

Transitive action on finite points of a full shift and a finitary Ryan's theorem

Ville Salo

September 28, 2017

Abstract

We show that on the four-symbol full shift, there is a finitely generated subgroup of the automorphism group whose action is (set-theoretically) transitive of all orders on the points of finite support, up to the necessary caveats due to shift-commutation. As a corollary, we obtain that there is a finite set of automorphisms whose centralizer is \mathbb{Z} (the shift group), giving a finitary version of Ryan's theorem (on the four-symbol full shift), suggesting an automorphism group invariant for mixing SFTs. We show that any such set of automorphisms must generate an infinite group, and also show that there is also a group with this transitivity property which is a subgroup of the commutator subgroup and whose elements can be written as compositions of involutions. We ask many related questions and prove some easy transitivity results for the group of reversible Turing machines, topological full groups and Thompson's V .

1 Introduction

When Σ is a finite set, $\Sigma^{\mathbb{Z}}$ is homeomorphic to the Cantor set and under the self-homeomorphism $\sigma(x)_i = x_{i+1}$ becomes a dynamical \mathbb{Z} -system called the *full shift*. Our main result is about the full shift with $\Sigma = \{0, 1, 2, 3\}$, but the motivation comes from the more general setting of sofic shifts and more specifically *mixing SFTs*, which are the topologically mixing subsystems of full shifts defined by a finite set of forbidden patterns [30]. The *automorphism group* of a subshift X is the set of homeomorphisms $f : X \rightarrow X$ that commute with σ . It is indeed a group under function composition, and it acts on X in the obvious way.

Forgetting the action of the automorphism group of a mixing SFT,¹ it becomes an interesting abstract group [19, 9, 25]. Many group-theoretic questions about it are undecidable [25, 24, 40]. Ryan's theorem [38] states that the center of this group is as small as it possibly could be, namely the group of shifts $\langle \sigma \rangle$.

¹Mixing SFTs do not all have isomorphic automorphism groups, but the singular ‘group’ refers to a typical example; these groups are qualitatively similar in many key aspects.

More generally, in [18] it is shown that normal amenable subgroups consist of shift maps.

The finitely generated subgroups of an infinitely generated group are in many respects the essence of the group.² Much is known about the set of finitely generated subgroups of $\text{Aut}(X)$ for mixing SFTs X as abstract groups: It is closed under subgroups, (countable) free and direct products [40] and extensions by finite groups [25] and contains the right-angled Artin groups (also known as ‘graph groups’) [25, 13].³ On the side of limitations, we know that all groups it contains are residually finite, and finitely generated subgroups have a decidable word problem [9].

The group has been studied also through its action. Some of the most important developments have been on the dimension representation and the action on finite subsystems of $\Sigma^{\mathbb{Z}}$. See [9, 8, 26, 27, 7]. It is also known that the action is ‘as topologically transitive as possible’, in the sense that every aperiodic point has dense orbit [9]. See also [30] for a discussion of this group.

Actions of individual automorphisms (as \mathbb{Z} -actions) have been studied quite a bit, and in particular their expansivity is a very interesting topic [35, 6, 36]. Many results about possible dynamics and undecidability results are known for these actions, and are often proved under the name reversible cellular automata [22, 24, 32].

2 The results

In this article, we begin the study of actions of finitely generated (noncommutative) subgroups of $\text{Aut}(X)$. We construct a particular finitely generated subgroup of $\text{Aut}(X)$ for a particular mixing SFT X with an interesting action, namely we find an action of a finitely generated group G on $\{0, 1, 2, 3\}^{\mathbb{Z}}$ by automorphisms, which is as transitive as possible on the *nonzero finite points*, that is, points having finite and nonempty support. More precisely, for any k and every pair of k -tuples (x_1, \dots, x_k) and (y_1, \dots, y_k) of nonzero points of finite support, there is an element $f \in G$ such that $(y_1, \dots, y_k) = (f(x_1), \dots, f(x_k))$, assuming that x_i and x_j (resp. y_i and y_j) come from different (shift) orbits when $i \neq j$. In the terminology of the following section, this amounts to the following:

Theorem 2.1. *For $\Sigma = \{0, 1, 2, 3\}$ there is a finitely generated subgroup of $\text{Aut}(\Sigma^{\mathbb{Z}})$ that acts ∞ -orbit-transitively on the set of nonzero finite points.*

We prove this in Theorem 6.6. The finite points are a natural set to study,

²In group theory, properties are called local if they are determined by finitely-generated subgroups. Many properties of interest are local, for example amenability, residual finiteness and soficness.

³Note that the closure properties alone imply that all f.g. abelian groups and all f.g. nonabelian free groups are subgroups: since the trivial group is a subgroup, using finite group extensions, we get all finite groups. With free products, we then get \mathbb{Z} , from which we get all f.g. abelian and free groups using direct and free products, respectively.

since they are preserved by the automorphism group⁴ and form a countable set.

Our proof is explicit in the sense that we give a finite list of automorphisms, and show how to turn a tuple of nonzero finite points into another one by a finite composition of them. Proving this is equivalent to proving that we can perform any permutation of any finite set of nonzero finite points from different orbits. Thus it is also equivalent to the fact that given any set of nonzero finite points from different orbits, we can transpose two of them without changing the others. (These observations are not used in the proof of the main result, but see Lemma 7.12 for a proof.)

An interesting corollary of this theorem is the following stronger version of Ryan's theorem [38] (on the four-symbol full shift):

Theorem 2.2. *For $\Sigma = \{0, 1, 2, 3\}$ there is a finite set $F \subset \text{Aut}(\Sigma^{\mathbb{Z}})$ such that for $g \in \text{Aut}(\Sigma^{\mathbb{Z}})$, we have $g \in \langle \sigma \rangle$ if and only if $\forall f \in F : f \circ g = g \circ f$.*

Without further ado, let us prove this using Theorem 2.1.

Proof. Let F be the set of generators of the group in Theorem 2.1 together with all the cellwise symbol-permutations. If g is not a shift, then if $g(0^{\mathbb{Z}}) \neq 0^{\mathbb{Z}}$, g does not commute with some symbol-permutation. Otherwise, there is a nonzero finite point $x \in \{0, 1, 2, 3\}^{\mathbb{Z}}$ such that $g(x)$ is not in the shift orbit of x by Lemma 7.5. Then there exists $f \in \langle F \rangle$ mapping $(x, g(x))$ to $(\sigma(x), g(x))$ by 2-orbit-transitivity. Then $g(f(x)) = \sigma(g(x)) \neq g(x) = f(g(x))$. Since g does not commute with f , it cannot commute with all maps in F . \square

We also prove the following stronger version of Theorem 2.1. This is shown in Theorem 7.15.

Theorem 2.3. *For $\Sigma = \{0, 1, 2, 3\}$ there is a finite set F such that $\langle F \rangle$ acts ∞ -orbit-transitively on the set of nonzero finite points $x \in \Sigma^{\mathbb{Z}}$, and each element of F is a commutator of two automorphisms, and a composition of involutive (= order two) automorphisms.*

We also prove a version of Ryan's theorem for such a set, see Theorem 7.16.

While F is finite in the statement of the theorem, the group $\langle F \rangle$ is infinite. This is necessary by the following result, whose proof we give in Theorem 7.2.

Theorem 2.4. *Let G be any finite group of automorphisms on a mixing SFT X , and Γ any finite alphabet. Then there is an embedding $\phi : \text{Aut}(\Gamma^{\mathbb{Z}}) \rightarrow \text{Aut}(X)$ such that $\phi(f)$ commutes with g for all $f \in \text{Aut}(\Gamma^{\mathbb{Z}})$ and $g \in G$.*

In the context of finite permutation groups, it is known that the only faithful k -transitive actions for $k \geq 6$ are those of symmetric groups and alternating groups [16, Section 7.3]. The proof is a case analysis based on the classification of finite simple groups. For infinite groups, high-order transitivity is presumably quite common. We give two examples of ∞ -transitivity in other contexts that have a symbolic dynamical interpretation:

⁴More precisely, the finite-index subgroup of the automorphism group that stabilizes the point $0^{\mathbb{Z}}$ – or alternatively the automorphism group of the corresponding 0-pointed subshift.

Example 2.5. Thompson's V is defined by its action on the interval. This action is well-defined on the countable set of dyadic rationals, and on this set the action is ∞ -transitive.

Example 2.6. The topological full group of a minimal subshift is defined by its action on the subshift. This action is well-defined on the (countable) shift-orbit of every point. There is a finitely generated subgroup of this group, namely its commutator subgroup, that is ∞ -transitive on every shift-orbit.

See Section 7 for the (easy) proofs, and [11] for a reference for Thompson's V . As an auxiliary result, in Lemma 5.4 we also prove that a certain natural group of homeomorphisms on the full shift $A^{\mathbb{Z}}$ called G_0 , which corresponds to the reversible one-state oblivious Turing machines of [1], acts ∞ -transitively on finite points.

3 Questions

A result similar to Theorem 2.2 is known for the endomorphism monoid of a full shift [43], elaborated on in [39, page 151], namely that there is a finite set of endomorphisms of any full shift $\Sigma^{\mathbb{Z}}$ with $|\Sigma| \geq 3$ whose common centralizer consists of the shift maps.⁵ Note that on any mixing SFT, the set $F \subset \text{Aut}(\Sigma^{\mathbb{Z}})$ in Theorem 2.2 must be of size at least 2 and that the minimal cardinality of such F is an isomorphism invariant for $\text{Aut}(X)$, implying that computing it could theoretically separate $\text{Aut}(X)$ and $\text{Aut}(Y)$ for some non-flip-conjugate mixing SFTs X, Y without roots (which is an open problem [7]).

Definition 3.1. For a subshift X , let $k(X) \in \mathbb{N} \cup \{\infty, \perp\}$ be the minimal cardinality of a set F such that for $g \in \text{Aut}(\Sigma^{\mathbb{Z}})$, we have $g \in \langle \sigma \rangle$ if and only if $\forall f \in F : f \circ g = g \circ f$, if such a set exists, and $k(X) = \perp$ otherwise.

Our result implies that $k(\{0, 1, 2, 3\}^{\mathbb{Z}}) \in \mathbb{N}$. See Section 7 for a discussion of this invariant and related questions.

In particular with this application in mind, it is interesting to ask how small we can make the subgroup of $\text{Aut}(\Sigma^{\mathbb{Z}})$ in the proof of Theorem 2.1. The one in our proof has a reasonable⁶ number of generators, but presumably more than are needed.

Question 3.2. *In Theorem 2.1, how many generators do we need? Can we pick the finitely generated subgroup to have only two generators?*

One automorphism is not enough, and more generally abelian actions cannot be ∞ -orbit-transitive (see Proposition 7.1). In fact, no individual automorphism is even transitive on nonzero finite points,⁷ but we cannot show that one cannot be transitive on the set of orbits of nonzero finite points.

⁵In [39], it is shown that a set of size $|\Sigma|$ suffices to get a trivial centralizer, but a trivial modification of the proof gives an upper bound of 3.

⁶At most eight, see Section 7.

⁷If $f^p(x) = \sigma(x)$ for some p , then $\{f^n(x) \mid n \in \mathbb{Z}\}$ intersects finitely many σ -orbits.

Question 3.3. Does there exist an infinite pointed mixing SFT X and $f \in \text{Aut}(X)$ such that $\langle \sigma, f \rangle$ acts (set-theoretically) transitively on the set of nonzero finite points?

A transitive action of $\langle \sigma, f \rangle$ on nonzero finite points would look rather interesting. It would necessarily have to be free, and would give every nonzero finite point y a unique coordinate $(m, n) \in \mathbb{Z}^2$ by $y = \sigma^m \circ f^n(\dots 000w000\dots)$, where $\dots 000w000\dots \in X$ is chosen arbitrarily.

In this context, we should mention the closely related result of Kari that, up to shifting, automorphisms can be *topologically* transitive on the set of nonzero finite points:

Theorem 3.4 ([23]). Let $\Sigma = \{0, 1, 2, 3, 4, 5\}$. Then there exists $f \in \text{Aut}(\Sigma^\mathbb{Z})$ such that $\langle \sigma, f \rangle$ acts topologically transitively on the set of nonzero finite points.

Just like our proof requires the alphabet size to be composite, 6 here comes from the fact that it is the smallest product of distinct primes, and the result seems to be open for the binary full shift and non-full mixing SFTs.

Theorem 3.4 says in particular that a \mathbb{Z}^2 -action by automorphisms can be topologically transitive on the set of nonzero finite points. It is an open question whether the \mathbb{Z} -action given by an individual automorphism can do the same. We ask the question more generally for pointed mixing SFTs.

Question 3.5 ([23]). Does there exist an infinite pointed mixing SFT X and $f \in \text{Aut}(X)$ such that $\langle f \rangle$ acts topologically transitively on the set of nonzero finite points?

Often results about finite points are really results about pairwise asymptotic points in disguise (or the other way around). We note that Theorem 2.1 is not equivalent to being able to perform an arbitrary permutation on a set of points all (left and right) asymptotic to a given point; in fact even the full automorphism group cannot have this property since if (x_1, \dots, x_k) are all asymptotic to a point whose forward orbit is dense, then any nontrivial permutation of the points will necessarily change the tails. Of course one can ask whether we could take any set of mutually asymptotic points and have transitivity up to this ‘obvious’ restriction:

Question 3.6. Let X be a mixing SFT. Is there a finitely generated subgroup $G \leq \text{Aut}(X)$ such that if (x_1, \dots, x_k) are pairwise asymptotic and each x_i contains a word w_i that occurs only once in x_i and does not occur in x_j for $j \neq i$, every permutation of the x_i can be performed by the G -action?

