Universal groups of cellular automata

Ville Salo
vosalo@utu.fi

August 27, 2018

Abstract

We prove that the group of reversible cellular automata (RCA), on any alphabet A, contains a perfect subgroup generated by six involutions which contains an isomorphic copy of every finitely-generated group of RCA on any alphabet B. This result follows from a case study of groups of RCA generated by symbol permutations and partial shifts with respect to a fixed full Cartesian product decomposition of the alphabet. For prime alphabets, we show that this group is virtually cyclic, and that for composite alphabets it is non-amenable. For alphabet size four, it is a linear group, while for non-prime non-four alphabets, it is not a subdirect product of linear groups. For all composite alphabets of size at least ten, the group contains copies of all finitely-generated groups of RCA. We also obtain that RCA of biradius one on all large enough alphabets generate copies of all finitely-generated groups of RCA. We ask a long list of questions.

1 Introduction

Automorphism groups of subshifts have been a topic of much interest in recent years [38, 47, 44, 15, 12, 14, 18, 17, 13, 20, 42, 45, 2], with most results dealing with either the case of highly constrained subshifts such as minimal and low-complexity subshifts, or the case of weakly constrained subshifts such as SFTs. This paper is about the second case.

Reversible cellular automata or *RCA* (on a finite alphabet A) are the automorphisms, i.e. shift-commuting self-homeomorphisms, of the full shift $A^{\mathbb{Z}}$, and form a group denoted by $\mathrm{Aut}(A^{\mathbb{Z}})$. We write this group also as $\mathrm{RCA}(A)$, and as $\mathrm{RCA}(|A|)$ up to isomorphism. Since this group is not finitely-generated [9], from the perspective of geometric group theory it is of interest to try to understand its finitely-generated subgroups. In this paper, we construct "universal" such subgroups, with a maximal set of finitely-generated subgroups.

A simple way to construct RCA is the technique of partitioned cellular automata. Fix a Cartesian product decomposition $A = B_1 \times B_2 \times \cdots \times B_k$ of the finite alphabet A. The *partial shifts* shift one of the tracks with respect to this decomposition of the alphabet, e.g. identifying $x \in A^{\mathbb{Z}}$ as $(y^1, y^2, \cdots, y^k) \in B_1^{\mathbb{Z}} \times B_2^{\mathbb{Z}} \times \cdots \times B_k^{\mathbb{Z}}$ in an obvious way, we map $\sigma_1(y^1, y^2, \cdots, y^k) = (\sigma(y^1), y^2, ..., y^k)$ where σ is the usual shift map, and similarly we allow shifting the other tracks independently. The *symbol permutations* apply the same permutation of A in

each position of $x \in A^{\mathbb{Z}}$. These maps are reversible, and thus any composition of them is as well.

When a partial shift and a symbol permutation are composed (in some fixed order), we obtain a *partitioned RCA*. In this paper, we denote the group generated by symbol permutations and partial shifts by $\mathrm{PAut}[B_1; B_2; ..., B_k]$ – this group contains the partitioned RCA and their inverses, but also several other things, see Section 2.2 for details. The group $\mathrm{PAut}[B_1; B_2; ..., B_k]$ is a subgroup of $\langle \mathrm{RCA}_1(A^{\mathbb{Z}}) \rangle$, the group of RCA generated by those with biradius one. When $n_1, n_2, ..., n_k \in \mathbb{N}$, we also write $\mathrm{PAut}[n_1; ...; n_k]$ for the abstract group $\mathrm{PAut}[B_1; B_2; ..., B_k]$ where $|B_i| = n_i$, up to isomorphism.

A theorem of Kari [27] shows that, up to passing to a subaction of the shift (and using the induced basis for the algebra of clopen sets), all RCA come from composing partial shifts and symbol permutations. Our main result is that for any robust enough composite alphabet $B \times C$, even without passing to a subaction of the shift, RCA in $\mathrm{PAut}[B; C]$ can *simulate* any RCA on any alphabet in the following algebraic sense.

Definition 1. *Let G be a group. A finitely-generated subgroup $H \leq G$ is* universal *if there is an embedding $G \hookrightarrow H$. It is* f.g.-universal *if for every finitely-generated subgroup $K \leq G$ there exists an embedding $K \hookrightarrow H$.*

Theorem 1. *If $m \geq 2, n \geq 5$, then $\mathrm{PAut}[m; n]$ is f.g.-universal in $\mathrm{RCA}(mn)$.*

The set of finitely-generated subgroups of $\mathrm{RCA}(A)$ does not depend on A as long as $|A| \geq 2$ by [30], so when $\mathrm{PAut}[m; n]$ is f.g.-universal in $\mathrm{RCA}(mn)$, it also contains a copy of every finitely-generated subgroup of $\mathrm{RCA}(k)$ for any other $k \in \mathbb{N}_+$. For the same reason, the theorem implies that for any nontrivial alphabet A, $\mathrm{RCA}(A)$ contains an f.g.-universal finitely-generated subgroup since it contains a copy of each $\mathrm{PAut}[m; n]$ (a stronger statement about sofic shifts is given below).

In five cases, namely $\mathrm{PAut}[m; n]$ for $(m, n) \in \{(2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$, we do not know whether the group is f.g.-universal, but in terms of amenability and linearity we have a complete understanding.

Theorem 2. *Let $m, n \geq 1$.*

- $\mathrm{PAut}[m] \cong \langle \sigma \rangle \times S_m$, *while*
- *if $m \geq 2, n \geq 2$ then $\mathrm{PAut}[m; n]$ is nonamenable, and*
- $\mathrm{PAut}[2; 2]$ *is a linear group, while*
- *if $m \geq 2, n \geq 3$ then $\mathrm{PAut}[m; n]$ is not a subdirect product of linear groups.*

Note that $\mathrm{PAut}[B]$ has only one track, and thus is generated by the shift and symbol permutations, so the first item is straightforward since two distinct cells cannot communicate in any way. In the case $\mathrm{PAut}[2; 2]$ we give an explicit 8-dimensional representation over a field of characteristic 2. A linear group cannot be f.g.-universal. The nonamenability results and non-linearity results follow from explicit embeddings of free products of infinite direct sums of finite cyclic groups, namely groups of the form $\mathbb{Z}_k^\omega * \mathbb{Z}_\ell^\omega$.

We can also state a result in terms of alphabet size alone. Write $\mathrm{PAut}(A)$ for the group $\mathrm{PAut}[B_1; B_2; ..., B_k]$ seen through any bijection $\pi : A \to B_1 \times B_2 \times$

$\cdots \times B_k$ where $|A| = |B_1||B_2|\cdots|B_k|$ is a full prime decomposition of A. The subgroup of $\mathrm{RCA}(A)$ obtained does not depend (even as a set) on the choice of the B_i and that of π, see Section 2.2. Again up to isomorphism we write $\mathrm{PAut}(n)$ for the group $\mathrm{PAut}(A)$ where $|A| = n$.

Theorem 3. *Let $n \geq 2$.*

- *If $n \in \mathbb{P}$, then $\mathrm{PAut}(n) \cong \langle\sigma\rangle \times S_n$.*
- *If $n = 4$, then $\mathrm{PAut}(n)$ is a linear group.*
- *If $n \in \{6, 8, 9\}$, then $\mathrm{PAut}(A)$ is not a subdirect product of linear groups.*
- *If $n \notin \mathbb{P} \cup \{4, 6, 8, 9\}$, then $\mathrm{PAut}(n)$ is f.g.-universal in $\mathrm{RCA}(n)$.*

The group is virtually cyclic if and only if it is amenable if and only if $n \in \mathbb{P}$.

Note that $n \notin \mathbb{P} \cup \{4, 6, 8, 9\}$ is equivalent to $n \notin \mathbb{P}, n \geq 10$.

In all our constructions, we will need only two tracks, so the practical difference between the setting of this theorem and Theorem 1 is that when dealing with $\mathrm{PAut}(n)$ we are allowed to pick a "good" Cartesian product decomposition of the alphabet into a Cartesian product $A = B \times C$. When $n \notin \mathbb{P} \cup \{4, 6, 8, 9, 12, 16\}$, *every* non-trivial decomposition $n = k\ell$ satisfies either $k \geq 2, \ell \geq 5$ or $k \geq 5, \ell \geq 2$ and thus in these cases we obtain an f.g.-universal group no matter how we split the alphabet.

Finally, we obtain a corollary about the group $\langle \mathrm{RCA}_1(n) \rangle$ of RCA generated by those with biradius one. Again this classifies the possible sets of f.g. subgroups for a cofinite set of alphabet sizes.

Theorem 4. *$\langle \mathrm{RCA}_1(n) \rangle \leq \mathrm{RCA}(n)$ is f.g.-universal for all large enough n.*

As mentioned above, one motivation for the result is that the groups $\mathrm{Aut}(A^{\mathbb{Z}})$, and more generally $\mathrm{Aut}(X)$ for mixing SFTs X, are not finitely-generated, and thus do not fit very neatly in the framework of geometric group theory. Thus, it is of interest to look for finitely-generated subgroups which are representative of the entire group. On the other hand, even in cases where we do not obtain universality, the study provides new examples of "naturally occurring" finitely-generated RCA groups.

The set of finitely-generated subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$ is relatively big: It is closed under direct and free products and finite extensions [42], contains the graph groups (a.k.a. right-angled Artin groups) [30], and contains a group not satisfying the Tits alternative [43] (we give another proof in Proposition 4). In the journal version of [2] we prove that there is an f.g. subgroup with undecidable torsion problem. Since the constructions of the present paper are constructive, Theorem 1 combined with [28] provides a new proof of this.[1]

We state one corollary obtained in the symbolic dynamics setting (other embedding theorems are surveyed in [43]). A *sofic shift* is a subshift defined by a regular language of forbidden patterns; in particular all full shifts $A^{\mathbb{Z}}$ are trivially sofic.

