(\mathbb{Z}[\frac{1}{3}])$, and so $\mathrm{Aut}^{(\infty)}(\mathcal{G}_A, \mathcal{G}_A^+) \cong \mathbb{Z} \oplus \mathrm{GL}_2(\mathbb{Z}[\frac{1}{3}])$ and $\mathrm{Aut}^{(\infty)}(\mathcal{G}_A, \mathcal{G}_A^+)_{\mathrm{ab}}$ is isomorphic to $\mathbb{Z} \oplus \mathrm{GL}_2(\mathbb{Z}[\frac{1}{3}])_{\mathrm{ab}}$. By Theorem 3.20, the dimension representation is surjective and coincides with the abelianization of $\mathrm{Aut}^{(\infty)}(\sigma_A)$.

The remainder of this example is devoted to computing $\mathrm{GL}_2(\mathbb{Z}[\frac{1}{3}])_{\mathrm{ab}}$. Consider the determinant map

$$\det\colon \mathrm{GL}_2(\mathbb{Z}[\frac{1}{3}]) \to \mathbb{Z}[\frac{1}{3}]^\times,$$

where $\mathbb{Z}[\frac{1}{3}]^\times$ denotes the group of units. This map is a split surjection with kernel $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{3}])$, with the splitting coming from embedding $\mathbb{Z}[\frac{1}{3}]^\times = \mathrm{GL}_1(\mathbb{Z}[\frac{1}{3}]) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}[\frac{1}{3}])$. Hence, $\mathrm{GL}_2(\mathbb{Z}[\frac{1}{3}])$ is isomorphic to the semidirect product $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{3}]) \rtimes \mathbb{Z}[\frac{1}{3}]^\times$.

In general, the abelianization of a semidirect product $H \rtimes G$ is given by $(H_{\mathrm{ab}})_G \times G_{\mathrm{ab}}$, where the subscript G denotes the coinvariants of the G-action on H_{ab} (arising from the G-action on H). Since $\mathbb{Z}[\frac{1}{3}]^\times$ is abelian, the abelianization of the semidirect product $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{3}]) \rtimes \mathbb{Z}[\frac{1}{3}]^\times$ has the form

$$(\mathrm{SL}_2(\mathbb{Z}[\frac{1}{3}])_{\mathrm{ab}})_{\mathbb{Z}[\frac{1}{3}]^\times} \times \mathbb{Z}[\frac{1}{3}]^\times.$$

This leaves us with computing $(\mathrm{SL}_2(\mathbb{Z}[\frac{1}{3}])_{\mathrm{ab}})_{\mathbb{Z}[\frac{1}{3}]^\times}$.

The abelianization of $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{3}])$ is $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{3}])_{\mathrm{ab}} \cong \mathbb{Z}/4$, as computed by Serre [35] (see also [1]). Thus, we only need to determine the coinvariants of the induced $\mathbb{Z}[\frac{1}{3}]^\times$-action on this copy of $\mathbb{Z}/4$.

The ring map $\mathbb{Z}[\frac{1}{3}] \to \mathbb{Z}/4$ given by $\frac{a}{3^k} \mapsto a \mod 4$ induces a surjection mapping $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{3}])$ to $\mathrm{SL}_2(\mathbb{Z}/4)$. The group $\mathrm{SL}_2(\mathbb{Z}/4)$ has a normal subgroup N of order 12 (this is its commutator subgroup), which is generated by the matrices $\begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix}$ and $\begin{pmatrix} 3 & 1 \\ 3 & 0 \end{pmatrix}$. Thus, $\mathrm{SL}_2(\mathbb{Z}/4)$ factors onto an abelian group G of order 4. Let π denote the composition of the two maps given by

$$\mathrm{SL}_2(\mathbb{Z}[\frac{1}{3}]) \to \mathrm{SL}_2(\mathbb{Z}/4) \to G.$$

One can check directly that the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and its square do not lie in the normal subgroup N and hence do not lie in the kernel of π. Thus, $\pi(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix})$ has order 4, and $\pi(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix})$ is a generator for G and hence also pushes down to a generator for the abelianization.

To compute the coinvariants, we are left with determining the action of $\mathbb{Z}[\frac{1}{3}]^\times$ on the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (since it pushes down to a generator of the abelianization). Note that $\mathbb{Z}[\frac{1}{3}]^\times$ is generated by -1 and 3. The action of these units on $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is given by (modulo commutators)

$$-1\colon \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

$$3\colon \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}.$$

It follows that the orbit of a generator for the abelianization under this action is a subgroup of order 2, and the coinvariants are

$$(\mathrm{SL}_2(\mathbb{Z}[\frac{1}{3}])_{\mathrm{ab}})_{\mathbb{Z}[\frac{1}{3}]^\times} \cong \mathbb{Z}/2.$$

Thus, we have that

$$\mathrm{GL}_2(\mathbb{Z}[\frac{1}{3}])_{\mathrm{ab}} \cong \mathbb{Z}[\frac{1}{3}]^\times \oplus \mathbb{Z}/2 \cong \mathbb{Z}/2 \oplus \mathbb{Z} \oplus \mathbb{Z}/2$$

and

$$\mathrm{Aut}^{(\infty)}(\mathcal{G}_A, \mathcal{G}_A^+)_{\mathrm{ab}} \cong \mathbb{Z} \oplus \mathbb{Z}/2 \oplus \mathbb{Z} \oplus \mathbb{Z}/2.$$

4 Stabilized Kim–Roush Embedding

4.1 Extending the embedding result

The purpose of this section is to extend the following theorem of Kim and Roush to the stabilized setting.

Theorem 4.1 (Kim–Roush Embedding [16]). Let (X_A, σ_A) be a mixing shift of finite type. Then, for any $n \geq 2$, the group $\mathrm{Aut}(\sigma_n)$ embeds into the group $\mathrm{Aut}(\sigma_A)$.

Thus, our goal is to prove the following.

Theorem 4.2. Let (X_A, σ_A) be a mixing shift of finite type. Then, for any $n \geq 2$, the group $\mathrm{Aut}^{(\infty)}(\sigma_n)$ embeds into $\mathrm{Aut}^{(\infty)}(\sigma_A)$.

The proof follows much of the original argument given in [16], with a few modifications. Before beginning, we briefly indicate the idea. We proceed by constructing a bijection h from the given shift X_A to some other space K. While h is nothing more than a bijection, the advantage in making use of the 2nd space K is that it admits a natural faithful $\mathrm{Aut}^{(\infty)}(\sigma_n)$-action. This action of $\mathrm{Aut}^{(\infty)}(\sigma_n)$ leaves the image of h invariant, and so upon pulling back by h, we obtain an embedding of $\mathrm{Aut}^{(\infty)}(\sigma_n)$ into the set of bijections from X_A to itself. We then show that this embedding actually lands in $\mathrm{Aut}^{(\infty)}(\sigma_A)$. The construction of the map h uses markers, as used in [6, 11], and we review this technique in the proof.

Proof of Theorem 4.2 Let (X_A, σ_A) be a mixing shift of finite type. The proof consists of multiple steps constructing the embedding.

Finding markers. Assume that there exists a word $M \in \mathcal{L}(X_A)$ (a *marker*) and a collection $\mathcal{D} \subset \mathcal{L}(X_A)$ of n^2 words of some fixed length such that the word M overlaps MDM, for any $D \in \mathcal{D}$, only in the initial and final segments (the *data*). The existence of such pairs of marker and a data set of size n^2 is guaranteed for any $n \in \mathbb{N}$ since we assume that X_A is a mixing shift of finite type.

Since there are n^2 words in $\mathcal{D}$, we can view them as pairs of words, from some collection of size n of some other words. Namely, we define an abstract set of n words $\mathcal{W}$ such that each $D \in \mathcal{D}$ is a pair of two words from $\mathcal{W}$. Since there are n words in $\mathcal{W}$, we can view the full shift over these words as (X_n, σ_n), and the stabilized automorphism group of this shift is the one we realize as a subgroup of $\mathrm{Aut}^{(\infty)}(\sigma_A)$.

It is convenient to consider the elements in $\mathcal{D}$ as vertical pairs, viewing them as

$$D = \begin{pmatrix} W^u \\ W^l \end{pmatrix},$$

where $W^u, W^l \in \mathcal{W}$. For simplicity of the presentation, we assume that all of the words $\mathcal{D}$ are words of length 1, which is possible after passing via a conjugacy, if needed, to a

copy of (X_A, σ_A). Then, for $x \in X_A$ and some index j, if $x_j = D$ we can write

$$x_j = \begin{pmatrix} x_j^u \\ x_j^l \end{pmatrix}.$$

Coded stretches in the shift. Fix some $R \in \mathbb{N}$. An $(R, M, \mathcal{D})$-*coded stretch* in $x \in X_A$ is an R-gapped (possibly finite) arithmetic progression $C \subset \mathbb{Z}$ such that $x_j \in \mathcal{D}$ for all $j \in C$, and C is maximal with respect to these properties. That is, if $\max(C)$ exists then $x_{\max(C)+R} \notin \mathcal{D}$, and if $\min(C)$ exists, then $x_{\min(C)-R} \notin \mathcal{D}$.

Note that coded stretches may be finite, two-sided infinite, or one-sided infinite. Since X_A is mixing, there are points $x \in X_A$ with arbitrarily long-coded stretches (including infinite ones). Moreover, each word in $\mathcal{L}(X_n)$, whether finite or infinite, appears as a coded stretch of some $x \in X_A$. For each $x \in X_A$, let $\mathbb{S}_x \subset \mathbb{Z}$ denote the union of all the coded stretches in x.

Fix some $x \in X_A$. Recall that for $j \in \mathbb{S}_x$, x_j^u and x_j^l are two words in $\mathcal{W}$. Again, we consider elements in $\{u, l\} \times \mathbb{S}_x$ as vertical pairs, so if $p = \begin{pmatrix} \epsilon \\ j \end{pmatrix} \in \{u, l\} \times \mathbb{S}_x$, we write $x_p = x_j^\epsilon \in \mathcal{W}$.

The function next. We define an invertible map $\text{next}_x \colon \{u, l\} \times \mathbb{S}_x \to \{u, l\} \times \mathbb{S}_x$ by setting

$$\text{next}_x\begin{pmatrix} u \\ j \end{pmatrix} = \begin{cases} \begin{pmatrix} u \\ j+R \end{pmatrix} & \text{if } j + R \in \mathbb{S}_x \\ \begin{pmatrix} l \\ j \end{pmatrix} & \text{if } j + R \notin \mathbb{S}_x \end{cases}$$

and

$$\text{next}_x\begin{pmatrix} l \\ j \end{pmatrix} = \begin{cases} \begin{pmatrix} l \\ j-R \end{pmatrix} & \text{if } j - R \in \mathbb{S}_x \\ \begin{pmatrix} u \\ j \end{pmatrix} & \text{if } j - R \notin \mathbb{S}_x \end{cases}.$$

Fix $\begin{pmatrix} \epsilon \\ j \end{pmatrix}$ where $j \in \mathbb{S}_x$. Repeated application of the next function produces an element in X_n when starting with an element in X_A, by reading the words appearing in the current

coded stretch when applying this function; for example,

$$\begin{array}{ccccccccc} \dots & * & W_1^u & \to & W_2^u & \to & W_3^u & * & \dots \\ & & \uparrow & & & & \downarrow & & \\ \dots & * & W_1^l & \leftarrow & W_2^l & \leftarrow & W_3^l & * & \dots . \end{array}$$

Let C be a finite or one-sided coded stretch, and let $j, j' \in C$. Note that starting to read from $\begin{pmatrix} \epsilon \\ j \end{pmatrix}$ or from $\begin{pmatrix} \epsilon' \\ j' \end{pmatrix}$ yields the same element in X_n, up to a shift. However, for a two-sided stretch C, the element of X_n read from the u row has nothing to do with the element read from the l row.

The function read. To maintain the group structure when embedding the group $\mathrm{Aut}^{(\infty)}(\sigma_n)$, we are forced to keep track of which level an element belongs to (as $\phi \in \mathrm{Aut}^{(k)}(\sigma_n)$ applies k different block maps, depending on the index mod k). For this, we define a *read* map that depends on the index, in such a way that the word read from $\begin{pmatrix} \epsilon \\ j \end{pmatrix}$ and from $\begin{pmatrix} \epsilon \\ j' \end{pmatrix}$ would be identical (where identical means not just up to a shift). Formalizing this, define $\mathrm{read}_x \colon \mathbb{S}_x \to X_n^2$ by setting $\mathrm{read}_x(i) = \left(y^u, y^l\right)$ where

$$y^u_{\left\lfloor \frac{i}{R} \right\rfloor + z} = x_{(\mathrm{next}_x)^z \begin{pmatrix} u \\ i \end{pmatrix}} \quad \text{and} \quad y^l_{-\left\lfloor \frac{i}{R} \right\rfloor + z} = x_{(\mathrm{next}_x)^z \begin{pmatrix} l \\ i \end{pmatrix}}$$

for all $z \in \mathbb{Z}$.

We note that this complication does not arise in the original embedding of Kim and Roush [16] of $\mathrm{Aut}(\sigma_n)$ in $\mathrm{Aut}(\sigma_A)$, as one can define the read map without the floor functions (similarly for the multidimensional version of Hochman [12]).

Let $Y = \mathcal{A} \cup X_n^2$, where $\mathcal{A}$ is the alphabet of X_A, and consider the set $\bar{K} = \prod_{j \in \mathbb{Z}} Y$.

Definition of the map h. Define a map $h \colon X_A \to \bar{K}$ by setting

$$h(x)_j = \begin{cases} \mathrm{read}_x(j) & \text{if } j \in \mathbb{S}_x \\ x_j & \text{otherwise} \end{cases}. \tag{4}$$

Thus, h assigns to every $x \in X_A$ a sequence in $\bar{K}$ in the following way. If x_j is not included in any coded stretch, h copies the symbol x_j to the j coordinate of the new element in $\bar{K}$. If x_j is included in a coded stretch, there are two elements in X_n that are read from this stretch: the one associated with the upper row, and the one associated with the lower row, and this pair of elements is placed in the j coordinate of the new element in $\bar{K}$.

Set $K = \mathrm{Im}(h) \subset \bar{K}$.

The map h is injective. We claim that the map h is injective. To see this, we check the action of the inverse of h on its image. For any coordinate of a given point in K, there is either an element from $\mathcal{A}$ or there is a pair in X_n^2. In the 1st case, h^{-1} copies the symbol. In the 2nd case, we (re)-form the pair composed of one symbol from the 1st element and the other from the 2nd element from X_n^2. More precisely, in this case,

$$h^{-1}(k)_j = \begin{cases} \begin{pmatrix} ((k_j)_1)_{-\left\lfloor \frac{j}{R} \right\rfloor} \\ ((k_j)_2)_{\left\lfloor \frac{j}{R} \right\rfloor} \end{pmatrix} & \text{if } k_j \in X_n^2 \\ k_j & \text{if } k_j \in \mathcal{A} \end{cases}.$$

This verifies the claim.

We now make use of the representation of the element x as $h(x)$ by exploiting the natural associated $\mathrm{Aut}^{(\infty)}(\sigma_n)$ action. On Y, we have a pointwise action of $\mathrm{Aut}^{(\infty)}(\sigma_n)$ (and trivial action on the $\mathcal{A}$ part), and this action naturally extends to a diagonal action on $\bar{K}$. In other words, there is a group homomorphism $\mathrm{Aut}^{(\infty)}(\sigma_n) \to \mathrm{Bijection}(\bar{K})$.

Stabilized automorphisms keep the set K invariant. Next, we claim that every element in $\mathrm{Aut}^{(\infty)}(\sigma_n)$ is a bijection that keeps the set K invariant, and the restriction action of $\mathrm{Aut}^{(\infty)}(\sigma_n)$ on K is faithful. To check this, note that each element of $\mathrm{Aut}^{(\infty)}(\sigma_n)$ keeps K invariant by the mixing assumption. As K is invariant, we can consider the restriction of the $\mathrm{Aut}^{(\infty)}(\sigma_n)$-action to K. Since all words of $\mathcal{L}(X_n)$ appear as coded stretches for some $x \in X_A$, every word in X_n appears in some coordinate of some element in K, and as the action of $\mathrm{Aut}^{(\infty)}(\sigma_n)$ on X_n is faithful (by definition), we conclude that the action on K is faithful as well. Thus, the claim follows.

In other words, this realizes $\mathrm{Aut}^{(\infty)}(\sigma_n)$ as a subgroup of $\mathrm{Bijection}(K)$. Furthermore, the bijection $h\colon X_A \to K$ induces a group isomorphism $h_*\colon \mathrm{Bijection}(K) \to \mathrm{Bijection}(X_A)$.

Stabilized automorphisms give rise to continuous maps commuting with some power of the shift. By pushing $\mathrm{Aut}^{(\infty)}(\sigma_n)$ through the injective map h_*, we realize $\mathrm{Aut}^{(\infty)}(\sigma_n)$ as a subgroup of $\mathrm{Bijection}(X_A)$. To verify that the image lies in $\mathrm{Aut}^{(\infty)}(\sigma_n)$, we are left with checking that every $\phi \in \mathrm{Aut}^{(\infty)}(\sigma_n) \subseteq \mathrm{Bijection}(K)$ gives rise to a continuous $h_*\phi \in \mathrm{Homeo}(X_A)$, which commutes with some power of σ_A.