Our construction fails to prove this result for at least two reasons. First, we use the fact that the four-symbol full shift is decomposable into a Cartesian product in a nontrivial way, as we use this in the proof for introducing Turing machine heads. Some⁸ mixing SFTs, in particular the two-symbol full shift,

⁸I would like to say ‘most’, but there are many concrete ways to sample SFTs at random (see in particular [34]), and I do not know how uniformly the number-theoretic properties of entropies (such as primality of the corresponding Perron numbers) distribute.

do not have this property [29, 10]. Another difficulty is that in the proof that the action of the group G_0 is transitive on finite points (see Definition 5.3 and Lemma 5.4), we use the fact that the full shift is closed under permutations of cells – a property that characterizes full shifts among transitive subshifts. It seems likely that these difficulties can be addressed with careful application of marker methods.

A more natural way to prove Theorem 2.1 would be to find a natural subgroup of $\text{Aut}(X)$ (in terms of the action or properties as a subgroup), and separately show finitely-generatedness and the transitivity property as theorems. To the best of our knowledge, the commutator subgroup could be a candidate for this. It is not difficult to show that the commutator subgroup satisfies the statement of Theorem 2.1, and we show this in Theorem 7.14. However, we do not know if it is finitely generated.

Question 3.7. *For which mixing SFTs X is the commutator subgroup of $\text{Aut}(X)$ finitely generated?*

4 Definitions and conventions

Our convention is $0 \in \mathbb{N}$. We do not need real intervals, so by $[a, b]$ we mean the discrete interval $[a, b] \cap \mathbb{Z}$. Positions in words are indexed starting from 0.

A *word* is a (possibly empty) list of symbols over a finite set, or *alphabet* Σ . Formally, we think of words as elements of the free monoid Σ^* generated by Σ , with concatenation as the monoid operation. Elements of $\Sigma^{\mathbb{Z}}$ (functions from \mathbb{Z} to Σ) are called *configurations* or *points* and for $x \in \Sigma^{\mathbb{Z}}$ and $i \in \mathbb{Z}$ we write x_i instead of $x(i)$. For $a, b \in \mathbb{Z}$ we write $x_{[a, b]}$ for the subword $x_a x_{a+1} \cdots x_b$ of x . A point $x \in \Sigma^{\mathbb{Z}}$ is sometimes denoted as $y.z$ where $y \in \Sigma^{(-\infty, -1]}$ and $z \in \Sigma^{\mathbb{N}}$, and $x_i = y_i$ and $x_i = z_i$ on the respective domains. If $a \in \Sigma$ and $w \in \Sigma^*$, we write $|w|_a = |\{i \mid w_i = a\}|$.

All groups in this paper are countable discrete groups, unless otherwise mentioned. If G is a group, a *G-set* is a set X equipped with a (left) action of G by bijections. A *G-set* where all $g \in G$ act by continuous maps is a (*dynamical*) *G-system*.

Definition 4.1. Let X be any topologically closed subset of $\Sigma^{\mathbb{Z}}$ in the product topology, where Σ is finite, such that $\sigma(X) = X$ where σ is the *shift* defined by $\sigma(x)_i = x_{i+1}$ for all $i \in \mathbb{Z}$. Then X is called a *subshift*, and the homeomorphism σ makes it a \mathbb{Z} -system. If a homeomorphism $f : X \rightarrow X$ commutes with σ , we call it an *automorphism* of X . We write $\text{Aut}(X)$ for the automorphism group of a subshift X . A *pointed subshift* is a pair (X, x) where $x = a^{\mathbb{Z}} \in X$ for some $a \in \Sigma$. Then a is called the *zero (symbol)* and x the *zero (point)*. Automorphisms of pointed subshifts are the automorphisms of the underlying subshift that additionally preserve the zero point.

Our zero a will be 0 in text and \square in figures.

Definition 4.2. Let $0 \in \Sigma$ and let $X \subset \Sigma^{\mathbb{Z}}$ be a pointed subshift with zero $0^{\mathbb{Z}}$. A point $x \in X$ is called *finite*⁹ if the support $\{i \mid x_i \neq 0\}$ is a finite set. Write $X_0 = \{x \in X \mid x \text{ is finite and } x \neq 0^{\mathbb{Z}}\}$ for the set of nonzero finite points and $X'_0 = X_0 \cup \{0^{\mathbb{Z}}\}$ for all finite points.

We now define our notions of transitivity for Theorem 2.1.

If H is a group, X is an H -set and $Z \subset X$, then write

$$Z^{(k)} = \{(z_1, \dots, z_k) \in Z^k \mid z_i \in Hz_j \implies i = j\}.$$

Thus $Z^{(k)}$ is the k th Cartesian power of Z with the additional restriction that coordinates should be from different H -orbits (and H and its action are clear from context).

Definition 4.3. Let X be an H -set, and let G act on X by H -commuting maps and $Z \subset X$. We say the action of G is *transitive around* Z if $\forall y, z \in Z : y \in Gz$. We say G *k -orbit-transitive around* Z if the diagonal action of G on $Z^{(k)}$ is transitive around $Z^{(k)}$. If the action of G is k -orbit-transitive (around a set) for all k , then we say it is *∞ -orbit-transitive* (around that set).

Note that when we say G is *transitive around* Z we do not necessarily imply that G has a well-defined action on Z , but on some $X \supset Z$. This is a technical notion that is useful for stating the intermediate steps of the proof – our main result will be about the usual kind of (set-theoretic) transitivity: G acts *transitively on* Z if $GZ \subset Z$ and G acts transitively around Z .

In our application, X is the subshift, the group H is the \mathbb{Z} -action of σ , and G the finitely generated subgroup of the automorphism group. For $x \in \Sigma^{\mathbb{Z}}$, write the σ -orbit of x as $\mathcal{O}(x) = \{\sigma^n(x) \mid n \in \mathbb{Z}\}$ instead of $\mathbb{Z}x$. For a set of points Y , write $\mathcal{O}(Y) = \bigcup_{y \in Y} \mathcal{O}(y)$.

In the proofs, we deal with many subgroups of $\text{Aut}(X)$, and for F_1, F_2, \dots, F_ℓ individual automorphisms or sets of them, we write $\langle F_1, \dots, F_\ell \rangle$ for the smallest subgroup of $\text{Aut}(X)$ containing all automorphisms in the list, or in the sets F_i . We do not need presentations, so we use the following non-standard ‘group-builder notation’ when F is a set of elements of a group and P is a property of elements of that group:

$$\langle a \mid a \in F, P(a) \rangle = \langle \{a \mid a \in F, P(a)\} \rangle$$

instead of the usual meaning of $\langle A \mid R \rangle$ where R is a set of relations. This should cause no confusion.

⁹Such points are examples of the *homoclinic* points in continuous dynamics. The term ‘homoclinic’ is used as a synonym of our ‘finite’ in for example [31] in the context of subshifts with algebraic structure, but it can also mean a point of the form $\dots u u u u u u \dots$ where u is a word of not necessarily unit length. The term ‘finite point’ is commonly used in the theory of cellular automata.

5 The generators and transitivity results

In this section, we define the finite set of automorphisms generating the group \mathcal{G} acting ∞ -orbit-transitively in Theorem 2.1. We also prove some auxiliary transitivity results. Namely, we prove that the automorphism group of a full shift is transitive around certain marked configurations, and we also define the ‘reset system’, a transitive monoid action used in the proof of the main theorem.

Most of the hard work in the main proof is performed by the action of the group \mathcal{G}_s , which is constructed in several steps in the subsections below but we will also need the following simpler transformations:

Definition 5.1. Let A, B be finite alphabets. The (A, B) -particle rule is the automorphism P of $(A \times B)^\mathbb{Z}$ defined by $P(x, y) = (\sigma(x), y)$. A symbol-permutation is an automorphism $g_\pi : \Sigma^\mathbb{Z} \rightarrow \Sigma^\mathbb{Z}$ defined by a permutation $\pi : \Sigma \rightarrow \Sigma$ by $g_\pi(x)_i = \pi(x_i)$.

5.1 ‘Gates and Turing machines’

The idea of transitivity around marked configurations, which we will prove in the next section, comes from [1], where it was (implicitly) shown that there is a finitely generated subgroup of the group of reversible (generalized) Turing machines which acts ∞ -transitively around configurations where the head of the machine is at the origin. This is further based on the study of ‘reversible clones’ [3, 2] or equivalently ‘monoidal groupoids’ [28, 44] of bijections on A^* , where A is a finite alphabet.

We assume no familiarity with these notions, and to keep terminology to a minimum, in this section we only deduce the necessary facts, based on the following lemma, which is a direct corollary of [3, Theorem 20]:

Lemma 5.2. *Let A be any finite alphabet. Then there exists n such that for all even permutations $\pi : A^m \rightarrow A^m$ with $m \geq n$, we have $\pi = \alpha_1 \circ \alpha_2 \circ \dots \circ \alpha_\ell$ where for all $i \in \mathbb{N}$, $\alpha_i : A^m \rightarrow A^m$ and there exists $k_i \in [0, m - n]$ and an even permutation $\beta_i : A^n \rightarrow A^n$ such that*

$$\alpha_i(uvw) = u \cdot \beta_i(v) \cdot w$$

for all $u \in A^{k_i}, v \in A^n, w \in A^{m-k_i-n}$.

In [3, Theorem 20], this is proved with $n = 4$. In the case when $|A|$ is odd, $n = 2$ suffices [2, 44].

Definition 5.3. Let $N \subset \mathbb{Z}$ be finite. If $\pi : A^N \rightarrow A^N$ is a permutation, then the homeomorphism $P_\pi : A^\mathbb{Z} \rightarrow A^\mathbb{Z}$ defined by

$$P_\pi(x)_i = \begin{cases} x_i & \text{if } i \notin N \\ \pi(x_N)_i & \text{otherwise.} \end{cases}$$

is called a *local permutation* with *neighborhood* N . Define

$$G''_0 = \langle P_\pi \mid \exists \text{ finite } N \subset \mathbb{Z} : \pi : A^N \rightarrow A^N \text{ is an even permutation} \rangle,$$

$$G'_0 = \langle P_\pi \mid \exists \text{ finite } N \subset \mathbb{Z} : \pi : A^N \rightarrow A^N \text{ is a permutation} \rangle,$$

$$G_0 = \langle \sigma, g \mid g \in G'_0 \rangle.$$

Thus by G_0 we denote group of self-homeomorphisms of $A^\mathbb{Z}$ generated by σ and the local permutations (of all finite neighborhoods).

Note that $G''_0 = G'_0$ when $|A|$ is even, since every permutation becomes even when its neighborhood is increased. On the other hand, when $|A|$ is odd, one can consistently assign a parity to each $g \in G'_0$, and we obtain $[G'_0 : G''_0] = 2$. Every element of G_0 is clearly of the form $\sigma^\ell \circ g$ where $g \in G'_0$, $\ell \in \mathbb{Z}$. The group G'_0 is a direct union of groups of local permutations with fixed neighborhoods.

In the terminology of [1], the group G_0 is denoted $\text{OB}(\mathbb{Z}, n, 1)$ and is called the group of oblivious one-state Turing machines in the moving tape model.

Lemma 5.4. *Let $X = A^\mathbb{Z}$ with $|A| \geq 2$ and let G''_0 , G'_0 and G_0 be as above. Then the following hold:*

- G_0 is finitely generated,
- $G''_0 = [G_0, G_0]$ is a locally finite simple group,
- G''_0 acts ∞ -transitively on the set of finite points X'_0 , and
- there is a unique homomorphism $\psi : G_0 \rightarrow \mathbb{Z}$ with $\psi(\sigma) = 1$, $\psi(G'_0) = \{0\}$, and we have $G'_0 = \ker(\psi)$.

Proof. First, we prove finitely generatedness of G_0 . Let H be the subgroup of G_0 generated by σ and the local permutations with neighborhood $\{0, 1, \dots, n-1\}$, where n satisfies the claim of Lemma 5.2 and $n \geq 2$.

We will show $H = G_0$. It is enough to show that our generators generate G'_0 , as σ is in our generating set. For this, first let $\pi : A^N \rightarrow A^N$ be any even permutation, where $N = \{0, 1, \dots, m-1\}$ for some $m \geq n$. We can apply arbitrary finite support permutations to the coordinates of a point, because the swaps $(n \ n+1)$ generate the symmetric groups, and because our set of generators contains the shift map and the ‘coordinate swap’ P_γ , where $\gamma : A^{\{0,1\}} \rightarrow A^{\{0,1\}}$ is defined by $\gamma(ab) = ba$ for all $a, b \in A$. By conjugating with a permutation of coordinates, we can apply any permutation of A^n to any ordered subset of coordinates in N with size at most n . Since π is even, by Lemma 5.2, π can be decomposed into such permutations, and thus so can P_π .

Suppose then that $\pi : A^N \rightarrow A^N$ is an odd permutation. If $|A|$ is even, π can be seen as an even permutation on $A^{N \cup \{m\}}$ by ignoring the coordinate m , and is thus in H . If $|\Sigma|$ is odd, then let $a \neq b$ be two elements of A , and consider the transposition $(a \ b)$ on Σ . Extending this to a permutation $\pi' : A^N \rightarrow A^N$ by permuting only the 0th coordinate, we obtain an odd permutation that is clearly in H . Then $\pi \circ \pi' : A^N \rightarrow A^N$ is even, and thus in H . This concludes the proof that $H = G_0$.