Theorem 5. *Let X be a sofic shift. Then the following are equivalent:*

[1] Though the journal version of [2] is not submitted or available online, it precedes the results of this paper and uses different methods – there the work of producing a "generating set" is done in the group of Turing machines, while here it is done in the group of RCA.

- *The group* $\mathrm{Aut}(X)$ *has a perfect subgroup generated by six involutions containing every f.g. subgroup of* $\mathrm{Aut}(A^{\mathbb{Z}})$ *for any alphabet* A*.*
- X *has uncountable cardinality.*

We also summarize some properties of the abstract group obtained, for easier reference.

Theorem 6. *There exists a finitely-generated residually finite perfect group* G *such that, letting* $\mathcal{G}$ *be the class of subgroups of* G*:*

- G *has decidable word problem and undecidable torsion problem, and does not satisfy the Tits alternative, and*
- $\mathcal{G}$ *is closed under finite extensions, direct products and free products, and contains all graph groups.*

Any group with this list of properties is necessarily not a linear group over any field, contains every finite group, and every finitely-generated abelian group and free group. We are not aware of many naturally occurring residually finite groups with such properties; for example the Tits alternative rules out linear groups, hyperbolic groups[2] and fundamental groups of 3-manifolds [31, 19], and having all finite groups as subgroups rules out automata groups.

We note that it is entirely normal for a non-finitely generated group to have universal finitely-generated subgroups:

Example 1: The free group on $\aleph_0$ (free) generators has a universal finitely-generated subgroup, namely the free group on two generators, since free groups with finitely or countably many generators all embed into each other. The free group on $\aleph_1$ generators does not have a universal finitely-generated subgroup (since f.g. groups are countable), but the free group on two generators is an f.g.-universal subgroup of it, for the same reason as in the previous case. ○

In Section 6, we state some open questions. We include old classics, restated in terms of our new universal subgroups, and we also ask some new ones. We also ask several questions about the existence of (f.g.-)universal subgroups in other non-finitely generated groups of interest, namely other cellular automata groups, automata groups and the rational group, the group of Turing machines [2], topological full groups and (full) homeomorphism groups.

2 Definitions

2.1 Conventions and terminology

Our conventions for the naturals are $0 \in \mathbb{N}$, $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$, and the set of primes is $\mathbb{P}$. Intervals are discrete unless otherwise specified, i.e. $[a, b] = [a, b] \cap \mathbb{Z}$. Some basic knowledge of group theory [40], symbolic dynamics [34] and cellular automata is assumed, and we try to follow standard conventions.

An *alphabet* is a finite set. A *subshift* is a shift-invariant closed subset of $A^{\mathbb{Z}}$ for an alphabet A, where the shift $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is $\sigma(x)_i = x_{i+1}$. The subshift carries the knowledge of the alphabet (the alphabet represents a fixed basis of

[2]It is not known whether all hyperbolic groups are residually finite [23].

expansivity). If X is a subshift, a *basic cylinder* is a cylinder of the form $[a]_i$ where a is in the alphabet of X. Basic cylinders form a subbase of the topology.

The *automorphisms* of a subshift X are the shift-commuting self-homeomorphisms of X, and they form a group denoted by $\mathrm{Aut}(X)$. When $X = A^{\mathbb{Z}}$, we write $\mathrm{Aut}(X)$ also as $\mathrm{RCA}(A)$, and $\mathrm{RCA}(|A|)$ for the abstract group up to isomorphism.

Words over an alphabet A [35] form a monoid A^* under concatenation, which is denoted $u \cdot v$ or uv. A word u is *unbordered* if $vu = uv' \implies |v| = 0 \vee |v| \geq |u|$. Configurations $x \in A^{\mathbb{Z}}$ are two-way infinite words. Often they have a periodic left and right tail, and a left tail with repeating word u is written ${}^{\infty}u$ and a right tail as u^{∞}. The position of the origin is left implicit when specifying infinite words. Finite words are 0-indexed in formulas. In text we use the standard English ordinals, so the "first symbol" of a word w is w_0 rather than w_1.

For two words u, v of the same length, write $D(u, v)$ for $\{i \in [1, |u|] \mid u_i \neq v_i\}$. The *Hamming distance* of two words u, v is $|D(u, v)|$. The Hamming distance is the path metric in the *Hamming graph* (of length n over alphabet Σ) whose vertices are Σ^n and edges (u, v) where $|D(u, v)| = 1$. If $a \in A$ and $u \in A^*$ write $|u|_a$ for the number of a-symbols in u.

The *reversal* of a word is denoted by w^T and defined by $w^T_i = w_{|w|-1-i}$. We also reverse other things such as subshifts, by reversing points in the sense $x^T_i = x_{-i}$, and cellular automata, by conjugating with the reversal map.

If X and Y are subshifts and $X \times Y$ their Cartesian product subshift (with the diagonal action), then X and Y are referred to as *tracks*, and the first track is also referred to as the *left* or *top* track. Write $\mathrm{RAut}(X \times Y)$ for the subgroup of $\mathrm{Aut}(X \times Y)$ containing those f that never modify the X-track (i.e. $\forall x, y : \exists y' : f(x, y) = (x, y')$).

An RCA $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is *of radius* r if $f(x)_0$ depends only on the word $x_{[-r,r]}$. A *biradius* of a reversible cellular automaton f is any number larger than the radii of f and f^{-1}. The *bineighborhoods* are defined similarly.

For two groups G, H, we write $H \leq G$ for the literal inclusion, and $H \hookrightarrow G$ when H can be embedded into G.

The symmetric (resp. alternating) group on a set A is $\mathrm{Sym}(A)$ (resp. $\mathrm{Alt}(A)$) and S_n is the group $\mathrm{Sym}(A)$ for any $|A| = n$, up to isomorphism; similarly $A_n = \mathrm{Alt}(A)$ for $|A| = n$.

Composition of functions is from right to left and all groups (including permutation groups) act from the left unless otherwise specified. When permutations are written in cycle notation, we use whitespace or ; as the separator of the permutees. Usually we permute initial segments of $\mathbb{N}$ and elements of Σ^n for a fixed finite alphabet Σ and $n \in \mathbb{N}$.

$$[g, h] = g^{-1}h^{-1}gh, \quad [g_1, g_2, ..., g_k] = [[g_1, g_2], g_3, ..., g_k]$$

For g, h elements of the same group, write $g^h = h^{-1}gh$. If $\phi : X \to Y$ is bijection, we also use the notion for conjugation in the groupoid sense: if $h : Y \to Y$ is a bijection, write $h^{\phi} = \phi^{-1} \circ h \circ \phi : X \to X$. If A, B are groups, then an A-by-B group is one that admits an epimorphism to B with kernel A. A virtually H group is one that admits H as a subgroup of finite index. If A, B or H are properties instead, the interpretation is existential quantification over groups with said property.

A *linear group* is a (not necessarily finitely-generated) subgroup of a group of finite-dimensional matrices over a field, i.e. a subgroup of $\mathrm{GL}(n, F)$ for some field F and some $n \in \mathbb{N}$. We also use "linear" as an adjective, in the same sense.

We make a few simple observations about decidability, and an informal understanding suffices: Let $\mathcal{P}$ be a family of propositions. We say $\mathcal{P}$ is *semidecidable* if there exists an algorithm that, given $P \in \mathcal{P}$, eventually writes the answer "yes", and eventually writes "no" or never writes anything if $P \notin \mathcal{P}$. We say $\mathcal{P}$ is *decidable* if $\mathcal{P}$ and $\{\neg P \mid P \in \mathcal{P}\}$ are both semidecidable.

2.2 $\mathrm{PAut}(A)$, $\mathrm{PAut}[B; C]$

If $B_1, B_2, ..., B_k$ are finite alphabets, then $\mathrm{PAut}[B_1; B_2; \cdots; B_k]$ refers to the smallest subgroup of $\mathrm{Aut}((B_1 \times B_2 \times \cdots \times B_k)^{\mathbb{Z}})$ containing the following maps: The *partial shifts* σ_i, $i \in [1, k]$ defined by

$$\sigma_i(y^1, y^2, \cdots, y^k) = (y^1, y^2, ..., y^{i-1}, \sigma(y^i), y^{i+1}, ..., y^k),$$

where $\sigma : B_i^{\mathbb{Z}} \to B_i^{\mathbb{Z}}$ is the usual shift map, and the *symbol permutations* $\bar{\pi}$ defined by applying a permutation π in every cell, or

$$\bar{\pi}((y^1, y^2, \cdots, y^k))_j = \pi((y^1, y^2, \cdots, y^k)_j),$$

in symbols, where $\pi \in \mathrm{Sym}(B_1 \times B_2 \times \cdots \times B_k)$ is arbitrary. We usually identify $\bar{\pi}$ with π.

These maps are reversible, so $\mathrm{PAut}[B_1; B_2; \cdots; B_k] \leq \mathrm{Aut}((B_1 \times B_2 \times \cdots \times B_k)^{\mathbb{Z}})$.

We write $\mathrm{PAut}(A)$ for the following subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$: Let $|A| = n$ and let $n = p_1 \cdot p_2 \cdot ... \cdot p_k$ where p_i are the prime factors of n in any order. Pick a bijection $\pi : A \to B_1 \times B_2 \times ... \times B_k$ where $|B_i| = p_i$ for all i. Define $\mathrm{PAut}(A)$ as the group obtained by conjugating $\mathrm{PAut}[B_1; B_2; ...; B_k]$ through π. A priori, the resulting subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$ could depend on the choice of π and the B_i. Let us show that this is not the case.