To do this, we make use of the block map description of the stabilized automorphism group (Lemma 3.2). Fix some $\phi \in \mathrm{Aut}^{(k)}(\sigma_n)$ of radius r. That is, ϕ can be represented as k block maps of radius r, where r is some number greater than k. Now, if x and x' are two points in X_A, which are close, then by definition they agree

on a large number of coordinates around the 0 coordinate. In particular, their coded stretches (if they exist) in this area coincide. So there exists large $s > 0$ such that $\mathbb{S}_x \cap [-s, s] = \mathbb{S}_{x'} \cap [-s, s]$. Since ϕ is of radius r, $h_*\phi(x)$, and $h_*\phi(x')$ agree on $[-s+r, s-r]$, and hence $h_*\phi$ is a continuous map. Finally, to check that $h_*\phi$ commutes with a power of the shift, using the fact that $\phi \in \mathrm{Aut}^{(k)}(\sigma_n)$ is induced by a k-tuple of block maps on X_n, it is easy to check that $h_*\phi$ can be modeled by a $k \cdot R$-tuple of block maps on X_A.

This concludes the proof of Theorem 4.2. ■

4.2 Residual finiteness and subgroup properties

For a mixing shift of finite type (X_A, σ_A), the classical automorphism group $\mathrm{Aut}(\sigma_A)$ is residually finite (see [6, Section 3]). Simplicity of the stabilized inerts for the full shifts (proved in Section 5), together with the stabilized Kim–Roush Embedding, implies that the stabilized group $\mathrm{Aut}^{(\infty)}(\sigma_A)$ is never residually finite. In addition, we show below that $\mathrm{Aut}^{(\infty)}(\sigma_A)$ always contains a divisible group, and hence cannot be residually finite.

Proposition 4.3. Let (X_A, σ_A) be a mixing shift of finite type. Then, $\mathrm{Aut}^{(\infty)}(\sigma_A)$ contains a divisible subgroup. In particular, the group $\mathrm{Aut}^{(\infty)}(\sigma_A)$ is not residually finite.

Proof. Since any subgroup of a residually finite group is residually finite, and any nontrivial divisible group is not residually finite, by Theorem 4.2, it suffices to prove that $\mathrm{Aut}^{(\infty)}(\sigma_2)$ contains a divisible subgroup. Let $m \geq 2$. We show that $\mathrm{Aut}^{(\infty)}(\sigma_2)$ contains the divisible group $\mathbb{Z}[\frac{1}{m}]/\mathbb{Z}$. We claim that if $\phi_0 \in \mathrm{Aut}(\sigma_2^k)$ is given by a 0-block code, then there exists $\phi_1 \in \mathrm{Aut}(\sigma_2^{mk})$ such that $\phi_1^m = \phi_0$. The result then follows by letting ϕ_0 be any 0-block code of order m in $\mathrm{Aut}(\sigma_2^j)$ for some j, m, and induction.

To prove the claim, suppose we have such ϕ_0. We consider the alphabet for the shift σ_2^{mk} as symbols $\begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \end{pmatrix}$ where $a_i \in \{0,1\}^k$. Define 0-block codes in $\mathrm{Aut}(\sigma_2^{mk})$ as follows:

$$\alpha_0\left(\begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \end{pmatrix}\right) = \begin{pmatrix} \phi_0(a_0) \\ a_1 \\ \vdots \\ a_{m-1} \end{pmatrix}, \qquad a_i \in \{0,1\}^k$$

and

$$c_m \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-1} \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_0 \end{pmatrix}.$$

Then, it is easy to check that

$$(\alpha_0 c_m)^m = \phi_0,$$

as desired. ■

The method used in Proposition 4.3 can also produce embeddings of other groups into $\mathrm{Aut}^{(\infty)}(\sigma_n)$. Given a prime $p \geq 2$, consider the direct limit $\mathrm{SL}_\infty^{\mathrm{diag}}(\mathbb{F}_p)$ of the systems $(\mathrm{SL}_{2^n}(\mathbb{F}_p), i_n)$ where $i_n \colon \mathrm{SL}_{2^n}(\mathbb{F}_p) \to \mathrm{SL}_{2^{n+1}}(\mathbb{F}_p)$ is the map given by $A \mapsto A \oplus A$. A construction analogous to the one given in the proof of Proposition 4.3 can be used to produce an embedding of $\mathrm{SL}_\infty^{\mathrm{diag}}(\mathbb{F}_p)$ into $\mathrm{Aut}^{(\infty)}(\sigma_p)$.

We end this section with an example of how results in the stabilized setting can be used to study the classical automorphism group $\mathrm{Aut}(\sigma_A)$.

Lemma 4.4. For a full shift (X_n, σ_n), the group $\mathrm{Aut}(\sigma_n)$ embeds into the group $\mathrm{Inert}(\sigma_n)$.

Proof. For a symbol a, let R_a denote the 0-ray of points x such that $x_i = a$ for all $i \leq 0$. Following the proof of the embedding theorem in [16], there exists an injective group homomorphism $f \colon \mathrm{Aut}(\sigma_n) \to \mathrm{Aut}(\sigma_n)$ such that for some symbol a, $f(\phi)(R_a)$ is again a 0-ray. Since we are considering a full shift, for any $\phi \in \mathrm{Aut}(\sigma_n)$, the action of $f(\phi)$ on the dimension group $\mathcal{G}_n$ is determined by its action on any 0-ray R, since the equivalence class of any 0-ray rationally generates $\mathcal{G}_n$. Since all 0-rays in (X_n, σ_n) are equivalent, this implies that $f(\phi)$ acts trivially on the dimension group, meaning that $f(\phi) \in \mathrm{Inert}(\sigma_n)$. ■

Theorem 4.5. Let G be a finitely generated group that embeds into $\mathrm{Aut}(\sigma_n)$. Then, G embeds (using a possibly different embedding) into $[\mathrm{Aut}(\sigma_n), \mathrm{Aut}(\sigma_n)]$.

Proof. Suppose G embeds into $\mathrm{Aut}(\sigma_n)$. Composing this embedding with a Kim–Roush embedding f gives an embedding of G into $\mathrm{Inert}(\sigma_n)$ (by the previous lemma).

In particular, G embeds in $\mathrm{Inert}^{(\infty)}(\sigma_n)$, which, by Theorem 3.14, is a subgroup of $[\mathrm{Aut}^{(\infty)}(\sigma_n), \mathrm{Aut}^{(\infty)}(\sigma_n)]$. Since G is finitely generated, it follows that G embeds inside $[\mathrm{Aut}^{(m)}(\sigma_n), \mathrm{Aut}^{(m)}(\sigma_n)]$ for some $m \in \mathbb{N}$. We can then apply another Kim–Roush Embedding, this time to embed $\mathrm{Aut}^{(m)}(\sigma_n)$ (which is isomorphic to $\mathrm{Aut}(\sigma_{n^m})$) into $\mathrm{Aut}(\sigma_n)$. The composition of these embeddings takes G into $[\mathrm{Aut}(\sigma_n), \mathrm{Aut}(\sigma_n)]$. ■

In [6, Proposition 2.8], Boyle *et al.* prove that if (X_A, σ_A) is a mixing shift of finite type, then $\mathrm{Aut}(\sigma_A)$ contains no finitely generated subgroup with unsolvable word problem (this argument is attributed to Kitchens). The same proof immediately gives the following proposition.

Proposition 4.6. Let (X_A, σ_A) be any mixing shift of finite type. Then, any finitely generated subgroup of $\mathrm{Aut}^{(\infty)}(\sigma_A)$ has a solvable word problem.

We note that this is the only obstruction, of which we are aware, for realization of a countable group as a subgroup of $\mathrm{Aut}^{(\infty)}(\sigma_A)$.

5 Simplicity of the Stabilized Inerts for Full Shifts

5.1 Simplicity

For a mixing shift of finite type (X_A, σ_A), the classical inert subgroup $\mathrm{Inert}(\sigma_A)$ has an abundance of normal subgroups. For example, given $\phi \in \mathrm{Inert}(\sigma_A)$ and $k \in \mathbb{N}$, ϕ leaves invariant the set $P_k(\sigma_A)$ of σ_A-periodic points of period k, and there is a well-defined homomorphism from $\mathrm{Inert}(\sigma_A)$ to $\mathrm{Sym}(P_k(\sigma_A))$. Moreover, if $\mathrm{Id} \neq \phi$, then there exists some k such that ϕ acts nontrivially on $P_k(\sigma_A)$, and it follows from this that the group $\mathrm{Inert}(\sigma_A)$ is in fact residually finite (see [6, Section 3] for details).

In contrast, different behavior arises in the stabilized setting, where the inert subgroup has no nontrivial normal subgroups. The remainder of this section is devoted to the proof of Theorem 1.2, which we restate for convenience.

Theorem [Theorem 1.2]. For any $n \geq 2$, the group of stabilized inert automorphisms of the full shift (X_n, σ_n) is simple.

Simplicity of various groups defined via dynamical systems has been shown in other contexts (see, e.g., [26, 27, 29]). For many of these groups, an important and useful property is the existence of elements of the group, which act by the identity on certain regions of the domain space. In contrast to such groups, the action of the group $\mathrm{Inert}^{(\infty)}(\sigma_n)$ on the shift space is of a very different nature; for example, for any mixing

shift of finite type (X_A, σ_A), and in particular any full shift, if $\mathrm{Id} \neq \phi \in \mathrm{Inert}^{(\infty)}(\sigma_A)$, then for any open subset $U \subset X_A$, $\phi \neq \mathrm{Id}$ on U (in other words, $\mathrm{Inert}^{(\infty)}(\sigma_A)$ never contains nontrivial elements with small support).

5.2 Stabilized simple automorphisms

Many of the ingredients in the proof of Theorem 1.2 hold more generally, and so we start with some preliminaries that hold for more than the full shift.

Assume (X_A, σ_A) is a mixing shift of finite type defined by a $\kappa \times \kappa$ primitive $\mathbb{Z}_+$-matrix A (note that the full shift on n symbols corresponds to $A = (n)$). Let Γ_A denote a directed labeled graph associated with A, and let $\mathrm{Simp}(\Gamma_A)$ denote the subgroup of simple automorphisms in $\mathrm{Aut}(\sigma_A)$ induced by simple graph symmetries of Γ_A. Note that $\mathrm{Simp}(\Gamma_A)$ is contained in $\mathrm{Simp}(\sigma_A)$, but the converse inclusion does not hold.

Recall that $E_{i,j}$ denotes the set of edges between vertices i and j in the graph Γ_A. There is a natural isomorphism

$$\mathrm{Simp}(\Gamma_A) \cong \prod_{i,j=1}^{\kappa} \mathrm{Sym}(E_{i,j}), \tag{5}$$

where we adopt the convention that if $E_{i,j} = \emptyset$ for some choice of i and j, we assume that $\mathrm{Sym}(E_{i,j})$ is the trivial group with one element.

We define the subgroup of even simple graph automorphisms $\mathrm{Simp}_{\mathrm{ev}}(\Gamma_A)$ in $\mathrm{Simp}(\Gamma_A)$ by pulling back the associated product of alternating subgroups, meaning the subgroup $\prod_{i,j=1}^{\kappa} \mathrm{Alt}(E_{i,j})$, via the isomorphism in (5).

Let $\Gamma_A^{(m)}$ denote a graph that presents the shift (X_A, σ_A^m); thus, $\mathrm{Simp}(\Gamma_A^{(m)}) \subset \mathrm{Aut}(\sigma_A^m)$. We note the graphs $\Gamma_A^{(m)}$ and Γ_{A^m} differ only up to a choice of labeling. For any $k, m \geq 1$, we have an inclusion map

$$i_{m,k} \colon \mathrm{Simp}(\Gamma_A^{(m)}) \hookrightarrow \mathrm{Simp}(\Gamma_A^{(km)}), \tag{6}$$

and by making the natural identifications among the iterates, this homomorphism agrees with the restriction of the map

$$\mathrm{Aut}(\sigma_A^m) \hookrightarrow \mathrm{Aut}(\sigma_A^{km})$$

to $\mathrm{Simp}(\Gamma_A^{(m)})$.

Proposition 5.1. For any $k, m \geq 1$, the map $i_{m,k}$ takes $\mathrm{Simp}_{\mathrm{ev}}(\Gamma_A^{(m)})$ into $\mathrm{Simp}_{\mathrm{ev}}(\Gamma_A^{(km)})$.

Proof. Fix vertices I, J in $\Gamma_A^{(m)}$, and let $\tau \in \mathrm{Alt}(E_{I,J})$. Letting $\tilde{\tau}$ denote the element of $\mathrm{Simp}_{\mathrm{ev}}(\Gamma_A^{(m)})$ corresponding to τ under the isomorphism in (5), it suffices to show that $i_{m,k}(\tilde{\tau})$ lies in $\mathrm{Simp}_{\mathrm{ev}}(\Gamma_A^{(km)})$. We may write $\tilde{\tau}$ as a product of an even number of transpositions $\tilde{\tau} = \prod_{i=1}^{2l} \tilde{\tau}_i$, and for each $1 \leq i \leq 2l$, since $\tilde{\tau}_i$ is an involution, we may write $i_{m,k}(\tilde{\tau}_i) = \prod_{j=1}^{r_i} c_j$ where each c_j is a 2-cycle. It suffices then to show that $r_p = r_q$ for any $1 \leq p, q \leq 2l$. Given some $1 \leq p \leq 2l$, suppose the involution $\tilde{\tau}_p$ corresponds (under the isomorphism (5)) to the transposition in $\mathrm{Alt}(E_{I,J})$ that permutes a pair of edges e_p, f_p between vertices I and J. Then, the value r_p is given by $\frac{1}{2}M_p$, where M_p denotes the number of distinct words w of length k, over the alphabet given by the edge set of $\Gamma_A^{(m)}$, where each word w contains at least one e_p or f_p. Since the number M_p of such words is independent of what e_p, f_p are, it follows that $M_p = M_q$ for any other $1 \leq q \leq 2l$, as desired. ∎

We consider the corresponding stabilized groups, defining the subgroups

$$\mathrm{Simp}^{(\infty)}(\Gamma_A) = \bigcup_{m=1}^{\infty} \mathrm{Simp}(\Gamma_A^{(m)}) \subset \mathrm{Aut}^{(\infty)}(\sigma_A)$$

and

$$\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) = \bigcup_{m=1}^{\infty} \mathrm{Simp}_{\mathrm{ev}}(\Gamma_A^{(m)}) \subset \mathrm{Simp}^{(\infty)}(\Gamma_A).$$

Thus, $\alpha \in \mathrm{Aut}^{(\infty)}(\sigma_A)$ lies in $\mathrm{Simp}^{(\infty)}(\Gamma_A)$ when α is induced by a simple graph symmetry of $\Gamma_A^{(m)}$ for some $m \geq 1$, and $\alpha \in \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)$ if for some $m \geq 1$, α is induced by a simple graph symmetry of $\Gamma_A^{(m)}$ that consists of only even permutations on every edge set for $\Gamma_A^{(m)}$. We note that it follows from the definitions that

$$\mathrm{Simp}^{(\infty)}(\Gamma_A) \subset \mathrm{Inert}^{(\infty)}(\sigma_A).$$

With this notation, Wagoner's theorem (Theorem 3.13) states that for a mixing shift of finite type (X_A, σ_A), $\mathrm{Inert}^{(\infty)}(\sigma_A)$ is generated by the collection of subgroups $\Psi_*^{-1}(\mathrm{Simp}^{(\infty)}(\Gamma_B))$, where $\Psi\colon (X_A, \sigma_A^m) \to (X_B, \sigma_B^m)$ is any conjugacy and $m \geq 1$ is any integer.

The key lemma in the proof Theorem 1.2 is the following.

Lemma 5.2. Let $n \geq 2$, and let N be a nontrivial normal subgroup of $\mathrm{Inert}^{(\infty)}(\sigma_n)$. There exist $m \geq 0$ and $\mathrm{Id} \neq \zeta \in \mathrm{Simp}^{(\infty)}(\Gamma_n)$ such that $\sigma_n^m \zeta \sigma_n^{-m} \in N$.

The proof of Lemma 5.2 is technical and long, and we postpone it until Section 5.3. For now, we assume this result and proceed to develop the other tools needed in the proof of Theorem 1.2.

Lemma 5.3. Assume (X_A, σ_A) is a mixing shift of finite type defined by a primitive $\mathbb{Z}_+$-matrix A. Then, the following hold:

(i) the commutator subgroup of $\mathrm{Simp}^{(\infty)}(\Gamma_A)$ is $\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)$;
(ii) the group $\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)$ is simple;
(iii) if $A = (n)$ for some $n \geq 2$, then $\mathrm{Simp}^{(\infty)}(\Gamma_n) = \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_n)$.

Proof. For Part (1), clearly $\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)$ is contained in $[\mathrm{Simp}^{(\infty)}(\Gamma_A), \mathrm{Simp}^{(\infty)}(\Gamma_A)]$. For the other inclusion, consider a commutator $\alpha\beta\alpha^{-1}\beta^{-1} \in \mathrm{Simp}^{(\infty)}(\Gamma_A)$, where $\alpha, \beta \in \mathrm{Simp}^{(\infty)}(\Gamma_A)$. We may assume that both $\alpha, \beta \in \mathrm{Simp}(\Gamma_A^{(m)})$ for some $m \geq 1$. Then, for each vertex pair i and j in the graph $\Gamma_A^{(m)}$, the component of $\alpha\beta\alpha^{-1}\beta^{-1}$ in $\mathrm{Sym}(E_{i,j})$ lies in $\mathrm{Alt}(E_{i,j})$. Thus, $\alpha\beta\alpha^{-1}\beta^{-1} \in \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)$.