Next, we show $G''_0 = [G_0, G_0]$. Consider first $P_\pi \in G''_0$ where $\pi : A^N \rightarrow A^N$ is an even permutation and $|N| \geq 3$. Then π is in the commutator subgroup

of the symmetric group on A^N , from which it easily follows that $P_\pi \in [G_0, G_0]$. Let then $g = \sigma^{\ell_1} \circ g'$ and $h = \sigma^{\ell_2} \circ h'$ where $g', h' \in G'_0$. Then

$$\begin{aligned} ghg^{-1}h^{-1} &= (\sigma^{\ell_1} \circ g') \circ (\sigma^{\ell_2} \circ h') \circ (g'^{-1} \circ \sigma^{-\ell_1}) \circ (h'^{-1} \circ \sigma^{-\ell_2}) \\ &= \sigma^{\ell_1+\ell_2} \circ g''h'g'^{-1}h'^{-1} \circ \sigma^{-\ell_1-\ell_2} \end{aligned}$$

where g'' and h'' are conjugate by a power of the shift to g' and h' , respectively, and $g''h'g'^{-1}h'^{-1}$ is a local permutation P_π for some $\pi : A^{N'} \rightarrow A^{N'}$ for some $N' \subset \mathbb{Z}$. If $|A|$ is even, and we pick $|N'|$ large, then this is an even permutation, and we are done. If $|A|$ is odd, then g'' and h'' have the same parity as permutations on $A^{N'}$ as g' and h' , respectively, and again $g''h'g'^{-1}h'^{-1}$ is even, implying that $ghg^{-1}h^{-1} \in G''_0$.

The local finiteness of G''_0 is obvious. For simplicity, let $P_\pi \in G''_0$ where $\pi : A^N \rightarrow A^N$ is a nontrivial even permutation. Then for any $N' \supset N$, the domain extension $\pi : A^{N'} \rightarrow A^{N'}$ (ignoring the coordinates $N' \setminus N$) is an even permutation of $A^{N'}$. Since the alternating group on $A^{N'}$ is simple if $|A^{N'}| \geq 5$, we can write any even permutation $\pi' : A^{N'} \rightarrow A^{N'}$ as a composition of conjugates of π . It follows that the same is true for any $P_{\pi'} \in G''_0$.

Next, let us show that G''_0 acts ∞ -transitively on X'_0 . Let $\vec{x}, \vec{y} \in (X'_0)^k$ be such that the components of \vec{x} are pairwise distinct, and assume the same for \vec{y} . Let r be such that the supports of \vec{x}_i and \vec{y}_i are contained in $[-r, r]$ for all $i \in [1, k]$. Let $u_i = (\vec{x}_i)_{[-r-1, r+1]}$ and $v_i = (\vec{y}_i)_{[-r-1, r+1]}$. Then there is an even permutation of A^{2r+3} that maps u_i to v_i for all i . The corresponding local permutation with $N = [-r-1, r+1]$ maps x_i to y_i for all i , and is an element of G''_0 .

The existence and uniqueness of $\psi : G_0 \rightarrow \mathbb{Z}$ is proved as follows: To $g \in G_0$ associate $j \in \mathbb{Z}$ such that $g(x)_i = x_{i+j}$ for all large enough $|i|$ and all $x \in A^\mathbb{Z}$. Clearly the choice of such j is unique, and this becomes a homomorphism from $G_0 \rightarrow \mathbb{Z}$ with the required properties. Uniqueness follows because σ and G'_0 generate G_0 .

Next we show $G'_0 = \ker(\psi)$. We have $G'_0 \subset \ker(\psi)$ by definition. To see that $\ker(\psi) \subset G'_0$, observe that if $\psi(g) = 0$ then $g(x)_i = x_i$ for $|i|$ large enough, so g is a local permutation, showing $\ker(\psi) \subset G'_0$. \square

5.2 Transitivity on marked configurations

The idea is next to apply the previous lemma to show that the automorphism group of $\Sigma^\mathbb{Z}$ acts ∞ -transitively around configurations where for some $s \in \Sigma$, there is only one occurrence of s , which is at the origin. To do this, we will think of s as the head of a Turing machine (so that it marks the zero-cell of a configuration of $(\Sigma \setminus \{s\})^\mathbb{Z}$ where G_0 acts), translate local permutations to local changes near s , and turn $\sigma \in G_0$ into movements of the head s . The difficult part is moving s with an automorphism, and most of the work in this section is about proving Lemma 5.8 which accomplishes this.¹⁰

¹⁰In an older draft [41], I left it open whether Lemma 5.8 is true, and proved the result in a different way. The cellular automaton $f_{\sigma, s}$ used now was suggested by Jarkko Kari. The

Let $\Sigma = \{0, 1, \dots, n-1\}$ and let $u, v \in \Sigma^k$. Then u and v are ℓ -boundary-equivalent if $u_{[0,\ell-1]} = v_{[0,\ell-1]}$ and $u_{[k-\ell,k-1]} = v_{[k-\ell,k-1]}$. For $x \in \Sigma^{\mathbb{Z}}$ and $U \subset \Sigma^k$, define $\chi_U(x) \subset \mathbb{Z}$ by $i \in \chi_U(x) \iff x_{[i,i+k-1]} \in U$.

Definition 5.5. Let $X \subset \Sigma^{\mathbb{Z}}$ be an SFT with window size at most $h-1$. Let $U \subset \Sigma^k$ and $V \subset \Sigma^h$ for some $h \leq k$. Then U is V -safe (for X) if the following three conditions hold: First, every word $u \in U$ contains a word of V as a subword. Second, whenever $u, v \in U$ are $(h-1)$ -boundary-equivalent and $x \in X$ satisfies $x_{[0,k-1]} = u$, we have

$$\chi_U(x) = \{0\}, \chi_V(x) \subset [0, k-h] \implies \chi_U(x_{(-\infty,-1]}.vx_{[k,\infty)}) = \{0\}.$$

Third, for each $u \in U$ there is at least one point $x \in X$ such that $\chi_U(x) = \{0\}$, $\chi_V(x) \subset [0, k-h]$ and $x_{[0,k-1]} = u$.

Note that in particular U must be contained in the language of X by the third condition.

If $U \subset \Sigma^k$, a function $\pi : U \rightarrow U$ is ℓ -safe if u and $\pi(u)$ are ℓ -boundary-equivalent for all $u \in U$.

Safe bijections on safe sets of words give rise to automorphisms by local rewriting, provided that we are very selective in where we apply the rewriting rule:

Lemma 5.6. Let $X \subset \Sigma^{\mathbb{Z}}$ be an SFT with window size at most $h-1$. Let $U \subset \Sigma^k$ and $V \subset \Sigma^h$ for some $h \leq k$, and suppose U is V -safe. Let Γ be the group of $(h-1)$ -safe permutations of U . Then there is a group monomorphism $\gamma : \Gamma \rightarrow \text{Aut}(X)$ such that, letting

$$Y_1 = \{x \in X \mid \chi_U(x) = \{0\}, \chi_V(x) \subset [0, k-h]\},$$

we have

$$\forall x \in Y_1 : \forall \pi \in \Gamma : \gamma(\pi)(x) = x_{(-\infty,-1]}. \pi(x_{[0,k-1]})x_{[k,\infty)}.$$

Proof. It is enough to construct a homomorphism with this property, as it is then automatically an embedding by the third condition of safety.

We will define a local rule $\chi : X \rightarrow 2^{\mathbb{Z}}$ that picks a set of coordinates where the rule can be safely applied. We need to ensure that $\chi(x) \subset \chi_U(x)$ for all x , so that we can apply each rule π at this coordinate. The same local rule χ is used when defining each $\gamma(\pi)$, and we also ensure that $\chi(\gamma(\pi)(x)) = \chi(x)$ for all $x \in X$ and $\pi \in \Gamma$, so that we obtain a group homomorphism. We also have to make sure that the behavior on Y_1 is correct.

Let $|\Sigma| = n$. We pick $m, \ell \in \mathbb{N}$ with $\ell > n^h$ and $m \geq \ell + 2k + h$.¹¹ Let $k' = k-1, h' = h-1$.

basic idea is the same, but we transpose different kinds of word pairs. The construction is written in much more detail than in the previous version, because there was a mistake.

¹¹The reason we need n^k is that since we allow V to be any set of words in the definition, it is possible that a word that does not contain V has only continuations containing V , and a padding of n^h is sufficient to get around this. In our application V consists of a single word of length one, and in this special case one could simplify the construction, and reduce the radius.

We let $i \in \chi(x)$ if and only if

$$\chi_U(x) \cap [i-m, i+m] = \{i\}$$

and

$$\chi_V(x) \cap [i-\ell, i+\ell] \subset [i, i+k-h] = [i, i+k'-h'].$$

We can now define the map $\gamma(\pi)$: if $i \in \mathbb{Z}$ and $0 \leq j < k$, then

$$i-j \in \chi(x) \implies \gamma(\pi)(x)_i = \pi(x_{[i-j, i-j+k']})_j$$

and $\gamma(\pi)(x)_i = x_i$ otherwise. This clearly defines a continuous shift-commuting function, and it is well-defined since $m \geq k$, and thus for each $i \in \mathbb{Z}$ the first defining rule can apply to at most one j .

With this definition, we already have the correct behavior on Y_1 . To show that the rules $\gamma(\pi)$ are automorphisms and γ is a group homomorphism, it is sufficient to prove that $\chi(\gamma(\pi)(x)) = \chi(x)$ for all x , as then $\gamma(\pi)(\gamma(\pi')(x)) = \gamma(\pi \circ \pi')(x)$ for all $x \in \Sigma^{\mathbb{Z}}$ and $\pi \in \Gamma$.

Suppose that $i \in \chi(x)$, that is, $\chi_U(x) \cap [i-m, i+m] = \{i\}$ and $\chi_V(x) \cap [i-\ell, i+\ell] \subset [i, i+k'-h']$. Then the symbols at coordinates $[i-m+k', i-1] \cup [i+k, i+m]$ do not change when $\gamma(\pi)$ is applied. Thus, if we had

$$\chi_U(\gamma(\pi)(x)) \cap [i-m+k', i+m-k'] \neq \{i\},$$

then we would necessarily have $\chi_U(\gamma(\pi)(x)) \cap [i-k', i+k'] \neq \{i\}$. Since $m-2k' - h' > \ell > n^h$, by a pigeonhole argument, we could then find a point y which is eventually periodic both left and right, $y_{[i-k', i+2k']} = x_{[i-k', i+2k']}$, and $\chi_V(y) \subset [i, i+k'-h']$, and the fact we obtain two occurrences of words in U when changing the word $x_{[i, i+k']}$ to $\pi(x_{[i, i+k']})$ contradicts the V -niceness of U .

Thus, if $i \in \chi(x)$, we have $\chi_U(\gamma(\pi)(x)) \cap [i-m+k', i+m-k'] = \{i\}$. From this, the fact that coordinates in $[i-m+k', i-1] \cup [i+k, i+m]$ do not change when a rewrite happens at i , and $m-k' > k'$, we have $\chi_U(\gamma(\pi)(x)) = \chi_U(x)$ for all x .

We do not necessarily have $\chi_V(\gamma(\pi)(x)) = \chi_V(x)$, but if $i \in \chi(x)$, then since the coordinates $[i-m+k', i-1] \cup [i+k, i+m]$ do not change when $x_{[i, i+k-1]}$ is rewritten, after the rewrite we have

$$\chi_V(\gamma(\pi)(x)) \cap [i-\ell, i+\ell] \subset \chi_V(\gamma(\pi)(x)) \cap [i-m+k', i+m] \subset [i, i+k'-h'],$$

so $i \in \chi(\gamma(\pi)(x))$.

Finally, if $i \notin \chi(x)$ but $\chi_U(x) \cap [i-m, i+m] = \{i\}$, then we have $j \in \chi_V(x) \cap [i-\ell, i+\ell]$ for some $j \notin [i, i+k'-h']$. We then also have $j \in \chi_V(\gamma(\pi)(x)) \cap [i-\ell, i+\ell]$, since $m-2k' - h' \geq \ell$, implying $i \notin \chi(\gamma(\pi)(x))$, as $i \in \chi_U(x)$ prevents rewritings affecting $j \in \chi_V(\gamma(\pi)(x))$ (by a similar argument as above). \square

Clearly being V -safe is a decidable condition for any $V \subset \Sigma^h$, but a precise characterization would presumably involve some intricate combinatorics on words. In our application, we have X a full shift, $V = \{s\}$, and we will guarantee safety by assuming no words in U contain s at their border, and the following sufficient condition for a set of words to be safe is sufficient for our purposes.

Lemma 5.7. Let $\Sigma = \{0, 1, \dots, n-1\}$, $A = \Sigma \setminus \{s\}$ and $s = n-1$. Let $U \subset A^k \Sigma^k A^k$ be a set of words such that every word in U contains s , and if $u, v \in U$ and $|u|_s = |v|_s$, then the leftmost occurrence of s is in the same coordinate in u and v . Then U is an $\{s\}$ -safe set of words on the full shift $\Sigma^\mathbb{Z}$.

Proof. The first condition of the definition of safety is trivial.

For the second, let $V = \{s\}$ and suppose that x satisfies $x_{[0,3k-1]} = u$, $\chi_U(x) = \{0\}$ and $\chi_V(x) \subset [0, 3k-1]$. Let $y = x_{(-\infty, -1]} \cdot vx_{[3k, \infty)}$ where $v \in U$. Then by the form of U , we in fact have $\chi_V(y) \subset [k, 2k-1]$. If $\chi_U(y) \neq \{0\}$, then $y_{[i, i+3k-1]} = w \in U$ for some $i \in [-3k+1, 3k-1] \setminus \{0\}$. Since only the middle third of each of v and w contains ss and $\chi_V(x) \subset [k, 2k-1]$, it is easy to see that $|i| < k$, and thus v and w contain the same number of ss . This is a contradiction, since $i \neq 0$ so the leftmost s is not in the same coordinate in these two words.

