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

Ville Salo

October 19, 2016

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. We ask many related questions and mention some easy transitivity results in 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 [29]. The *automorphism group* of a subshift X is the set of homeomorphisms $f : X \to X$ 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, 8, 24]. Many group-theoretic questions about it are undecidable [24, 23, 38]. Ryan's theorem [35] states that the center of this group is as it possible could be, namely the group of shifts $\langle\sigma\rangle$. More generally, in [18] it is shown that normal amenable subgroups consist of shift maps.

[1] Mixing 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.

The finitely generated subgroups of an infinitely generated group are in many respects the essense of the group.[2] Much is known about the set of finitely generated subgroups of $\mathrm{Aut}(X)$ for mixing SFTs X as abstract groups: It contains the trivial group and is closed under subgroups, free and direct products [38] and extensions by finite groups [24] and contains the right-angled Artin groups (also known as 'graph groups') [24, 13]. On the side of limitations, we know that all groups it contains are residually finite and have a decidable word problem [8].

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 [8, 7, 26, 25, 6]. It is also known that the action is 'as topologically transitive as possible', in the sense that every aperiodic point has dense orbit [8]. See also [29] for a discussion of this group.

Actions of individual automorphisms (as $\mathbb{Z}$-actions) have been studied quite a bit. Their expansivity is a very interesting topic [32, 5, 33] and no characterization of this property is known. Many results about possible dynamics and undecidability results are known for these actions, and often proved under the name reversible cellular automata [21, 23, 30].

2 The results

In this article, we begin the study of actions of finitely generated (noncommutative) subgroups of $\mathrm{Aut}(X)$. We construct a particular finitely generated subgroup of $\mathrm{Aut}(X)$ 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 *finite points*, that is, points having finite support. More precisely, for any k and every pair of k-tuples $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ of nonzero points of finite support, there is an element $f \in G$ such that $(y_1, \ldots, y_k) = (f(x_1), \ldots, f(x_k))$, 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 1. *For $\Sigma = \{0,1,2,3\}$ there is a finitely generated subgroup of $\mathrm{Aut}(\Sigma^{\mathbb{Z}})$ that acts ∞-orbit-transitively on the set of finite points $x \in \Sigma^{\mathbb{Z}}$.*

We prove this in Theorem 4. The finite points are a natural set to study, since they are preserved by the automorphism group[3] 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 finite points into another one by a finite composition of them. Proving this is equivalent to proving that we can perform any

[2]Many properties of interest are local, for example amenability, residual finiteness and soficness. Topological full groups and automorphism groups of subshifts on a group G are direct limits of the corresponding groups on the finitely generated subgroups of G due to the existence of local rules.

[3]More 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.

permutation of any finite set of points from different orbits, which is equivalent to the fact that given any set of finite points from different orbits, we can swap two of them without changing the others. (Our proof is not essentially simplified by these observations, so we use the first definition.)

An interesting corollary of this theorem is the following stronger version of Ryan's theorem [35] (on the four-symbol full shift):

Theorem 2. *For* $\Sigma = \{0,1,2,3\}$ *there is a finite set* $F \subset \mathrm{Aut}(\Sigma^{\mathbb{Z}})$ *such that for* $g \in \mathrm{Aut}(\Sigma^{\mathbb{Z}})$*, 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 1.

Proof. Let F be the set of generators of the group in Theorem 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 finite-support point $x \in \{0,1,2,3\}^{\mathbb{Z}}$ such that $g(x)$ is not in the shift orbit of x by Lemma 13. 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. □

While F is finite in the statement of the theorem, the group $\langle F \rangle$ is infinite. This is necessary by the following result, proved in Lemma 11.

Lemma 1. *Let G be any finite group of automorphisms on a mixing SFT X. Then* $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}}) \leq \mathrm{Aut}(X)$ *by automorphisms that commute with G. In particular, the centralizer of a finite subgroup is never abelian.*

In the context of finite permutation groups, it is known that the only 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:

Example 1. 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. 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.

3 Questions

A result similar to Theorem 2 is known for the endomorphism monoid of a full shift [39], elaborated on in [36, 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.[4] Note that on any mixing SFT, the set $F \subset \mathrm{Aut}(\Sigma^{\mathbb{Z}})$ in Theorem 2 must be of size at least 2 and that the minimal cardinality of such F is an isomorphism invariant for $\mathrm{Aut}(X)$, implying that computing it could theoretically separate $\mathrm{Aut}(X)$ and $\mathrm{Aut}(Y)$ for some non-flip-conjugate mixing SFTs X, Y (which is an open problem [6]).

Definition 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 $g \in \mathrm{Aut}(\Sigma^{\mathbb{Z}})$, 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 $\mathrm{Aut}(\Sigma^{\mathbb{Z}})$ in the proof of Theorem 1. The one in our proof has a reasonable[5] number of generators, but presumably many more than are needed.

Question 1. *In Theorem 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 Lemma 10). In fact no individual automorphism is even transitive on finite points,[6] but we cannot show that one cannot be transitive up to a shift.