For Part (2), let $\{\mathrm{Id}\} \neq N$ be a normal subgroup of $\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)$. For $k \geq 1$ and a pair of vertices i, j in the graph $\Gamma_A^{(k)}$, let $\mathrm{Alt}_{i,j}^{(k)}$ denote the subgroup of $\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)$ obtained by pulling back the alternating subgroup contained in the $\mathrm{Sym}(E_{i,j})$ component of $\mathrm{Simp}_{\mathrm{ev}}^{(k)}(\Gamma_A)$.

Let $\mathrm{Id} \neq \alpha \in N$, and choose $K \geq 1$ such that $\alpha \in \mathrm{Simp}_{\mathrm{ev}}(\Gamma_A^{(K)})$. By passing to larger K if necessary, since A is primitive we may assume that all entries in A^K are greater than or equal to five. We claim that for any $i, j \geq 1$ and for all m sufficiently large, we have $N \cap \mathrm{Alt}_{i,j}^{(Km)} \neq \{\mathrm{Id}\}$. Since α is nontrivial, for some choice of I, J we have that $\alpha_{I,J}$, the component of α in $\mathrm{Alt}_{I,J}^{(K)}$, is also nontrivial. Choose a path γ of length $m \geq 3$ in $\Gamma_A^{(K)}$ such that γ begins at i, ends at j, and passes through an edge from I to J on which $\alpha_{I,J}$ acts nontrivially. Then, γ corresponds to an edge in $\Gamma_A^{(Km)}$ starting at vertex i and ending at vertex j on which $i_{K,m}(\alpha_{I,J})$ acts nontrivially. It follows that

$$N \cap \mathrm{Alt}_{i,j}^{(Km)} \tag{7}$$

is nontrivial, proving the claim.

Since each entry of A^K is at least 5, it follows that $\mathrm{Alt}_{i,j}^{(Km)}$ is simple for all $i, j \geq 1$ and $m \geq 3$. Moreover, N is normal in $\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)$, and so $N \cap \mathrm{Alt}_{i,j}^{(Km)}$ is normal in $\mathrm{Alt}_{i,j}^{(Km)}$. Thus, since the intersection in (7) is nontrivial, it follows that for all $i, j \geq 1$ and $m \geq 3$, we have that $\mathrm{Alt}_{i,j}^{(Km)} \subset N$. Therefore, N contains the subgroup generated by the collection

of subgroups

$$\left\{\mathrm{Simp}_{\mathrm{ev}}(\Gamma_A^{(Km)})\right\}_{m=3}^{\infty}.$$

Given any $r \geq 1$, there exists $M \geq 3$ such that r divides M, so the subgroup $\mathrm{Simp}(\Gamma_A^{(KM)})$ contains the subgroup $\mathrm{Simp}(\Gamma_A^{(r)})$. It follows that $\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)$ is contained in the group generated by the collection

$$\left\{\mathrm{Simp}_{\mathrm{ev}}(\Gamma_A^{(Km)})\right\}_{m=3}^{\infty},$$

and hence,

$$\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \subset N,$$

proving Part (2).

For Part (3), let $l \geq 1$, and suppose $\iota \in \mathrm{Simp}(\Gamma_n^{(l)})$ is an order two automorphism induced by the simple graph symmetry of $\Gamma_n^{(l)}$ that permutes two edges e and f and leaves all other edges fixed. We claim $i_{l,2}(\iota) \in \mathrm{Simp}_{ev}(\Gamma_n^{(2l)})$ (recall that the inclusion map $i_{l,2}$ is defined in (6)). To check this, observe that $i_{l,2}(\iota)$ is induced by the action of ι on paths of length two in $\Gamma_n^{(l)}$ of the form ab, where at least one of a or b is either e or f. The action of $i_{l,2}(\iota)$ on such pairs of words is given by the composition of $2n-2$ transpositions, and it follows that $i_{l,2}(\iota) \in \mathrm{Simp}_{ev}(\Gamma_n^{(2l)})$, proving the claim. Since such involutions generate all of $\mathrm{Simp}^{(\infty)}(\Gamma_n)$, the equality in Part (3) follows. ■

It follows from Parts (2) and (3) of Lemma 5.3 that for a full shift $A = (n)$, $\mathrm{Simp}^{(\infty)}(\Gamma_n)$ is a simple group.

Lemma 5.4. Suppose (X_A, σ_A) is a mixing shift of finite type such that for all $m \geq 1$, A^m contains an entry greater than or equal to 3. Then,

(i) for any $\alpha \in \mathrm{Aut}^{(\infty)}(\sigma_A)$, the group $\alpha\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)\alpha^{-1}$ is a simple subgroup of $\mathrm{Inert}^{(\infty)}(\sigma_A)$. Moreover, if N is a normal subgroup in $\mathrm{Inert}^{(\infty)}(\sigma_A)$ such that

$$\alpha\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)\alpha^{-1} \cap N \neq \{\mathrm{Id}\},$$

then

$$\alpha\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A)\alpha^{-1} \subset N;$$

(ii) if for some $m_1 \geq 0$,

$$\sigma_A^{m_1} \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \sigma_A^{-m_1} \subset N,$$

then for any $m \geq 0$

$$\sigma_A^{m} \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \sigma_A^{-m} \subset N.$$

Proof. The 1st part follows immediately from Lemma 5.3. For the 2nd part, by assumption, we have that A contains an entry greater than or equal to 3. It follows there exists some $\gamma \in \mathrm{Simp}_{\mathrm{ev}}(\Gamma_A)$ that commutes with σ_A, so that

$$\sigma_A^{m_1} \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \sigma_A^{-m_1} \cap \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \neq \{\mathrm{Id}\}.$$

Then, since

$$\sigma_A^{m_1} \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \sigma_A^{-m_1} \subset N,$$

we have

$$\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \cap N \neq \{\mathrm{Id}\}.$$

Part (i) now implies

$$\mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \subset N.$$

Given $m \geq 1$, since A^m contains an entry greater than or equal to 3, the group $\mathrm{Simp}_{\mathrm{ev}}(\Gamma_A^{(m)})$ is nontrivial. Thus, we have that

$$\sigma_A^{m} \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \sigma_A^{-m} \cap \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \neq \{\mathrm{Id}\},$$

and hence,

$$\sigma_A^{m} \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \sigma_A^{-m} \cap N \neq \{\mathrm{Id}\}.$$

Part (i) then implies that

$$\sigma_A^{m} \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_A) \sigma_A^{-m} \subset N,$$

as desired. ■

Finally, we use a lemma of Boyle, which is a stronger version of Wagoner's Theorem (Theorem 3.13).

Lemma 5.5 (Boyle [2]). Let (X_A, σ_A) be a mixing shift of finite type, and suppose $\alpha \in \mathrm{Inert}^{(\infty)}(\sigma_A)$. There exist $m_1, m_2 \geq 1$ and $\psi_1, \psi_2 \in \mathrm{Simp}(\Gamma_A^{(m_1)})$ such that $\alpha = \psi_1 \sigma_A^{m_2} \psi_2 \sigma_A^{-m_2}$.

We have now assembled the ingredients to prove Theorem 1.2.

Proof of Theorem 1.2. Since $\mathrm{Inert}^{(\infty)}(\sigma_n) \cong \mathrm{Inert}^{(\infty)}(\sigma_{n^m})$ for any $m \geq 1$, we may assume without loss of generality that $n \geq 3$. Suppose N is a nontrivial normal subgroup of $\mathrm{Inert}^{(\infty)}(\sigma_n)$. By Lemma 5.2, there exists $m_1 \geq 1$ such that

$$\sigma_n^{m_1} \mathrm{Simp}^{(\infty)}(\Gamma_n) \sigma_n^{-m_1} \cap N \neq \{\mathrm{Id}\}.$$

Since $\mathrm{Simp}^{(\infty)}(\Gamma_n) = \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_n)$ by Part (3) of Lemma 5.3, we have that

$$\sigma_n^{m_1} \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_n) \sigma_n^{-m_1} \cap N \neq \{\mathrm{Id}\}.$$

Then, since $n \geq 3$, by Lemma 5.4,

$$\sigma_n^{m_1} \mathrm{Simp}_{\mathrm{ev}}^{(\infty)}(\Gamma_n) \sigma_n^{-m_1} \subset N,$$

and applying Lemma 5.4 again, it follows that N contains $\sigma_n^{-m} \mathrm{Simp}^{(\infty)}(\Gamma_n) \sigma_n^m$ for all $m \geq 0$. By Lemma 5.5, the collection of subgroups $\sigma_n^{-m} \mathrm{Simp}^{(\infty)}(\Gamma_n) \sigma_n^m$, $m \geq 0$, generate $\mathrm{Inert}^{(\infty)}(\sigma_n)$, completing the proof. ■

5.3 Proof of Lemma 5.2

5.3.1 *Notation*

We start with some notation used in the proof of Lemma 5.2, and we maintain this notation for the remainder of this section.

For $m \geq 1$, let $E^{(m)}(\Gamma_n)$ denote the edge set of $\Gamma_n^{(m)}$. Label the edges of $E^{(1)}(\Gamma_n)$ by $\{1, 2, \ldots, n\}$. Note that we may label the edge sets $E^{(m)}(\Gamma_n)$ such that for all $m \geq 2$,

$$E^{(m)}(\Gamma_n) = \prod_{i=1}^{m} E^{(1)}(\Gamma_n).$$

When working with $E^{(2)}(\Gamma_n)$ for some Γ_n, we denote points in $E^{(2)}(\Gamma_n)$ by $\left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right)$ where $x_1, y_1 \in E^{(1)}(\Gamma_n)$. We refer to rows and columns of $E^{(2)}(\Gamma_n)$, with the convention that row i of $E^{(2)}(\Gamma_n)$ refers to the set of points in $E^{(2)}(\Gamma_n)$ of the form

$$\left\{\left(\begin{smallmatrix} i \\ y \end{smallmatrix}\right) : y \in E^{(1)}(\Gamma_n)\right\},$$

while column i refers to the set of points in $E^{(2)}(\Gamma_n)$ of the form

$$\left\{\left(\begin{smallmatrix} x \\ i \end{smallmatrix}\right) : x \in E^{(1)}(\Gamma_n)\right\}.$$

Assume (X_n, σ_n) is a full shift, and let $\mathcal{A}_{\sigma_n}$ denote the corresponding alphabet for the shift space. By definition, $\mathcal{A}_{\sigma_n} = E^{(1)}(\Gamma_n)$. Thus, for $m \geq 1$, we identify the alphabet $\mathcal{A}_{\sigma_n^m}$ with the set of elements of the form $\begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \end{pmatrix}$ where $a_i \in \mathcal{A}_{\sigma_n}$ for $i = 1, \ldots, m-1$.

Given a point $x \in X$, as usual we write $x = (x_i)_{i \in \mathbb{Z}}$. When we need to indicate where x_0 is located, we use a dot to indicate this; thus, the point

$$x = \ldots \dot{a}bc \ldots$$

has $x_0 = b$.

Given any $a \in \mathcal{A}_{\sigma_n}$, let p_a denote the point $\ldots aaa \ldots$, which is fixed by σ_n.

We let $P_k(\sigma_n)$ denote the set of k-periodic points for σ_n, so $P_k(\sigma_n)$ consists of all points x for which $\sigma_n^k(x) = x$ (note that $P_k(\sigma_n)$ in general contains, but is *not* equal to, the set of points of *least* period k). We can identify $P_k(\sigma_n)$ with $E^{(k)}(\Gamma_n)$, and similarly, given $m \geq 1$, we can identify $P_k(\sigma_n^m)$ with $E^{(k)}(\Gamma_n^{(m)})$.

Thus, for the remainder of this section, we assume (X_n, σ_n) is a full shift on $n \geq 2$ symbols, and without loss of generality, we assume that $n \geq 7$. This is not a restrictive assumption, as in the stabilized setting, $\mathrm{Inert}^{(\infty)}(\sigma_n) \cong \mathrm{Inert}^{(\infty)}(\sigma_n^m) \cong \mathrm{Inert}^{(\infty)}(\sigma_{n^m})$ for any $m \geq 1$.

Finally, for the remainder of this section, we fix a nontrivial normal subgroup N of $\mathrm{Inert}^{(\infty)}(\sigma_n)$, and our goal is to prove Lemma 5.2, showing that there exists $m \geq 0$ and $\mathrm{Id} \neq \zeta \in \mathrm{Simp}^{(\infty)}(\Gamma_n)$ such that $\sigma_n^m \zeta \sigma_n^{-m} \in N$.

5.3.2 *Existence of an inert with additional properties*

We start by recording a slightly stronger version of Lemma 5.5.

Lemma 5.6 (Boyle [2]). Suppose $\alpha \in \mathrm{Inert}^{(\infty)}(\sigma_n)$. There exists $M \geq 1$ such that for all $m \geq M$, there exist $\psi_1^{(m)}, \psi_2^{(m)} \in \mathrm{Simp}(\Gamma_n^{(2m)})$ such that $\alpha = \psi_1^{(m)} \sigma_n^m \psi_2^{(m)} \sigma_n^{-m}$.

Proof. This can be deduced from the proof of [2, Theorem, p. 970] (in the notation used in the proof there, for m large enough, we can choose $n = 2p - k + m \geq 0$, so that $t = k + m + n = 2p + 2m = 2(p + m)$). ■

To avoid overly cumbersome notation, we often suppress the n, writing Γ and σ instead of Γ_n and σ_n, with the understanding that we are still working with a full shift on n symbols.

Suppose $\alpha \in \mathrm{Inert}(\sigma)$ and that α is induced by a block code h_α of range $r \geq 1$; thus, $h_\alpha : \mathcal{A}_\sigma^{2r+1} \to \mathcal{A}_\sigma$. We say that

($*$) α satisfies property (*) if there exist distinct $a, b, c \in \mathcal{A}_\sigma$ such that

(i) $\alpha(p_a) = p_a$;
(ii) $h_\alpha\left(a^r a b a^{r-1}\right) \neq a \in \mathcal{A}_\sigma$;
(iii) For all $0 \leq i \leq r$, $h_\alpha(a^{r-i} b a^{r+i}) = a$ and $h_\alpha(a^{2r-i} c a^i) = a$.

Lemma 5.7. Suppose $\alpha \in \mathrm{Inert}(\sigma)$ is induced by a block code h_α of range r and satisfies (*) for some $a, b, c \in \mathcal{A}_\sigma$. Then, there exists $m \geq 1$ such that, upon viewing α as an element of $\mathrm{Inert}(\sigma^{2m})$, all of the following hold:

(i) for some $\psi_1^{(m)}, \psi_2^{(m)} \in \mathrm{Simp}(\Gamma^{(2m)})$, we have $\alpha = \psi_1^{(m)} \sigma^m \psi_2^{(m)} \sigma^{-m}$;
(ii) $\alpha(p_a) = p_a$;
(iii) for $w = b a^{m-2} c$, the point $p_{aw} = \ldots a^m w \dot{a} a^{m-1} w \ldots$ is a point of least period two for σ^m, and in particular, $\alpha(p_{aw}) \in P_2(\sigma^m)$;
(iv) the point $\alpha(p_{aw})$ in $P_2(\sigma^m)$ satisfies $\left(\alpha(p_{aw})\right)_{m-1} \neq a$ and satisfies $\left(\alpha(p_{aw})\right)_i = a$ for all $m \leq i \leq 2m - 1$.

Furthermore, using the identification of $P_2(\sigma^m)$ and $E^{(2)}(\Gamma^{(m)})$, we have the following:

(a) $\alpha\begin{pmatrix} a^m \\ a^m \end{pmatrix} = \begin{pmatrix} a^m \\ a^m \end{pmatrix}$;
(b) $\alpha\begin{pmatrix} a^m \\ w \end{pmatrix} = \begin{pmatrix} w' \\ a^m \end{pmatrix}$ for some word w' of length m where $w' \neq a^m$.

Proof. By Lemma 5.6, Part (i) holds for all sufficiently large m, so in particular for some $m \geq 2r + 2$. Part (ii) is obvious, and since a, b, c are distinct, Part (iii) follows. To prove Part (iv), note that since $\alpha(p_a) = p_a$, it follows that $h_\alpha(a^{2r+1}) = a$. Since $m \geq 2r+2$,

we have that $m - r - 1 \geq r + 1$, and it follows that

$$\sigma^{m-1}(p_{aw}) = \ldots w \underbrace{a \ldots a}_{m-r-1} \underbrace{a \ldots a}_{r} \dot{a} w \ldots$$

Thus, $\big(\alpha(p_{aw})\big)_{m-1} = \big(\sigma^{m-1}\alpha(p_{aw})\big)_0 = \big(\alpha\sigma^{m-1}(p_{aw})\big)_0 = h_\alpha(a^r a b a^{r-1}) \neq a$. Using Condition (3) of (*), it follows that $\big(\alpha(p_{aw})\big)_i = a$ for all $m \leq i \leq 2m-1$.

Parts (a) and (b) follow immediately by translating the results via the identification. ■

Given symbols $a, b \in \mathcal{A}_\sigma$, we use the shorthand $a \leftrightarrow b$ to denote the 0-block code involution in $\mathrm{Aut}(\sigma)$ which permutes the symbols a and b and leaves all other symbols fixed.

Lemma 5.8. There exists $\alpha \in N$ satisfying property (*).