The third condition of the definition is satisfied by $\dots 000.u000\dots$ by a similar argument. \square

Lemma 5.8. Let $\Sigma = \{0, 1, \dots, n-1\}$ and $s = n-1$. Let $Y_{1,s} \subset \Sigma^\mathbb{Z}$ be the set of configurations containing s at the origin and having no other occurrence of s . Then there is an automorphism $f \in \text{Aut}(\Sigma^\mathbb{Z})$ with the property

$$\forall x \in Y_{1,s} : f(x)_0 = x_1 \wedge f(x)_1 = x_0 \wedge \forall i \notin \{0, 1\} : f(x)_i = x_i.$$

Proof. Let $A = \Sigma \setminus \{s\}$. Intuitively, the solution is that we first perform an involution that changes every occurrence of s (that is suitably isolated) preceded by $a \in A$ into an occurrence of saw , where the distance between the ss codes a , and w is taken from the configuration (so no information is lost). Another involution changes this to sa , so that composing the two involutions, we effectively move s to the left or right, depending on the order of composition.

Pick $U_1 = \{A^{m+1}sA^{m-1}\}$ and $U_2 = \{A^m s A^k s A^{m-1-k} \mid k \in \{0, \dots, n-2\}\}$. Observe that U_1 and U_2 are disjoint, both have $(n-1)^{2m}$ elements, and all words in these sets are of length $2m+1$. Let $U = U_1 \cup U_2$ and pick any bijection $\pi' : U_1 \rightarrow U_2$. For example, one can pick $\pi'(uasv) = usv_{[0,a-1]}sv_{[a,m-2]}$ for $u \in A^m, a \in A, v \in A^{m-1}$. This gives us an involution $\pi : U \rightarrow U$ defined by $\pi|_{U_1} = \pi'$ and $\pi|_{U_2} = (\pi')^{-1}$.

If we pick m large enough, and such that $2m+1$ is divisible by 3, then the assumptions of Lemma 5.7 are satisfied, and there is a homomorphism γ from the group of 0-safe bijections (that is, all bijections) on U to $\text{Aut}(\Sigma^\mathbb{Z})$ which satisfies the conclusion of Lemma 5.6. Let $f_\pi = \gamma(\pi)$.

Pick now $V_1 = \{A^m s A^m\}$, $V_2 = U_2$ and $V = V_1 \cup V_2$ and construct similarly an involution $\tau : V \rightarrow V$, picking the bijection $\tau' : V_1 \rightarrow V_2$ so that $(\pi')^{-1} \circ \tau'(uasv) = uasv$ for all $a \in A, u \in A^m, v \in A^{m-1}$. Construct the automorphism f_τ as above, using the involution τ .

It is now easy to verify that $f = f_\pi \circ f_\tau$ acts correctly on $Y_{1,s}$. \square

Let $s \in \Sigma \setminus \{0\}$, and let $Y_{1,s}$ be as in the previous lemma. Let $A = \Sigma \setminus \{s\}$ and $Y_{0,s} = A^\mathbb{Z}$.

Lemma 5.9. *Let $s \in \Sigma \setminus \{0\}$. Then there is a finitely generated subgroup \mathcal{G}_s of $\text{Aut}(\Sigma^{\mathbb{Z}})$ that acts trivially on $Y_{0,s}$, and is ∞ -orbit-transitive around $Y_{1,s}$.*

Proof. Let $A = \Sigma \setminus \{s\}$. We define a map $\phi : G_0 \rightarrow \text{Aut}(\Sigma^{\mathbb{Z}})$ with the following properties:

- for all $g \in G_0$, $\phi(g)(x)_i = x_i$ unless x contains s at a bounded distance from i (the bound depending on g), and
- for $g \in G_0$ and for all $x \in A^{-\mathbb{N}}$, $y \in A^{\mathbb{N}}$ we have

$$g(x.y) = x'.y' \implies \phi(g)(x.sy) = \sigma^{-\psi(g)}(x'.sy'),$$

where $\psi : G_0 \rightarrow \mathbb{Z}$ is the homomorphism from Lemma 5.4.

From these properties it will follow that if F is a finite generating set for G_0 , then $\phi(F)$ generates a finitely generated subgroup of $\text{Aut}(\Sigma^{\mathbb{Z}})$ with the required properties: the first implies that $\phi(g)$ acts trivially on $Y_{0,s}$ and ∞ -orbit-transitivity around $Y_{1,s}$ comes from the second, since the action of $[G_0, G_0]$ is ∞ -transitive on X'_0 and $\psi(g) = 0$ for $g \in [G_0, G_0]$.

We remark that these properties also imply that if we let Y be the (sofic) subshift obtained as the orbit closure of $Y_{1,s}$ under the shift, then the restriction $\phi(g)|_Y : Y \rightarrow Y$ is well-defined for all $g \in G_0$, and the map $g \mapsto \phi(g)|_Y$ is a group embedding from G_0 to $\text{Aut}(Y)$. However, ϕ will not be a group embedding of G_0 to $\text{Aut}(\Sigma^{\mathbb{Z}})$, and could not be, since $\text{Aut}(\Sigma^{\mathbb{Z}})$ is residually finite while G_0 contains the infinite simple group $[G_0, G_0]$.

Let G_0 be the finitely generated group of homeomorphisms of $A^{\mathbb{Z}}$ defined in Definition 5.3. To each permutation $\pi : A^{[-r,r]} \rightarrow A^{[-r,r]}$, we associate the CA $f_{\pi,s}$ defined by rewriting words usv where $u \in A^r$, $v \in A^r$ to $u'sv'$ where $u'v' = \pi(uv)$ and $|u'| = r$, whenever there are no other occurrences of the symbol s are at distance less than $2r + 3$ from the central s in the pattern usv . Since occurrences of s are neither removed nor introduced, this gives a well-defined automorphism.

Now, if $g : A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$ is a local homeomorphism with $\psi(g) = 0$, choose a presentation $g = P_{\pi}$ with $\pi : A^{[-r,r]} \rightarrow A^{[-r,r]}$ arbitrarily (for example, pick the smallest possible r) and let $\phi(g) = f_{\pi,s}$. It is clear that $\phi(g)$ then has the required properties for any $g \in G'_0$.

Let then $\phi(\sigma) = f_{\sigma,s}$, where $f_{\sigma,s}$ is the automorphism constructed in Lemma 5.8. Let $x \in A^{-\mathbb{N}}$, $a \in A$ and $y \in A^{\mathbb{N}}$. Plugging $\sigma(x.ay) = xa.y$ and $\psi(\sigma) = 1$ in the second requirement for ϕ above, we get

$$\sigma(x.ay) = xa.y \implies \phi(\sigma)(x.say) = \sigma^{-1}(xa.sy) = x.asy,$$

and indeed $f_{\sigma,s}(x.say) = x.asy$.

Now, if F is a finite set of permutations $\pi : \Sigma^N \rightarrow \Sigma^N$ such that G_0 is generated by σ and $\{P_{\pi} \mid \pi \in F\}$, then

$$\mathcal{G}_s = \langle f_{\pi,s}, f_{\sigma,s} \mid \pi \in F \rangle$$

is a finitely generated subgroup of $\text{Aut}(\Sigma^{\mathbb{Z}})$ with the required properties. \square

5.3 The reset system

We also define the following somewhat peculiar monoid action that is helpful for book-keeping in the proof of our main theorem.

Definition 5.10. Let M be the free (noncommutative) monoid generated by $(\mathbb{Z} \times \mathbb{N})^k$.¹² The generator $\vec{x} \in (\mathbb{Z} \times \mathbb{N})^k$ of M acts on $(\mathbb{Z} \times \mathbb{N})^k$ by

$$(\vec{x} \cdot \vec{y})_i = \begin{cases} (n_i, t_i) & \text{if } \vec{y}_i = (n_i, t_i + 1) \text{ and} \\ x_i & \text{if } \vec{y}_i = (n, 0). \end{cases}$$

The dynamical system $(M, (\mathbb{Z} \times \mathbb{N})^k)$ is called the *reset system*.

One may think of the reset system as a dynamical system modeling a finite set of alarm clocks that, when they buzz, are reset to buzz at a later time. In addition to the counter \mathbb{N} , the alarm clocks carry a position in \mathbb{Z} indicating *where* they buzz next.

Lemma 5.11. *The reset system is transitive. In particular, for all $\vec{v} \in (\mathbb{Z} \times \mathbb{N})^k$ there exists $m \in M$ such that $m \cdot \vec{v} = (0, 0)^k$.*

Proof. Let $\vec{u}, \vec{v} \in (\mathbb{Z} \times \mathbb{N})^k$ be arbitrary. Then for large enough ℓ we have $((0, 0)^k)^\ell \cdot \vec{v} = (0, 0)^k$. Thus $(\vec{u} \cdot ((0, 0)^k)^\ell) \cdot \vec{v} = \vec{u}$, proving transitivity since $\vec{u} \cdot ((0, 0)^k)^\ell \in M$ and \vec{u}, \vec{v} were arbitrary. \square

In the proof of the main theorem, the positions \mathbb{Z} will be eventual positions of heads, and \mathbb{N} will represent the times when heads first appear in those positions when a suitable particle rule P is applied repeatedly. We can simulate the (highly non-reversible) action of the reset system by automorphisms, as we only need to act in a controlled way on a finite set of points.

We remark that in the proof of the main theorem, most of the real work happens when a (simulated) clock is snoozed, that is, when the second component of some \vec{y}_i reaches zero and $(\vec{x} \cdot \vec{y})_i = \vec{x}_i$. If one wants ‘efficient transitivity’ (where the transporter has small word norm in the group) in the proof of the main theorem, one might prefer a more elegant proof of the previous lemma. With a bit of arithmetic, one can prove the lemma without snoozing any clock more than once.

6 Proof of the main result

In this section, we prove the main result Theorem 2.1. For this section, fix $X = \Sigma^{\mathbb{Z}}$ where $\Sigma = \{0, 1, 2, 3\}^{\mathbb{Z}}$. Let P be the particle rule with the decomposition $\Sigma \cong \{0, 1\} \times \{0, 1\}$ given by $n \mapsto (n \bmod 2, \lfloor n/2 \rfloor)$.

The ∞ -orbit-transitive action will be given by the group

$$\mathcal{G} = \langle \mathcal{G}_3, P, g_{(13)}, g_{(23)} \rangle$$

¹²In other words, M is the set of words $\vec{x}_1 \vec{x}_2 \cdots \vec{x}_\ell$ where $\vec{x}_i \in (\mathbb{Z} \times \mathbb{N})^k$ for all $i \in [1, \ell]$, with concatenation as the monoid operation.

where $g_{(13)}$ is the symbol-permutation $(1\ 3)$, $g_{(23)}$ the symbol-permutation $(2\ 3)$, and the group \mathcal{G}_3 is that from Lemma 5.9.

We call 1 a *particle* and 2 a *wall*. We call 3 a *head*, also understanding it as a particle on top of a wall. By a *collision*, we refer to the intuitive concept of the appearance of a head due to the particle rule (or its inverse) moving a particle on top of a wall. Note that P moves particles to the left and keeps walls fixed.

Though in the proofs we only use these numbers and names, we fix the following pictorial presentation as well:

$$0 = \square, 1 = \blacksquare, 2 = \blacksquare\square, \text{ and } 3 = \blacksquare\square\square.$$

We refer to tuples $\vec{x} \in X_0^{(k)}$ as *vectors*, and the points $\vec{x}_i, i \in [1, k]$ are called its *components*.

Definition 6.1. A nonzero finite point $x \in X_0$ is

- *pregood* if it contains no heads and all the particles are to the left of all the walls,
- *pregood* if it is pregood and contains a particle,
- *good* if it is pregood and contains a wall, and
- *great* if it contains exactly one head which is at 0.

For any of these properties P, a vector is P if all its components are.

Note that great points are just the points in $Y_{1,3}$. Note that pregood points are pregood and pregood points are good, but good points are never great and great points are never good.

6.1 Outline and example

Suppose $k = 3$, and begin with the following vector \vec{x} of configurations:

$$\vec{x} = \square\square\square + \square\square\square \quad \square\square\square | \square\square\square - \square\square\square \quad \square\square\square | \square\square\square \quad \square\square\square$$

Since we are dealing with a group action, it is enough to transform \vec{x} into a fixed vector \vec{y} , as the inverse steps of such transformations can be used to transform \vec{y} into any other vector. We use the great vector

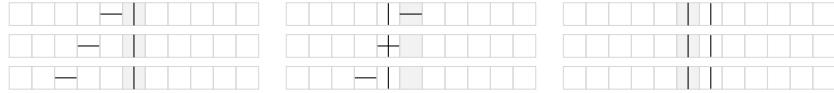
$$\vec{y} = \square\square\square + - \square\square\square \quad \square\square\square + - \square\square\square \quad \square\square\square + \square - \square$$

The outline of the proof is that we first make \vec{x} pregood, then pregood, then good, by a few applications of the particle rule and symbol-permutations. We then simulate the reset system using Lemma 5.9 to make \vec{x} great. A final application of Lemma 5.9 finishes the proof, turning \vec{x} into \vec{y} .

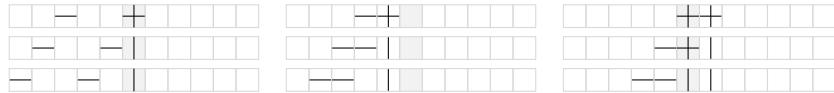
Figure 1 shows how to do this, using Lemma 5.9 as a black box. We have taken some artistic liberties in Figure 1; it does not follow the proof to the letter. Intuitively, Lemma 5.9 allows us to do *anything* around any individual head, as long as the relative movement of every head is the same.