Question 2. *Does there exist a nontrivial alphabet Σ and $f \in \mathrm{Aut}(\Sigma^{\mathbb{Z}})$ such that $\langle \sigma, f \rangle$ acts transitively on the set of finite points of $\Sigma^{\mathbb{Z}}$?*

In this context, we should mention the closely related result of Kari that finitely generated $\mathbb{Z}^2$-actions by automorphisms can be *topologically* transitive on points of finite support:

Theorem 3 ([22])**.** *Let $\Sigma = \{0,1,2,3,4,5\}$. Then there exists $f \in \mathrm{Aut}(\Sigma^{\mathbb{Z}})$ such that $\langle \sigma, f \rangle$ acts topologically transitively on the set of finite points $x \in \Sigma^{\mathbb{Z}}$.*

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 other mixing SFTs.

It is an open question whether a $\mathbb{Z}$-action can do the same:

Question 3 ([22])**.** *Does there exist a nontrivial alphabet Σ and $f \in \mathrm{Aut}(\Sigma^{\mathbb{Z}})$ such that $\langle f \rangle$ acts topologically transitively on the set of finite points of $\Sigma^{\mathbb{Z}}$?*

---

[4]In [36], 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.

[5]Less than 20 generators. See Section 7 for even more precision.

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

Often results about finite points are really results about pairwise asymptotic points in disguise (or the other way around). We note that Theorem 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 the automorphisms will necessarily also act on the tails in uncontrollable ways. Of course one can ask whether we could take any set of mutually asymptotic points and have transitivity up to this 'obvious' restriction:

Question 4. *Is there a finitely generated subgroup $G \leq \mathrm{Aut}(\Sigma^{\mathbb{Z}})$ 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?*

Another natural generalization would be to prove the result on (pointed) mixing SFTs in general. Our construction fails to prove this 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. Some[7] mixing SFTs, in particular the two-symbol full shift, do not have this property [28, 10]. Another difficulty is that the main technical tool, namely Turing machines implementing universal logic gates, uses 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 1 would be to find a natural subgroup of $\mathrm{Aut}(X)$ (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 my knowledge, the commutator subgroup could be a candidate for this:

Question 5. *Is the commutator subgroup of $\mathrm{Aut}(X)$ finitely generated for a mixing SFT X? Does it satisfy the statement of Theorem 1?*

4 Definitions

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.

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.*

[7] Most?

Definition 2. 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 $f : X \to X$ commutes with σ, we call it an *automorphism* of X. We write $\mathrm{Aut}(X)$ 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 pictures.

Definition 3. 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*[8] 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 $X_0' = X_0 \cup \{0^{\mathbb{Z}}\}$.

We now define our notions of transitivity for Theorem 1.

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

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

Thus $Z^{(k)}$ is the kth Cartesian power of Z with the additional restriction that coordinates should be from different orbits.

Definition 4. 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 $X^{(k)}$ 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 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 $\mathcal{O}(Y) = \bigcup_{y \in Y} \mathcal{O}(y)$.

Note that by the definition above, if there is a transitive G-action on an H-set, then necessarily every H-orbit has the same cardinality. In our application, we discuss finite points, whose stabilizers are trivial. (For this, we need the fact that $\mathbb{Z}$ is torsion-free, see Section 7.)

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

In the proofs, we deal with many subgroups of $\mathrm{Aut}(X)$, and for $F_1, F_2, \ldots, F_\ell$ individual automorphisms or sets of them, we write $\langle F_1, \ldots, F_k \rangle$ for the smallest subgroup of $\mathrm{Aut}(X)$ 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.

5 The generators and transitivity results

In this section, we give the finite set of automorphisms generating the group $\mathcal{G}$ acting ∞-orbit-transitively in Theorem 1. We also prove some technical auxiliary transitivity results, namely that the automorphism group of a full shift is transitive on certain marked configurations, that a finitely generated subgroup of the group of Turing machines acts ∞-transitively around configurations where the head is at the origin. We also define the 'reset system', a transitive monoid action used in the proof of the main theorem.

There are finite reversible gate sets generating the even permutations of Σ^n for any finite alphabet Σ and $n \in \mathbb{N}$, in the sense that there exists $k \in \mathbb{N}$ such that every even permutation of Σ^n for $n \geq k$ is a finite composition of bijections $\phi : \Sigma^k \to \Sigma^k$ applied to length-k subsequences of the coordinates. See [27, 2, 40] for formal definitions and proofs in the case when $|\Sigma|$ is odd (in which case also the odd permutations are finitely generated) and [3] for the case of even $|\Sigma|$. In [1], this observation is used to show that a certain group of reversible Turing machines is finitely generated. This is essentially a generalization of Lemma 2 below.

Definition 5. Let $N \subset \mathbb{Z}$ be finite. If $\pi : \Sigma^N \to \Sigma^N$ is a permutation, then the homeomorphism $P_\pi : \Sigma^\mathbb{Z} \to \Sigma^\mathbb{Z}$ 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*[9] with *neighborhood* N. We denote the group of self-homeomorphisms of $\Sigma^\mathbb{Z}$ generated by σ and the local permutations (of all finite neighborhoods) by G_0:

$$G_0 = \langle \sigma, P_\pi \mid \exists n \in \mathbb{N} : \pi : \Sigma^n \to \Sigma^n \text{ is a permutation} \rangle$$

[9] Here, and in many situations where we are discussing positions on a configuration of symbols, we mean 'local' in the topology of $\mathbb{Z}$, as in the 'local rule' of a cellular automaton. In terms of the topology of $\Sigma^\mathbb{Z}$, 'global permutation' would be more appropriate, as we are making large-scale changes at the origin, and keeping the small-diameter tails fixed.