Proof. Suppose $\mathrm{Id} \neq \alpha \in N$ and $\alpha \in \mathrm{Inert}(\sigma^\ell)$ for some $\ell \geq 1$. By passing to a larger ℓ if necessary, we may assume that α acts nontrivially on $P_1(\sigma^\ell)$. Since $\mathrm{Inert}(\sigma^\ell)$ can induce any permutation on $P_1(\sigma^\ell)$, and since N is normal, by replacing α with some other $\alpha' \in N$ if needed, we can assume that α satisfies

$$\alpha(p_A) = p_A \text{ for some } p_A \in P_1(\sigma^\ell) \text{ with } A \in \mathcal{A}_{\sigma^\ell};$$
$$\alpha(p_{D_1}) = p_{D_2} \text{ for some } p_{D_1}, p_{D_2} \in P_1(\sigma^\ell) \text{ with } D_1, D_2 \in \mathcal{A}_{\sigma^\ell};$$
$$\alpha(p_{E_1}) = p_{E_2} \text{ for some } p_{E_1}, p_{E_2} \in P_1(\sigma^\ell) \text{ with } E_1, E_2 \in \mathcal{A}_{\sigma^\ell};$$

and A, D_1, D_2, E_1, E_2 are all distinct.

Suppose α is induced by a block code h_α of range r. Without loss of generality, we may assume that $r \geq 1$ (if $r = 0$, the conclusion of Lemma 5.2 already holds).

Set $k = 2\ell r + 1$. By considering α as an element of $\mathrm{Inert}(\sigma^k)$, we may assume that α is given by a block code $h_\alpha^{(k)}$ of range 1.

Consider the words

$$v_d = \begin{pmatrix} A^k \\ D_1^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ D_1^k \\ A^k \end{pmatrix}$$

and

$$v_e = \begin{pmatrix} A^k \\ E_1^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ E_1^k \\ A^k \end{pmatrix}$$

of length three over the alphabet $\mathcal{A}_{\sigma^{3k}}$. Viewing α as an automorphism lying in $\mathrm{Inert}(\sigma^{3k})$, we have that α is induced by some block $h_\alpha^{(3k)}$ of radius one, and this block code satisfies

$$h_\alpha^{(3k)}(v_d) = \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix}, \quad h_\alpha^{(3k)}(v_e) = \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix},$$

while

$$h_\alpha^{(3k)}\left(\begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ D_1^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix}\right) = \begin{pmatrix} * \\ D_2 \\ * \end{pmatrix} \neq \begin{pmatrix} A^k \\ D_1^k \\ A^k \end{pmatrix}, \tag{8}$$

$$h_\alpha^{(3k)}\left(\begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ E_1^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix}\right) = \begin{pmatrix} * \\ E_2 \\ * \end{pmatrix} \neq \begin{pmatrix} A^k \\ E_1^k \\ A^k \end{pmatrix} \tag{9}$$

(note that $h_\alpha(D_1^r) = D_2 \neq D_1$ and $h_\alpha(E_1^r) = E_2 \neq E_1$).

Define the words

$$w_d = \begin{pmatrix} D_1^k \\ D_1^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ D_1^k \\ D_1^k \end{pmatrix}, \quad w_e = \begin{pmatrix} E_1^k \\ E_1^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix} \begin{pmatrix} A^k \\ E_1^k \\ E_1^k \end{pmatrix}$$

and note that $h_\alpha^{(3k)}(w_d) = \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix}$ and $h_\alpha^{(3k)}(w_e) = \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix}$.

We set convenient notation for some letters in $\mathcal{A}_{\sigma^{3k}}$: given $X \in \mathcal{A}_{\sigma^k}$, we define

$$x = \begin{pmatrix} X^k \\ X^k \\ X^k \end{pmatrix}.$$

Thus, for example,

$$a = \begin{pmatrix} A^k \\ A^k \\ A^k \end{pmatrix}.$$

Choose $b, c \in \mathcal{A}_{\sigma^{3k}}$ such that $a, b, c, d_1, d_2, e_1, e_2$ are all distinct and such that $h_\alpha^{(3k)}(aac) \neq b$ (this is possible since, e.g., $h_\alpha^{(3k)}(aac)$ contains letters from the original alphabet).

Define the automorphism $\beta_1 \in \mathrm{Inert}(\sigma^{9k})$ by

$$\beta_1 = \sigma^{3k}\left(e_1e_1e_1 \leftrightarrow aab\right)\sigma^{-3k}$$

(note that this is the conjugacy by σ^{3k} of the involution $e_1e_1e_1 \leftrightarrow aab$), and let $\alpha_1 = \beta_1^{-1}\alpha\beta_1$. Then, $\alpha_1 \in N$ and can be induced by a block code of range 4 on the alphabet $\mathcal{A}_{\sigma^{3k}}$. Furthermore, we have

$$\ldots a^4\dot{a}ba^3\ldots \xrightarrow{\beta_1} \ldots a^3e_1\dot{e}_1e_1a^3\ldots \xrightarrow{\alpha} \ldots \dot{e}_2\ldots \xrightarrow{\beta_1^{-1}} \ldots \dot{e}_2\ldots$$

and $\beta_1(p_a) = p_a$, and so α_1 satisfies conditions (1) and (2) of (*) for the letters a, b.

Define the automorphism $\beta_2 \in \mathrm{Inert}(\sigma^{9k})$ by $\beta_2 = \sigma^{3k}\beta_2'\sigma^{-3k}$, where β_2' is the 0-block code involution on the alphabet $\mathcal{A}_{\sigma^{3k}}$ that performs the following permutation on symbols:

$$\beta_2' : \begin{cases} aba \leftrightarrow v_d \\ baa \leftrightarrow w_d \\ aac \leftrightarrow w_e \\ aca \leftrightarrow v_e \end{cases} \tag{10}$$

and consider $\alpha_2 = \beta_2^{-1}\alpha_1\beta_2$. Then, $\alpha_2 \in N$, and still satisfies conditions (1) and (2) of (*). To see that it satisfies condition (3) is a matter of checking case by case. For example,

$$\ldots a^3\dot{a}baa^3\ldots \xrightarrow{\beta_2} \ldots a^3\dot{v}_da^3\ldots \xrightarrow{\alpha_1} \ldots *\dot{a}\ldots \xrightarrow{\beta_2^{-1}} \ldots *\dot{a}\ldots$$

since, by (8), $*$ is some word containing D_2s. Next,

$$\ldots a^3b\dot{a}aa^3\ldots \xrightarrow{\beta_2} \ldots a^3\dot{w}_da^3\ldots \xrightarrow{\alpha_1} \ldots *\dot{a}\ldots \xrightarrow{\beta_2^{-1}} \ldots *\dot{a}\ldots$$

since $*$ also contains some D_2s. Furthermore,

$$\dots a^3 \dot{a}\dot{c}a a^3 \dots \xrightarrow{\beta_2} \dots a^3 \dot{v}_e a^3 \dots \xrightarrow{\alpha_1} \dots * \dot{a} \dots \xrightarrow{\beta_2^{-1}} \dots * \dot{a} \dots$$

since, by (9), $*$ contains E_2s and

$$\dots a^3 a\dot{a}\dot{c}a^3 \dots \xrightarrow{\beta_2} \dots a^3 \dot{w}_e a^3 \dots \xrightarrow{\alpha_1} \dots * \dot{a} \dots \xrightarrow{\beta_2^{-1}} \dots * \dot{a} \dots$$

since $*$ contains some E_2s. ■

Combining Lemmas 5.7 and 5.8, we obtain the existence of an automorphism, which for convenience we also denote by α, with $\alpha \in N$, such that α satisfies the conditions in Lemma 5.7 for some $m \geq 1$. The automorphism α constructed in Lemma 5.8 also satisfies an additional property that we note for use in the sequel: there exists some word z_1 (e.g., let $z_1 = be_1^{m-1}$) such that, with the symbol a given by Lemma 5.8, writing $\alpha\left(\begin{smallmatrix} a^m \\ z_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$, we have $x \neq a^m$ and $y \neq a^m$.

For ease of notation, for the remainder of the section, we suppress the power m, and write σ instead of σ^m, and write ψ_1, ψ_2 for the simple automorphisms $\psi_1^{(m)}, \psi_2^{(m)}$ produced by Lemma 5.7.

It is convenient to recode the alphabet for our shift, and to do so we choose a bijection $\mathcal{A}_\sigma \leftrightarrow \{1, 2, \dots, n\}$ such that $1 \mapsto a^m$, and let $\{1, 2, \dots, n\}$ be the alphabet of our shift. Summarizing, we have shown the following lemma.

Lemma 5.9. There exists $\alpha \in \mathrm{Inert}(\sigma^2)$ satisfying the following properties:

(i) $\alpha \in N$;
(ii) $\alpha = \psi_1 \sigma \psi_2 \sigma^{-1}$, for some $\psi_1, \psi_2 \in \mathrm{Simp}(\Gamma^{(2)})$;
(iii) $\alpha\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$;
(iv) $\alpha\left(\begin{smallmatrix} 1 \\ u_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} u_2 \\ 1 \end{smallmatrix}\right)$ for some $1 \neq u_1$ and some $u_2 \in \{1, 2, \dots, n\}$;
(v) there exists $u_3 \in \{1, 2, \dots, n\}$ such that neither component of $\alpha\left(\begin{smallmatrix} 1 \\ u_3 \end{smallmatrix}\right)$ is 1.

5.3.3 *Constructing a particular subgroup $\mathcal{K}$ of $Sym(E^{(2)}) \times Sym(E^{(2)})$*

Consider the set

$$\mathcal{K}_N = \{(\phi_1, \phi_2) \in \mathrm{Simp}(\Gamma^{(2)}) \times \mathrm{Simp}(\Gamma^{(2)}) \colon \phi_1 \sigma \phi_2^{-1} \sigma^{-1} \in N\}. \tag{11}$$

Lemma 5.10. The set $\mathcal{K}_N$ defined in (11) is a subgroup of $\mathrm{Simp}(\Gamma^{(2)}) \times \mathrm{Simp}(\Gamma^{(2)})$.

Proof. Assume $\phi_1\sigma\phi_2^{-1}\sigma^{-1}, \phi_3\sigma\phi_4^{-1}\sigma^{-1} \in N$. Then, $\sigma\phi_4^{-1}\sigma^{-1}\phi_3 \in N$, and hence,

$$\sigma\phi_4^{-1}\sigma^{-1}\phi_3\phi_1\sigma\phi_2^{-1}\sigma^{-1} \in N$$

and

$$\phi_3\phi_1\sigma\phi_2^{-1}\phi_4^{-1}\sigma^{-1} = \phi_3\phi_1\sigma(\phi_4\phi_2)^{-1}\sigma^{-1} \in N.$$

Lastly, if $\phi_1\sigma\phi_2^{-1}\sigma^{-1} \in N$, then $\phi_1^{-1}\sigma\phi_2\sigma^{-1} = \phi_1^{-1}\sigma\phi_2\sigma^{-1}\phi_1^{-1}\phi_1 \in N$. ■

To simplify notation, for the remainder of this section, we write $E^{(m)}$ instead of $E^{(m)}(\Gamma)$. By definition, $E^{(2)}$ is the edge set of $\Gamma^{(2)}$, so there is an isomorphism

$$\mathcal{H}\colon \mathrm{Simp}(\Gamma^{(2)}) \longrightarrow \mathrm{Sym}(E^{(2)}), \tag{12}$$

and hence an isomorphism,

$$\mathcal{H}\times\mathcal{H}\colon \mathrm{Simp}(\Gamma^{(2)})\times\mathrm{Simp}(\Gamma^{(2)}) \longrightarrow \mathrm{Sym}(E^{(2)})\times\mathrm{Sym}(E^{(2)}).$$

Define

$$\mathcal{K} = (\mathcal{H}\times\mathcal{H})(\mathcal{K}_N), \tag{13}$$

meaning that $\mathcal{K}$ is the image of $\mathcal{K}_N$ under this isomorphism. Thus, we have

$$\mathcal{K} \subset \mathrm{Sym}(E^{(2)})\times\mathrm{Sym}(E^{(2)}).$$

Let $\alpha \in \mathrm{Inert}(\sigma^2)$ be the element in N given by Lemma 5.9. Maintaining the notation of that lemma, we have $\alpha = \psi_1\sigma\psi_2\sigma^{-1}$, for some $\psi_1, \psi_2 \in \mathrm{Simp}(\Gamma^{(2)})$ and so

$$(\psi_1, \psi_2^{-1}) \in \mathcal{K}_N.$$

Defining

$$\gamma_1 = \mathcal{H}(\psi_1), \quad \gamma_2 = \mathcal{H}(\psi_2), \tag{14}$$

it follows that

$$(\gamma_1, \gamma_2^{-1}) \in \mathcal{K}. \tag{15}$$

Recall we have $E^{(2)} = E^{(1)} \times E^{(1)}$, and we write points in $E^{(2)}$ as $\begin{pmatrix} x \\ y \end{pmatrix}$ where $x, y \in E^{(1)}$. We embed $\mathrm{Sym}(E^{(1)}) \times \mathrm{Sym}(E^{(1)})$ into $\mathrm{Sym}(E^{(2)})$ via the map

$$(\phi_1, \phi_2) \mapsto \begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix}, \tag{16}$$

where $\begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \phi_1(x) \\ \phi_2(y) \end{pmatrix}$. Define

$$xP \text{ to be the subgroup of } \mathrm{Sym}(E^{(2)}) \text{ that is the image of this embedding.} \tag{17}$$

Lemma 5.11. For any $\begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix} \in P$, we have $\left(\begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix}, \begin{pmatrix} \phi_2 \\ \phi_1 \end{pmatrix}\right) \in \mathcal{K}$.

Proof. Let $\begin{pmatrix} \tilde{\phi}_1 \\ \tilde{\phi}_2 \end{pmatrix} \in \mathrm{Simp}(\Gamma^{(2)})$ be the automorphism induced by the permutation $\begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix}$ on the edge set $E^{(2)}(\Gamma)$. Thus, $\begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix} = (\mathcal{H} \times \mathcal{H})\begin{pmatrix} \tilde{\phi}_1 \\ \tilde{\phi}_2 \end{pmatrix}$. It is straightforward to check that

$$\begin{pmatrix} \tilde{\phi}_1 \\ \tilde{\phi}_2 \end{pmatrix}\sigma\begin{pmatrix} \tilde{\phi}_2^{-1} \\ \tilde{\phi}_1^{-1} \end{pmatrix}\sigma^{-1} = \begin{pmatrix} \tilde{\phi}_1 \\ \tilde{\phi}_2 \end{pmatrix}\begin{pmatrix} \tilde{\phi}_1^{-1} \\ \tilde{\phi}_2^{-1} \end{pmatrix} = \mathrm{Id} \in N,$$

so

$$\left(\begin{pmatrix} \tilde{\phi}_1 \\ \tilde{\phi}_2 \end{pmatrix}, \begin{pmatrix} \tilde{\phi}_2 \\ \tilde{\phi}_1 \end{pmatrix}\right) \in \mathcal{K}_N.$$

■

Define the swapping element $\mathfrak{s} \in \mathrm{Sym}(E^{(2)})$ by

$$\mathfrak{s}\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} q \\ p \end{pmatrix}. \tag{18}$$

Recall we can identify period two points for σ with the set $E^{(2)}$. Then, σ induces an action on $E^{(2)}$, and this action agrees with the action of $\mathfrak{s}$ on $E^{(2)}$.

Lemma 5.12. For the elements γ_1, γ_2 defined in Equation (14), we have $\gamma_2^{-1} \neq \mathfrak{s}^{-1}\gamma_1\mathfrak{s}$.

Proof. By Lemma (5.9), $\alpha = \psi_1\sigma\psi_2\sigma^{-1}$ for some $\psi_1, \psi_2 \in \mathrm{Simp}(\Gamma^{(2)})$. If $\gamma_2^{-1} = \mathfrak{s}^{-1}\gamma_1\mathfrak{s}$, then α acts on $E^{(2)}$ by the permutation

$$\gamma_1\mathfrak{s}\mathfrak{s}^{-1}\gamma_1^{-1}\mathfrak{s}\mathfrak{s}^{-1} = \gamma_1\gamma_1^{-1} = \mathrm{Id}.$$

But this contradicts Lemma 5.9, as α acts nontrivially on $E^{(2)}$. ■

5.3.4 *Completion of the proof of Lemma 5.2*

To translate properties of $\mathcal{K}$ to subgroups of $\mathrm{Sym}(E^{(2)})$, we make use of the following result.

Lemma 5.13 (Goursat's lemma (see [23])). Let G_1, G_2 be groups, and let H be a subgroup of $G_1 \times G_2$. Then, there exist subgroups $H_1 \subset G_1, H_2 \subset G_2$, normal subgroups $N_1 \trianglelefteq H_1, N_2 \trianglelefteq H_2$, and an isomorphism $\Psi\colon H_1/N_1 \to H_2/N_2$ such that

$$H = \{(x, y) \in H_1 \times H_2 \colon \Psi([x]) = [y]\}.$$

Applying Goursat's lemma to the group $\mathcal{K}$, we obtain the following corollary.

Corollary 5.14. Let $\mathcal{K}$ be the subgroup defined in (13). There exist $H_1, H_2 \subset \mathrm{Sym}(E^{(2)})$, normal subgroups $N_1 \trianglelefteq H_1, N_2 \trianglelefteq H_2$, and an isomorphism $\Psi\colon H_1/N_1 \to H_2/N_2$ such that

$$\mathcal{K} = \{(\phi_1, \phi_2) \in H_1 \times H_2 \colon \Psi([\phi_1]) = [\phi_2]\}.$$

We turn our attention then to studying the subgroups H_1, H_2, N_1, N_2. The key lemma regarding their structure is the following.

Lemma 5.15. Assume both subgroups N_1 and N_2 of Corollary 5.14 are trivial. Then, at least one of the following holds:

(i) $H_1 = \mathrm{Sym}(E^{(2)})$ and $H_2 = \mathrm{Sym}(E^{(2)})$;
(ii) $H_1 = \mathrm{Alt}(E^{(2)})$ and $H_2 = \mathrm{Alt}(E^{(2)})$.