Apply P^t for some t such that \vec{x} becomes pregood. In the case of \vec{x} above, we use $t = 3$:



Apply the symbol-permutation $\square \leftrightarrow +$ and repeat the particle rule to make the vector pregood:



Our vector is now pregood. Were it not good, we would apply the symbol-permutation $\square \leftrightarrow +$ and apply the particle rule again. It happens to be good, so we omit this step. Next, we apply the inverse of the particle rule, and wait for collisions to happen in some of the components:



A collision happens in the third component. Applying Lemma 5.9, we organize a new collision to happen at the origin of the third component after 4 applications of P^{-1} :



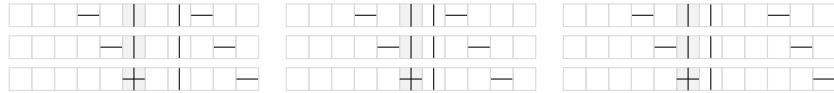
Apply P^{-1} until the next collision (that is, once):



Applying Lemma 5.9, we organize new collisions to happen at the origin of the first and second components after 3 applications of P^{-1} :



Apply P^{-1} repeatedly until simultaneous collisions happen at the origin in all three components, to get a great vector:



Applying Lemma 5.9, change the vector to \vec{y} :



In summary, for some T_1, T_2, T_3 provided by Lemma 5.9, we have obtained

$$\vec{y} = (T_3 \circ P^{-3} \circ T_2 \circ P^{-1} \circ T_1 \circ P \circ (\square \leftrightarrow +) \circ P^3)(\vec{x}).$$

Figure 1: How to get from \vec{x} to \vec{y} , using Lemma 5.9 as a black box. The shaded square denotes the origin.

6.2 Making vectors good

The first step in the proof is showing that we can always make our vector of configurations good. This is done in three steps: we first make the vector pregood, then pregood, and then good.

Lemma 6.2. *Let $\vec{x} \in X_0^{(k)}$. Then there is an element $g \in \langle g_{(13)}, g_{(23)}, P \rangle$ such that $g\vec{x}$ is good.*

Proof. Applying P moves particles to the left while keeping walls still. Clearly after some amount of steps of P on \vec{x} , there are no heads and all particles are to the left of all the walls in all components of \vec{x} , so \vec{x} can be transformed to a pregood vector \vec{x}^2 .

Now, apply $g_{(23)}$ to the pregood vector \vec{x}^2 , turning walls into heads, and repeatedly apply P until all particles are again to the left of all the walls. Note that after this, every component of \vec{x}^2 contains a particle: if a component $x = \vec{x}_i^2$ contains a particle before applying $g_{(23)}$, it still does after applying it and repeating P . If it contains a wall, then a head is introduced, giving a particle after the application of P . Note that x must contain either a particle or a wall, since $x \in X_0$ and $0^\mathbb{Z} \notin X_0$. We obtain that \vec{x}^2 can be transformed to a pregood vector \vec{x}^3 .

By the same argument, by applying $g_{(13)}$ and then repeating P , we eventually turn \vec{x}^3 into a good vector \vec{x}^4 . \square

6.3 Making vectors great

We give a precise connection between the reset system and our automorphism action. For this we need to measure when and where our points are great, and we give the following definition: A point $x \in \Sigma^\mathbb{Z}$ is *clock-like* if there exists $(a, t) \in \mathbb{Z} \times \mathbb{N}$ such that $\sigma^a(P^{-t-1}(x))$ is great (in particular $P^{-t-1}(x)_a = s$) and for $0 \leq t' < t$, $P^{-t'-1}(x)$ does not contain a collision. Note that we do not require that x not contain a head (it typically will contain one in our application). A vector \vec{x} is *clock-like* if all its components are. Write $C \subset X_0$ for the set of finite clock-like points.

Define $\phi : C^{(k)} \rightarrow (\mathbb{Z} \times \mathbb{N})^k$ by associating to a clock-like point x the pair (a, t) as defined above. Note that the time value t in the reset system corresponding to a component in a vector \vec{x} is one less than the actual collision time when applying P^{-1} .

The following lemma gives a natural correspondence between the action of automorphisms on $C^{(k)}$, and the action of the reset system with k clocks.¹³

Lemma 6.3. *Let $\vec{x} \in C^{(k)}$ and $\vec{v} \in (\mathbb{Z} \times \mathbb{N})^k$. Then there exists $g \in \mathcal{G}_3$ such that $gP^{-1}(\vec{x}) \in C^{(k)}$ and $\phi(gP^{-1}(\vec{x})) = \vec{v}$ if and only if there exists $m \in (\mathbb{Z} \times \mathbb{N})^k$ such that $m \cdot \phi(\vec{x}) = \vec{v}$.*

¹³We are essentially saying that ϕ is a ‘homomorphism’, which could be formalized in terms of abstract rewriting systems or categories.

Proof. We show that applying an element of the form gP^{-1} where $g \in \mathcal{G}_3$ to a vector $\vec{x} \in C^{(k)}$ either takes \vec{x} out of $C^{(k)}$ or corresponds to a translation in the reset system: Consider the application of some element gP^{-1} to \vec{x} such that $gP^{-1}(\vec{x}) \in C^{(k)}$. If $\phi(\vec{x})_i = (a, t)$ with $t > 0$, we necessarily have $\phi(gP^{-1}(\vec{x}))_i = (a, t - 1)$, since no collision happens when P^{-1} is applied, and g behaves as identity on points without heads. We simply choose $m \in (\mathbb{Z} \times \mathbb{N})^k$ so that the action is correct on other components.

We now show a converse, namely that maps of the form gP^{-1} implement all possible transitions in the reset system. More precisely, that for all $\vec{x} \in C^{(k)}$ and $m \in (\mathbb{Z} \times \mathbb{N})^k$, there is an element $g \in \mathcal{G}_3$ such that $\phi(gP^{-1}(\vec{x})) = m \cdot \phi(\vec{x})$. For this, let $I \subset [1, k]$ be the set of those $i \in [1, k]$ such that there is a great point in the σ -orbit of $x = P^{-1}(\vec{x}_i)$. We need to find an element of \mathcal{G}_3 that resets the next buzz times and positions of these clocks according to the corresponding coordinates of m_i . Let $m_i = (n_i, t_i)$ for all i .

The fact that the points come from different σ -orbits means that we can really do any transformation we like using Lemma 5.9, as long as the relative positions of the heads do not change. However, since Lemma 5.9 cannot get rid of heads, and heads dissolve into a wall and a particle when P^{-1} is applied, we need to be careful so that the particle they introduce does not lead to sporadic collisions. Thus, we make the heads the rightmost symbols of the support, so that particles simply escape to infinity when we start applying P^{-1} .

We describe this in more detail. Note that automorphisms of the form $f_{\pi,3}$ and $f_{\sigma,3}$ act trivially on $Y_{0,3}$, and thus only modify components $P^{-1}(\vec{x})_i$ where $i \in I$, so we can ignore coordinates $i \notin I$: they are already handled correctly, as P^{-1} decrements the right components of their ϕ -images.

On the components $P^{-1}(\vec{x})_i$ where $i \in I$, first apply $f_{\sigma,3}^k$ for some large k so that all heads are at least two steps to the right of the values n_i . Let the head on $\vec{y}_i = f_{\sigma,3}^k(P^{-1}(\vec{x})_i)$ be in coordinate k_i for all $i \in I$. Note that the points \vec{y}_i , $i \in I_1$, are from different σ -orbits by the definition of $C^{(k)}$, and since automorphisms preserve orbits. Now, use the ∞ -transitivity of the action of $f_{\pi,3}$ and $f_{\sigma,3}$ around $Y_{1,3}$ given by Lemma 5.9 to, for all $i \in I_1$, transform \vec{y}_i to the vector \vec{z}_i where

$$(\vec{z}_i)_j = \begin{cases} 3, & \text{if } j = k_i, \\ 2, & \text{if } j = n_i, \\ 1, & \text{if } j \in \{n_i - t_i - 1, k_i + i + 1\}, \text{ and} \\ 0, & \text{otherwise.} \end{cases}$$

Here, the particle in coordinate $n_i - t_i - 1$ and the wall at n_i generate the collision at n_i after $t_i + 1$ steps of applying P^{-1} . The particle at $k_i + i + 1$ is included so that we are sure that these points are from distinct orbits.¹⁴

Let $f \in \mathcal{G}_3$ be the transformation mapping $\vec{y}_i \rightarrow \vec{z}_i$. Then

$$\phi(f \circ f_{\sigma,3}^k \circ P^{-1}(\vec{x}))_i = \phi(P^{-1}(\vec{x}_i)) = m_i \cdot \phi(\vec{x}_i)$$

¹⁴Omitting this particle was the main ‘artistic liberty’ taken in Figure 1.

for $i \notin I$ and

$$\phi(f \circ f_{\sigma,3}^k \circ P^{-1}(\vec{x}))_i = \phi(\vec{z}_i) = (n_i, t_i) = m_i \cdot \phi(\vec{x}_i)$$

for $i \in I$, which concludes the proof. \square

Lemma 6.4. *If \vec{x} is good, there exists $g \in \mathcal{G}' = \langle \mathcal{G}_3, P \rangle \leq \mathcal{G}$ such that $g\vec{x}$ is great.*

Proof. It is clear that every good vector is clock-like. The reset system is transitive, so by the previous lemma for every $\vec{x} \in C^{(k)}$ there is a group element $g \in \mathcal{G}'$ such that $g\vec{x} = \vec{x}' \in C^{(k)}$ and $\phi(\vec{x}') = (0, 0)^k$. Then $P^{-1}(\vec{x}')$ is great. \square

6.4 Proof of ∞ -orbit-transitivity

Let \vec{y} be the vector where the support of \vec{y}_i is $\{0, i\}$, $(\vec{y}_i)_0 = 3$ and $(\vec{y}_i)_i = 1$.

Lemma 6.5. *If \vec{x} is great, then there exists $g \in \mathcal{G}_3$ such that $g\vec{x} = \vec{y}$.*

Proof. This is a direct corollary of Lemma 5.9. \square

We can now prove our main theorem.

Theorem 6.6. *Let $X = \{0, 1, 2, 3\}^{\mathbb{Z}}$. Then*

$$\mathcal{G} = \langle \mathcal{G}_3, P, g_{(13)}, g_{(23)} \rangle \leq \text{Aut}(X)$$

acts ∞ -orbit-transitively on X_0 .

Proof. Let $\vec{x} \in X_0^{(k)}$ be arbitrary. Then

- by Lemma 6.2 there exists $g \in \mathcal{G}$ such that $\vec{x}' = g\vec{x}$ is good,
- by Lemma 6.4, there exists $g' \in \mathcal{G}$ such that $\vec{x}'' = g'\vec{x}'$ is great, and
- by Lemma 6.5, there exists $g'' \in \mathcal{G}$ such that $g''\vec{x}'' = \vec{y}$.

Since \vec{x} and $k \in \mathbb{N}$ were arbitrary, and \vec{y} is a function of k only, this proves ∞ -orbit-transitivity. \square

7 Notes

7.1 The number of generators

We have made little effort to minimize the generating set. The group \mathcal{G}_3 requires at most 5 generators, as one can extract from the fact that four gates are enough to generate the ternary reversible clone [2]. Thus, we need at most 8 generators for the group \mathcal{G} . It is difficult to make the set essentially smaller without a new idea.

It is theoretically possible to find smaller generating sets by computer search – any set of automorphisms generating our generators will naturally satisfy the

conclusion of Theorem 2.1. We have not attempted this. The radius of our generators is small, and within reach of complete enumeration of rules, apart from $f_{\sigma,3}$, whose neighborhood size (if obtained abstractly from our proof) is big.

7.2 Abelian actions are not 2-orbit-transitive

As mentioned in the introduction, at least two automorphisms are needed for ∞ -orbit-transitivity. We obtain this from the following more general proposition.

Proposition 7.1. *No action of a finitely generated abelian group G on an H -set X with infinitely many orbits is 2-orbit-transitive.*

Proof. Assume G acts 2-orbit transitively on X . We may assume G acts freely: If G_0 is the stabilizer of some x , then it is the stabilizer of every element of X , since G is abelian and its action is transitive. Thus, the group G/G_0 acts 2-orbit-transitively on X with trivial stabilizers.

Let $x, y \in X$ be representatives of two distinct H -orbits. Then there exists g such that $(x+g, y+g) = (y, x)$, so that $x+2g = x$. It follows that the torsion subgroup of G acts transitively on X .

Since every subgroup of a finitely generated abelian group is finitely generated, the torsion subgroup of G is finitely generated, and thus finite. From the freeness of the action, it follows that G is finite, contradicting the fact that X has infinitely many orbits. \square

7.3 Finite groups of automorphisms have big centralizer

In [43], it was shown that on every large enough full shift, there is a finite set of cellular automata having a trivial centralizer. A crucial difference between the monoid and group case is that the cellular automata of [43] in fact generate a finite monoid, while in the case of group actions, any group of cellular automata having a trivial centralizer has to be infinite, according to the following theorem. We follow [40], but this is a modest elaboration of [25].

Theorem 7.2. *Let G be any finite group of automorphisms on a mixing SFT X , and Γ any finite alphabet. Then there is an embedding $\phi : \text{Aut}(\Gamma^{\mathbb{Z}}) \rightarrow \text{Aut}(X)$ such that $\phi(f)$ commutes with g for all $f \in \text{Aut}(\Gamma^{\mathbb{Z}})$ and $g \in G$.*

Proof. Without loss of generality, we may assume $\Gamma = \{0, 1\}$, since the automorphism groups of full shifts embed into each other [25]. (Alternatively, one can directly modify the proof below.)

Let $X \subset \Sigma^{\mathbb{Z}}$. Without loss of generality, we can assume G acts by cellwise symbol-permutations. Namely, by the conjugacy mapping $x \in X$ to $y \in (\Sigma^G)^{\mathbb{Z}}$ by $(y_i)_g = g(x)_i$, the action of G becomes a cellwise symbol-permutation. We may of course also assume the action is faithful.

Since X is mixing, there exists a point $x \in X$ on which the action of G is free ($|Gx| = |G|$) and thus there exists a word $w \in X$ such that whenever

w appears in a point, the action is free on that point. Using a higher block presentation [30],¹⁵ we can thus further assume that there is a symbol $a \in \Sigma$ such that $|A| = |G|$ where $A = Ga$ (where by Ga we mean the orbit of a under the symbol permutations by which G acts). We may further assume that the subshift Y of points $x \in X$ where no element of A appears has positive entropy, by possibly passing to yet another higher block presentation. We may assume that the forbidden patterns defining X are of size 2, again by passing to a higher block presentation.