Lemma 1. *The group* $\mathrm{PAut}(A)$ *is well-defined.*

Proof. Let $\pi : A \to B_1 \times B_2 \times ... \times B_k$ and $\pi' : A \to B_1' \times B_2' \times ... \times B_k'$ be two bijections. By the fundamental theorem of arithmetic, and by reordering of the product (which clearly does not change the obtained subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$), we may assume $|B_i| = |B_i'|$ for all i. Clearly the subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$ obtained by using a particular bijection does not depend on the contents of the sets, but only their cardinalities, so we may hide the bijection coming from $|B_i| = |B_i'|$ and simply assume $B_i = B_i'$ for all i. Let G and G' be the two subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$ generated by symbol permutations and partial shifts using the two bijections. Now, by definition, G and G' are conjugate subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$, by the symbol permutation $\pi^{-1} \circ \pi'$ by a direct computation. This symbol permutation is in both of the groups G and G', so in fact the groups are equal. □

2.3 Clopen sets with length

In this section we define CSWLs. One should mostly think of "CSWL" as a synonym for "clopen set", except that we make sense of composition FF' for two CSWLs F, F' by adding extra information.

To write the main argument, we had to decide whether to use clopen sets or words. The problem with words is that expressing complicated local conditions is difficult, since words do not form a Boolean algebra ("either u or v" is not a word). The problem with clopen sets is that while they allow expressing complicated local conditions, they cannot be concatenated, and thus do not take advantage of the very special geometry of $\mathbb{Z}$ the way words do. When describing the contents of some portion of an infinite word in terms of more primitive clopen sets, we need to keep track of indices (and long sums of lengths of words) explicitly, which can get unwieldy. For example writing "the words $u_1, ..., u_k$ appear consecutively at the origin" becomes

$$[u_1 u_2 \cdots u_k]_0 = \bigcap_{i=1}^{k} \sigma^{-\sum_{1 \leq j < i} |u_j|} [u_i]_0$$

in clopen-speak, when we write the set in terms of the sets $[u_i]_0$.

To combine the benefits of words and clopens, we use *clopen-sets-with-length*, or *CSWLs*, which are simply clopen sets for which we have decided a "length" (in any way we like). A CSWL F (in some space X) is a pair $(c(F), \ell(F))$ where $c(F)$ is clopen (in X) and $\ell(F)$ is natural number, which we also write as $|F|$. For two CSWLs F, F', define FF' as the CSWL with $c(FF') = F \cap \sigma^{-\ell(F)}(F'), \ell(FF') = \ell(F) + \ell(F')$. This product is associative and has an identity element, so we obtain a monoid, and we can then define powers of CSWLs in the usual way. For a word $w \in A^*$, we define the length of $[w]_i$ to be $|w|$, and then the formula

$$[u_1 u_2 \cdots u_k]_i = [u_1]_i [u_2]_i \cdots [u_k]_i$$

holds for all $i \in \mathbb{Z}$. A CSWL F is *n-unbordered* if $c(F) \cap \sigma^i(c(F)) = \emptyset$ for all $i \in [1, n-1]$, and *unbordered* if it is $\ell(F)$-unbordered. A word u is unbordered if and only if the CSWL $[u]_0$ is unbordered.

For a CSWL F, write $[F]_i$ for the set $\sigma^{-i}(F)$, i.e. the set of configurations whose translation by i is in F, intuitively the set of configurations where F "occurs" in coordinate i (in particular $[[u]_0]_i = [u]_i$).

Note that the concatenation of two CSWLs may well be empty, and we define equality simply by comparing the clopen set and the length separately. We make no claims about compatibility of the Boolean operations and the concatenation operation.

We also use *partial words*, i.e. words having wildcard symbols ␣. A partial word appears in a configuration if the non-wildcard symbols match, and unborderedness, concatenation and the corresponding clopen sets and CSWLs are defined in the obvious way. For example by default we represent a partial word 1␣0 over the binary alphabet by $([100]_0 \cup [110]_0, 3)$. The word 1␣0␣ would be represented by $([100]_0 \cup [110]_0, 4)$.

3 Generators for some groups

3.1 Controlled actions

Suppose we are dealing with a group action that is conditioned on some type of events, and write $g|_E$ for the "action of g in case E holds". Then

$$[g|_E\,, h|_F] = [g, h]|_{E \cap F}\,,$$

since in the case of less than two events, the commutator cancels. When the acting group is perfect (e.g. an alternating group on at least 5 objects), commutators $[g, h]$ run over the whole group, so if we can condition actions of G on some set of events $\mathcal{E}$, we can condition them on any event in the Boolean algebra generated by $\mathcal{E}$.

We do not give a general formalization of this idea, as often the events are entangled with whatever is being acted on, so one should rather consider this a proof technique. Informally, we refer to actions that "depend on events" as *controlled actions*, and to the trick of the previous paragraph as the *commutator trick*. The main application is to subshifts, whose Boolean algebra of clopen sets is generated by basic cylinders $[a]_i$, but we also use the trick in some other contexts.

Definition 3 and Lemma 5 are one formal incarnation of the commutator trick.

3.2 Alternating groups and 3-hypergraphs

The following lemma is from [6], and is probably a well-known fact about alternating groups. A hypergraph $\mathcal{G}$ is *weakly connected* if the graph $\mathcal{G}'$, whose edges are those 2-subsets of $V(\mathcal{G})$ that are contained in some hyperedge of $\mathcal{G}$, is connected.

Lemma 2. *Let $\mathcal{G}$ be a hypergraph with all hyperedges of size 3, and let G be the group generated by three-cycles corresponding to the hyperedges of $\mathcal{G}$. If $\mathcal{G}$ is weakly connected, then $G = \mathrm{Alt}(V(\mathcal{G}))$.*

Often in the context of word permutations it is obvious that a relevant hypergraph of 3-rotations is connected, even if the precise set of cycles in linearized form (as a permutation of $[1, n]$) seems difficult to work with.

3.3 Universal families of reversible logical gates

If you can permute two adjacent cells of words (evenly), you can permute words of any length (evenly), by the following Lemma 4 which strengthens a result of [6]. Many results like this are known, see e.g. [1, 5, 48], but usually (conjugation by) free reordering of wires is allowed, so these results are not directly compatible with ours. In our application, wire reordering is not possible. First, we prove a lemma about swaps, as it allows a simpler proof for half of the possible alphabet sizes.

Lemma 3. *Let A be a finite set. Then the permutation $s : A^2 \to A^2$ defined by $s(ab) = ba$ is even if and only if $|A| \equiv 0, 1 \bmod 4$.*

Proof. If $|A| = n$, the number of transpositions in s is $\frac{n(n-1)}{2}$. We have

$$2|n(n-1)/2 \iff 4|n(n-1) \iff 4|n \vee 4|(n-1).$$

□

Lemma 4. *Let A be a nontrivial finite alphabet with $|A| \geq 3$. If $n \geq 2$, then every even permutation of A^n can be decomposed into even permutations of A^2 applied in adjacent cells. That is, the permutations*

$$w \mapsto w_0 w_1 \cdots w_{i-1} \cdot \pi(w_i w_{i+1}) \cdot w_{i+2} \cdots w_{n-1}$$

are a generating set of $\mathrm{Alt}(A^n)$ *where* π *ranges over* $\mathrm{Alt}(A^2)$*, and* i *ranges over* $0, 1, 2, ..., n-2$*.*

Proof. First suppose that $|A| \geq 5$. In this case in particular for every fixed $b \in A$, every even permutation of the words $\{ab \mid a \in A\}$ is generated. Suppose first that $|A| \equiv 0, 1 \bmod 4$, so the swap $ab \mapsto ba$ in any position is among the generators by the previous lemma. We can then apply even permutations to any two cells at the time, so we can use the commutator trick in a straightforward way to permute any particular position evenly, exactly when the other cells have some prescribed contents. The result follows by applying Lemma 2 to the hypergraph with vertices A^n and edges (u, v, w) such that for some i, $u_i \neq v_i \neq w_i \neq u_i$ and the words are equal elsewhere.

We now prove the general case $|A| \geq 5$, where the swap is not necessarily among the generators. We can still condition an even permutation at i on the precise contents of the word to the right (symmetrically to the left) using the commutator trick, though we have to be slightly more careful: Write the permutation π we want to perform as $\pi = [\alpha, \beta]$. Suppose we can permute the ith coordinate by any even permutation conditioned on the values at $i+1, i+2, ..., i+k$ being equal to any given word $u \in A^k$. Pick any 3-rotation of A^2 which changes the first coordinate of the word $u_{k-1}a \in A^2$, but does not change the first coordinate of $u_{k-1}b$ for $b \neq a$. When such a rotation is applied, the information of whether the $(i+k+1)$th coordinate is a moves to the left, as long as $i+k$ contains u_{k-1}, and otherwise we have little control on what happens, though we note that the ith coordinate (and the ones left of it) are not modified.

Repeating this argument, we can find a sequence of even permutations of length-2 subwords which modifies the $(i+1)$st coordinate to some $c \neq u_0$ if the word in coordinates $i+1, i+2, ..., i+k, i+k+1$ is ua, but does not modify the coordinate if the word is ub for $b \neq a$. Again, we have no control on what happens if the cells $i+1, ..., i+k$ do not contain the word u, but again note that the ith coordinate is untouched. Let ψ be this map, and observe that now

$$[\alpha|_{w_{i+1,\ldots,i+k}=u}, (\beta|_{w_{i+1}=c})^{\psi}]$$

is the desired controlled application of π, where $\alpha|_{w_{i+1,\ldots,i+k}=u}$ permutes the ith coordinate by α if $w_{i+1,\ldots,i+k} = u$ and otherwise does not do anything (this map is generated by induction), and $\beta|_{w_{i+1}=c}$ applies β at i if $w_{i+1} = c$, and is the identity otherwise (this map is directly among the generators).