As the proof of this lemma is lengthy and involves checking multiple cases, we defer its proof to Section 5.4.

For use in the proof of Lemma 5.2, we recall the following classical theorem.

Theorem 5.16. Suppose $|X| > 6$, G is either $\mathrm{Sym}(X)$ or $\mathrm{Alt}(X)$, and $\Psi\colon G \to G$ is an automorphism. Then, there exists $g \in \mathrm{Sym}(X)$ such that $\Psi(h) = g^{-1}hg$ for all $h \in G$.

We have now assembled the tools to prove Lemma 5.2 (modulo the deferral of the technical statement in Lemma 5.15).

Proof of Lemma 5.2. Let N_1, N_2 be the subgroups produced in Corollary 5.14, and let $\Psi : H_1/N_1 \to H_2/N_2$ be the isomorphism in the same result.

Assume first that $N_1 \neq \{\mathrm{Id}\}$, so there is some $\phi_1 \neq \mathrm{Id}$ with $\phi_1 \in N_1$. Then, $\Psi([\phi_1]) = \Psi([\mathrm{Id}]) = [\mathrm{Id}] \in H_2/N_2$, so $(\phi_1, \mathrm{Id}) \in \mathcal{K}$. This implies that

$$\mathcal{H}^{-1}(\phi_1)\sigma\sigma^{-1} = \mathcal{H}^{-1}(\phi_1) \in N.$$

But since $\mathcal{H}^{-1}(\phi_1) \in \mathrm{Simp}(\Gamma)$, the statement of Lemma 5.2 follows. Likewise, if $N_2 \neq \{\mathrm{Id}\}$, then $(\mathrm{Id}, \phi_2) \in \mathcal{K}$ for some $\phi_2 \in N_2$, and again the result follows. Thus, we are left with showing that either $N_1 \neq \{\mathrm{Id}\}$ or $N_2 \neq \{\mathrm{Id}\}$.

We proceed by contradiction and suppose that both $N_1 = \{\mathrm{Id}\}$ and $N_2 = \{\mathrm{Id}\}$. Combining Corollary 5.14 and Lemma 5.15, we have that the isomorphism Ψ is either

$$\Psi : \mathrm{Sym}(E^{(2)}) \to \mathrm{Sym}(E^{(2)})$$

or

$$\Psi : \mathrm{Alt}(E^{(2)}) \to \mathrm{Alt}(E^{(2)}).$$

By Theorem 5.16, we have that Ψ is given by $\Psi(h) = g^{-1}hg$ for some $g \in \mathrm{Sym}(E^{(2)})$.

We claim that g is the swap map $\mathfrak{s}$, defined in (18).

To check this claim, note that for any $\begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix} \in P$, where P is defined in (17), it follows from Lemma 5.11 that $\left(\begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix}, \begin{pmatrix} \phi_2 \\ \phi_1 \end{pmatrix}\right) \in K$. Thus,

$$g^{-1}\begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix} g = \begin{pmatrix} \phi_2 \\ \phi_1 \end{pmatrix},$$

and hence,

$$g^{-1}\mathfrak{s}\begin{pmatrix} \phi_2 \\ \phi_1 \end{pmatrix}\mathfrak{s}^{-1}g = \begin{pmatrix} \phi_2 \\ \phi_1 \end{pmatrix} \tag{19}$$

for all $\phi_1, \phi_2 \in \mathrm{Sym}(E^{(1)})$. We now check that this implies that $\mathfrak{s}^{-1}g = \mathrm{Id}$. If not, there exists $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \in E^{(2)}$ such that $\mathfrak{s}^{-1}g\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$ and $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \neq \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$. Either $x_1 \neq x_2$ or $y_1 \neq y_2$; assume $x_1 \neq x_2$ (the other case is similar). Choose $z \in E^{(1)}$ such that $z \neq x_1, x_2$, and define $\phi_3 \in \mathrm{Sym}(E^{(1)})$ to be the transposition swapping x_2 and z. Then,

$$\begin{pmatrix} \phi_3 \\ \mathrm{Id} \end{pmatrix}\mathfrak{s}^{-1}g\begin{pmatrix} \phi_3 \\ \mathrm{Id} \end{pmatrix}^{-1}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} \phi_3 \\ \mathrm{Id} \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} z \\ y_2 \end{pmatrix} \neq \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \mathfrak{s}^{-1}g\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

contradicting (19), thus proving the claim.

Since $(\gamma_1, \gamma_2^{-1}) \in \mathcal{K}$ (see (15)) we have $\gamma_2^{-1} = \Psi(\gamma_1)$. It then follows from the claim that $\gamma_2^{-1} = \mathfrak{s}^{-1}\gamma_1\mathfrak{s}$. But this contradicts Lemma 5.12, completing the proof. ■

5.4 The proof of Lemma 5.15

5.4.1 *Preliminary reductions*

We are left with showing Lemma 5.15. Recall that Corollary 5.14 gives us the existence of subgroups $H_1, H_2 \subset \mathrm{Sym}(E^{(2)})$, normal subgroups $N_1 \trianglelefteq H_1, N_2 \trianglelefteq H_2$, and an isomorphism $\Psi : H_1/N_1 \to H_2/N_2$ such that

$$\mathcal{K} = \{(\phi_1, \phi_2) \in H_1 \times H_2 : \Psi([\phi_1]) = [\phi_2]\}.$$

The statement of Lemma 5.15 is that when both subgroups N_1 and N_2 are trivial, at least one of the following holds:

(i) $H_1 = \mathrm{Sym}(E^{(2)})$ and $H_2 = \mathrm{Sym}(E^{(2)})$;
(ii) $H_1 = \mathrm{Alt}(E^{(2)})$ and $H_2 = \mathrm{Alt}(E^{(2)})$.

We start with some terminology used to study these subgroups.

For a finite set X, recall that $\mathrm{Sym}(X)$ denotes the group of permutations of the set X. If $K \subset \mathrm{Sym}(X)$ is a subgroup, a nonempty subset $A \subset X$ is called a *K-block* if for all $g \in K$ either $g(A) = A$ or $g(A) \cap A = \emptyset$. A subgroup $K \subset \mathrm{Sym}(X)$ is called *primitive* if the only K-blocks are singletons and X. We say the subgroup $K \subset \mathrm{Sym}(X)$ *contains a p-cycle* if it contains some element $\tau \in K$ such that τ consists of a single p-cycle.

Theorem 5.17 (Jordan ([38, Theorem 13.9])). Suppose $K \subset \mathrm{Sym}(X)$ is primitive and contains a p-cycle for some prime $p < |X| - 2$. Then, $K = \mathrm{Alt}(X)$ or $K = \mathrm{Sym}(X)$.

Thus, to prove Lemma 5.15, by Jordan's theorem, since $H_1, H_2 \subset \mathrm{Sym}(E^{(2)})$, it suffices to show that at least one of H_1, H_2 is primitive and also contains a p-cycle for some prime $p < |E^{(2)}| - 2$.

We start with some technical results on subgroups of $\mathrm{Sym}(E^{(2)})$, then prove primitivity, and then show how to generate a p-cycle for some prime $p < |E^{(2)}| - 2$.

5.4.2 *Subgroups of Sym$(E^{(2)})$*

To denote the 1st and 2nd components of an element $\binom{x}{y} \in E^{(2)}$, we write

$$\binom{x}{y}_1 = x, \quad \binom{x}{y}_2 = y.$$

We say that an element $\tau \in \mathrm{Sym}(E^{(2)})$ is

(i) *row-preserving* if $\tau\binom{x_1}{y_1}_1 = \tau\binom{x_1}{y_2}_1$ for all $y_1, y_2 \in E^{(1)}$;
(ii) *column-preserving* if $\tau\binom{x_1}{y_1}_2 = \tau\binom{x_2}{y_1}_2$ for all $x_1, x_2 \in E^{(1)}$;
(iii) *free* if τ is neither row-preserving nor column-preserving.

For any element $\tau \in \mathrm{Sym}(E^{(2)})$, there exists a pair of functions $\tau_1, \tau_2 \colon E^{(2)} \to E^{(1)}$ such that

$$\tau\binom{x_1}{y_1} = \begin{pmatrix} \tau_1\binom{x_1}{y_1} \\ \tau_2\binom{x_1}{y_1} \end{pmatrix}.$$

It follows quickly from the definitions that

(i) τ is row-preserving if and only if $\tau_1\binom{x}{y}$ is independent of y,
(ii) τ is column-preserving if and only if $\tau_2\binom{x}{y}$ is independent of x.

It is also easy to check that

(i) the collection of $\tau \in \mathrm{Sym}(E^{(2)})$ that are row-preserving forms a subgroup;
(ii) the collection of $\tau \in \mathrm{Sym}(E^{(2)})$ that are column-preserving forms a subgroup;
(iii) any $\tau \in P$, where P is the subgroup defined in (17), is both row-preserving and column-preserving.

In Lemma 5.9, we showed the existence of $\alpha \in N$ of the form $\alpha = \psi_1 \sigma \psi_2 \sigma^{-1}$ for some $\psi_1, \psi_2 \in \mathrm{Simp}(\Gamma^{(2)})$. The automorphism α acts on $P_2(\sigma)$, and upon identifying $P_2(\sigma)$ with $E^{(2)}$, there is a corresponding permutation of $E^{(2)}$ induced by α, which we denote by $\overline{\alpha} \in \mathrm{Sym}(E^{(2)})$. (Recall that we are identifying $E^{(2)}$ with $E^{(1)} \times E^{(1)}$ and that $E^{(1)} = \{1, 2, \ldots, n\}$.)

Recall that γ_1, γ_2 are defined in (14) and the swap map $\mathfrak{s}$ is defined in (18). By Part (iii) of Lemma 5.9, we have that $\overline{\alpha}(\begin{pmatrix} 1 \\ 1 \end{pmatrix}) = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Since the subgroup P (see (17)) acts transitively on $E^{(2)}$, there exists some $\phi \in P$ such that $\gamma_1\phi\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Letting $\tilde{\phi}$ denote the automorphism in $\mathrm{Simp}(\Gamma^{(2)})$ corresponding to $\phi \in \mathrm{Sym}(E^{(2)})$, we have that

$$\alpha = \psi_1\sigma\psi_2\sigma^{-1} = \psi_1\tilde{\phi}\tilde{\phi}^{-1}\sigma\psi_2\sigma^{-1} = \psi_1\tilde{\phi}\sigma\sigma^{-1}\tilde{\phi}^{-1}\sigma\psi_2\sigma^{-1} \in N.$$

Since $\phi \in P$, it is straightforward to check that $\sigma^{-1}\tilde{\phi}^{-1}\sigma \in \mathrm{Simp}(\Gamma^{(2)})$, and hence $(\psi_1\tilde{\phi}, \psi_2^{-1}\sigma^{-1}\tilde{\phi}\sigma) \in \mathcal{K}_N$. Furthermore (recall that the isomorphism $\mathcal{H}$ is defined in (12)),

$$\mathcal{H}(\sigma^{-1}\tilde{\phi}\sigma) = \mathfrak{s}^{-1}\phi\mathfrak{s},$$

and it follows that $(\gamma_1\phi, \gamma_2^{-1}\mathfrak{s}^{-1}\phi\mathfrak{s}) \in \mathcal{K}$. Abusing notation, we replace γ_1 and γ_2^{-1} by $\gamma_1\phi$ and $\gamma_2^{-1}\mathfrak{s}^{-1}\phi\mathfrak{s}$, respectively. Then, $\gamma_1\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Since $\overline{\alpha}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\sigma\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, it follows that $\gamma_2\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ as well.

By Part (b) of Lemma 5.7, $\overline{\alpha}\begin{pmatrix} 1 \\ u_1 \end{pmatrix} = \begin{pmatrix} u_2 \\ 1 \end{pmatrix}$ for some $u_1 \neq 1, u_2 \neq 1$. Since $\alpha \in \mathrm{Aut}(\sigma)$, it follows that $\overline{\alpha}\begin{pmatrix} u_1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ u_2 \end{pmatrix}$ as well. Finally, recall in our notation the action $\overline{\alpha}$ of α on $E^{(2)}$ is given by

$$\overline{\alpha} = \gamma_1\mathfrak{s}\gamma_2\mathfrak{s}^{-1}.$$

Lemma 5.18. Either γ_1 is free or γ_2 is free.

Proof. Suppose γ_2 is row-preserving. Then, $\gamma_2\begin{pmatrix} 1 \\ u_1 \end{pmatrix} = \begin{pmatrix} 1 \\ v_1 \end{pmatrix}$ for some $v_1 \in E^{(1)}$, $v_1 \neq 1$, since γ_2 fixes $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Then,

$$\begin{pmatrix} 1 \\ u_2 \end{pmatrix} = \overline{\alpha}\begin{pmatrix} u_1 \\ 1 \end{pmatrix} = \gamma_1\mathfrak{s}\gamma_2\mathfrak{s}^{-1}\begin{pmatrix} u_1 \\ 1 \end{pmatrix} = \gamma_1\mathfrak{s}\gamma_2\begin{pmatrix} 1 \\ u_1 \end{pmatrix} = \gamma_1\mathfrak{s}\begin{pmatrix} 1 \\ v_1 \end{pmatrix} = \gamma_1\begin{pmatrix} v_1 \\ 1 \end{pmatrix}.$$

Thus, $\gamma_1\begin{pmatrix} v_1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ u_2 \end{pmatrix}$. Since γ_1 fixes $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, it follows that γ_1 is free.

Suppose instead that γ_2 is column-preserving. Then, likewise, we have $\gamma_2\begin{pmatrix} u_1 \\ 1 \end{pmatrix} = \begin{pmatrix} v_2 \\ 1 \end{pmatrix}$ for some $v_2 \in E^{(1)}$, $v_2 \neq 1$, since γ_2 fixes $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Thus, as in the 1st case, we then have

$$\begin{pmatrix} u_2 \\ 1 \end{pmatrix} = \overline{\alpha}\begin{pmatrix} 1 \\ u_1 \end{pmatrix} = \gamma_1\mathfrak{s}\gamma_2\mathfrak{s}^{-1}\begin{pmatrix} 1 \\ u_1 \end{pmatrix} = \gamma_1\mathfrak{s}\gamma_2\begin{pmatrix} u_1 \\ 1 \end{pmatrix} = \gamma_1\mathfrak{s}\begin{pmatrix} v_2 \\ 1 \end{pmatrix} = \gamma_1\begin{pmatrix} 1 \\ v_2 \end{pmatrix}.$$

Since γ_1 fixes $\binom{1}{1}$, it again follows that γ_1 is free. ■

For a subgroup $H \subset \mathrm{Sym}(E^{(2)})$, we say *$H$ contains the arrangement*

$$\begin{cases} \binom{x_1}{y_1} \mapsto \binom{x_1'}{y_1'} \\ \vdots \\ \binom{x_n}{y_n} \mapsto \binom{x_n'}{y_n'} \end{cases} \tag{20}$$

if H contains an element ϕ such that ϕ maps points as in (20). Note that not all points of $E^{(2)}$ may be listed, and if a point is not listed, it means we make no claim how ϕ acts on that point. Instead of writing $\binom{x_1}{y_1} \mapsto \binom{x_1}{y_1}$, we simply write Id on $\binom{x_1}{y_1}$.

Lemma 5.19. Suppose H is a subgroup of $\mathrm{Sym}(E^{(2)})$ and $P \subset H$, where P is the subgroup defined in (17).

(i) Suppose there exists $\tau \in H$ such that τ is not row-preserving. Then, at least one of the following holds:

(a) H contains the arrangement

$$\begin{cases} \text{Id on } \binom{1}{1} \\ \binom{1}{2} \mapsto \binom{2}{2}; \end{cases} \tag{21}$$

(b) H contains the arrangement

$$\begin{cases} \text{Id on } \binom{1}{1} \\ \binom{2}{1} \mapsto \binom{1}{2} \end{cases}. \tag{22}$$

(ii) Suppose there exists $\tau \in H$ such that τ is not column-preserving. Then, at least one of the following holds:

(a) H contains the arrangement

$$\begin{cases} \text{Id on } \binom{1}{1} \\ \binom{2}{1} \mapsto \binom{2}{2}; \end{cases} \tag{23}$$

(b) H contains the arrangement

$$\begin{cases} \text{Id on } \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 2 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 2 \end{pmatrix} \end{cases}. \tag{24}$$

(iii) If H contains some τ where τ is free, then H contains the arrangement

$$\begin{cases} \text{Id on } \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 1 \\ 2 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 1 \end{pmatrix} \end{cases}. \tag{25}$$

Proof. The proofs of Parts (1) and (2) are similar, so we only prove case (2), assuming that τ is not column-preserving.