In the terminology of [1], the group G_0 is called the group of oblivious one-state Turing machines in the fixed-tape model.

Lemma 2. *Let $X = \Sigma^{\mathbb{Z}}$. Then G_0 is finitely generated and acts ∞-transitively on the set of finite points X_0'.*

Proof. First, we prove finitely generatedness. Let G' be the subgroup of G_0 generated by σ and the local permutations with neighborhood $\{0, 1, \ldots, n-1\}$, where n is such that reversible gates with at most n inputs and outputs generate all even permutations of Σ^m for all m. From the result of [3] it follows that $n = 4$ suffices in general, and [2, 40] show that $n = 2$ suffices in the case of odd $|\Sigma|$.

We will show $G' = G_0$. For this, let $\pi : \Sigma^N \to \Sigma^N$ be arbitrary, where $N = \{0, 1, \ldots, m-1\}$ for some m. Since the swaps $(n\ n+1)$ generate the symmetric groups, and the 'coordinate swap' $P_{(ab\ ba)}$ and the shift are among our generators, we can apply arbitrary permutations to the coordinates of a point. By conjugating with such a reordering, we can apply a permutation of Σ^n to any ordered subset of coordinates in N with size at most n. By the assumption on n, π can be decomposed into such permutations, and thus so can P_π.

Next, let us show that G_0 acts ∞-transitively on X_0'. Let $\vec{x}, \vec{y} \in (X_0')^{(k)}$. 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 Σ^{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. $\square$

The idea is next to apply the previous lemma to show that the automorphism group of $\Sigma^{\mathbb{Z}}$ acts ∞-transitively around 'marked' configurations where for some $s \in \Sigma$, there is only one occurrence of s, which is at the origin. A naive way to do this would be to think of s as the head of a Turing machine (so that it marks the zero-cell G_0), translate local changes to local changes near s, and turn $\sigma \in G_0$ into movements of the head s. This seems difficult:

Question 6. *Let $\Sigma = \{0, 1, 2, 3\}$ and $s = 3$. Let Y_0 be the set of finite configurations in X_0 not containing the symbol s, and let $Y_1 \subset X_0$ be the set of nonzero finite configurations of X_0 containing s at the origin and having no other occurrence of s. Is there an automorphism $f \in \mathrm{Aut}(\Sigma^{\mathbb{Z}})$ with the following properties:*

- *if $x \in Y_0$ then $f(x) = x$, and*
- *if $x \in Y_1$ then $f(x)_0 = x_1$, $f(x)_1 = x_0$ and $f(x)_i = x_i$ for $i \notin \{0, 1\}$?*

In other words, the question is whether there is an automorphism of $\{0, 1, 2, 3\}^{\mathbb{Z}}$ that shifts the symbol 3 on finite configurations with only one occurrence of 3, and preserves all points not containing 3.

We do not solve this problem, and instead go around it. An easy way that does not require increasing the alphabet is to use two words as and bs as the head, for two distinct symbols $a, b \neq s$, as being a normal head and bs an evil head whose movement is left-right mirrored. Then colliding heads can simply change their type between normal and evil, a variant of a common technique for ensuring reversibility. This does not complicate the proof much, as we are very careful never to introduce an evil head when transforming our points. The theoretical possibility of conversion is simply needed to fill the local rule of the automorphism.

Let $s \in \Sigma \setminus \{0\}$. Let $Y_{0,s}$ (read: zero ss) be the set of nonzero finite configurations in X_0 not containing the symbol s, and for $a \in \Sigma \setminus \{s\}$ let $Y_{1,s,a} \subset X_0$ (read: one s, after a) be the set of nonzero finite configurations $x \in X_0$ with $x_{[-1,0]} = as$, having no other occurrence of s.

Lemma 3. *Let $s \in \Sigma \setminus \{0\}$ and $a, b \in \Sigma \setminus \{s\}$, $a \neq b$. Then there is a finitely generated subgroup $\mathcal{G}_{s,a,b}$ of $\mathrm{Aut}(\Sigma^{\mathbb{Z}})$ that acts trivially on $Y_{0,s}$ and on $Y_{1,s,c}$ for $c \notin \{a, b\}$, and is ∞-orbit-transitive around $Y_{1,s,a}$.*

Proof. Our generators will only modify the points at a bounded distance from an s-symbol, and only if the symbol immediately to the left of the s-symbol is a or b. Thus, $Y_{0,s}$ and $Y_{1,s,c}$ for $c \notin \{a, b\}$ will be fixed. We will never remove an s or add one, and thus we do not need to worry about what happens when more than one s occurs in the point. The idea of the proof is to think of the word as as the origin of $\mathbb{Z}$ and to apply the previous lemma around this word. We only need to make sure that our finitely many generators can be turned into automorphisms.

More precisely, let $A = \Sigma \setminus \{s\}$ and let G_0 be the finitely generated group of homeomorphisms of $A^{\mathbb{Z}}$ defined in Lemma 2. To each local permutation $\pi : A^{[-r,r]} \to A^{[-r,r]}$ in the finite generating set of G_0 we associate the CA $f_{\pi,s,a}$ defined by rewriting words $uasv$ where $u \in A^r, v \in A^{r+1}$ to $u'asv'$ where $u'v' = \pi(uv)$ and $|u'| = r$, whenever the symbol immediately after v is not s. Since occurrences of as are neither removed nor introduced, this gives a well-defined automorphism.