Since X is mixing and Y has positive entropy, there exist $v, v' \in \Sigma^*$ such that for any large enough m there are many words $avwv'a$ and $w \in (\Sigma \setminus A)^m$. To see this, observe that by mixing and positive entropy of Y , for some symbols $b, c \in A$ and for all large enough $m = |w|$ there are many words of the form bwc which occur in X , such that w does not contain symbols in A . By mixing of X , there are then many words of the form $aubwcu'a$ where u and u' are two fixed words. By picking a large m , performing yet another block coding and replacing a by $cu'aub$, we may assume there are at least 4 words occurring in X of the form awa where $|w| = m$ and w contains no symbol in A , and enumerate them as $\{aw_{(0,0)}a, aw_{(0,1)}a, aw_{(1,0)}a, aw_{(1,1)}a\}$. Let $B = \{(0,0), (0,1), (1,0), (1,1)\}$.

Now, all words of the form $aw_{i_1}aw_{i_2}a \cdots aw_{i_\ell}a$ for $i_j \in B$ occur in X . Write ψ for the obvious bijection between words of this form and words over the alphabet B . A word of length ℓ over the alphabet B represents an element of $\{0,1\}^{2\ell}$ through the bijection $\pi : B^\ell \rightarrow \{0,1\}^{2\ell}$ defined by

$$\pi(u)_i = \begin{cases} c & \text{if } 0 \leq i < \ell, u_i = (c,d), \\ d & \text{if } \ell \leq i < 2\ell, u_{2\ell-i-1} = (c,d). \end{cases}$$

If $f \in \text{Aut}(\{0,1\}^{\mathbb{Z}})$, abusing notation we define an action of f on words of the form $v = aw_{i_1}aw_{i_2}a \cdots aw_{i_\ell}a$ by

$$\phi(f)(v) = \psi^{-1}(\pi^{-1}(f(\pi(\psi(v))^{\mathbb{Z}})_{[0,2\ell-1]})),$$

where by $\pi(\psi(v))^{\mathbb{Z}}$ we denote the unique point y with σ -period 2ℓ and $y_{[0,2\ell-1]} = \pi(\psi(v))$. Intuitively, this means applying the local rule of f ‘on the top track’ of the word $\psi(v)$, the left-right reverse of its local rule on the bottom track, and turning around corners in a natural way, to simulate an action of f on a periodic point of period 2ℓ . Then ϕ is a homomorphism from $\text{Aut}(\{0,1\}^{\mathbb{Z}})$ to the permutation group of $\{0,1\}^{2\ell}$.

We now define $\phi(f)$ to X by applying $\phi(f)$ as defined above to maximal subwords of the form $aw_{i_1}aw_{i_2}a \cdots aw_{i_\ell}a$ (extending to the infinite case in the only possible consistent way), obtaining a homomorphism from $\text{Aut}(\{0,1\}^{\mathbb{Z}})$ to $\text{Aut}(X)$.

The images of this homomorphism do not commute with the action of G . To make them commute, note that the set positions of a point $x \in X$ where a symbol from A appears is preserved under the action of G . In particular, words of the form $bu_{i_1}bu_{i_2}b \cdots bu_{i_\ell}b$ that are in the G -orbit of a word $aw_{i_1}aw_{i_2}a \cdots aw_{i_\ell}a$

¹⁵Note that this preserves the property of G acting cellwise.

have no nontrivial overlaps for distinct b , ℓ and i_j . Thus, we modify the definition of the maps $\phi(f)$, and define them on such words $bu_{i_1}bu_{i_2}b\cdots bu_{i_\ell}b$ by conjugating by the unique $g \in G$ such that $gb = a$. \square

Note that centralizers of finite groups of automorphisms are precisely the automorphisms of G -SFTs [5] where G is finite and acts faithfully (though not necessarily freely), if a G -SFT is considered as a $(G \times \mathbb{Z})$ -dynamical system.

One may wonder if there is a compactness result about Ryan's theorem stating that any set of automorphisms having trivial centralizer in fact has a finite subset with this property. This is doubtful, as if there exists a locally finite group acting by automorphisms and having a trivial centralizer, then there is no such compactness result by the previous theorem. However, we do not attempt to construct such an action here.

7.4 Full shifts on other groups

In the introduction we emphasized the mixing SFTs as a natural setting for the result. Another natural setting are full shifts on more general groups [12]. There are technical difficulties with generalizing the result to torsion groups (already in the abelian case). Namely, finite points can have nontrivial stabilizers when G has torsion elements:

Proposition 7.3. *Let G be a countable group and $\Sigma \ni 0$ a nontrivial alphabet. Then there is a nonzero finite point $x \in \Sigma^G$ with a nontrivial stabilizer if and only if G has a torsion element. In particular the automorphism group of a full shift on a non-torsion-free group never acts transitively on nonzero finite points.*

Proof. For the first claim, let x be a finite nonzero point with a nontrivial stabilizer, and suppose $g \neq 1$ and $gx = x$. Let $A \subset G$ be the support of x , so that the support of gx is $gA = A$. Then g acts bijectively on the finite set $A \subset G$ by $a \mapsto g \cdot a$, so that $g^n \cdot a = a$ for some n and $a \in A$. It follows that $g^n = 1$, and g is a torsion element. Conversely, if $g^n = 1$, define $x \in \Sigma^G$ by $x_h = 1 \iff h \in \langle g \rangle$. Then $gx = x$.

For the second claim, defining $y_h = 1 \iff h = 1$ we have $gy \neq y$ for any $g \neq 1$. If $gx = x$, then no automorphism can take x to y . \square

As for torsion-free groups, the proof of the main theorem seems to generalize directly to \mathbb{Z}^d and the same idea seems to work more generally on biorderable groups, but the general case is harder, since it is hard to make heads appear in a controlled way without knowing the geometry of the group.

Question 7.4. *Let $\Sigma = \{0, 1, 2, 3\}$, and let G be finitely generated and torsion-free. Is there a finitely generated subgroup of $\text{Aut}(\Sigma^G)$ that acts ∞ -transitively on the nonzero finite points?*

In the case of nontrivial torsion, one could of course require only transitivity between finite points with the same stabilizer, or alternatively only consider finite points with a trivial stabilizer, to get a definition for an action to be ‘as transitive as possible’, and ask similar questions.

7.5 Finite witnesses for not being a shift map

The following lemma was needed in the introduction.

Lemma 7.5. *Let X be a pointed mixing SFT and $g \in \text{Aut}(X) \setminus \langle \sigma \rangle$. Then there is a nonzero finite point $x \in X$ such that $g(x) \notin \mathcal{O}(x)$.*

Proof. We may suppose $g(0^{\mathbb{Z}}) = 0^{\mathbb{Z}}$, as the claim is trivial otherwise. Let r be the radius of g , that is, the minimal $r \in \mathbb{N}$ such that $g(x)_i$ is uniquely determined by $x_{[i-r, i+r]}$. Consider a point where a pattern $0^m u 0^m$ occurs, where $m \geq 2r$ and u is nonzero. Since g is an automorphism, there must be a nonzero symbol at distance at most r from the support of u , since otherwise $\dots 000.u000\dots$ is mapped to $0^{\mathbb{Z}}$. It follows that for any point $x = \dots 000.u0^m v 000\dots$, if $g(x) = \sigma^k(x)$, then necessarily $|k| \leq r + |u|$. If $g \notin \langle \sigma \rangle$, then there is a point $y \in X$ such that $g(y) \notin \{\sigma^j(y) \mid j \in [-r - |u|, r + |u|]\}$. Picking $x = \dots 000.u0^m v 000\dots$ so that v contains a large central pattern of y , we obtain that $g(x)$ cannot be in the σ -orbit of x . \square

7.6 Basic facts about k

We defined the invariant $k(X)$ for a subshift X in Definition 3.1. Here we make some easy observations and ask some questions.

First, note that the automorphism group is always countable, so that we need not distinguish between infinities, justifying the a priori sloppy notation $k(X) = \infty$. The case $k(X) = 1$ cannot happen for any subshift X : if we can take $F = \{f\}$, then since $f \circ f = f \circ f$, f is a power of the shift. But then $F = \{\}$ suffices since every automorphism commutes with the shift. The case $k(X) = 0$ is equivalent to shift maps being the only automorphisms, which is common for minimal subshifts [37, 14, 15, 17]. It can also happen for trivial reasons, and in particular it is true for the minimal SFTs, that is, subshifts consisting of the orbit of one periodic point. The case $k(X) = \perp$ is equivalent to the center of the automorphism group containing an automorphism that is not a power of a shift, which is again common for minimal systems [9, 42, 20, 17] and can also happen for SFTs for trivial reasons, as it happens in the two-point subshift $X = \{0^{\mathbb{Z}}, 1^{\mathbb{Z}}\}$. By Ryan's theorem, $k(X) \neq \perp$ for all mixing SFTs. For the finite SFT $X_n = \{0^{\mathbb{Z}}, 1^{\mathbb{Z}}, \dots, (n-1)^{\mathbb{Z}}\}$ where $n \geq 3$ (in other words, the identity function on $\{0, \dots, n-1\}$), we have $k(X_n) = 2$ since symmetric groups are generated by two permutations and have trivial center. (For the general case of a finite subshift see Proposition 7.9.)

Question 7.6. *What is $k(X)$ for an infinite mixing SFT X ? Is it computable? Is it always finite? Is it always 2? Is $k(\text{Aut}(\{0, 1\}^{\mathbb{Z}})) = k(\text{Aut}(\{0, 1, 2\}^{\mathbb{Z}}))$?*

In the proof of Theorem 2.2, we needed symbol-permutations in addition to the generators of \mathcal{G} to ensure g fixes $0^{\mathbb{Z}}$. Two symbol-permutations suffice for this, so $k(\{0, 1, 2, 3\}^{\mathbb{Z}}) \leq 10$.

For a group G , write $k(G)$ for the cardinality of the smallest subset F of G that has trivial centralizer, that is, $\bigcap_{g \in F} C_G(g) = \{1_G\}$ if such F exists, and $k(G) = \perp$ otherwise (that is, when G has nontrivial center).

Lemma 7.7. *For every finite group G , there exists a minimal subshift X_G with $k(X_G) = k(G)$.*

Proof. Let X_G be a minimal subshift with $\text{Aut}(X_G) \cong G \times \mathbb{Z}$ where the \mathbb{Z} corresponds to powers of the shift. Such a subshift exists by [20, 17]. Then if $F \subset G$ is such that $\bigcap_{g \in F} C_G(g) = \{1_G\}$, there is clearly a corresponding set of automorphisms of size F , so that $k(X_G) \leq k(G)$. If $F \subset \text{Aut}(X_G)$ is a set of automorphisms, then these automorphisms are of the form $f_i \circ \sigma^{k_i}$ for some $k_i \in \mathbb{Z}$. Then $f \circ \sigma^k$ commutes with all of $f_i \circ \sigma^{k_i}$ if and only if f commutes with all of f_i . But this happens if and only if the f_i correspond to a subset of G with trivial centralizer. \square

I do not know what values $k(G)$ occur for finite groups G . If every value occurs, then it occurs also as $k(X)$ for a minimal subshift X by the lemma.

In the category of countable subshifts, we can have $k(X) = \infty$:

Example 7.8. Let $X \subset \{0, 1\}^{\mathbb{Z}}$ be the (Cantor-Bendixson rank 3 countable sofic) subshift where every word with at least 3 symbols 1 is forbidden. Then up to a shift, every automorphism is simply a finite-support permutation of \mathbb{N} (as it permutes the distance of two 1s). Thus if F is any finite set of automorphisms, we can assume it to come from a finite set of finite-support permutations P of \mathbb{N} . Any permutation π that is the identity on the support of the permutations in P commutes with them, and automorphisms corresponding to such π need not be shift maps. On the other hand, the automorphism group is easily seen to have only shifts in its center, so $k(X) = \infty$.

In the category of finite subshifts (which are just permutations on a finite set), it is easy to solve the possible values of $k(X)$ by a bit of case analysis.

If X is a nonempty finite subshift, then the shift map $\sigma : X \rightarrow X$ is a permutation. Let c_i be the number of cycles of length i in the cycle decomposition of σ . Let $P = \{i \mid c_i \geq 1\}$ and $n = |P \cap [2, \infty)|$. If $P \cap [2, \infty) = \{\ell\}$ let $c = c_\ell$ and otherwise let $c = \perp$.

Proposition 7.9. *Let X be a nonempty finite subshift, and let c_i, P, n, c be as above. Then $k(X) \in \{\perp, 0, 2\}$ and*

$$\begin{aligned} k(X) = \perp &\iff c_1 = 2 \vee n \geq 2, \\ k(X) = 0 &\iff c_1 \in \{0, 1\} \wedge (n = 0 \vee (n = 1 \wedge c = 1)), \\ k(X) = 2 &\iff (c_1 \geq 3 \wedge n < 2) \vee (c_1 \neq 2 \wedge n = 1 \wedge c \geq 2). \end{aligned}$$

Proof. We perform a case analysis based on the values of c_1 , n and c . The Boolean formulas in the statement are obtained by picking the corresponding rows.

c_1	n	c	$k(X)$	reason(s)
0	0	\perp	0	$X = \emptyset$
0	1	1	0	(c)
0	1	≥ 2	2	(d)
0	≥ 2	\perp	\perp	(a)
1	0	\perp	0	$ X = 1$
1	1	1	0	(c)
1	1	≥ 2	2	(d)
1	≥ 2	\perp	\perp	(a)
2	0	\perp	\perp	(b)
2	1	1	\perp	(b)
2	1	≥ 2	\perp	(b)
2	≥ 2	\perp	\perp	(a), (b)
≥ 3	0	\perp	2	(e)
≥ 3	1	1	2	(e)
≥ 3	1	≥ 2	2	(d), (e)
≥ 3	≥ 2	\perp	\perp	(a)

The subshift X is a disjoint union of the subsystem consisting of cycles of cycle length 1 (fixed points), which we call the *unary part*, and the rest of the points, which we call the *cycle part*. The reasons in the table are the following:

- (a) there are cycles of multiple lengths, which we can cycle independently
- (b) there are exactly two unary points, so their transposition is in the center
- (c) there is only one nontrivial cycle, so automorphisms are shifts
- (d) the cycle part of X requires 2 automorphisms, and two suffice (see below)
- (e) the unary part of X requires 2 automorphisms, and two suffice

Note that in the case $c_1 \geq 3, n = 1, c \geq 2$, naively dealing separately with the unary part and the cycle part of X , we need four generators – two generators for each part. However, automorphisms do not mix these parts, so we need only two generators in total to reduce the centralizer to shifts, by using the same automorphisms to generate both parts. All of the observations used above are all either trivial or basic permutation theory, except (d) which may require a short explanation. This explanation is provided below.