Since τ is not column-preserving, there exist $a_1, a_2, b_1 \in E^{(1)}$ such that $\left(\tau\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}\right)_2 \neq \left(\tau\begin{pmatrix} a_2 \\ b_1 \end{pmatrix}\right)_2$. The group P acts transitively on $E^{(2)}$, so there exists $\phi_1 \in P$ such that $\phi_1\tau\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$. It follows that $\phi_1\tau\begin{pmatrix} a_2 \\ b_1 \end{pmatrix}_2 \neq b_1$. Choose $\phi_2 \in P$ such that $\phi_2\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$, let $\phi_3 = \phi_2^{-1}\phi_1\tau\phi_2$, and let $\begin{pmatrix} a_3 \\ 1 \end{pmatrix} = \phi_2^{-1}\begin{pmatrix} a_2 \\ b_1 \end{pmatrix}$. Note that $a_3 \neq 1$. We have $\phi_3\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, and setting $k = \phi_3\begin{pmatrix} a_3 \\ 1 \end{pmatrix}_2$, we have $k \neq 1$ (since $\phi_1\tau\begin{pmatrix} a_2 \\ b_1 \end{pmatrix}_2 \neq b_1$). Letting $\phi_4 = \begin{pmatrix} \text{Id} \\ k \leftrightarrow 2 \end{pmatrix}\phi_3$, it follows that $\phi_4\begin{pmatrix} a_3 \\ 1 \end{pmatrix}_2 = 2$. Finally, let $\phi_5 = \phi_4\begin{pmatrix} 2 \leftrightarrow a_3 \\ \text{Id} \end{pmatrix}$, so that $\phi_5\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} t \\ 2 \end{pmatrix}$ for some t. Note that we still have $\phi_5\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. If $t = 1$, then ϕ_5 gives arrangement (24). If $t > 1$, then letting $\phi_6 = \begin{pmatrix} t \leftrightarrow 2 \\ \text{Id} \end{pmatrix}\phi_5$, ϕ_6 gives arrangement (23).

Turning to Part (3), suppose $\tau \in H$ and τ is free. By Parts (1) and (2), either H contains the arrangement

$$\begin{cases} \text{Id on } \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 2 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 2 \end{pmatrix} \end{cases} \tag{26}$$

in which case (upon taking an inverse) we are done, or H contains both arrangements

$$\begin{cases} \text{Id on } \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 2 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 2 \end{pmatrix} \end{cases} \quad \text{and} \quad \begin{cases} \text{Id on } \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 1 \\ 2 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 2 \end{pmatrix}. \end{cases} \tag{27}$$

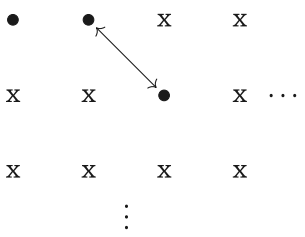
In the latter case, if ϕ_1, ϕ_2 implement these arrangements, then $\phi_1^{-1}\phi_2$ implements the arrangement

$$\begin{cases} \text{Id on } \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 1 \\ 2 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 1 \end{pmatrix}. \end{cases} \tag{28}$$

■

5.4.3 *Structures in the subgroups H_1, H_2*

We use pictures to depict the action of elements of $\mathrm{Sym}(E^{(2)})$. Since $E^{(2)} = E^{(1)} \times E^{(1)}$, each point $p \in E^{(2)}$ corresponds to an ordered pair $p = (p_1, p_2) \in E^{(1)} \times E^{(1)}$; we choose an ordering on $E^{(1)}$ and may then consider $E^{(2)}$ as a grid of points with respect to the ordering chosen for $E^{(1)}$. When we say $\phi \in \mathrm{Sym}(E^{(2)})$ *acts by*



we mean that ϕ acts on $E^{(2)}$ as drawn in the picture, with the following conventions:

(i) An arrow drawn from one • (representing a point (p_1, q_1)) to another • (representing a point (p_2, q_2)) indicates the point (p_1, q_1) is mapped to the point (p_2, q_2). A two-headed arrow between two bullets indicates the two corresponding points are swapped.

(ii) A • associated with no arrow represents a point fixed by ϕ.

(iii) An **x** means the point could be mapped anywhere, meaning that we make no assumption on how that point is mapped by ϕ.

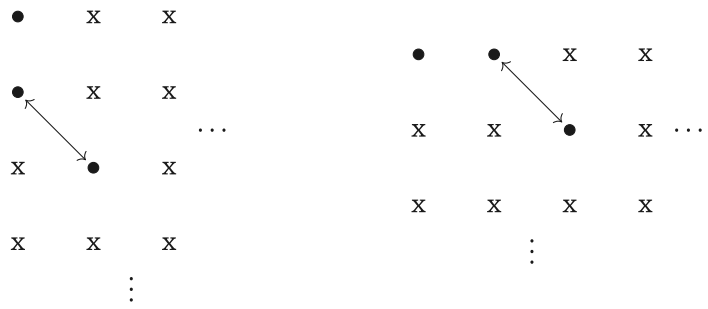
(iv) Ellipses indicate the type of action continues in that direction. For example, the use of ellipses following **x**s means that we make no assumption on how ϕ acts on points in that direction. When ellipses are between specified behavior, we mean a continuation of the same type of action (this is not relevant until Figure 1b.2 (i).

(v) When no ellipses are present, ϕ acts by the identity on any unrepresented points (meaning points in $E^{(2)}$ that do not appear in the picture).

Definition 5.20. We say a subgroup $H \subset \mathrm{Sym}(E^{(2)})$ is *substantial* if it contains both of the following:

(i) a free element;

(ii) an involution implementing at least one of the following arrangements:



Arrangement (a) Arrangement (b)

Lemma 5.21. At least one of the subgroups H_1, H_2 in $\mathrm{Sym}(E^{(2)})$ is substantial.

Before the proof, we introduce some notation. Define

$$\mathrm{CR} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in E^{(2)} : \text{either } x = 1 \text{or } y = 1 \right\}, \tag{29}$$

and so CR is the union of row one and column one in $E^{(2)}$ (CR stands for column row). Define

$$\mathrm{IS} = E^{(2)} \setminus \mathrm{CR} \tag{30}$$

(IS stands for inner square).

Proof. First, suppose H is a subgroup of $\mathrm{Sym}(E^{(2)})$ with $P \subset H$, and suppose $\phi \in H$ satisfies both of the following:

(i) $\phi \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$;

(ii) $\phi \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \in \mathrm{IS}$ for some $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \in \mathrm{CR}$.

Note that since ϕ satisfies both of the above conditions, $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$ cannot be equal to $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. We prove that H contains an involution implementing at least one of the arrangements in Part (2) of Definition 5.20. Thus, suppose that we have such a ϕ and

some $\binom{1}{1} \neq \binom{x_1}{y_1} \in \mathrm{CR}$ with $\phi\binom{x_1}{y_1} = \binom{x_2}{y_2} \in \mathrm{IS}$. Suppose first that $\binom{x_1}{y_1}$ is in column one (so $y_1 = 1$ and $x_1 > 1$, since $\binom{x_1}{y_1} \neq \binom{1}{1}$). By replacing ϕ by $\binom{2 \leftrightarrow x_1}{id}^{-1}\phi\binom{2 \leftrightarrow x_1}{id}$, we may assume that $x_1 = 2$. Set

$$L_1 = \{\binom{x}{y} \in E^{(2)} : x > 2 \text{ and } y > 1\}.$$

Since n is large, there exists some $\binom{x_3}{y_3} \in L_1$ such that $\phi\binom{x_3}{y_3} \in \mathrm{IS}$. Choose some involution $\tau_1 \in P$ such that $\tau_1\binom{1}{1} = \binom{1}{1}$ and $\tau_1\phi\binom{x_3}{y_3} = \binom{x_2}{y_2}$. Then,

$$\phi^{-1}\tau_1\phi\binom{x_3}{y_3} = \phi^{-1}\binom{x_2}{y_2} = \binom{x_1}{y_1} = \binom{2}{1}.$$

Thus, $\phi^{-1}\tau_1\phi$ is an involution in H fixing $\binom{1}{1}$ that satisfies $\phi^{-1}\tau_1\phi\binom{2}{1} = \binom{x_3}{y_3} \in L_1$, and we may choose another involution $\tau_2 \in P$ such that τ_2 fixes $\binom{1}{1}$, and $\tau_2\binom{x_3}{y_3} = \binom{3}{2}$. Now, the involution $\tau_2^{-1}\phi^{-1}\tau_1\phi\tau_2$ is in H and implements the 1st arrangement. The case that $\binom{x_1}{y_1}$ is in row one is similar and produces an involution in H implementing the 2nd arrangement. This completes the proof of the claim.

Recall we have $\gamma_1 \in H_1, \gamma_2^{-1} \in H_2$ (see (14)) and both γ_1 and γ_2 fix $\binom{1}{1}$. By Lemma 5.18, either γ_1 is free or γ_2 is free. Suppose then that γ_1 is free. If γ_1 maps any point (necessarily not $\binom{1}{1}$) in CR into IS, then H_1 satisfies both parts of Definition 5.20 by the claim above. Suppose then that γ_1 leaves CR invariant. Then, $\gamma_1\mathfrak{s}$ leaves CR invariant, and fixes $\binom{1}{1}$. By condition (v) of Lemma 5.9, $\overline{\alpha} = \gamma_1\mathfrak{s}\gamma_2\mathfrak{s}^{-1}$ maps the points $\binom{1}{u_3}$ and $\binom{u_3}{1}$ into IS. Since $\mathfrak{s}$ leaves CR and hence IS invariant, this means γ_2 maps both $\binom{1}{u_3}$ and $\binom{u_3}{1}$ into IS. Since γ_2 fixes $\binom{1}{1}$, this implies γ_2 is neither row-preserving nor column-preserving and so is free. Furthermore, γ_2 maps a point in CR (specifically, $\binom{1}{u_3}$) into IS. By the claim, this implies H_2 satisfies both conditions (1) and (2) of Definition 5.20.

A similar argument shows that if γ_2 is free and preserves CR, then H_1 satisfies both conditions (1) and (2) of Definition 5.20, finishing the proof. ■

5.4.4 *Primitivity*

Our goal now is to show that any substantial subgroup of $\mathrm{Sym}(E^{(2)})$, which contains P is primitive.

We make use of the following lemma from [13].

Lemma 5.22 (See [13, p. 735]). Suppose X is a finite set, $K \subset \mathrm{Sym}(X)$ is transitive, and $x \in X$. Then, K is primitive if the only blocks that contain x are $\{x\}$ and X.

Lemma 5.23. Suppose $H \subset \mathrm{Sym}(E^{(2)})$ is a subgroup that contains P and is substantial. Then, H is primitive.

Proof. Since the subgroup P (see (17)) acts transitively on $E^{(2)}$ and $P \subset H$, the subgroup H also acts transitively on $E^{(2)}$. By Lemma 5.22, it suffices to show that if A is any H-block containing $\binom{1}{1}$ and at least one other point, then A must be all of $E^{(2)}$.

Let A be an H-block containing $\binom{1}{1}$ and some other point $\binom{x_1}{y_1}$. We claim that if A contains a point in IS (recall that the set IS is defined in (30)), then $A = E^{(2)}$. To check this, suppose A contains $\binom{u_1}{v_1} \in \mathrm{IS}$. If $\binom{u_2}{v_2}$ is any other point in IS, then there exists $\phi \in P$ such that

$$\phi\colon \begin{cases} \mathrm{Id \ on} \ \binom{1}{1} \\ \binom{u_1}{v_1} \mapsto \binom{u_2}{v_2}. \end{cases}$$

It follows that A contains IS. Now, $\binom{\mathrm{Id}}{1 \leftrightarrow 2} A \cap A \neq \emptyset$ and $\binom{\mathrm{Id}}{1 \leftrightarrow 2} A$ contains all of column 1 except $\binom{1}{1}$, so A contains all of column 1 (since A already contained $\binom{1}{1}$). Likewise, $\binom{1 \leftrightarrow 2}{\mathrm{Id}} A \cap A \neq \emptyset$ so A must contain all of row 1. Thus, A must contain all of $E^{(2)}$, proving the claim.

To finish the proof of the lemma, it suffices then to show that A contains some point in IS. By assumption, A contains some point $\binom{x_1}{y_1} \neq \binom{1}{1}$. The only remaining cases then are that either $\binom{x_1}{y_1}$ lies in row 1 or $\binom{x_1}{y_1}$ lies in column 1. We prove the first case; the 2nd case is analogous.

Assume $x_1 = 1$. Then, for any $1 \neq z \in E^{(1)}$, $\binom{\mathrm{Id}}{z \leftrightarrow y_1} A \cap A$ contains $\binom{1}{1}$, so A contains $\binom{1}{z}$ for all such z, and A contains row 1. Let $\rho \in \mathrm{Sym}(E^{(1)})$ denote the 3-cycle mapping $3 \mapsto 2, 2 \mapsto 1, 1 \mapsto 3$. Since H is substantial, it contains a free element. Thus, by Part (*iii*) of Lemma 5.19, there is some $\tilde{\gamma} \in H$ such that

$$\tilde{\gamma}\colon \begin{cases} \mathrm{Id \ on} \ \binom{1}{1} \\ \binom{1}{2} \mapsto \binom{2}{1}. \end{cases}$$

Then, $\binom{\mathrm{Id}}{\rho^{-1}} \tilde{\gamma} \binom{\mathrm{Id}}{\rho} \in H$ and

$$\binom{\mathrm{Id}}{\rho^{-1}} \tilde{\gamma} \binom{\mathrm{Id}}{\rho}\colon \begin{cases} \mathrm{Id \ on} \ \binom{1}{2} \\ \binom{1}{3} \mapsto \binom{2}{2}. \end{cases}$$

Since A contains row 1, it contains $\binom{1}{2}$, so this implies that A contains $\binom{2}{2}$, completing the proof. ■

5.4.5 *Obtaining a p-cycle*

The main goal of this subsection is to prove the following lemma.

Lemma 5.24. Let $H \subset \mathrm{Sym}(E^{(2)})$ be a subgroup that contains P and is substantial. Then, H contains a p-cycle for some prime $p < |E^{(2)}| - 2$.

We start with some notation to aid in describing the arrangements. Define

$$R_{i,j} = \left\{ \binom{i}{y} : y \in E^{(1)}(\Gamma) \right\} \cup \left\{ \binom{j}{y} : y \in E^{(1)}(\Gamma) \right\} \tag{31}$$

and

$$C_{i,j} = \left\{ \binom{x}{i} : x \in E^{(1)}(\Gamma) \right\} \cup \left\{ \binom{x}{j} : x \in E^{(1)}(\Gamma) \right\}. \tag{32}$$

Thus, $R_{i,j}$ denotes the set of points in $E^{(2)}$ that belong to either row i or j, and $C_{i,j}$ denotes the set of points in $E^{(2)}$ that belong to either column i or j.

Given $1 \leq i,j \leq n$, let $\phi^C_{i,j}$ denote the involution in P swapping columns i and j, and let $\phi^R_{i,j}$ denote the involution in P swapping rows i and j. Given any $\phi_1, \phi_2 \in H_1$, we let $\phi_2^{\phi_1} = \phi_1^{-1}\phi_2\phi_1$, and for $\tau, \phi \in H_1$, define

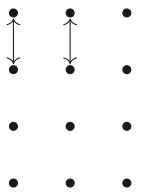
$$\tau \star \phi = \left(\tau^{\phi}\right)^{-1} \tau = \phi^{-1}\tau^{-1}\phi\tau.$$

(While $\tau \star \phi$ is usually denoted by $[\phi, \tau]$, we find the $\star$ notation to be more readable.)

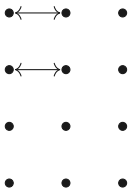
We frequently use the following observation: if c is a cycle whose support does not intersect $C_{i,j}$ (respectively, $R_{i,j}$), then $c \star \phi^C_{i,j} = \mathrm{Id}$ ($c \star \phi^R_{i,j} = \mathrm{Id}$, respectively).

Let us briefly outline the proof of Lemma 5.24. Suppose H is a substantial subgroup of $\mathrm{Sym}(E^{(2)})$, which contains P. To show H contains a p-cycle, we begin by letting γ_3 denote some element of H that acts by one of the arrangements in Definition 5.20; say Arrangement (a). Letting $\gamma_4 = \gamma_3 \star \phi^R_{1,2}$, by passing from γ_3 to this γ_4, any 2-cycles in γ_3 whose support were disjoint from rows one and two vanish. Moreover, the element γ_4 has a distinguished 3-cycle whose support consists of the points $\binom{1}{1}, \binom{2}{1}, \binom{3}{2}$, and we use this distinguished cycle to reduce to a collection of cases, which we then handle. The proof of this occupies the remainder of this section.

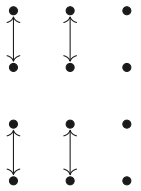
Lemma 5.25. Suppose H is a subgroup of $\mathrm{Sym}(E^{(2)})$ that contains P and any of the following arrangements.



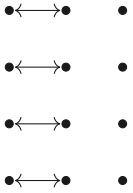
Arrangement (1)



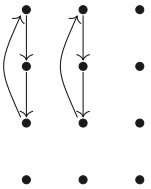
Arrangement (4)



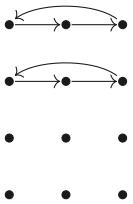
Arrangement (2)



Arrangement (5)



Arrangement (3)



Arrangement (6)

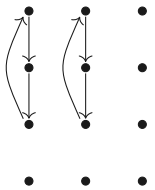
Then H contains a 3-cycle.

Proof. We prove the lemma for arrangements (1), (2), (3); the proofs for arrangements (4), (5), (6) are similar.

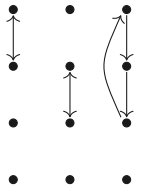
Suppose the arrangement (1) is implemented by the involution γ_3. Then,

$$\gamma_4 = \left(\gamma_3^{\phi_{2,3}^R}\right)\gamma_3$$

acts by the arrangement

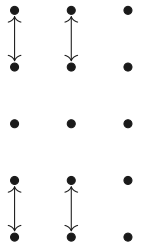


and $\gamma_3\gamma_4^{\phi^C_{1,3}}$ acts by the arrangement



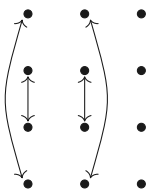
Squaring now produces a 3-cycle.