The more difficult part is turning the shift $\sigma \in G_0$ into an automorphism. Let $g \in \mathrm{Aut}(\Sigma^{\mathbb{Z}})$ be the automorphism defined as follows: for every $c \in A$, subwords asc that do not intersect another word of the form asc or cbs are rewritten to cbs, and similarly subwords cbs that do not intersect a word of the form asc or cbs are rewritten to asc. This is indeed an automorphism because $g^2 = \mathrm{id}$. Let $h \in \mathrm{Aut}(\Sigma^{\mathbb{Z}})$ be the automorphism that changes occurrences of as to bs and vice versa. Similarly $h^2 = \mathrm{id}$. Define $f_{\sigma,s,a,b} = h \circ g$.

On $Y_{1,s,a}$, $f_{\sigma,s,a,b}$ simply shifts the unique occurrence of as one step to the right.[10] It is then easy to see that the automorphisms $f_{\pi,s,a}$ and $f_{\sigma,s,a,b}$ yield a finitely generated subgroup

$$\mathcal{G}_{s,a,b} = \langle f_{\pi,s,a}, f_{\sigma,s,a,b} \mid \pi \in G_0 \rangle$$

of $\mathrm{Aut}(\Sigma^{\mathbb{Z}})$ with the required properties.[11] A finite generating set is obtained from any finite generating set of G_0. □

[10] When the head moves to the right, the configuration around it moves left from its viewpoint. Thus $f_{\sigma,s,a,b}$ corresponds to the left shift σ.

[11] Note, however, that we have *not* defined a group homomorphism from G_0 into $\mathrm{Aut}(\Sigma^{\mathbb{Z}})$. In fact there is no such homomorphism since G_0 is not residually finite but $\mathrm{Aut}(\Sigma^{\mathbb{Z}})$ is.

Definition 6. Let A, B be finite alphabets. The (A, B)*-particle rule* is the automorphism P of $(A \times B)^{\mathbb{Z}}$ defined by $P((x, y)) = (\sigma(x), y)$.

In the action of the particle rule, elements of A move to the left and elements of B stay put.

A *symbol permutation* is an automorphism $g_\pi : \Sigma^{\mathbb{Z}} \to \Sigma^{\mathbb{Z}}$ defined by a permutation $\pi : \Sigma \to \Sigma$ by $g_\pi(x)_i = \pi(x_i)$.

We need one more automorphism: We let S_s be the *side swap* that changes the pattern $abscd$ to $acsbd$ whenever $a, b, c, d \in \Sigma \setminus \{s\}$.

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

Definition 7. Let M be the free monoid generated by $(\mathbb{Z}\times\mathbb{N})^k$. Then generators $\vec{x} \in (\mathbb{Z} \times \mathbb{N})^k$ 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 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. Resetting each alarm clock at most k times, one proves the following lemma:

Lemma 4. *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 $m \cdot \vec{v} = (0, 0)^k$.*

In the proof of the main theorem, the positions $\mathbb{Z}$ will be positions of heads, and $\mathbb{N}$ will be represent the times when heads appear 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 sensibly on a finite set of points.

6 Proof of the main result

In this section, we prove the main result for the four-symbol full shift. 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 $n \mapsto (n \bmod 2, \lfloor n/2 \rfloor)$.

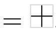
The ∞-orbit-transitive action will be given by the group

$$\mathcal{G} = \langle \sigma, \mathcal{G}_{3,0,2}, \mathcal{G}_{3,1,2}, P, g_{(13)}, g_{(23)}, S_3 \rangle$$

where $g_{(13)}$ is the symbol permutation $1 \leftrightarrow 3$, $g_{(23)}$ the symbol permutation $2 \leftrightarrow 3$ and S_3 the side swap CA.

We call 1 a *particle* and 2 a *wall*. We call 3 a *collision*, also understanding it as 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:

$0 =$, $1 =$, $2 =$, and $3 =$ .

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

Definition 8. A nonzero finite point is

- *prepregood* if it contains no collisions and all the particles are to the left of all the walls,
- *pregood* if it is prepregood and contains a particle,
- *good* if it is pregood and contains a wall,
- *great* if it contains exactly one collision which is at 0, $x_{-1} \neq 2$, and
- *marvelous* if it is great and $x_{-1} = 0$.

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

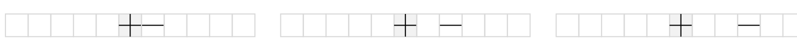
Note that great points are just the points in $Y_{1,3,0} \cup Y_{1,3,1}$ and marvelous points are the ones in $Y_{1,3,0}$.

6.1 Outline and example

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

$\vec{x} =$ 

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 can be used to transform $\vec{y}$ into any other vector. We use the marvelous vector

$\vec{y} =$ 

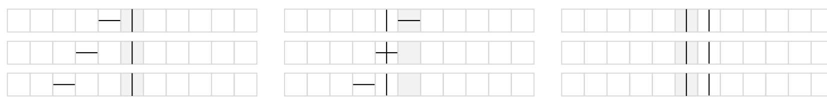
The outline of the proof is that we first make $\vec{x}$ prepregood, then pregood, then good by a few applications of the particle rule and symbol permutations. We then simulate the reset system using Lemma 3 to make $\vec{x}$ great, and finally make it marvelous using Lemma 8. A final application of Lemma 3 finishes the proof, turning $\vec{x}$ into $\vec{y}$.