In the cases $|A| \in \{3, 4\}$, even permutations of A^2 are not enough to set up the argument, but those of A^3 are, by a similar proof as above, using $|A^2| \geq 5$. The construction of ψ can be done by even permutations of A^2 directly. The fact that permutations of A^2 generate permutations of A^3 in these finitely many cases is a decidable statement, and can be verified by computer. □

We used GAP [21] for the proof that even permutations of A^2 generate those of A^3 when $|A| \in \{3, 4\}$. When $|A| = 4$, a manual proof can be obtained with the same tactic as in the proof, by splitting A into a Cartesian product $\{0, 1\}^2$. When $|A| = 3$, one can use the lower central series variant of the commutator trick from Lemma 5 to obtain that $\mathrm{Sym}(A^2)$ is a generating set, but we do not have a conceptual proof that $\mathrm{Alt}(A^2)$ is.

As hinted by the title of the section, it is useful to think of permutations applied to subwords as "reversible logical gates", and we say a family of gates is

universal if it generates all the even gates on A^n for large enough n. Combining the previous lemma with any standard set of generators for $\mathrm{Alt}(A^2)$, we obtain a set of two gates that generates all other gates. It is well-known that as n tends to infinity, the fraction of pairs $(g, h) \in \mathrm{Alt}(n)$ with $\langle g, h\rangle = \mathrm{Alt}(n)$ tends to 1 [16], so almost any two even random permutations of A^2 form a universal family of reversible gates. We conjecture that a single gate suffices for n large enough.

The previous lemma does not hold for $|A| = 2$: When $|A| = 2$, all permutations of A^2 are affine for the obvious linear structure of A^2, so they will also give only affine maps on A^n. In fact, they do not generate all even permutations of A^3. On the other hand, it is known that if $|A| = 2$, then the set of all even permutations of A^4 generates all even permutations of A^n for any n (swaps, flips and the Toffoli gate are even as permutations of A^4), and a quick search in GAP [21] shows that the set of all even permutations of A^4 is generated by the the even permutations of A^3. Thus, on the binary alphabet the lemma is true if A^2 is replaced by A^3 (starting from $n \geq 3$).

4 Structure and universality of PAut[...] groups

Theorem 7. *Let $m, n \geq 1$.*

- $\mathrm{PAut}[m] \cong \langle\sigma\rangle \times S_m$.
- *If $m \geq 2, n \geq 2$, then $\mathrm{PAut}[m; n]$ is nonamenable.*
- $\mathrm{PAut}[2; 2]$ *is a linear group.*
- *If $m \geq 2, n \geq 3$, $\mathrm{PAut}[m; n]$ is not a subdirect product of linear groups.*
- *If $m \geq 2, n \geq 5$, $\mathrm{PAut}[m; n]$ is f.g.-universal in $\mathrm{RCA}(mn)$.*

Proof. The first item is Lemma 11 below. The third item is Lemma 12 below. The second and fourth item are shown in Theorem 9. The fifth item is shown in Theorem 8. □

In addition to the results mentioned, we discuss some basic structural properties of subgroups which arise in the course of the proof, see in particular Section 4.5.

4.1 Universal groups

In this section, we perform the main engineering task of building copies of every finitely generated group of RCA in the $\mathrm{PAut}[B; C]$ groups.

Recall the definition of CSWL (clopen sets with length) from Section 2.3.

Definition 2. *Suppose $F \subset B^{\mathbb{Z}}$ is an n-unbordered CSWL and $\pi : C^n \to C^n$ is a permutation. Then define $\pi|_F \in \mathrm{Aut}((B \times C)^{\mathbb{Z}})$ by*

$$\pi|_F(x, y)_j = \begin{cases} (x_j, \pi(y_{[j-i,j-i+n-1]})_i) & \text{if } \exists i \in [0, n-1], x \in [F]_{j-i} \\ (x_j, y_j) & \text{otherwise.} \end{cases}$$

It is an instructive exercise to verify that this map is well-defined.

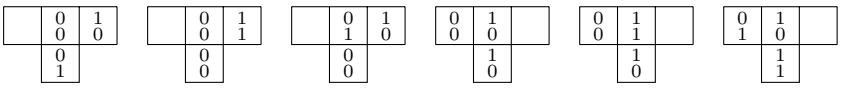
The map $\pi|_F$ performs the permutation π on the second track under every occurrence of F on the second track. One should think of this as a conditional application of π on the second track, where the condition is that the first track contains a point that is in F. The definition makes sense, since due to the fact F cannot overlap a translate of itself by less than n steps (by n-unborderedness), permutations can unambiguously modify a contiguous interval of n cells to the right of the place where F occurs.

Example 2: Let $f = (00; 10; 01)|_{[01]_0}$. To apply f, locate occurrences of 01 on the first track, and permute the words under the occurrences according to the permutation $(00; 10; 01)$:

$$f\begin{pmatrix}...0100111001001001001000110010010...\\ ...0101110011010011010101001001010...\end{pmatrix} =$$
$$f\begin{pmatrix}...0100111001001001001000110010010...\\ ...0101110011010011010101001001010...\end{pmatrix} =$$
$$\begin{matrix}...0100111001001001001000110010010...\\ ...0001110011001011001100101101000...\end{matrix}$$

where we write occurrences of the controlling CSWL $[01]_0$ in blue, words modified by the permutation in green, and the fixed points of the permutation (to which it is nevertheless applied) in red.

One can also extract an explicit local rule:



In all nonspecified cases we output the contents of the central cell. ○

Definition 3. *Let X be a subshift and G a group acting on a set A. For a clopen set $C \subset X$ and $g \in G$, define $g|_C : X \times A \to X \times A$ by*

$$g|_C(x, a) = \begin{cases} (x, ga) & \text{if } x \in C \\ (x, a) & \text{otherwise.} \end{cases}$$

Define the shift by $\sigma(x, a) = (\sigma(x), a)$ where σ denotes both the new and the usual shift map. We denote the group generated by these maps by $G|_X$. We denote by $P(X, G)$ the subgroup generated by the shift on X and maps $g|_C$ where $g \in G$ and C is a basic cylinder.

The $P(X, G)$ is by analog with the 'P' in PAut, as these groups can be simulated rather transparently with elements of PAut. See Section 4.5 for some basic observations about these groups.

Lemma 5. *Let $X \subset \Sigma^{\mathbb{Z}}$ be a subshift and G a group acting on a finite set A. Then for all clopen C, $P(X, G)$ contains $g|_C$ for all g in the intersection of the lower central series of G.*

Proof. It is enough to prove this for cylinders, i.e. $C = [w]_m$ for a word w and $m \in \mathbb{Z}$. This is clearly true if C is a basis set (conjugate by the shift to account for the m). Let then $C = [wa]_m$ where $a \in \Sigma$. If h is in the intersection

of the lower central series, then $h = [h_1, g_1][h_2, g_2]...[h_k, g_j]$ for some h_i in the intersection of the lower central series and g_i in G. It is thus enough to show that $[g_i, h_i]|_{[wa]_m} \in P(X, G)$. It is easy to verify that

$$[\, h_i|_{[w]_m} \,,\, g_i|_{[a]_{m+|w|}}] = [h_i, g_i]|_{[w]_m \cap [a]_{m+|w|}} = [h_i, g_i]|_{[wa]_m} \,.$$

□

The following lemma is what separates the PAut[2; 2] case from others, by finding a large locally finite subgroup in PAut[$B \times C$]. (The conclusion is true also for $|C| = 2$, but is trivial in that case.)

Lemma 6. *Let $|B|, |C| \geq 2$. Then for every even permutation ϕ of C and any clopen $F \subset B^{\mathbb{Z}}$, $\phi|_F$ is in* PAut[$B; C$].

Proof. For every n, the intersection of the lower central series of S_n is A_n. It is easy to see that the shift on either track, together with symbol permutations that only modify the second track, implement the group $P(B^{\mathbb{Z}}, G)$ in a natural way where $G = S_{|C|}$, and the claim follows from the previous lemma. □

Remark 1. *Note that it is important that all permutations, not just the even ones, are allowed in* PAut[$B; C$], *in order for G to contain all the maps $\phi|_F$ with ϕ an even permutation on C, since we are using the fact that the intersection of the lower central series of S_n is always A_n. If only even permutations are allowed, we can get all the $\phi|_F$ maps in the case $|C| \geq 5$ (since A_5 is perfect), but we also use the cases $|C| = 3, |C| = 4$ in Theorem 8. See also Question 3.*

Lemma 7. *Let $A = B \times C$, $|B| \geq 2$, $|C| \geq 3$ and let* PAut[$B; C$] $\leq G \leq$ Aut($A^{\mathbb{Z}}$). *Suppose that for some unbordered word $u \in BB$, $\pi|_{[u]_0} \in G$ for $\pi = (00;\ 10;\ 01)$. Then $\pi'|_{[u]_0}$ is in G for all $\pi' \in$ Alt(CC).*

Proof. Define the CSWLs $F_0 = ([u]_0, 1), F_1 = ([u]_{-1}, 1)$. Then $\pi|_{F_i} \in G$ for every $\pi \in \mathrm{Alt}(C)$, $i \in \{0, 1\}$. These maps separately permute the first and second coordinates under occurrences of the word u.

Let $F = ([u]_0, 2)$. Now define a 3-hypergraph with words CC as nodes, and an edge (v_0, v_1, v_2) for all triples of words such that $\psi|_F \in G$ where $\psi = (v_0\ v_1\ v_2)$ is the corresponding 3-cycle. By Lemma 2, we only need to show that this hypergraph is weakly connected.