Suppose now the arrangement (2) is implemented by some γ_3. Then, $\gamma_4 = \gamma_3^{\phi^R_{3,5}}$ acts by the arrangement

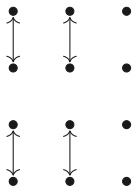


Setting $\gamma_5 = \left(\gamma_4^{\phi^R_{2,3}}\right)\gamma_4$, the element $\left(\gamma_4\gamma_5^{\phi^C_{1,3}}\right)^2$ consists of a single 3-cycle.

Suppose now the arrangement (3) is implemented by some γ_3. Then, $\gamma_4 = \left(\gamma_3^{\phi^R_{3,4}}\right)\gamma_3$ acts by the arrangement



and $\gamma_5 = \gamma_4^{\phi_{2,4}^R}$ acts by the arrangement



But this is exactly the arrangement in case (2), so the result follows for the same reason. ■

Lemma 5.26. Suppose H is a subgroup of $\mathrm{Sym}(E^{(2)})$ that contains P, and suppose H contains an involution τ_1 that satisfies the following:

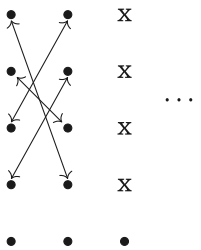
(i) τ_1 is supported in rows $1, 2, 3, 4$ and consists of an even number of 2-cycles d_i, $i = 1, \ldots, 2q$ for some $q \geq 1$;
(ii) each 2-cycle in τ_1 has support containing a point in $R_{1,2}$ and a point in $R_{3,4}$;
(iii) each 2-cycle in τ_1 has a companion 2-cycle, meaning that for each 2-cycle d_i, we have $d_{i+q \bmod 2q} = d_i^{\phi_{1,2}^R \phi_{3,4}^R}$;
(iv) τ_1 has a pair of 2-cycles d_1, d_{q+1} such that $d_1 = \left(\binom{1}{1}, \binom{4}{2}\right)$ and $d_{q+1} = \left(\binom{2}{1}, \binom{3}{2}\right)$.

Then, H contains a p-cycle for some prime $p < |E^{(2)}| - 2$.

Proof. We proceed by cases (recall that $C_{1,2}$ is defined in (32)).

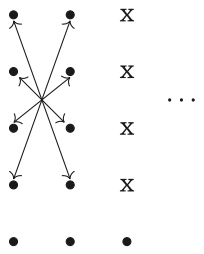
Case 1. Suppose τ_1 leaves $C_{1,2}$ invariant and acts nontrivially on $C_1 \cap R_{3,4}$ (and hence, given the setup, also nontrivially on $C_2 \cap R_{1,2}$). Then, one of the following two cases occurs.

Case 1a. Suppose τ_1 acts by the arrangement



on $C_{1,2}$. Then, $\tau_1 \star \phi_{1,2}^C$ acts by arrangement (2) of Lemma 5.25, and the result follows.

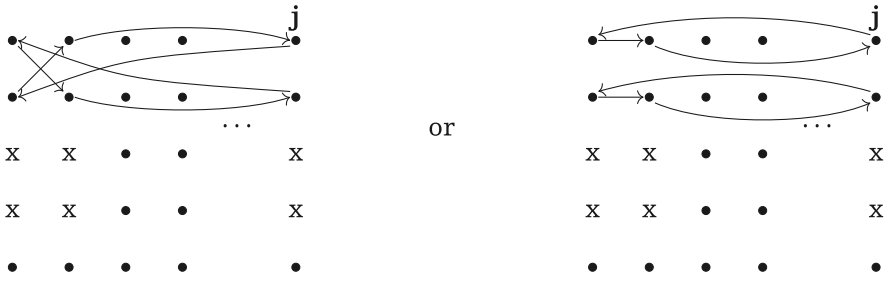
Case 1b: Suppose τ_1 acts by the arrangement



on $C_{1,2}$. We then split this into two further subcases.

Subcase 1b.1. Suppose that τ_1 leaves some column j invariant. If τ_1 acts by the identity on column j, we set $\tau_2 = \tau_1^{\phi^R_{2,4}}$ and $\tau_3 = \tau_2 \star \phi^C_{2,j}$. Then, setting $\tau_4 = \tau_3 \star \phi^R_{2,5}$, τ_4 consists of one 3-cycle and one 5-cycle. Thus, τ_4^3 consists of a single 5-cycle.

Suppose instead τ_1 acts nontrivially on column j. Let $\tau_2 = \tau_1 \star \phi^C_{2,j}$. Then, τ_2 acts by one of the following:

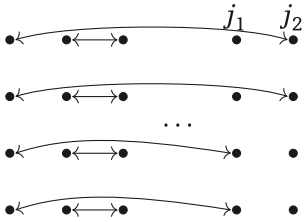


1b.1 (i) 1b.1 (ii)

In the 1st case, setting $\tau_3 = \tau_2 \star \phi^R_{2,5}$, we have that τ_3^3 consists of a single 5-cycle and the result follows. In the 2nd case, first let $\tau_3 = \tau_2 \star \phi^R_{2,5}$, then define $\tau_4 = \tau_3^{\phi^C_{j,3}}$, and $\tau_5 = \tau_4^{\phi^C_{3,4}}\tau_4$. Finally, letting $\tau_6 = \tau_5 \star \phi^R_{2,3}$, $\tau_7 = \tau_6^{\phi^C_{2,4}}$, and $\tau_8 = \tau_7^{\phi^R_{1,3}}$, then τ_8 acts by arrangement (5) in Lemma 5.25 and the result follows.

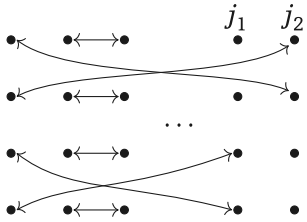
Subcase 1b.2. Suppose τ_1 leaves no column invariant. Then, we may assume that τ_1 maps points in column 3 into some columns j_1, j_2. We may assume at least one of j_1, j_2 is not equal to 3, since if not, we are in subcase 1b.1. Thus, without loss of generality, we can suppose that $j_1 \neq 3$.

Suppose first that $j_2 \neq 3$. Then, letting $\tau_2 = \tau_1 \star \phi^C_{2,3}$, τ_2 acts by one of the following arrangements:



1b.2 (i)

or

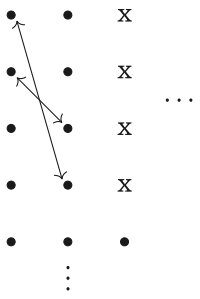


1b.2 (ii)

Note that while we have drawn these arrangements as if $j_1 \neq j_2$, we could also have $j_1 = j_2$ and the proof is the same. Thus, for arrangement 1b.2 (i), we set $\tau_3 = \tau_2 \star \phi^R_{1,5}$, and then $\tau_4 = \tau_3^{\phi^R_{2,5}}$, $\tau_5 = \tau_4^{\phi^C_{4,j_2}}$, $\tau_6 = \tau_5^{\phi^C_{1,3}}$, $\tau_7 = \tau_6 \star \phi^C_{2,5}$, and $\tau_8 = \tau_7^{\phi^C_{3,5}}$, τ_8 acts by arrangement (6) of Lemma 5.25. For the arrangement 1b.2 (ii), set $\tau_3 = \tau_2 \star \phi^R_{4,5}$ and then $\tau_4 = \tau_3^3$, $\tau_5 = \tau_4^{\phi^C_{1,3}}$, and $\tau_6 = \tau_5^{\phi^R_{1,4}\phi^R_{2,5}}$. Then, τ_6 acts by the arrangement (4) in Lemma 5.25.

Suppose instead that $j_2 = 3$. Then, τ_1 fixes two points in column 3. Set $\tau_2 = \tau_1 \star \phi^C_{2,3}$ and $\tau_3 = \tau_2^3$. Then, setting $\tau_4 = \tau_3 \star \left(\phi^R_{1,3}\phi^R_{2,4}\right)$, we have that τ_4 acts by one of the two arrangements 1b.2 (i) or 1b.2 (ii) above, and we proceed as when $j_2 \neq 3$.

Case 2. Suppose $C_{1,2}$ is invariant under τ_1 and τ_1 acts by the identity on $\binom{1}{2}, \binom{2}{2}, \binom{3}{1}, \binom{4}{1}$. Then, τ_1 acts by the arrangement

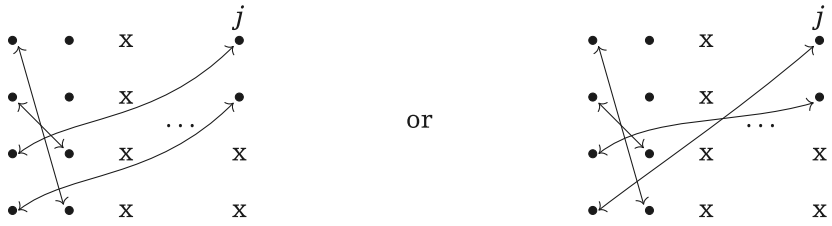


Setting $\tau_2 = \tau_1 \star \phi^C_{1,2}$, we have reduced to Case 1b, and the result follows.

Case 3. Suppose $C_{1,2}$ is not invariant under τ_1. Again, we split the analysis into cases.

Subcase 3a. Suppose τ_1 acts nontrivially on $\binom{4}{1}$, and hence also on $\binom{3}{1}$. Then, τ_1 maps $\binom{4}{1}$ into some column j, and by assumption, we must have $j \neq 1, 2$. It follows from the setup that τ_1 also maps $\binom{3}{1}$ into column j. We split the analysis into two subcases.

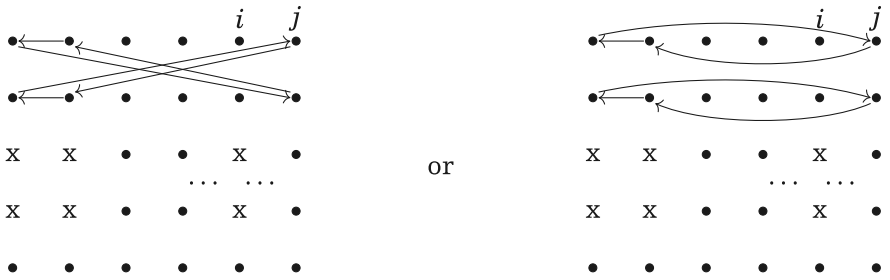
Subcase 3a.1. Suppose τ_1 fixes both $\binom{1}{2}$ and $\binom{2}{2}$, so τ_1 acts by one of the following arrangements:



or

In either case, setting $\tau_2 = \tau_1 \star \phi^C_{1,2}$ and $\tau_3 = \tau_2 \star \phi^R_{4,5}$, we have that τ_3 consists of a 7-cycle.

Subcase 3a2: Suppose τ_1 maps $\binom{1}{2}$ into column i where $i \neq 1, 2$ (it follows from the setup that τ_1 also maps $\binom{2}{2}$ into column i). Let $\tau_2 = \tau_1 \star \phi^C_{1,2}$. Then, τ_2 acts by one of the following arrangements:



or

For the 1st case, set $\tau_3 = \tau_2 \star \phi^R_{2,5}$. Then, $\tau_4 = \tau_3^3$ consists of a single 5-cycle. The 2nd case proceeds analogous to Subcase 1b.1, as illustrated in Figure 1b.1 (ii).

Subcase 3b. Suppose τ_1 fixes both $\binom{4}{1}$ and $\binom{3}{1}$. Then, by assumption, τ_1 maps $\binom{1}{2}$ and $\binom{2}{2}$ into some column $j \neq 1, 2$. Letting $\tau_2 = \tau_1^{\phi^C_{1,2}}$ and $\tau_3 = \tau_2^{\phi^R_{1,3}\phi^R_{2,4}}$, we are back in Subcase 3a.1. ■

We now prove Lemma 5.24.

Proof of Lemma 5.24. Since H is substantial, it satisfies both conditions (1) and (2) of Definition 5.20. Thus, H contains an involution implementing either arrangement (a) or (b) of Definition 5.20. First, we note that the subgroup H contains a p-cycle for some prime $p < |E^{(2)}| - 2$ if and only if the subgroup $\mathfrak{s}^{-1}H\mathfrak{s}$ does. Moreover, H contains an involution implementing arrangement (b) if and only if $\mathfrak{s}^{-1}H\mathfrak{s}$ contains an involution implementing arrangement (a). It follows that it suffices to consider the case that there

is an involution $\gamma_3 \in H$ implementing arrangement (a), and we call this arrangement $\mathcal{IC}$:

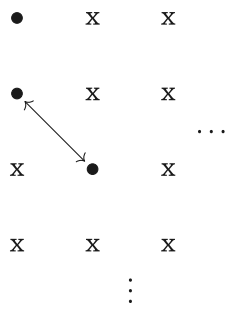
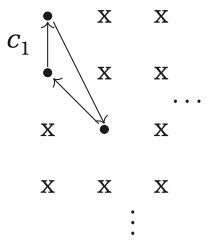


Fig. 1 Arrangement $\mathcal{IC}$

Set $\gamma_4 = \gamma_3 \star \phi^R_{1,2}$. Then, γ_4 acts by the arrangement



and we label the distinguished 3-cycle as c_1.

We claim that any cycle in γ_4 whose support does not intersect $R_{1,2}$ (see (31)) must be a 2-cycle. To see this, note that $\gamma_4^{\phi^R_{1,2}} = \gamma_3 \gamma_3^{\phi^R_{1,2}} = \gamma_4^{-1}$. If c is a cycle in γ_4 whose support does not intersect $R_{1,2}$, then $c^{\phi^R_{1,2}} = c$, and it follows that c is equal to its inverse, and hence order two, proving the claim.

Thus, we may choose a large $m_1 \in \mathbb{N}$ that is relatively prime to 3 such that $\gamma_5 = \gamma_4^{m_1}$ consists of cycles c_i, $i = 1, \ldots, L$, each cycle of length 3^{k_i} for some $k_i \geq 1$, and such that each of these c_i has support that intersects $R_{1,2}$. Note that $L \geq 1$ since γ_5 still contains the cycle c_1 (or its inverse). Define

$$\bar{I} = \{i \in \{1, \ldots, L\} : \text{the support of } c_i \text{is not contained in } R_{1,2}\}.$$

We adopt the following notation: if c is a cycle whose support intersects $E^{(2)} \setminus R_{1,2}$ in exactly one point, we denote this point by $\omega(c)$.

Observe that for each $i \in \bar{I}$, c_i has support with at most one point not in $R_{1,2}$ (since each c_i satisfies $c_i^{\phi_{1,2}^R} = c_i^{-1}$ and each cycle c_i is of odd length). Thus, for $i \in \bar{I}$, $\omega(c_i)$ is well defined. We also note that

$$\sum_{i \in \bar{I}} \left(|c_i| - 1\right) \leq 2n, \tag{33}$$

where $|c_i|$ denotes the length of a cycle c_i. In particular, in the case that all the c_is are 3-cycles, we have $|\bar{I}| \leq n$. We also have $1 \leq |\bar{I}|$ since $1 \in \bar{I}$ (the cycle c_1 has support not contained in $R_{1,2}$).

We now analyze the cases that arise.

Case 1. Suppose $k_i = 1$ for all $i \in \{1, \ldots, L\}$ (recall this means each cycle c_i has length 3^{k_i}). Thus, γ_5 consists of a collection of 3-cycles, and since we have the cycle c_1 in the arrangement, it follows that $1 \leq |\bar{I}| \leq n$. We split into two subcases.

Subcase 1a. Suppose there exists $j \geq 3$ such that γ_5 fixes $\binom{j}{2}$. Set $\gamma_6 = \left(\gamma_5^{\phi_{3,j}^R}\right)\gamma_5$. Then, γ_6 consists of cycles determined by the following.

(i) Let $i \in \bar{I}$ be an index such that, writing $\omega(c_i) = \binom{x_i}{y_i}$, either of the following occur:
   (a) $x_i = 3$ and $\binom{j}{y_i} = \omega(c_l)$ for some $l \in \bar{I}$;
   (b) $x_i = j$ and $\binom{3}{y_i} = \omega(c_l)$ for some $l \in \bar{I}$.
   Then, γ_6 contains a pair of 3-cycles supported in the union of the supports of c_i and c_l.

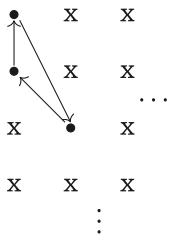
(ii) Let $i \in \bar{I}$ be an index such that, writing $\omega(c_i) = \binom{x_i}{y_i}$, either of the following occur:
   (a) $x_i = 3$ and γ_5 fixes $\binom{j}{y_i}$;
   (b) $x_i = j$ and γ_5 fixes $\binom{3}{y_i}$.
   Then, γ_6 contains a pair of 2-cycles whose support is contained in the set $(c_i \cap R_{1,2}) \cup \left\{\binom{3}{y_i}, \binom{j}{y_i}\right\}$.

Note that the index $1 \in \bar{I}$ falls into the 2nd case. Set $\gamma_7 = \gamma_6^3$ and set $\gamma_8 = \gamma_7^{\phi_{4,j}^R}$. Then, either γ_8 or $\gamma_8^{\phi_{1,2}^R}$ satisfies the hypotheses of Lemma 5.26, completing this case.

Subcase 1b. Suppose there is no $j \geq 3$ such that γ_5 fixes $\binom{j}{2}$. This means that for all $j \geq 3$, there exists some $i(j) \in \bar{I}$ such that the cycle $c_{i(j)}$ intersects column two, meaning that $\omega(c_{i(j)})$ lies in column two. Since $|\bar{I}| \leq n$, there exist at most two other cycles, call

them c_{ℓ_1}, c_{ℓ_2}, such that $\omega(c_{\ell_1})$ lies in some column L_1 and $\omega(c_{\ell_2})$ lies in some column L_2, with $L_1 \neq 2$ and $L_2 \neq 2$. The analysis of this splits into three subcases.