Figure 1 shows how to do this, using Lemma 3 as a black box. We have taken some artistic liberties in Figure 1; it does not follow the proof to the letter.

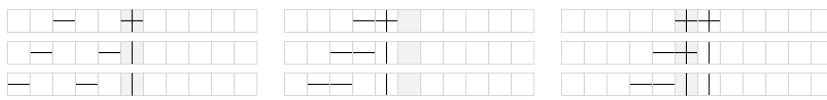
6.2 Making vectors good

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 prepregood, then pregood, and then good.

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



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



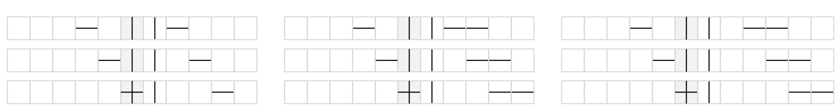
Our vector is now pregood. Were it not good, we would apply the symbol permutation $- \leftrightarrow +$ and apply the particle rule again. It happens to be good, so we omit this step. Next, we apply the inverse of the particle rule, and wait for collisions to appear in some of the components:

A collision appears in the third component. Applying Lemma 3 and S_3, we organize a new collision to happen at the origin of the third component after 4 applications of P^{-1}:

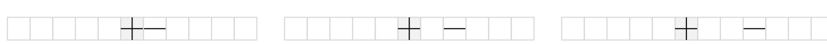
Apply P^{-1} until the next collision (that is, once):

Applying Lemma 3 (twice since $+$ has two different left neighbors) and S_3, 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 marvelous vector:



Applying Lemma 3, change the vector to $\vec{y}$:



In summary, for some T_1, T_2, T_3 provided by Lemma 3, we have obtained

$$\vec{y} = (T_3 \circ P^{-3} \circ S_3 \circ T_2 \circ P^{-1} \circ S_3 \circ T_1 \circ P \circ (| \leftrightarrow +) \circ P^3)(\vec{x}).$$

Figure 1: How to get from $\vec{x}$ to $\vec{y}$, using Lemma 3 as a black box.

Lemma 5. *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 collisions and all particles are to the left or all the walls in all components of $\vec{x}$, so $\vec{x}$ can be transformed to a prepregood vector $\vec{x}^2$.

Now, apply $g_{(23)}$ to the prepregood vector $\vec{x}^2$, turning particles into collisions, and repeat 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 $x = \vec{x}^2_i$ contains a particle before applying $g_{(23)}$, it still does after applying it and repeating P. If it contains a wall, then a collision is introduced, giving a particle after the application of P. Note that x must contain either a particle or a wall, since $x \in X_0$. We obtain that $\vec{x}^2$ an 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 $\vec{x}^4$. ∎

6.3 Making vectors marvelous

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 collision. 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 $\phi : C^{(k)} \to (\mathbb{Z} \times \mathbb{N})^k$ by associating to a clock-like point x the tuple (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.

Lemma 6. *Let $\vec{x} \in C^{(k)}$ and $\vec{v} \in (\mathbb{Z} \times \mathbb{N})^k$. Then there exists*

$$g \in \mathcal{G}' = \langle \mathcal{G}_{3,0,2}, \mathcal{G}_{3,1,2}, S_3 \rangle \leq \mathcal{G}$$

such that $\vec{x} \in C^{(k)}$ and $\phi(gP^{-1}(\vec{x})) = \vec{v}$ if and only if there exists $m \in (\mathbb{Z} \times \mathbb{N})^k$ such that $m\phi(\vec{x}) = \vec{v}$.

Proof. We show that applying an element of the form gP^{-1} where $g \in \mathcal{G}'$ 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 after the application of P^{-1}, no collision is introduced, and g behaves as identity on points without collisions. 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 $g \in \mathcal{G}'$ such that $\phi(gP^{-1}(\vec{x})) = m\phi(\vec{x})$. 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 $\mathcal{G}'$ that resets their next buzz times and positions according to the corresponding coordinates of m_i. Let $m_i = (n_i, t_i)$ for all i.

This is very easy: the fact that the points come from different σ-orbits means that we can really do any transformation we like using Lemma 3, as long as the relative positions of the heads do not change. The only problem is that some of the heads are of the form 13, and thus no matter where we put them, applying P^{-1} will give a collision at that symbol 3. We solve this by making the collisions 3 the rightmost symbols of the support and applying the swap automorphism S_3 as a final step, so that particles simply escape to infinity when we start applying P^{-1}.

We describe this in more detail. Note that for all $i \in I$ we have either $(P^{-1}(\vec{x}_i))_{[j-1,j]} \in \{03, 13\}$ for some (unique) j by the assumption that $\vec{x}_i$ is clock-like. Partition $I = I_0 \cup I_1$ based on these two cases. We first consider the case $i \in I_1$. Note that automorphisms of the form $f_{\pi,3,1}$ and $f_{\sigma,3,1,2}$ only modify components $P^{-1}(\vec{x})_i$ where $i \in I_1$. Namely, every other coordinate is in either $Y_{0,3}$ or $\mathcal{O}(Y_{1,3,0})$ where the maps $f_{\pi,3,1}$ and $f_{\sigma,3,1,2}$ act trivially.