Let $v, v' \in C^2$ be arbitrary. Observe that Alt(C) acts transitively on C (since $|C| \geq 3$) and acts transitively on unordered pairs $\{\{a, b\} \mid a, b \in C, a \neq b\}$ (for any $|C|$). Thus, using the maps of the first paragraph, we can conjugate $\{v_i, v_{i+1}\}$ to either $\{00, 10\}$, $\{00, 01\}$ or $\{10, 01\}$ depending on the coordinate where they differ. The hypergraph is then weakly connected since $\{00, 10\}, \{00, 01\}, \{10, 01\} \subset \{00, 10, 01\}$. □

Lemma 8. *Let $A = B \times C$, $|B| \geq 2$, $|C| \geq 3$ and let* PAut[$B; C$] $\leq G \leq$ Aut($A^{\mathbb{Z}}$). *Suppose that for some unbordered word $u \in B^n$ with $n \geq 2$, $\pi|_{[u]_0}$ is in G for all $\pi \in$ Alt(C^n). Then for any large enough $\ell \in \mathbb{N}$ there is a clopen set F such that $F \cap \sigma^i(F) = \emptyset$ for all $i \in [0, \ell - 1]$, $\bigcap_{i \in \mathbb{Z}} \sigma^{i\ell}(F) \neq \emptyset$, and $\pi|_F \in G$ for all $\pi \in$ Alt(C^ℓ).*

Proof. Let $\ell = 3n + (n+1)k + (2n+1)h$ and let v be the partial word $uuu(\_u)^k(\_uu)^h\_uuu$. Then the length of v is $\ell+3n = 6n+(n+1)k+(2n+1)h$, which can be picked to be any large enough number since $\gcd(n+1, 2n+1) = 1$. Since u is unbordered and $n \geq 2$, the partial word v is ℓ-unbordered, so the CSWL $F = ([v]_0, \ell)$ is unbordered and $F^m = ([(uuu(\_u)^k(\_uu)^h)^m\_uuu]_0, \ell m)$ is clearly nonempty for all m, that is, $c(F)$ has the first two claimed properties.

Observe that $\pi|_{([u]_i, n)}$ is in G for all $i \in \mathbb{Z}$ and $\pi \in \mathrm{Alt}(C^n)$ by conjugating with partial shifts. We can now perform any even permutation of C^n in n consecutive coordinates $[i+j, i+j+n-1]$ in every segment $[i, i+\ell-1]$ of the second track such that F occurs at i on the first track: To condition on a particular translate of F occuring over such a segment of n coordinates, write F as an intersection of translates of $[u]_0$ and use the commutator trick.

By the assumption that F is unbordered, length-n subsegments of $[i, i+\ell-1]$, such that F appears at i on the first track, do not overlap when the contents of the first track stays fixed, so these applications do not interfere with each other. Since $n \geq 2$ and $|C| \geq 3$, it follows from Lemma 4 that $\pi|_F \in G$ for all $\pi \in \mathrm{Alt}(C^\ell)$. □

Lemma 9. *Let $|B|, |C| \geq 2$ and $A = B \times C$, and let $\mathrm{PAut}[B; C] \leq G \leq \mathrm{Aut}(A^{\mathbb{Z}})$. Suppose that for any large enough $\ell \in \mathbb{N}$ there is a clopen set F such that $F \cap \sigma^i(F) = \emptyset$ for all $i \in [0, \ell-1]$, $\bigcap_{i\in\mathbb{Z}} \sigma^{i\ell}(F) \neq \emptyset$, and $\pi|_F \in G$ for all $\pi \in \mathrm{Alt}(C^\ell)$. Then G contains an embedded copy of every finitely-generated group of cellular automata.*

Proof. Let $r \geq 1$ be arbitrary, let $\ell = 24r$ and pick a corresponding clopen set F, considered as a CSWL with length ℓ. The assumption is that the clopen set $c(F^m)$ of F^m is nonempty for all m.

We first associate to any $f \in \mathrm{Aut}(C^{\mathbb{Z}})$ (with any radius) an element $\hat{f} \in \mathrm{RAut}((B \times C)^{\mathbb{Z}})$ which simulates the action of f in a natural way, so that $f \mapsto \hat{f}$ is an embedding.

The map $\hat{f}$ is defined as follows: Suppose $(x, y) \in B^{\mathbb{Z}} \times C^{\mathbb{Z}}$ and consider a maximal occurrence of F^m in x with m finite (points x with this property are dense since $|F| \geq 2$ and F is unbordered). We split the subword of y under the occurrence of F^m into $u_1v_1u_1'v_1' \cdot u_2v_2u_2'v_2' \cdots u_mv_mu_m'v_m'$ where $|u_i| = |v_i| = |u_i'| = |v_i'| = 6r$ for all i.

The application of $\hat{f}$ will be defined for f of any radius, but let us already address what will happen when the radius is at most r. When f has radius at most r, we will be able to construct $\hat{f}$ (which is defined below) inside G by performing a sequence of operations that changes the words u_i and v_i, by applying permutations to the subwords u_iv_i and the (non-contiguous) subwords $v_{i-1}u_i$ below the occurrence of F^m. The words u_i' and v_i' are changed exactly the same way, i.e. when we apply a permutation to the word u_iv_i, we apply the same permutation to $u_i'v_i'$, and a permutation applied to $v_{i-1}u_i$ is also applied to $v_{i-1}'u_i'$. The main simulation happens on the words u_i and v_i, while the purpose of the primed versions is simply to ensure that all the permutations performed are even: for any permutation $\pi : X \to X$, the diagonal permutation $\pi \times \pi : X \times X \to X \times X$ is even.

We think of u_i as being on top of the word v_i, and think of the boundaries of the maximal run F^m as completing the top and bottom word into a conveyor belt; similarly for the primed words u_i', v_i'. Accordingly, to define $\hat{f}$, we apply

f to the periodic point $(u_1u_2\cdots u_m(v_m)^T(v_{m-1})^T\cdots(v_1)^T)^{\mathbb{Z}}$ and decode the contents of $[0, 12rm]$ into the new contents below the occurrence of F^m; similarly for the primed words. Denote the new configuration below F^m as $\bar{u}_1\bar{v}_1\bar{u}'_1\bar{v}'_1 \cdot \bar{u}_2\bar{v}_2\bar{u}'_2\bar{v}'_2\cdots\bar{u}_m\bar{v}_m\bar{u}'_m\bar{v}'_m$.

This defines the global rule of $\hat{f}$ uniquely, as the unique continuous extension, and it is easy to see that $\hat{f}$ is always an automorphism (since $\hat{f}^{-1}$ is an inverse). If the biradius of f is r', then that of $\hat{f}$ is $4r' + O(1)$ where the factor 4 comes from skipping over words representing contents of other simulated tapes, e.g. skipping over v_i, u'_i, v'_i when rewriting u_i, and the constant term depends on F. Since the word to which f is applied only depends on x, and we are directly simulating the action of f on an encoded configuration, the map $f \mapsto \hat{f}$ is a homomorphism, and since F^m can appear in x for arbitrarily large m by the assumption, this is an embedding of $\mathrm{Aut}(C^{\mathbb{Z}})$ into $\mathrm{Aut}(A^{\mathbb{Z}})$. See [42] for more detailed explanations of similar arguments.

Now, we show that for any $f \in \mathrm{Aut}_r(C^{\mathbb{Z}})$, the map $\hat{f}$ is indeed in G, which implies that G contains an embedded copy of the subgroup of $\mathrm{Aut}(C^{\mathbb{Z}})$ generated by elements of biradius r or less, which concludes the proof since $\mathrm{Aut}(C^{\mathbb{Z}}) = \bigcup_r \langle \mathrm{RCA}_r(C)\rangle$ and every finitely-generated group of cellular automata over any alphabet is a subgroup of $\mathrm{Aut}(C^{\mathbb{Z}})$ [30].

Since $\pi|_F$ for all $\pi \in \mathrm{Alt}(C^\ell)$, and the group $\mathrm{Alt}(C^\ell)$ is perfect, we have $\pi|_{FF}, \pi|_{[FF]_{-12r}}, \pi|_{[FF]_{-\ell}} \in G$ for every $\pi \in \mathrm{Alt}(C^\ell)$ by the commutator trick. Similarly, writing $F^c = (c(F)^c, \ell(F))$, we have $\pi|_{[FF^c]_i} \in G, \pi|_{[F^cF]_i} \in G$ for all $i \in \mathbb{Z}$ and $\pi \in \mathrm{Alt}(C^\ell)$. Intuitively, we can perform any even permutation of words on the second track in every context that can be specified in terms of occurrences of F on the first track.

We now recall the concept of stairs from [27]. Define $L \subset C^{4r}$ as the left stairs of f, i.e. the possible contents 

of stairs in spacetime diagrams (where the arrow of time points down), or in symbols

$$L = \{uv \in C^{4r} \mid u, v \in C^{2r}, \exists x \in C^{\mathbb{Z}} : x_{[0,2r-1]} = u, f(x)_{[r,3r-1]} = v\},$$

and $R \subset C^{4r}$ the right stairs of f defined symmetrically.

Then $|L||R| = |C|^{6r}$ by the argument of [27], namely the local rules of f and f^{-1} set up an explicit bijection between suitably concatenated left and right stairs and words of length $6r$. Define $\gamma_L : C^{6r} \to L$ and $\gamma_R : C^{6r} \to R$ for the maps which extract the left and right stair corresponding to a word, and $\bar{\gamma}_L : C^{6r} \to \bar{L}$ and $\bar{\gamma}_R : C^{6r} \to \bar{R}$ for the corresponding versions for f^T.