By restricting to the cycle part of X , we may suppose that all cycles of X have the same length $\ell \geq 2$ and there are $c \geq 2$ such cycles. We show that $k(X) = 2$. Let $X = \mathbb{Z}_\ell \times \mathbb{Z}_c$ where dynamics $\sigma : X \rightarrow X$ is given by incrementation in all the components $\mathbb{Z}_\ell \times \{i\}$.

Let $f : X \rightarrow X$ be any bijection commuting with σ . Then f satisfies

$$\forall n, i : \exists n', i' : \forall j : f(n + j, i) = (n' + j, i').$$

The lower bound $k(X) \geq 2$ follows since $\text{Aut}(X)$ is non-abelian. If $c = 2$, then $k(X) = 2$, by taking $F = \{a, b\}$ where $a(n, 0) = (n + 1, 0)$ and $a(n, 1) = (n, 1)$,

and $b(n, i) = (n, i + 1)$. Namely, consider any bijection $f : X \rightarrow X$ commuting with a , b and σ . If $f(n, i) = (n', i')$ where $i = 0 \neq 1 = i'$, then $(a \circ f)(n, i) = a(n', i') = (n', i')$ and $(f \circ a)(n, i) = f(n + 1, i) = (n' + 1, i')$, so f does not commute with a . It follows that f preserves orbits, that is, $f(n, i) \in \mathbb{Z}_\ell \times \{i\}$ for all n, i . Commutation with b implies that f is a power of σ .

We also have $k(X) = 2$ for larger c : define $F = \{a, b\}$ where a and b are defined as follows: $a(n, 0) = (n, 1)$, $a(n, 1) = (n, 0)$ and $a(n, i) = (n, i)$ for $i \geq 2$, and $b(n, i) = (n, i + 1)$ for all n, i . Consider any bijection $f : X \rightarrow X$ commuting with a , b and σ . Observe that every permutation of the second component can be implemented with a and b . This implies that for all n, i , we have $f(n, i) = (n', i)$ for some n' , since the symmetric group on c elements has trivial center. By commutation with b , again f is a power of σ . \square

7.7 Other examples of ∞ -transitivity

We gave two examples of ∞ -transitivity in infinite groups in the introduction.

Example 7.10. Thompson's V is defined by its action on the half-open interval $[0, 1)$. This action is well-defined on the countable set of dyadic rationals, and on this set the action is ∞ -transitive.

Proof. We assume familiarity of the action of V on binary trees [11]. Let x_1, x_2, \dots, x_k be distinct dyadic rationals, and take n such that $x_i = k_i/2^n$ for all i and some $k_i \in [0, 2^n)$. Then a permutation π of the x_i can be implemented by permuting the n th level of the full binary tree. Every such permutation is in V. \square

Example 7.11. The topological full group of an infinite minimal subshift X is defined by its action on X . This action is well-defined on the (countable) shift-orbit of every point. There is a finitely generated subgroup of this group, namely its commutator subgroup, that is ∞ -transitive on every shift-orbit.

Proof. The commutator subgroup is finitely generated [33]. We sketch a proof that the commutator subgroup is ∞ -transitive on orbits directly, only using the assumption that X is aperiodic. Fix a point $x \in X$. Let k be arbitrary and let $n \in \mathbb{N}$. We show that we can permute the points $x^i = \sigma^{-i}(x)$ where $i \in [1, n]$ arbitrarily by an element of the commutator subgroup, proving ∞ -transitivity. Let π be any permutation of $[1, n]$.

First, we note that there exists a clopen set C such that $x \in C$, and $y \in C$ implies $\sigma^{-\ell}(y) \notin C$ for all $\ell \in [1, n+2]$. Namely, consider the word $w = x_{[-t', t']}$ for large t' . If $y_{[-t', t']} = w$ and $y_{[\ell-t', \ell+t']}$ for some ℓ , then x has a central pattern with period ℓ of length $t' - \ell$. Since X contains no ℓ -periodic points for any ℓ , for any individual ℓ there must be an upper bound t_ℓ on t' . Pick t to be the maximum of the t_ℓ for $\ell \in [1, n+2]$. Then $C = \{y \in X \mid y_{[-t, t]} = x_{[-t, t]}\}$ is the desired clopen set for some large enough t .¹⁶

¹⁶Alternatively, the existence of C can be seen by using the Marker Lemma [30] and such clopen sets are also the building blocks of Bratteli-Vershik representations of minimal subshifts.

Extend π to an even permutation of $[1, n+2]$ by acting either as a transposition or as identity on the two new elements. Given a point y , let $j(y) \in \mathbb{N}$ be minimal such that $\sigma^{j(y)}(y) \in C$ if such $j(y)$ exists (in the minimal case it always does) and otherwise $j(y) = \infty$. If $j(y) \in [1, n+2]$, define

$$f_\pi(y) = \sigma^{j(y)-\pi(j(y))}(y),$$

and otherwise define $f_\pi(y) = y$, so that f_π permutes the points $\sigma^{-i}(y)$ for $i \in [1, n+2]$ according to π whenever $y \in C$. Since the commutator subgroups of symmetric groups are the corresponding alternating groups, f_π is easily seen to be in the commutator subgroup of the topological full group of X . \square

Note that these examples are not about ‘orbit’-transitivity but normal transitivity. Orbit-transitivity is very specific to automorphism groups of dynamical systems (or more generally automorphisms of group-sets), and other types of groups would have their own ‘obvious restrictions’. For example, for linear groups we would require transitivity on linearly independent sets only, and for Thompson’s F and Thompson’s T we might only require transitivity on ordered sets of dyadic rationals rather than all tuples.

7.8 Commutator subgroup action on pointed mixing SFT

We sketch the proof that the commutator subgroup of the automorphism group of a pointed mixing SFT acts ∞ -orbit transitively on the set of nonzero finite points. Here it is useful to have a characterization of ∞ -orbit-transitivity in terms of permutations.

Lemma 7.12. *Let G and H be groups whose actions commute on a set X , and let $X_0 \subset X$ be a subset of X_0 closed under the action of H and containing infinitely many H -orbits. Then G acts ∞ -orbit-transitively on X_0 if and only if for every finite set (x_1, \dots, x_k) where the points x_i are from different H -orbits and every even permutation $\pi : \{1, \dots, k\} \rightarrow \{1, \dots, k\}$ there exists $g \in G$ such that $g(x_i) = x_{\pi(i)}$ for all i .*

Proof. Let (x_1, \dots, x_k) and (y_1, \dots, y_k) be k -tuples of elements of X_0 such that the elements x_i are pairwise in different H -orbits, and the same holds for the y_i as well, and we want to map x_i to y_i for all i . Since there are infinitely many disjoint H -orbits, we may assume k is even.

Let (z_1, \dots, z_k) be points with H -orbits distinct from those of the points x_i and y_j . The transformation $(x_1, \dots, x_k) \mapsto (z_1, \dots, z_k)$ is a restriction of the even permutation of $(x_1, \dots, x_k, z_1, \dots, z_k)$ that transposes x_i and z_i for all i , and thus by the assumption there exists $g \in G$ such that $g(x_i) = z_i$ for all i . We can deal with the transformation $(z_1, \dots, z_k) \mapsto (y_1, \dots, y_k)$ similarly, showing that G is ∞ -orbit-transitive on X_0 . \square

Note that we apply the assumption twice, and indeed we typically need to: the transformation $x \mapsto hx$ cannot be implemented by a permutation of a finite set of points from distinct H -orbits by an H -commuting action when h is not

a torsion element in H , as $gx = hx \implies g(h^k(x)) = h^k(g(x)) = h^{k+1}(x)$ so necessarily the orbit of x is infinite if g maps it to hx .

We also need the following sufficient condition for safety.

Lemma 7.13. *Let $\Sigma \ni 0$, let $V = \Sigma^n \setminus \{0^n\}$ and let $U \subset 0^n \Sigma^n 0^n \setminus \{0^{3n}\}$ satisfy*

$$0^{n+j} u 0^{n+j'}, 0^{n+\ell} u 0^{n+\ell'} \in U \implies j = \ell.$$

Then U is a V -safe set of words.

Proof. The proof is similar to that of Lemma 5.7. The first condition of safety is clearly satisfied, since 0^{3n} is not in U and V contains all nonzero words. To see that the second is satisfied, note that points x such that $\chi_U(x) = \{0\}$ and $\chi_V(x) \subset [0, 2n]$, which are considered in the definition of safety, in fact contain only 0s outside the interval $[0, 3n - 1]$. If we change the central U -word, and obtain a second occurrence of a word of U , as in Lemma 5.7 the distance between the two occurrences would be at most n . This violates the assumption of the lemma. Similarly, we see that the points ...000.u000..., $u \in U$, prove the third condition of safety. \square

Theorem 7.14. *Let $X \subset \Sigma^{\mathbb{Z}}$ be a pointed mixing SFT. Then the commutator subgroup of $\text{Aut}(X)$ acts ∞ -orbit-transitively on the nonzero finite points.*

Proof. Let (x_1, \dots, x_k) be nonzero finite points with distinct σ -orbits, and suppose $k \geq 5$. It is enough to show that for any even permutation $\beta : [1, k] \rightarrow [1, k]$ there is an automorphism in the commutator subgroup that performs the corresponding permutation. The result then follows from Lemma 7.12.

Let $w_i = (x_i)_{[-3m, 3m-1]}$ for all i , where m is large enough so that the words w_i contain the supports of the point x_i and such that for all i , $w_i = 0^{2m} u_i 0^{2m}$ for some u_i , and m is larger than the window size of X .

Now, picking $n = 2m$, $U = \{w_1, w_2, \dots, w_k\}$, and $V = \Sigma^n \setminus \{0^n\}$, by the previous lemma U is V -safe (the assumption of the lemma being satisfied because the points x_i are from distinct orbits) and there is an automorphism of X implementing any $(n-1)$ -safe permutation (thus in fact any permutation) of U by Lemma 5.6.

Since β is an even permutation and $k \geq 5$, β can be written as a composition of commutators. Thus, the same is true in the automorphism group of X . \square

A corollary of this result is that if $k(X) = \infty$ for some mixing SFT X containing $0^{\mathbb{Z}}$, then the commutator subgroup of $\text{Aut}(X)$ cannot be finitely generated.

From the theorem above, one ‘almost’ obtains Ryan’s theorem for the commutator subgroup (see the next section). Ryan’s theorem is proved for the subgroup of commutator subgroup generated by commutators of involutions in [4, Proposition 4.11].

7.9 Making generators commutators

In this section we explain the minor changes needed to show that a group with the transitivity properties we want can also be obtained in the commutator, in view of Theorem 7.14 and Question 3.7. We also show that all generators can be written as a composition of involutions.

Theorem 7.15. *For $\Sigma = \{0, 1, 2, 3\}$ there is a finite set F such that $\langle F \rangle$ acts ∞ -orbit-transitively on the set of nonzero finite points $x \in \Sigma^{\mathbb{Z}}$, and each element of F is a commutator of two automorphisms, and a composition of involutive automorphisms.*

Proof sketch. The ∞ -orbit-transitive group constructed in Theorem 6.6 is

$$\mathcal{G} = \langle \mathcal{G}_3, P, g_{(13)}, g_{(23)} \rangle \leq \text{Aut}(\Sigma^{\mathbb{Z}}).$$

Most of the generators are not of the required form; $g_{(13)}$ is an involution, but it is not in the commutator subgroup because it performs an odd permutation on $\{0^{\mathbb{Z}}, 1^{\mathbb{Z}}, 2^{\mathbb{Z}}, 3^{\mathbb{Z}}\}$ (which means it has a nontrivial image in some abelian quotient of $\text{Aut}(\Sigma^{\mathbb{Z}})$). For example the homomorphism constructed in [21] gives a nontrivial image for P in a torsion-free abelian group, implying that P is not in the commutator, and is not generated by involutions.

We revisit every step of our construction to obtain generators of the required form. We need the combinatorial fact about the symmetric group S_4 that an involution consisting of two disjoint cycles is a commutator:

$$(0 \ 1)(2 \ 3) = [(0 \ 3)(1 \ 2), (0 \ 3 \ 1 \ 2)] = (0 \ 3)(1 \ 2) \circ (0 \ 3 \ 1 \ 2) \circ (0 \ 3)(1 \ 2) \circ (0 \ 3 \ 1 \ 2)^{-1}.$$

We start with the particle rule P . Let Q be the rule the moves particles to the right and walls to the left, that is, $Q = Q' \circ Q''$ where Q' is the transposition $(1 \ 2)$ (which transposes particles and walls) and $Q'' = P \circ Q' \circ P^{-1}$. This is not immediately seen to be in the commutator, but $Q^2 = Q' \circ Q'' \circ Q' \circ Q'' = [Q', Q'']$ is. We replace P by Q^2 in our set of generators.