On the components $P^{-1}(\vec{x})_i$ where $i \in I_1$, first apply $f^k_{\sigma,3,1,2}$ for some k so that the collisions are moved to the right of the values n_i. Let the collision on $\vec{y}_i = f^k_{\sigma,3,1,2}(P^{-1}(\vec{x})_i)$ be in coordinate k_i. Note that the points $\vec{y}_i$, $i \in I_1$, are from different σ-orbits by the definition of $C^{(k)}$. Now, use the ∞-transitivity of the action of $f_{\pi,3,1}$ and $f_{\sigma,3,1,2}$ on $Y_{1,3,1}$ given by Lemma 3 to, for all $i \in I_1$, transform $\vec{y}_i$ to the vector $\vec{z}_i$ where

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

Apply a similar transformation to the components indexed by I_0, now using $f_{\pi,3,0}$ and $f_{\sigma,3,0,2}$. So that the components $\vec{z}_i$, $i \in I_1$, are not modified. Finally apply S_3 (so the occurrences of 13 at $\{k_i - 1, k_i\}$ do not lead to collisions). $\square$

Lemma 7. *If $\vec{x}$ is good, then there exists $g \in \mathcal{G}'' = \langle \mathcal{G}_{3,0,2}, \mathcal{G}_{3,1,2}, S_3, P \rangle \leq \mathcal{G}$ 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. $\square$

The proof of Lemma 6 in fact gives a marvelous vector automatically, but for clarity of exposition we prove this separately.

Lemma 8. *If $\vec{x}$ is great, then there exists $g \in \langle \sigma, f_{\sigma,3,1,2}, f_{\sigma,3,0,2}, S_3 \rangle$ such that $g\vec{x}$ is marvelous.*

Proof. Let $\vec{x}' = \sigma^{-k} \circ f^{-k}_{\sigma,3,1,2} \circ f^{-k}_{\sigma,3,0,2}(x)$ for large enough k so that the support of each vector in $\vec{x}$ is contained in $\{-1,0\} \cup [2,\infty)$ and $(\vec{x}_i)_{[-1,0]} \in \{03, 01\}$. Then $S_3(\vec{x}')$ is marvelous. □

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 9. *If $\vec{x}$ is marvelous, then there exists $g \in \mathcal{G}_{3,0,2}$ such that $g\vec{x} = \vec{y}$.*

Proof. This is a direct corollary of Lemma 3. □

We can now prove our main theorem.

Theorem 4. *Let $X = \{0,1,2,3\}^{\mathbb{Z}}$. Then*

$$\mathcal{G} = \langle \sigma, \mathcal{G}_{3,0,2}, \mathcal{G}_{3,1,2}, P, g_{(13)}, g_{(23)}, S_3 \rangle \leq \mathrm{Aut}(X)$$

acts ∞-orbit-transitively on X_0.

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

- by Lemma 5 there exists $g \in \mathcal{G}$ such that $\vec{x}' = g\vec{x}$ is good,
- by Lemma 7, there exists $g' \in \mathcal{G}$ such that $\vec{x}'' = g'\vec{x}'$ is great,
- by Lemma 8, there exists $g'' \in \mathcal{G}$ such that $\vec{x}''' = g''\vec{x}''$ is marvelous, and
- by Lemma 9, 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. □

7 Notes

7.1 The number of generators

We have made little effort at minimizing the generating set. The group $\mathcal{G}_{3,0,2}$ 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 15 generators for the group $\langle \sigma, \mathcal{G}_{3,0,2}, \mathcal{G}_{3,1,2}, P, \pi_{(13)}, \pi_{(23)}, S_3 \rangle$. It is easy to drop off a few by a bit of thinking – for example, σ is only used in the transition from greatness to marvelousness, which is not needed in practise. However, it is difficult to make the set essentially smaller without a new idea, since the proof has multiple steps. All of the generators have neighborhood size at most 5.

It is also theoretically possible to find smaller generating sets also by computer search – any set of automorphisms generating our generators will naturally satisfy the conclusion of Theorem 1. We have not attempted this.

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.

Lemma 10. *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 [39], it was shown that there is a finite set of cellular automata on every large enough full shift having a trivial centralizer. A crucial difference between the monoid and group case is that the cellular automata of [39] 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:

Lemma 11. *Let G be any finite group of automorphisms on a mixing SFT X. Then there is an embedding $\phi : \mathrm{Aut}(\{0,1\}^{\mathbb{Z}}) \to \mathrm{Aut}(X)$ such that each $\phi(f)$ commutes with G.*

Proof. 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. 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 [29],[12] 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 of points $x \in X$ where no element of A appears has positive entropy, by possibly passing to yet another higher block presentation. Finally, we may assume that the forbidden patterns defining X are of size 2, again by passing to a higher block presentation.

Now, let m be such that there are at least 4 words of the form awa where $|w| = m$ and w contains no symbol in A, and enumerate them as $w_1, \ldots, w_4$.

[12] Note that this preserves the property of G acting cellwise.