The left stairs of f^T are in bijection with the right stairs of f and vice versa: we have $\bar{\gamma}_L = \gamma_R(w^T)^T$ in a natural sense. Then, writing $\bar{L}$ for the left stairs of f^T, we have $|L||\bar{L}| = |L||R| = |C|^{6r}$ and similarly for right stairs. Let $\alpha_L : L \times \bar{L} \to C^{6r}$ and $\alpha_R : R \times \bar{R} \to C^{6r}$ be (arbitrary) bijections coming from the local rules of f and f^{-1} as described in [27].

Define also the maps $\beta_L, \beta_R : C^{6r} \to C^{3r}$ which simply extract the left and right half of a word.

We now do a sequence of rewrites. First, for all i (simultaneously) we do

$$\begin{aligned}
&u^i v^i u'^i v'^i \mapsto \\
&\alpha_L(\gamma_L(u_i), \bar{\gamma}_L(v_i))\alpha_R(\gamma_R(u_i), \bar{\gamma}_R(v_i)) \cdot \alpha_L(\gamma_L(u'_i), \bar{\gamma}_L(v'_i))\alpha_R(\gamma_R(u'_i), \bar{\gamma}_R(v'_i)) \mapsto \\
&\alpha_L(\gamma_L(u_i), \bar{\gamma}_L(v_i))\alpha_L(\gamma_L(u'_i), \bar{\gamma}_L(v'_i)) \cdot \alpha_R(\gamma_R(u_i), \bar{\gamma}_R(v_i))\alpha_R(\gamma_R(u'_i), \bar{\gamma}_R(v'_i)),
\end{aligned}$$

which can be performed by applying a suitable even permutation on the second track, conditioned on having F on the first track. To see that this permutation is even, observe that the first permutation is diagonal and the second is even as the words u^i, u'^i, v^i, v'^i are of even length (so in fact any permutation of the order of the words is even). Now "between" occurrences of F for $1 \leq i < m$ do

$$\begin{aligned}
&\alpha_R(\gamma_R(u_i), \bar{\gamma}_R(v_i))\alpha_R(\gamma_R(u'_i), \bar{\gamma}_R(v'_i))\cdot \\
&\qquad \alpha_L(\gamma_L(u_{i+1}), \bar{\gamma}_L(v_{i+1}))\alpha_L(\gamma_L(u'_{i+1}), \bar{\gamma}_L(v'_{i+1})) \mapsto \\
&\alpha_R(\gamma_R(u_i), \bar{\gamma}_R(v_i))\alpha_L(\gamma_L(u_{i+1}), \bar{\gamma}_L(v_{i+1}))\cdot \\
&\qquad \alpha_R(\gamma_R(u'_i), \bar{\gamma}_R(v'_i))\alpha_L(\gamma_L(u'_{i+1}), \bar{\gamma}_L(v'_{i+1})) \mapsto \\
&\beta_R(\bar{u}_i)\beta_L(\bar{u}_{i+1})\beta_R(\bar{v}_i)\beta_L(\bar{v}_{i+1}) \cdot \beta_R(\bar{u}'_i)\beta_L(\bar{u}'_{i+1})\beta_R(\bar{v}'_i)\beta_L(\bar{v}'_{i+1}) \mapsto \\
&\beta_R(\bar{u}_i)\beta_R(\bar{v}_i)\beta_R(\bar{u}'_i)\beta_R(\bar{v}'_i) \cdot \beta_L(\bar{u}_{i+1})\beta_L(\bar{v}_{i+1})\beta_L(\bar{u}'_{i+1})\beta_L(\bar{v}'_{i+1})
\end{aligned}$$

by performing a suitable even permutation of words of length $24r$ on the second track, conditioned on $[FF]_{-12r}$ on the first track. Note that the permutation is applied with an offset, and an individual application under an occurrence of FF will not modify the $12r$ leftmost and rightmost symbols under the occurrence. In total at this step we modify all but the $12r$ left- and rightmost cells under a maximal occurrence of F^m.

To see that this permutation is well-defined, observe that $\beta_R(\bar{u}_i)\beta_L(\bar{u}_{i+1})$ can be deduced from $(\gamma_R(u_i), \gamma_L(u_{i+1}))$ by applying the local rule of f (and similarly for v-words and the primed versions). This is clear from drawing the corresponding spacetime diagrams, see [27] for the detailed argument.

Now, we deal with the remaining $12r$ coordinates under left corners of maximal occurrences F^m by applying the (even) permutation

$$\begin{aligned}
&\alpha_L(\gamma_L(u_1), \bar{\gamma}_L(v_1))\alpha_L(\gamma_L(u'_1), \bar{\gamma}_L(v'_1)) \\
&\mapsto \beta_L(\bar{u}_1)\beta_L(\bar{v}_1)\beta_L(\bar{u}'_1)\beta_L(\bar{v}'_1)
\end{aligned}$$

of words of length $12r$ on the second track, conditioned on $[F^cF]_{-24r}$ on the first track. Here, observe that since the words $\bar{u}_i, \bar{u}'_i, \bar{v}_i, \bar{v}'_i$ were defined by applying f to a periodic point in a conveyor belt fashion, the word $\beta_L(\bar{u}_1)\beta_L(\bar{v}_1)$ can be deduced from $(\gamma_L(u_1), \bar{\gamma}_L(v_1))$, and similarly for the primed versions. We deal with the right borders similarly.

Finally, to obtain the correct contents under F^m, we only need to perform the position swap

$$\begin{aligned}
&\beta_L(\bar{u}_i)\beta_L(\bar{v}_i)\beta_L(\bar{u}'_i)\beta_L(\bar{v}'_i) \cdot \beta_R(\bar{u}_i)\beta_R(\bar{v}_i)\beta_R(\bar{u}'_i)\beta_R(\bar{v}'_i) \\
&\mapsto \beta_L(\bar{u}_i)\beta_R(\bar{u}_i)\beta_L(\bar{v}_i)\beta_R(\bar{v}_i) \cdot \beta_L(\bar{u}'_i)\beta_R(\bar{u}'_i)\beta_L(\bar{v}'_i)\beta_R(\bar{v}'_i) \\
&= \bar{u}_i\bar{v}_i \cdot \bar{u}'_i\bar{v}'_i
\end{aligned}$$

under each occurrence of F. □

Finally, we prove the only lemmas that need $|C| \geq 5$: that the element $(00; 10; 01)|_{[u]_0}$ from Lemma 7, which bootstraps the whole argument, is indeed in $\mathrm{PAut}[B; C]$.

Lemma 10. *Let $|B| \geq 2, |C| \geq 5$. Then for every unbordered word $u \in B^*$, $\pi|_{[u]_0} \in \mathrm{PAut}[B; C]$ for every $\pi \in \mathrm{Alt}(C^{|u|})$.*

Proof. For $|u| \leq 1$ this is trivial. Let $U = [u]_0$. We show that for any two words $v, w \in C^*$ such that $|vw| = |u| - 1$, and every even permutation π of C, the map $\phi_{v,\pi,w}$ is in well-defined and in $\mathrm{PAut}[B; C]$, where $\phi_{v,\pi,w} = \phi|_U$ where

$$\phi(v'aw') = \begin{cases} v'\pi(a)w' & \text{if } v'w' = vw, \\ v'aw' & \text{otherwise.} \end{cases}$$

Here, $v'aw'$ is always the decomposition with $|v'| = |v|$. The claim then follows by a straightforward application of Lemma 2, since the Hamming graph is connected, and the 3-rotations $(a\ b\ c)$ are even permutations and give rise to the word permutation $(vaw;\ vbw;\ vcw)$.

We in fact only need to show that we can realize $\phi_{v,\pi,w}$ for every even permutation π and a fixed vw, say $vw = 0^{n-1}$, as then the general case of vw and π follows by conjugating with maps constructed in Lemma 6 and composing.

In fact, it is enough to realize, for each even permutation π and every $b \in \{0, 1, 2, 3, 4\}$, the map $\psi_{b,\pi} = \psi|_U$ where

$$\psi(v'aw') = \begin{cases} v'\pi(a)w' & \text{if } |v'w'|_b = 0 \\ v'aw' & \text{otherwise.} \end{cases}$$

Here, $v'aw'$ is always the decomposition with $|v'| = |v|$. Namely,

$$\{0^{n-1}\} = \bigcap_{b \in \{1,2,3,4\}} \{v'w' \mid |v'w'|_b = 0\},$$

and we can condition on the intersection of two conditions using the commutator trick, observing that $\mathrm{Alt}(C) = \bigcup_{\pi_1,\pi_2,\pi_3,\pi_3 \in \mathrm{Alt}(C)} [\pi_1, \pi_2, \pi_3, \pi_3]$ and

$$\phi_{0^{|v|},[\pi_1,\pi_2,\pi_3,\pi_3],0^{|w|}} = [\psi_{1,\pi_1}, \psi_{2,\pi_2}, \psi_{3,\pi_3}, \psi_{4,\pi_4}].$$

To realize such a map for a given $b \in \{0, 1, 2, 3, 4\}$ and every π, it is in enough to realize it for a single permutation π whose conjugates form a generating set, as we can obtain all others by conjugating by the maps constructed in Lemma 6.

Now, observe that the conjugation action of A_n is transitive on permutations with cycle structure $(2, 2, 1, 1, ...)$ for all n, and that permutations with such a cycle structure are a generating set for A_n when $n \geq 5$. Thus, we find that it is enough to realize only $\psi_{0,(1\ 2)(3\ 4)}$.

Let π be any permutation of B without fixed points and let g be the map that applies π in a cell of the first layer when the second layer contains 0, or $g = (\pi|_{[0]_0})^{\updownarrow}$ in symbols, where $\updownarrow : (B \times C)^{\mathbb{Z}} \to (C \times B)^{\mathbb{Z}}$ exchanges the tracks (and conjugation by $\updownarrow$ is performed in the groupoid sense).