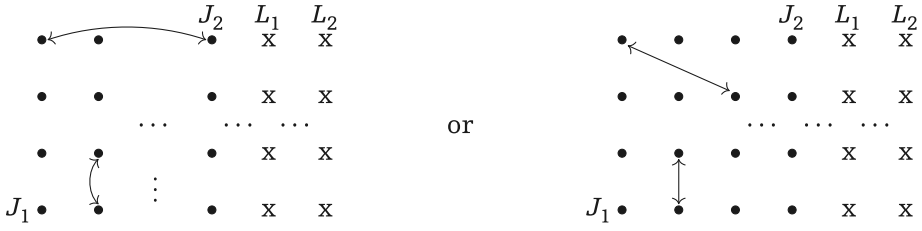
Subcase 1b.1. Suppose the support of c_{ℓ_1} is not contained entirely in column L_1, so the support of c_{ℓ_1} also intersects some column $L_3 \neq L_1$. By assumption, $\omega(c_{\ell_1})$ lies in column L_1, so we may write $\omega(c_{\ell_1}) = \binom{x_1}{L_1}$. Furthermore, it also follows from our assumptions that there must exist some $j \geq 3$ such that γ_5 fixes $\binom{j}{L_1}$. Setting $\gamma_6 = \gamma_5^{\phi^C_{L_3,1}}$, $\gamma_7 = \gamma_6^{\phi^R_{x_1,3}\phi^C_{L_1,2}}$, it follows that γ_7 acts by the arrangement



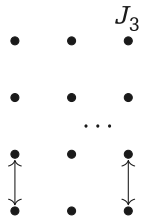
so γ_7 again consists of 3-cycles all of whose supports intersect $R_{1,2}$. Moreover, γ_7 has a distinguished 3-cycle which matches c_1 (or its inverse) and also acts by the identity on some $\binom{j}{2}$ for some $j \geq 3$, so we can apply Subcase 1a.

Subcase 1b.2: If the support of c_{ℓ_2} is not entirely contained in column L_2, the argument proceeds exactly as in Subcase 1b.1.

Subcase 1b.3: The remaining case is that the support of c_{ℓ_1} is entirely contained in L_1 and the support of c_{ℓ_2} is entirely contained in L_2 (note that if neither c_{ℓ_1} nor c_{ℓ_2} exist, their supports are viewed as empty, and so this scenario is covered by this subcase). There exists some cycle c_m such that $\omega(c_m) = \binom{J_1}{2}$ and the support of c_m intersects some column $J_2 \neq 2$. Set $\gamma_6 = \gamma_5 \star \phi^R_{3,J_1}$. Then, after conjugating by $\phi^R_{1,2}$ if necessary, γ_6 acts by one of the following:



In either case, there exists some column J_3 on which γ_6 acts by the identity, and setting $\gamma_7 = \gamma_6 \star \phi^C_{2,J_3}$, γ_7 acts by



We may then conjugate γ_7 to move this pair of 2-cycles into case (1) of Lemma 5.25.

Case 2. Suppose there exists a cycle c_i with $k_i \geq 2$ (recall this means the cycle c_i has length 3^{k_i} and note that this i may not be in $\bar{I}$). Let $k' = \max_i k_i$, let $I_1 \subset \{1, \ldots, L\}$ be the set of indices for which $k_i = k'$, and set $\gamma_6 = \gamma_5^{3^{k'-1}}$. Then, γ_6 is order 3 and contains $3^{k'-1}|I_1|$ 3-cycles d_i, each of whose support intersect $R_{1,2}$. We proceed by analyzing two subcases.

Subcase 2a. Suppose every d_i has support entirely contained in $R_{1,2}$. Note that we still have $\gamma_6^{\phi^R_{1,2}} = \gamma_6^{-1}$. As a result, any cycle $d_i = (z_1, z_2, z_3)$ in γ_6 has a companion cycle $d_{i'} = (z_3+1 \bmod 2, z_2+1 \bmod 2, z_1+1 \bmod 2)$ in γ_6. Moreover, for each cycle $d_i = (z_1, z_2, z_3)$ in γ_6, we must have z_1, z_2, and z_3 lying in distinct columns. We further note γ_6 acts by the identity on $\binom{1}{1}$, $\binom{2}{1}$. Among all the cycles d_i, there are two companion cycles, call them d_j and $d_{j'}$, whose supports intersect a column, say column J, which is furthest to the left. Thus, we have that $J < J'$ for any other column J' hit by cycles in the list d_i. Consider $\gamma_7 = \gamma_6^{\phi^C_{1,J}} \gamma_6$. Then, γ_7 consists of four 2-cycles, two of which intersect column one; call these e_1, e_2. Due to the structure of the companion cycles $d_j, d_{j'}$, it follows that e_1 and e_2 also intersect some distinct columns $J_1 < J_2$. Choose a column $J_3 \neq 1, J_1, J_2$, and set $\gamma_8 = \gamma_7 \star \phi^C_{1,J_3}$. Then, γ_8 consists of two 3-cycles, e_1', e_2', whose support columns consist of $1, J_1, J_3$ and $1, J_2, J_3$, respectively. Since n is large ($n \geq 7$), we may find yet another column $J_4 \neq 1, J_1, J_2, J_3$, and let $\gamma_9 = \gamma_8^{\phi^C_{J_1,J_4}} \gamma_8$. Then, γ_9 consists of two 2-cycles, whose supports intersect four distinct columns. Choosing again a new column J_5, we have $\gamma_9^{\phi^C_{J_4,J_5}} \gamma_9$ consists of only one 3-cycle, and we are done.

Subcase 2b. Suppose there exists a cycle d_i whose support is not contained in $R_{1,2}$. Then, $I_1 \cap \bar{I} \neq \emptyset$ and we can consider the nonempty set of indices

$$\bar{J} = \{ j \text{: the support of } d_j \text{ is not contained in } R_{1,2} \}.$$

Recall $\gamma_6 = \gamma_5^{3^{k'-1}}$ and that $2 \leq k' = \max_i k_i$. Since each cycle in γ_5 has at most one point not in $R_{1,2}$, each cycle of length $3^{k'}$ in γ_5 contributes one cycle of length 3 in γ_6 whose support is not contained in $R_{1,2}$. Thus, it follows that $|\overline{J}| = |I_1 \cap \overline{I}|$, and that, since the support of the cycles of length $3^{k'}$ in γ_5 have at least eight points in $R_{1,2}$, we must have

$$|\overline{J}| \leq \frac{n}{4}. \tag{34}$$

Thus, the collection $\{\omega(d_j) : j \in \overline{J}\}$ has at most $\frac{n}{4}$ points, and we may choose some $k \in \overline{J}$ such that, upon writing $\omega(d_k) = \begin{pmatrix} x_k \\ y_k \end{pmatrix}$, there exists some $3 \leq \ell \leq n$ such that γ_6 fixes the point $\begin{pmatrix} \ell \\ y_k \end{pmatrix}$. Consider

$$\gamma_7 = \gamma_6^{\phi^R_{x_k,\ell}} \gamma_6.$$

Then, γ_7 contains cycles determined by the following:

(i) a pair of 3-cycles corresponding to each (un-ordered) pair of indices $j_1, j_2 \in \overline{J}$ such that $\omega(d_{j_1}) \in R_{x_k}, \omega(d_{j_2}) \in R_\ell$, and $\omega(d_{j_1}), \omega(d_{j_2})$ lie in the same column;

(ii) a pair of 2-cycles corresponding to each index $j \in \overline{J}$ such that either $\begin{pmatrix} x_k \\ y_j \end{pmatrix} = \omega(d_j) \in R_{x_k}$ and γ_6 fixes $\begin{pmatrix} \ell \\ y_j \end{pmatrix}$, or $\begin{pmatrix} \ell \\ y_j \end{pmatrix} = \omega_{d_j} \in R_\ell$ and γ_6 fixes $\begin{pmatrix} x_k \\ y_j \end{pmatrix}$.

The 2-cycles that arise in case (ii) have support intersecting rows $1, 2, x_k, \ell$. Moreover, since $k \in \overline{J}$ satisfies case (ii), we have at least one pair of 2-cycles; suppose this pair has support contained in columns y_k, y_k' (note we could have $y_k = y_k'$). Setting $\gamma_8 = \gamma_7^3$, we have that γ_8 consists of only pairs of 2-cycles corresponding to each $j \in \overline{J}$ satisfying case (ii). Setting $\gamma_9 = \gamma_8^{\phi^R_{x_k,3}\phi^R_{\ell,4}}$, γ_9 is an involution satisfying the 1st three conditions of Lemma 5.26.

Now, by (34), there exists a column F_1 such that γ_9 acts by the identity on the column F_1. Suppose $y_k = y_k'$. Then, $\left(\gamma_9^{\phi^C_{y_k,F_1}}\right)^{-1} \gamma_9$ consists of two pairs of 2-cycles, supported in rows $1, 2, 3, 4,$; upon conjugating and moving these cycles if necessary, we can apply Lemma 5.25. If $y_k \neq y_k'$, then setting $\gamma_{10} = \gamma_9^{\phi^C_{1,y_k}\phi^C_{2,y_k'}}$, and if necessary, replacing γ_{10} with $\gamma_{11} = \gamma_{10}^{\phi^R_{1,2}}$, γ_{10} is an involution satisfying all four conditions of Lemma 5.26, and the result follows. ∎

We have now assembled all the ingredients to complete the proof of the technical lemma:

Proof of Lemma 5.15. Our goal is to show that at least one of

(i) $H_1 = \mathrm{Sym}(E^{(2)})$ and $H_2 = \mathrm{Sym}(E^{(2)})$ and
(ii) $H_1 = \mathrm{Alt}(E^{(2)})$ and $H_2 = \mathrm{Alt}(E^{(2)})$

holds. Since both N_1 and N_2 are trivial by assumption, and H_1 and H_2 are isomorphic by assumption, it suffices to show that at least one of H_1 or H_2 is either $\mathrm{Sym}(E^{(2)})$ or $\mathrm{Alt}(E^{(2)})$. By Jordan's theorem, it then suffices to show that at least one of H_1, H_2 is primitive and also contains a p-cycle for some prime $p < |E^{(2)}| - 2$. By Lemma 5.21, at least one of H_1 or H_2 is substantial. Since both H_1 and H_2 contain P, combining Lemmas 5.23 and 5.24 gives that at least one of H_1 or H_2 satisfies the hypotheses of Jordan's theorem and hence is either $\mathrm{Sym}(E^{(2)})$ or $\mathrm{Alt}(E^{(2)})$, as desired. ■

Acknowledgments

The authors gratefully thank Mike Boyle for helpful comments and the referees for suggesting numerous improvements.

Funding

This work was supported by the Israel Science Foundation [1175/18to Y.H.]; and the National Science Foundation [1800544to B.K., 1502643to S.S.].

References

[1] Adem, A. and N. Naffah. "On the Cohomology of $\mathrm{SL}_2(\mathbb{Z})\left[\frac{1}{p}\right]$." In *Geometry and Cohomology in Group Theorem (Durham 1994)*, vol. 252. London Mathematical Society Lecture Note Series. 1–9. Cambridge: Cambridge University Press, 1998.

[2] Boyle, M. "Eventual extensions of finite codes." *Proc. Amer. Math. Soc.* 104, no. 3 (1988): 965–72.

[3] Boyle, M. "Nasu's Simple Automorphisms." In *Dynamical Systems (College Park, MD, 1986–87)*, vol. 1342. Lecture Notes in Mathematics. 23–32.Berlin: Springer, 1988.

[4] Boyle, M. and U. Fiebig. "The action of inert finite-order automorphisms on finite subsystems of the shift." *Ergodic Theory Dynam. Systems* 11, no. 3 (1991): 413–25.

[5] Boyle, M. and W. Krieger. "Periodic points and automorphisms of the shift." *Trans. Amer. Math. Soc.* 302, no. 1 (1987): 125–49.

[6] Boyle, M., D. Lind, and D. Rudolph. "The automorphism group of a shift of finite type." *Trans. Amer. Math. Soc.* 306, no. 1 (1988): 71–114.

[7] Boyle, M., B. Marcus, and P. Trow. "Resolving maps and the dimension group for shifts of finite type." *Mem. Amer. Math. Soc.* 70 (1987): 377.

[8] Cyr, V. and B. Kra. "The automorphism group of a shift of linear growth: beyond transitivity." *Forum Math. Sigma* 3 (2015): 27.

[9] Cyr, V. and B. Kra. "The automorphism group of a minimal shift of stretched exponential growth." *J. Mod. Dyn.* 10 (2016): 483–95.

[10] Donoso, S., F. Durand, A. Maass, and S. Petite. "On automorphism groups of low complexity subshifts." *Ergodic Theory Dynam. Systems* 36, no. 1 (2016): 64–95.

[11] Hedlund, G. A. "Endomorphisms and automorphisms of the shift dynamical system." *Math. Systems Theory* 3 (1969): 320–75.

[12] Hochman, M. "On the automorphism groups of multidimensional shifts of finite type." *Ergodic Theory Dynam. Systems* 30, no. 3 (2010): 809–40.

[13] Isaacs, I. M. and T. Zieschang. "Generating symmetric groups." *Amer. Math. Monthly* 102, no. 8 (1995): 734–9.

[14] Kim, K. H. and F. W. Roush. "Some results on decidability of shift equivalence." *J. Comb. Inf. Syst. Sci.* 4 (1979): 123–46.

[15] Kim, K. H. and F. W. Roush. "Decidability of Shift Equivalence." In *Proceedings of Maryland Special Year in Dynamics 1986–87*, vol. 1342. Lecture Notes in Mathematics. 374–424. Springer, 1988.

[16] Kim, K. H. and F. W. Roush. "On the automorphism groups of subshifts." *Pure Math. Appl. Ser. B* 1, no. 4 (1990): 203–30.

[17] Kim, K. H. and F. W. Roush. "Solution of two conjectures in symbolic dynamics." *Proc. Amer. Math. Soc.* 112, no. 4 (1991): 1163–8.

[18] Kim, K. H., F. W. Roush, and J. B. Wagoner. "Automorphisms of the dimension group and gyration numbers." *J. Amer. Math. Soc.* 5, no. 1 (1992): 191–212.

[19] Kim, K. H., F. W. Roush, and J. B. Wagoner. "Characterization of inert actions on periodic points I." *Forum Math.* 12, no. 5 (2000): 565–602.

[20] Kim, K. H., F. W. Roush, and J. B. Wagoner. "Characterization of inert actions on periodic points II." *Forum Math.* 12, no. 6 (2000): 671–712.

[21] Krieger, W. "On a dimension for a class of homeomorphism groups." *Math. Ann.* 252 (1980): 87–95.

[22] Krieger, W. "On dimension functions and topological Markov chains." *Invent. Math.* 56, no. 3 (1980): 239–50.

[23] Lang, S. *Algebra*, vol. 211, 3rd ed. Graduate Texts in Mathematics. New York: Springer, 2002.

[24] Lind, D. A. "The entropies of topological Markov shifts and a related class of algebraic integers." *Ergodic Theory Dynam. Systems* 4, no. 2 (1984): 283–300.

[25] Lind, D. and B. Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge: Cambridge University Press, 1995.

[26] Matui, H. "Some remarks on topological full groups of Cantor minimal systems." *Internat. J. Math.* 17, no. 2 (2006): 231–51.

[27] Matui, H. "Topological full groups of one-sided shifts of finite type." *J. Reine Angew. Math.* 705 (2015): 35–84.

[28] Nasu, M. "Topological Conjugacy for Sofic Systems and Extensions of Automorphisms of Finite Subsystems of Topological Markov Shifts." In *Dynamical Systems (College Park, MD, 1986–87)*, vol. 1342. Lecture Notes in Mathematics. 564–607. Berlin: Springer, 1988.

[29] Nekrashevych, V. "Simple groups of dynamical origin." *Ergodic Theory Dynam. Systems* 39, no. 3 (2019): 707–32.

[30] Olli, J. "Endomorphisms of Sturmian systems and the discrete chair substitution tiling system." *Discrete Contin. Dyn. Syst.* 33 (2013): 4173–86.

[31] Pytheas Fogg, N. *Substitutions in Dynamics, Arithmetics and Combinatorics*, vol. 1794, edited by V. Berthé, S. Ferenczi, C. Mauduit, and A. Siegel. Lecture Notes in Mathematics. Berlin: Springer, 2002.

[32] Ryan, J. P. "The shift and commutativity." *Math. Systems Theory* 6 (1972): 82–5.

[33] Ryan, J. P. "The shift and commutivity II." *Math. Systems Theory* 8, no. 3 (1974/75): 249–50.

[34] Schmieding, S. "Local $\mathcal{P}$ Entropy and Stabilized Automorphism Groups of Subshifts." (forthcoming) arXiv:2007.02183.

[35] Serre, J. P. "Le problème des groupes de congruence pour SL2." *Ann. of Math. (2)* 92 (1970): 489–527.

[36] Wagoner, J. B. "Eventual finite order generation for the kernel of the dimension group representation." *Trans. Amer. Math. Soc.* 317, no. 1 (1990): 331–50.

[37] Wielandt, H. *Finite Permutation Groups*. Translated from the German by R. Bercov. New York–London: Academic Press, 1964.

[38] Whitehead, J. H. C. "Simple homotopy types." *Amer. J. Math.* 72 (1950): 1–57.

[39] Williams, R. F. "Classification of subshifts of finite type." *Ann. of Math.* 98, no. 2 (1973): 120–53; *errata*, *ibid.* 99, no. 2 (1974), 380–81.