Note that there exists such m because X is mixing and has a positive entropy of points not containing a. Then all words of the form $aw_{i_1}aw_{i_2}a\cdots aw_{i_\ell}a$ for $i_j \in [1,4]$ are in X. Such a finite word can be seen as presenting two words of $\{0,1\}^\ell$ through a bijection $\{w_1,w_2,w_3,w_4\} \leftrightarrow \{(0,0),(0,1),(1,0),(1,1)\}$. To such a word, we can apply any $f \in \mathrm{Aut}(\{0,1\}^\mathbb{Z})$ by applying its local rule on the top track and the left-right reverse of its local rule on the bottom track, turning around corners in a natural way, to simulate an action of f on a periodic point of period 2ℓ, so that this becomes a homomorphism from $\mathrm{Aut}(\{0,1\}^\mathbb{Z})$ to the permutation group of $(\{0,1\}^\ell)^2$. See [38] for more details. By applying this permutation in the 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), we obtain a homomorphism $\phi : \mathrm{Aut}(\{0,1\}^\mathbb{Z}) \to \mathrm{Aut}(X)$.

However, 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 $aw_{i_1}aw_{i_2}a\cdots aw_{i_\ell}a$ 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 $gb = a$. □

Note that centralizers of finite groups of automorphisms are precisely the automorphisms of G-SFTs [4] 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 nontrivial centralizer, then there is no such compactness result by the previous lemma. 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:

Lemma 12. *Let G be a countable group and $\Sigma \ni 0$ a nontrivial alphabet. Then there is a 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 the finite points.*

Proof. For the first claim, let x be a finite group with a nontrivial stabilizer g, so that $gx = x$. Let $A \subset G$ be the support of x, so that the support of gx is $gA = A$. But 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, define $y_h = 1 \iff h = 1$, then $gx = x$ and $gy \neq y$, so no automorphism can take x to y. $\square$

As for torsion-free groups, the proof 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 Turing machine heads appear in a controlled way without knowing the geometry of the group.

Question 7. *Let $\Sigma = \{0, 1, 2, 3\}$, and let G be torsion-free. Is there a finitely generated subgroup of $\mathrm{Aut}(\Sigma^G)$ 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 13. *Let X be a pointed mixing SFT and $g \in \mathrm{Aut}(X)$. Then there is a 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. 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. It follows that for any point $x = \ldots 000u0^m v000\ldots$, if $g(x) = \sigma^k(x)$, necessarily $|k| \leq r$. By picking v suitably, we can eliminate the finitely many choices. $\square$

7.6 Basic facts about k

We defined the invariant $k(X)$ for a subshift X in the Introduction. We make the 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 [34, 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 [8, 37, 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 $X_n = \{0^{\mathbb{Z}}, 1^{\mathbb{Z}}, \ldots, (n-1)^{\mathbb{Z}}\}$ where $n \geq 3$ (in other words, the identity function on $\{0, \ldots, n-1\}$), 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 1.)

Question 8. *What is $k(X)$ for a mixing SFT X? Can it be computed? Is it always finite? Is it always 2? Do we have $k(\mathrm{Aut}(\{0,1\}^{\mathbb{Z}})) = k(\mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}}))$?*

In the proof of Theorem 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 $k(\{0,1,2,3\}^{\mathbb{Z}}) \leq 17$.

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 14. *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 $\mathrm{Aut}(X_G) \cong G \times \mathbb{Z}$ where the $\mathbb{Z}$ corresponds to powers of the shift. Such 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 $F \subset \mathrm{Aut}(X_G)$ is a set of automorphisms, then these automorphisms are of the form $f_i \times \sigma^{k_i}$ for some $k_i \in \mathbb{Z}$. Then $f \circ \sigma^k$ commutes with all of $f_i \times \sigma^{k_i}$ 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 3. 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, 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 trivial 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.

Let c_i be the number of cycles of length i for $i \in \mathbb{N}$. Let P be the lengths that appear.

Proposition 1. *Let X be a nonempty finite subshift, conjugate to a permutation π on a finite set, and let c_i be the number of cycles of length i in the cycle decomposition of π and $P = \{i \mid c_i \geq 1\}$. Then $k(X) \in \{\perp, 0, 2\}$ and*

$$\begin{aligned}
k(X) = \perp &\iff c_1 = 2 \vee |P \cap [2, \infty)| \geq 2, \\
k(X) = 0 &\iff P \cap [2, \infty) \subset \{\ell\} \wedge c_1 \in \{0, 1\} \wedge c_\ell \in \{0, 1\}, \\
k(X) = 2 &\iff c_1 \geq 3 \vee (P \cap [2, \infty) = \{\ell\} \wedge c_1 \neq 2 \wedge c_\ell \geq 2).
\end{aligned}$$

Proof. We only show the interesting part of the proof, namely that when all cycles of X have the same length $\ell \geq 2$ and there are $c \geq 2$ such cycles, we have $k(X) = 2$. Let $X = \mathbb{Z}_\ell \times \mathbb{Z}_c$ where dynamics $\sigma : X \to X$ is given by incrementation in all the components $\mathbb{Z}_\ell \times \{i\}$. Then any bijection $f : X \to X$ commuting with σ 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 $\mathrm{Aut}(X)$ 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 $f : X \to X$ 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, $f(n, i) = (n', i)$ for all n, i for some n'. 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 $f : X \to X$ commuting with a, b and c. Observe that every permutation of the second component can be implemented with a and b. This implies that for all n, i, we have $c(n, i) = (n', i)$ for some n', since the symmetric group on c elements has trivial center. By commutation with b, again f is a power of σ. □

7.7 Other examples of ∞-transitivity

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

Example 4. 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 $x_1, x_2, \ldots, x_k$ 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 nth level of the full binary tree. Every such permutation is in V. □

Example 5. 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 [31]. We sketch a proof that the commutator subgroup is ∞-transitive on orbits directly, only using the assumption that X is aperiodic. Let $x \in X$. 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.[13]

Extend π to an even permutation of $[1, n+2]$ by acting either as a swap 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.