For a permutation $\pi \in \mathrm{Sym}(C)$ write $\bar{\pi}$ for the permutation that maps $\bar{\pi}(v'aw') = v'\pi(a)w'$ when $|v'| = |v|$. Then $\bar{\pi}|_U$ performs the permutation π in the $|v|$th coordinate under each occurrence of U, and for any $\pi \in \mathrm{Alt}(C)$, this map is in $\mathrm{PAut}[B; C]$ by Lemma 6.

By the reductions we have performed, the result now follows once we show

$$\psi_{0,(1\ 2)(3\ 4)} = \left[\overline{(1\ 4\ 3)}\Big|_U, \left(\overline{(4\ 3\ 2)}\Big|_U \right)^g \right].$$

To see this, observe first that $(4\ 3\ 2)|_U$ and $(1\ 4\ 3)|_U$ do not modify the positions where 0 occurs on the second track. It follows that the conjugation by g in the

rightmost operand of the commutator, $g^{-1} \circ \overline{(4\ 3\ 2)}\Big|_U \circ g$, is "safe", in the sense that the effect of g is undone on the first track, and so the net effect of $\left(\overline{(4\ 3\ 2)}\Big|_U\right)^g$ is "Perform the permutation (4 3 2) in a cell k of the second track of (x, y) if and only if, after rotating those coordinates j of x where $y_j = 0$, we have $x_{[k-|v|,k-|v|+n-1]} = u$. Do not modify the first track."

The only case where something non-trivial happens in a cell is then the case when both of the permutations are performed, in which case we perform precisely $(1\ 2)(3\ 4) = [(1\ 4\ 3), (4\ 3\ 2)]$ on the second track. Clearly both permutations happen at k if and only if $x_{[k-|v|,k-|v|+n-1]} = u$ (so that the second operand of the commutator is applied) and $y_{[k-|v|,k-|v|+n-1]}$ does not contain any 0s (since, assuming the second operand of the commutator is applied, we have $x_{[k-|v|,k-|v|+n-1]} = u$, so that any 0 would necessarily remove or move this occurrence). □

Theorem 8. *Let $A = B \times C$ where $|B| \geq 2$. If $|C| \geq 3$, then $\langle \mathrm{RCA}_1(A) \rangle$ contains an isomorphic copy of every group of RCA over any alphabet. If $|C| \geq 5$, then so does* PAut$[B; C]$.

Proof. Let $G = \mathrm{PAut}[B; C]$ if $|B| = 2, |C| \geq 5$, and let $G = \langle \mathrm{RCA}_1(A) \rangle$ otherwise. Lemma 10 implies that $(00;\ 10;\ 01)|_{[01]_0}$ is in G when $|A| \notin \mathbb{P} \cup \{4, 6, 8, 9\}$, and it is in G by definition in the cases $|A| \in \{6, 8, 9\}$, since it is in $\langle \mathrm{RCA}_1(A) \rangle$ by Example 2.

Now, Lemma 7 shows that all even permutations of CC under occurrences of $[01]_0$ are in G. Then Lemma 8 shows that all even permutations of words under CSWL F of any sufficiently large length can be performed. Then Lemma 9 shows that G contains every finitely-generated group of RCA. □

4.2 The prime case

Lemma 11. *If $n \in \mathbb{P}$, then* PAut$(n) \cong \langle \sigma \rangle \times S_n$.

Proof. Let $|A| = n$ and observe that PAut$(A) =$ PAut$[A]$. The shift σ commutes with symbol permutations, no symbol permutation is a non-trivial shift map on a full shift, and PAut$[A]$ is by definition generated by symbol permutations and the shift $\langle \sigma \rangle$. Thus, the shift and the symbol permutations form a complementary pair of subgroups in PAut$[A]$, and thus PAut$[A]$ is an internal direct product of $\langle \sigma \rangle$ and the symbol permutations, which form a finite group isomorphic to Sym(A). □

4.3 The linear case

By Lemma 11, PAut(A) is linear (even over $\mathbb{R}$) for somewhat uninteresting reasons when $|A|$ is prime. The case $|A| = 4$ gives a linear group as well, but a more interesting one. The crucial point is that all permutations of $\mathbb{Z}_2^2$ are affine, so all symbol permutations are "affine".

Lemma 12. *The group* PAut(4) *has an* 8*-dimensional representation over a field of characteristic* 2.

Proof. By renaming, we may assume the Cartesian product decomposition is $A = \{(0,0),(0,1),(1,0),(1,1)\}$, and we give A the $\mathbb{Z}_2^2$-structure that arises from bitwise addition modulo 2 with respect to this decomposition.

The basic idea of the proof is that maps of the form $x \mapsto f(x) + a^{\mathbb{Z}}$, where f is a linear cellular automaton and $a \in A$, form a subgroup G of $\mathrm{Aut}(A^{\mathbb{Z}})$, and the subgroup of linear cellular automata is of finite index in it, so G is virtually linear, thus linear by using the induced representation. The generators of PAut(4) are contained in G so also PAut(4) is linear. We perform a slightly modified version of this argument, and give the explicit set of matrices.

For $a \in A$, let

$$X_a = \{x \in A^{\mathbb{Z}} \mid \exists n \in \mathbb{N} : \forall i < -n : x_i = a\}.$$

Since $\mathrm{Aut}(A^{\mathbb{Z}})$ acts bijectively on $\{a^{\mathbb{Z}} \mid a \in A\}$, we can associate to every element $f \in \mathrm{Aut}(A^{\mathbb{Z}})$ a unique homeomorphism of

$$X = X_{(0,0)} \times X_{(0,1)} \times X_{(1,0)} \times X_{(1,1)}$$

in an obvious way by for applying f to all tracks, and then permuting the tracks so that the left tails are in the correct order (and this reordering only depends on f). Note that this is a faithful action of $\mathrm{Aut}(A^{\mathbb{Z}})$ since each $X_{(a,b)}$ is dense.

Now, let $(a,b) \in A$ and $x \in X_{(a,b)}$. Then we can, in a unique way, write $x = (a,b)^{\mathbb{Z}} + y$ where y can be seen as a two-dimensional vector over the field $F = \mathbb{Z}_2((\boldsymbol{x}))$ of formal Laurent series over $\mathbb{Z}_2$. We define a vector space structure on each $X_{(a,b)}$ by addition of the vectors y, so that in $X_{(a,b)}$, the zero vector is $(a,b)^{\mathbb{Z}}$, and similarly scalar multiplication by F by multiplying the y part only. Then X is an 8-dimensional vector space over F, with the first two dimensions corresponding to $X_{(0,0)}$, the second two to $X_{(0,1)}$ and so on.

We claim that with respect to this linear structure of X, the generators of PAut(A) act by linear maps on X, so we obtain a representation. It is enough to show that the shift, the partial shift on the first track, and the symbol permutations all have this property.

For the shift, we have

$$\sigma \cong \mathrm{diag}(\boldsymbol{x}^{-1}, \boldsymbol{x}^{-1}, \boldsymbol{x}^{-1}, \boldsymbol{x}^{-1}, \boldsymbol{x}^{-1}, \boldsymbol{x}^{-1}, \boldsymbol{x}^{-1}, \boldsymbol{x}^{-1}),$$

and for the partial shift we have

$$\sigma_1 \cong \mathrm{diag}(\boldsymbol{x}^{-1}, 1, \boldsymbol{x}^{-1}, 1, \boldsymbol{x}^{-1}, 1, \boldsymbol{x}^{-1}, 1).$$

For the symbol permutations, we recall that $S_4 \cong \mathrm{AGL}(2,2)$, where $\mathrm{AGL}(2,2)$ denotes the two-dimensional general affine group over the field $\mathbb{Z}_2$. In other words, every symbol permutation is in fact an affine map on the alphabet. We now simply need to write the matrices corresponding to the action of the generators on X, and furthermore it is enough to do this for any generating set of $S_4 \cong \mathrm{AGL}(2,2)$, in other words the addition of constants, and the elementary matrices suffice.

Addition of the constant $(0,1)^{\mathbb{Z}}$ is performed by $\begin{pmatrix} 0&1&0&0\\ 1&0&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix} \otimes I_2$ where $\otimes$ is the Kronecker product, with the convention that the "large-scale" matrix is on the left side and I_2 is the identity. Similarly addition of the constant $(1,0)^{\mathbb{Z}}$ is performed by $\begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0 \end{pmatrix} \otimes I_2$

As for the linear part of $\mathrm{Sym}(A)$, i.e. $GL(2,\mathbb{Z}_2)$, we have the following correspondences:

$$\begin{pmatrix}0&1\\1&0\end{pmatrix} \text{ becomes } \begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix} \otimes \begin{pmatrix}0&1\\1&0\end{pmatrix}$$

$$\begin{pmatrix}1&1\\0&1\end{pmatrix} \text{ becomes } \begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix} \otimes \begin{pmatrix}1&1\\0&1\end{pmatrix}$$

$$\begin{pmatrix}1&0\\1&1\end{pmatrix} \text{ becomes } \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \otimes \begin{pmatrix}1&0\\1&1\end{pmatrix}$$

□

The group $\mathrm{PAut}(A)$ contains free groups when $|A| = 4$, as shown in the next section. It also contains a copy of the lamplighter group (actually two natural embeddings of it, one acting on the first track and one on the second). The subshift $(\mathbb{Z}_2^2)^{\mathbb{Z}}$ has a natural abelian group structure by cellwise addition, and the subgroup of $\mathrm{Aut}((\mathbb{Z}_2^2)^{\mathbb{Z}})$ preserving this linear structure is easily shown to be generated by symbol permutations. Thus $\mathrm{PAut}(A)$ contains this group for $|A| = 4$.

4.4 Non-linear and non-amenable cases

We prove that apart from trivial cases, none of $\mathrm{PAut}[B;C]$ are amenable, and that $\mathrm{PAut}[2;2]$ is the only linear case.