Assuming that other generators are not changed, \mathcal{G}_3 is generated by our generators. We conjugate the generators of \mathcal{G}_3 by P , P^2 and P^3 to obtain groups \mathcal{G}_3^2 , \mathcal{G}_3^3 and \mathcal{G}_3^4 which act just like \mathcal{G}_3 , but in ‘heads’, there is a offset 1, 2 or 3 between the particle and the wall.

We can now go through the proof of the main theorem: we first construct a good vector using $g_{(13)}$ and $g_{(23)}$ and Q^2 , and once we have a good vector we apply Q^{-2} until the rightmost particle of some configuration in our vector gets within distance at most 3 to the left of a wall. With four applications of Lemma 5.9, using the correct conjugate of \mathcal{G}_3 , we can perform any operations simultaneously in all coordinates of the vector where this happens. In particular, we can freely organize positions and times where a head appears when Q^2 is applied repeatedly, and move all heads far enough to the right not to affect subsequent steps. This shows that we can replace P by Q^2 in the generating set, and Q^2 is a commutator generated by involutions.

While $g_{(13)}$ and $g_{(23)}$ are not in the commutator subgroup, we note that the only important property of $g_{(23)}$ is that it allows turning prepgood vectors into pregood ones. For this we need that in a word containing only walls it introduces at least one particle, does not remove every wall, and does not eliminate every particle in a word containing only particles.

We can reproduce the behavior of $g_{(23)}$ as follows: Consider a prepgood vector $\vec{x} \in X_0^{(k)}$. First, apply the automorphism that performs the permutation $(0200\ 0210) \circ (0220\ 0230)$ in every coordinate where it applies. A short case analysis shows that this rule gives a well-defined involutive automorphism, which can be written as a commutator as in the second paragraph of the proof. When applied to a subword $w \in \{0, 2\}^*$ of a configuration, it introduces a particle to the right of, or on top of, the rightmost wall, unless there are three walls at the right end of the word. We then repeatedly apply the particle rule. After this, all points that contain walls and do not contain at least three walls as their rightmost symbols contain particles, and still every coordinate of \vec{x} is prepgood. Then use the automorphism implementing the permutation $(22000\ 22010) \circ (22020\ 22030)$. This is again well-defined and is a commutator, and it introduces particles in all coordinates of \vec{x} that contain(ed) at least two walls as their rightmost symbols. After again applying the particle rule, we get that every coordinate of the resulting vector contains a particle, giving a pregood vector. To get good vectors, we replace $g_{(13)}$ by two automorphisms in a symmetric way.

As for the replacement of \mathcal{G}_3 , we know that it is enough to take $f_{\pi,s}$ with $\pi : A^\ell \rightarrow A^\ell$ taken from a finite set of even permutations, by Lemma 5.2 and a slight modification of the proof of Lemma 5.4. The only problem is that the coordinate swap $(ab\ ba)$, which is needed to apply rules to arbitrary subsequences, does not give an even permutation of words (since our alphabet is of odd cardinality). However, one can use even coordinate permutations to obtain a finite generating set for $\langle G''_0, \sigma \rangle$, and G''_0 already acts ∞ -transitively by Lemma 5.4. Even permutations are generated by pairs of disjoint two-cycles when ℓ is large enough, since large enough alternating groups are simple and cycle type is conjugacy invariant, so each $f_{\pi,s}$ can be written as a composition of involutions that are in the commutator as in the second paragraph of the proof.

Finally we replace $f_{\sigma,s}$ by a map that is a composition of involutions that are commutators. For this, we retrace the steps of the proof of Lemma 5.8, but when defining π we pick a large m and use four sets: $U_1 = \{A^{m+1}sA^{m-1}\}$, $U_2 = \{A^m s A^k s A^{m-1-k} \mid k \in \{0, \dots, n-2\}\}$, $U_3 = \{A^m s A^{n+k} s A^{m-n-1-k} \mid k \in \{0, \dots, n-2\}\}$, and $U_4 = \{A^m s A^{2n+k} s A^{m-2n-1-k} \mid k \in \{0, \dots, n-2\}\}$. All of these sets have cardinality $(n-1)^{2m}$, and are disjoint. Now we can have π act on $U_1 \cup U_2$ as an involution, mapping $\pi(U_i) = U_{3-i}$, and similarly defining π on $U_3 \cup U_4$ in an involutive way, to get an involution π on $U_1 \cup U_2 \cup U_3 \cup U_4$.

The lengths $2m + 1$ can be chosen to be divisible by three, and for large enough m , Lemma 5.7 applies, and we can perform π by a local rule by Lemma 5.6. On U , π can be written as a composition of pairs of cycles, and thus as a com-

position of involutions that are also commutators, as in the second paragraph of the proof. Thus the automorphism f_π , obtained from Lemma 5.6, can be written in terms of automorphisms that are involutions and commutators because the map γ obtained from the lemma is a group homomorphism. We deal with τ similarly, obtaining a map f which is a composition of involutions that are commutators, and acts as $f_{\sigma,s}$ on $Y_{1,s}$. \square

We also obtain a version of Theorem 2.2 in this setting.

Theorem 7.16. *For $\Sigma = \{0, 1, 2, 3\}$ there is a finite set $F \subset \text{Aut}(\Sigma^\mathbb{Z})$ such that each element of F is a commutator of two automorphisms, and a composition of involutive automorphisms, and if f commutes with every $g \in F$, then $f \in \langle \sigma \rangle$.*

Proof. If f commutes with the cellwise symbol-permutation $(1\ 2\ 3)$ (which is a commutator of two automorphisms and a composition of involutive automorphisms), then it maps $0^\mathbb{Z}$ to $0^\mathbb{Z}$. We conclude as in the proof of Theorem 2.2 using Theorem 7.15. \square

Acknowledgements

I thank Thomas Worsch for discussions on transitivity and reversibility of the action of the monoid of cellular automata, which lead to the study of the corresponding questions for the automorphism group. I thank the referee for their comments, in particular for spotting an error in the proof of the predecessor of Lemma 5.9 and several smaller mistakes, which led to the rewriting of many parts of the paper, and for suggesting that I prove Theorem 7.14 (which was part of Question 3.7 originally). I thank Jarkko Kari for Lemma 5.8, which was originally a question – this led to a serious rewrite, which in turn led to the addition of Theorem 7.15. I thank Johan Kopra for suggesting the symbol permutation $(1\ 2\ 3)$ in the last theorem. I thank the support of COST Action IC1405.

References

- [1] Sebastián Barbieri, Jarkko Kari, and Ville Salo. *The Group of Reversible Turing Machines*, pages 49–62. Springer International Publishing, Cham, 2016.
- [2] Tim Boykett. Closed Systems of Invertible Maps. *ArXiv e-prints*, December 2015. Available at <https://arxiv.org/abs/1512.06813>.
- [3] Tim Boykett, Jarkko Kari, and Ville Salo. *Strongly Universal Reversible Gate Sets*, pages 239–254. Springer International Publishing, Cham, 2016.
- [4] M. Boyle and S. Chuysurichay. The Mapping Class Group of a Shift of Finite Type. *ArXiv e-prints*, April 2017. Available at <https://arxiv.org/abs/1704.03916>.

- [5] M. Boyle, T. Meier Carlsen, and S. Eilers. Flow Equivalence of G-SFTs. *ArXiv e-prints*, December 2015. Available at <https://arxiv.org/abs/1512.05238>.
- [6] Mike Boyle. Some sofic shifts cannot commute with nonwandering shifts of finite type. *Illinois J. Math.*, 48(4):1267–1277, 2004.
- [7] Mike Boyle. Open problems in symbolic dynamics. In *Geometric and probabilistic structures in dynamics*, volume 469 of *Contemp. Math.*, pages 69–118. Amer. Math. Soc., Providence, RI, 2008.
- [8] Mike Boyle and Ulf-Rainer Fiebig. The action of inert finite-order automorphisms on finite subsystems of the shift. *Ergodic Theory and Dynamical Systems*, 11(03):413–425, 1991.
- [9] Mike Boyle, Douglas Lind, and Daniel Rudolph. The automorphism group of a shift of finite type. *Transactions of the American Mathematical Society*, 306(1):pp. 71–114, 1988.
- [10] Mike Boyle and Selim Tuncel. Infinite-to-one codes and markov measures. *Transactions of the American Mathematical Society*, 285(2):657–684, 1984.
- [11] James W. Cannon, William J. Floyd, and Walter R. Parry. Introductory notes on Richard Thompson’s groups. *Enseignement Mathématique*, 42:215–256, 1996.
- [12] T. Ceccherini-Silberstein and M. Coornaert. *Cellular Automata and Groups*. Springer Monographs in Mathematics. Springer-Verlag Berlin Heidelberg, 2010.
- [13] Ruth Charney. An introduction to right-angled artin groups. *Geometriae Dedicata*, 125(1):141–158, 2007.
- [14] E. Coven and R. Yassawi. Endomorphisms and automorphisms of minimal symbolic systems with sublinear complexity. *ArXiv e-prints*, November 2014. Available at <https://arxiv.org/abs/1412.0080>.
- [15] Van Cyr and Bryna Kra. The automorphism group of a shift of subquadratic growth. *Proceedings of the American Mathematical Society*, 144(2):613–621, 2016.
- [16] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163. Springer, New York, NY, 1996.
- [17] Sebastian Donoso, Fabien Durand, Alejandro Maass, and Samuel Petite. On automorphism groups of low complexity subshifts. *Ergodic Theory and Dynamical Systems*, 36(01):64–95, 2016.
- [18] Joshua Frisch, Tomer Schlank, and Omer Tamuz. Normal amenable subgroups of the automorphism group of the full shift. *Ergodic Theory and Dynamical Systems*, pages 1–9, 2017.

- [19] Gustav A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory*, 3:320–375, 1969.
- [20] B. Host and F. Parreau. Homomorphismes entre systèmes dynamiques définis par substitutions. *Ergodic Theory and Dynamical Systems*, 9:469–477, 8 1989.
- [21] Jarkko Kari. Representation of reversible cellular automata with block permutations. *Theory of Computing Systems*, 29:47–61, 1996. 10.1007/BF01201813.
- [22] Jarkko Kari. Theory of cellular automata: a survey. *Theoret. Comput. Sci.*, 334(1-3):3–33, 2005.
- [23] Jarkko Kari. Universal pattern generation by cellular automata. *Theor. Comput. Sci.*, 429:180–184, 2012.
- [24] Jarkko Kari and Nicolas Ollinger. Periodicity and immortality in reversible computing. In *Proceedings of the 33rd international symposium on Mathematical Foundations of Computer Science*, MFCS ’08, pages 419–430, Berlin, Heidelberg, 2008. Springer-Verlag.
- [25] K. H. Kim and F. W. Roush. On the automorphism groups of subshifts. *Pure Mathematics and Applications*, 1(4):203–230, 1990.
- [26] Ki Hang Kim, F. W. Roush, and J. B. Wagoner. Characterization of inert actions on periodic points, Part I. In *Forum Mathematicum*, volume 12, pages 565–602, 2000.
- [27] Ki Hang Kim, F. W. Roush, and J. B. Wagoner. Characterization of inert actions on periodic points. Part II. In *Forum Mathematicum*, volume 12, pages 671–712, 2000.
- [28] Yves Lafont. Towards an algebraic theory of boolean circuits. *Journal of Pure and Applied Algebra*, 184:2003, 2003.
- [29] D. A. Lind. The entropies of topological markov shifts and a related class of algebraic integers. *Ergodic Theory and Dynamical Systems*, 4:283–300, 6 1984.
- [30] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding*. Cambridge University Press, Cambridge, 1995.
- [31] Douglas Lind and Klaus Schmidt. Homoclinic points of algebraic \mathbb{Z}^d -actions. *Journal of the American Mathematical Society*, 12(4):953–980, 1999.
- [32] Ville Lukkarila. Sensitivity and topological mixing are undecidable for reversible one-dimensional cellular automata. *J. Cellular Automata*, 5(3):241–272, 2010.

- [33] Hiroki Matui. Some remarks on topological full groups of cantor minimal systems. *International Journal of Mathematics*, 17(02):231–251, 2006.
- [34] Kevin McGoff. Random subshifts of finite type. *Ann. Probab.*, 40(2):648–694, 03 2012.
- [35] Masakazu Nasu. Textile systems for endomorphisms and automorphisms of the shift. *Mem. Amer. Math. Soc.*, 114(546):viii+215, 1995.
- [36] Masakazu Nasu. Textile systems and one-sided resolving automorphisms and endomorphisms of the shift. *Ergodic Theory and Dynamical Systems*, 28:167–209, 2 2008.
- [37] Jeanette Olli. Endomorphisms of sturmian systems and the discrete chair substitution tiling system. *Dynamical Systems*, 33(9):4173–4186, 2013.
- [38] J. Patrick Ryan. The shift and commutativity. *Mathematical systems theory*, 6(1-2):82–85, 1972.
- [39] Ville Salo. *Subshifts with Simple Cellular Automata*. PhD thesis, University of Turku, 2014.
- [40] Ville Salo. A note on subgroups of automorphism groups of full shifts. *Ergodic Theory and Dynamical Systems*, page 113, 2016.
- [41] Ville Salo. Transitive action on finite points of a full shift and a finitary Ryan’s theorem. *ArXiv e-prints*, October 2016. Available at <https://arxiv.org/abs/1610.05487v1>.
- [42] Ville Salo. Toeplitz subshift whose automorphism group is not finitely generated. *Colloquium Mathematicum*, 146:53–76, 2017.
- [43] Ville Salo and Ilkka Törmä. Color blind cellular automata. *J. Cellular Automata*, 9(5-6):477–509, 2014.
- [44] Peter Selinger. Reversible k-valued logic circuits are finitely generated for odd k. *ArXiv e-prints*, April 2016. Available at <https://arxiv.org/abs/1604.01646>.