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 support of COST Action IC1405.

[13] Alternatively, the existence of C can be seen by using the Marker Lemma [29] and such clopen sets are also the building blocks of Bratteli-Vershik representations of minimal subshifts.

References

[1] Sebastián Barbieri, Jarkko Kari, and Ville Salo. *The Group of Reversible Turing Machines*, pages 49–62. Springer International Publishing, Cham, 2016.

[2] T. Boykett. Closed Systems of Invertible Maps. *ArXiv e-prints*, December 2015.

[3] Tim Boykett, Jarkko Kari, and Ville Salo. *Strongly Universal Reversible Gate Sets*, pages 239–254. Springer International Publishing, Cham, 2016.

[4] M. Boyle, T. Meier Carlsen, and S. Eilers. Flow Equivalence of G-SFTs. *ArXiv e-prints*, December 2015.

[5] Mike Boyle. Some sofic shifts cannot commute with nonwandering shifts of finite type. *Illinois J. Math.*, 48(4):1267–1277, 2004.

[6] 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.

[7] 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.

[8] 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.

[9] Mike Boyle and Michael Schraudner. $\mathbb{Z}^d$ group shifts and Bernoulli factors. *Ergodic Theory Dynam. Systems*, 28(2):367–387, 2008.

[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, 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.

[15] V. Cyr and B. Kra. The automorphism group of a shift of subquadratic growth. *ArXiv e-prints*, March 2014.

[16] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163. Springer Science & Business Media, 1996.

[17] Sebastián Donoso, Fabien Durand, Alejandro Maass, and Samuel Petite. On automorphism groups of low complexity minimal subshifts, 2014.

[18] J. Frisch, T. Schlank, and O. Tamuz. Normal amenable subgroups of the automorphism group of the full shift. *ArXiv e-prints*, December 2015.

[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. Theory of cellular automata: a survey. *Theoret. Comput. Sci.*, 334(1-3):3–33, 2005.

[22] Jarkko Kari. Universal pattern generation by cellular automata. *Theor. Comput. Sci.*, 429:180–184, 2012.

[23] 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.

[24] K. H. Kim and F. W. Roush. On the automorphism groups of subshifts. *Pure Mathematics and Applications*, 1(4):203–230, 1990.

[25] KH Kim, FW Roush, and JB Wagoner. Characterization of inert actions on periodic points. part ii. In *Forum Mathematicum*, volume 12, pages 671–712. WALTER DE GRUYTER & CO., 2000.

[26] Ki Hang Kim, FW Roush, and JB Wagoner. Characterization of inert actions on periodic points. In *I, Forum Math*. Citeseer, 2000.

[27] Yves Lafont. Towards an algebraic theory of boolean circuits. *Journal of Pure and Applied Algebra*, 184:2003, 2003.

[28] D.A. Lind. Applications of ergodic theory and sofic systems to cellular automata. *Physica D: Nonlinear Phenomena*, 10(1 - 2):36 – 44, 1984.

[29] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding*. Cambridge University Press, Cambridge, 1995.

[30] Ville Lukkarila. Sensitivity and topological mixing are undecidable for reversible one-dimensional cellular automata. *J. Cellular Automata*, 5(3):241–272, 2010.

[31] Hiroki Matui. Some remarks on topological full groups of cantor minimal systems. *International Journal of Mathematics*, 17(02):231–251, 2006.

[32] Masakazu Nasu. Textile systems for endomorphisms and automorphisms of the shift. *Mem. Amer. Math. Soc.*, 114(546):viii+215, 1995.

[33] Masakazu Nasu. Textile systems and one-sided resolving automorphisms and endomorphisms of the shift. *Ergodic Theory and Dynamical Systems*, 28:167–209, 2 2008.

[34] Jeanette Olli. Endomorphisms of sturmian systems and the discrete chair substitution tiling system. *Dynamical Systems*, 33(9):4173–4186, 2013.

[35] J. Patrick Ryan. The shift and commutativity. *Mathematical systems theory*, 6(1-2):82–85, 1972.

[36] Ville Salo. *Subshifts with Simple Cellular Automata*. PhD thesis, University of Turku, 2014.

[37] Ville Salo. Toeplitz subshift whose automorphism group is not finitely generated. *ArXiv e-prints*, November 2014.

[38] Ville Salo. A note on subgroups of automorphism groups of full shifts. *ArXiv e-prints*, July 2015.

[39] Ville Salo and Ilkka Törmä. Color blind cellular automata. *J. Cellular Automata*, 9(5-6):477–509, 2014.

[40] P. Selinger. Reversible k-valued logic circuits are finitely generated for odd k. *ArXiv e-prints*, April 2016.