For G a group, write G^ω for the direct union of G^n as $n \to \infty$ (with the natural inclusions). For groups G, H write $G * H$ for their free product.

Lemma 13. *Let $|B| = m, |C| = k$. Let $G \leq S_m, H \leq S_k$ be abelian groups that have at least one free orbit as permutation groups. Then $G^\omega * H^\omega \leq \mathrm{PAut}[B;C]$.*

Proof. Let $B = \{0, ..., m-1\}, C = \{0, ..., k-1\}$. By renaming, we may assume $1 \in \{0, ..., m-1\}$ and $1 \in \{0, ..., k-1\}$ are representatives of the free orbits of G and H, respectively. The group G^ω is generated by the following maps: for $g \in G$ and $i \in \mathbb{Z}$, define

$$f_{g,i}(x,y)_0 = \begin{cases} (g(x_0), y_0) & \text{if } y_{-i} = 1. \\ (x_0, y_0) & \text{otherwise} \end{cases}$$

Extend $f_{g,i}$ to a cellular automaton by shift-commutation. These maps are easily seen to be in $\mathrm{PAut}[B;C]$, as $f_{g,0}$ is a symbol permutation and the others are conjugate to it by partial shifts. Clearly we obtain a copy of G by fixing i. Varying i, the maps commute since G is abelian. By applying them to $(0^{\mathbb{Z}}, ...000.1000...)$ we see that they do not satisfy any additional relations, and thus we have a copy of G^ω. Define similarly $f_{h,i}$ for $h \in H$, by changing the roles of the tracks.

Of course restricting i to $\mathbb{N}_+$, the maps $f_{g,i}$ and $f_{h,i}$ still give copies of G^ω and H^ω, respectively. Denote these copies by $G' \cong G^\omega$ and $H' \cong H^\omega$. We show that together they satisfy no other relations, that is, the maps $f_{g,i}, f_{h,i}$ for $i > 0$ generate a copy of $G' * H' \cong G^\omega * H^\omega$.

Suppose that $f_w = f_\ell \circ \cdots \circ f_2 \circ f_1$ is a reduced element where $f_i \in G'$ for odd i, $f_i \in H'$ for even i, and that ℓ is even (the other three cases are completely symmetric). For each odd i there is a "maximal" copy of G used by f_i, i.e. the reduced presentation of f_i contains some f_{g_i,r_i} with $r_i \geq 1$ maximal and $g_i \in G \setminus \{1_G\}$. Similarly, for even i there is some maximal copy of H used, denote $r_i \geq 1$, $h_i \in H \setminus \{1_H\}$.

Now, a direct computation shows the f_w acts nontrivially on the following configuration:

$$\infty \binom{0}{0}\binom{0}{1}\binom{0}{0}^{r_1-1}\begin{pmatrix} g_1^{-1}\cdot 1 \\ 0 \end{pmatrix}\binom{0}{0}^{r_2-1}\begin{pmatrix} 0 \\ h_2^{-1}\cdot 1 \end{pmatrix}\binom{0}{0}^{r_3-1}\cdots\binom{0}{0}^{r_\ell-1}\begin{pmatrix} 0 \\ h_\ell^{-1}\cdot 1 \end{pmatrix}\binom{0}{0}^{\infty}$$

For this, observe that $g_i^{-1} \cdot 1 \neq 1$ and $h_i^{-1} \cdot 1 \neq 1$ since 1 is a representative of the free orbit on both tracks, and thus the rightmost "active" 1 moves to the right on each step. □

Lemma 14. *Let G and H be nontrivial groups. Then $G^\omega * H^\omega$ is not amenable.*

Proof. We prove the stronger fact that a free product of two groups G, H does not contain the free group on two generators if and only if it is amenable if and only if it is virtually cyclic if and only if $G \cong H \cong \mathbb{Z}_2$. Namely, $\mathbb{Z}_2 * \mathbb{Z}_2$ is the infinite dihedral group, which is virtually abelian. If $g, g' \in G \setminus \{1_G\}$, $g \neq g'$ and $h \neq 1_H$, then gh and $g'h$ freely generate a free group. This follows from the normal form theorem of free products [36]. □

The following lemma is classical. We give a direct proof mimicking [40, Theorem 8.1.11] as suggested by user Panurge on the mathoverflow website [26].

Lemma 15. *Suppose G is a linear p-group with bounded exponent over a field of characteristic $q \neq p$. Then G is finite.*

Proof. We may assume G acts on a vector space V of dimension d over an algebraically closed field F. Suppose $g^e = 1$ for all $g \in G$, where e is a power of p. It follows from $g^e = 1$ that each root of the characteristic polynomial of g is an eth root of unity (consider for example the Jordan normal form of g). There are at most e such roots $\lambda_1, ..., \lambda_{e'}$, $e' \leq e$, so there are at most $(e')^d$ choices for the trace $\mathrm{tr}(g) = \sum_{j=1}^{d} \lambda_{i_j}$ of any element of $g \in G$.

Suppose now that G is irreducible. In this case by [40, Theorem 8.1.9], the fact that elements of G have finitely many possible traces implies that G itself is finite.

Otherwise, there is a non-trivial subspace closed under the action of G. The subgroup L of G that fixes both U and V/U is of finite index in G, by induction on dimension: the assumptions on characteristic and bounded exponent hold for actions on subspaces and quotient spaces, so the actions of G on these spaces factor through finite groups, and the intersection of two finite index subgroups is of finite index.

Now, picking any basis of m vectors for U and extending it by n vectors to a basis of V, we see that the corresponding matrix representation of L is by

unitriangular matrices: each matrix is a block matrix of the form $\left(\begin{smallmatrix} I_n & M \\ 0 & I_m \end{smallmatrix}\right)$ where I_m, I_n are the $m \times m$ and $n \times n$ identity matrices, respectively, and M is an $n \times m$ matrix.

Suppose $M \neq 1$ is a unitriangular matrix over a field of characteristic q, and has order dividing e. Suppose the nonzero entries are above the diagonal, and consider the action of M on row vectors from the right. Let i be the leftmost column of M containing a nonzero off-diagonal entry.

Now clearly the exponent of M, acting on the subspace of row vectors where all but the i leftmost coordinates are 0, is divisible by q. Thus the exponent of M on the whole space is also divisible by q. Since the order of M divides e, a power of p, the order of M must be 1, which is a contradiction with $M \neq 1$. This means we must have $L = 1$.

It follows that $|G| = [G : L]|L| < \infty$. □

Lemma 16. *Let G and H be non-trivial finite groups. If G and H are not p-groups for the same prime p, then $G^\omega * H^\omega$ is not a subdirect product of finitely many linear groups.*

In particular the assumption includes the case where one of G, H is not a p-group for any p.

Proof. The assumption implies that $p||G|, q||H|$ for some distinct primes p, q, so by Cauchy's theorem there exist $g \in G$, $h \in H$ such that $\mathrm{ord}(g) = p, \mathrm{ord}(h) = q$. It is then enough to prove that $\mathbb{Z}_p^\omega * \mathbb{Z}_q^\omega$ is not a subdirect product of finitely many linear groups.

Suppose it is, and let $\mathbb{Z}_p^\omega * \mathbb{Z}_q^\omega \cong K \leq G_1 \times G_2 \times \cdots \times G_\ell$ where the G_i are linear groups. Let the characteristics of the underlying fields be $p_1, ..., p_\ell$, respectively. Let $I_p, I_q \subset [1, ..., \ell]$ be defined by $i \in I_p \iff p_i = p$ and $i \in I_q \iff p_i = q$. Let π_i be the natural projection $\pi_i : K \to G_i$.

By the previous lemma, $\pi_i(\mathbb{Z}_p^\omega)$ is finite for $i \notin I_p$. Thus, the intersection of the kernels of all these maps is some $K_p \leq \mathbb{Z}_p^\omega$ of finite index, in particular K_p is non-trivial. Similarly we have a finite-index subgroup $K_q \leq \mathbb{Z}_q^\omega$. Then $K_p, K_q \leq K$ commute, which is a contradiction, since the subgroup they generate should be a free product $K_p * K_q \leq K$. □

The previous lemma implies in particular that, not surprisingly, a free product of linear groups need not be linear (or even a subdirect product of finitely many linear groups) when the characteristics of the fields over which they are linear are distinct, since the group $\mathbb{Z}_p^\omega$ is a linear group for every prime p (for example a linear group of RCA by a matrix implementation of Lemma 13). By [37] (see also [49]), the group $G^\omega * H^\omega$ is linear if and only if G^ω and H^ω are both linear over a field of the same characteristic.

Theorem 9. *If $|B|, |C| \geq 2$, then $\mathrm{PAut}[B; C]$ is non-amenable. If further $|C| \geq 3$, then $\mathrm{PAut}[B; C]$ is not a subdirect product of finitely many linear groups.*

Proof. For non-linearity, when $|B| \geq m$ and $|C| \geq k$, then $\mathbb{Z}/m\mathbb{Z}$ acts on B with a free orbit, and $\mathbb{Z}/k\mathbb{Z}$ acts on C with a free orbit, and thus $(\mathbb{Z}/m\mathbb{Z})^\omega * (\mathbb{Z}/k\mathbb{Z})^\omega \leq \mathrm{PAut}[B; C]$ by Lemma 13. If $m = k = 2$, Lemma 14 gives non-amenability. If $m = 2, k = 3$, Lemma 16 gives the second claim. □

We note that to just prove non-linearity of $\mathrm{PAut}[B;C]$ for $|B| \geq 2, |C| \geq 3$, it suffices to observe that this group contains copies of $\mathbb{Z}_2^n$ and $\mathbb{Z}_3^n$ for all n (which is slightly easier than finding the free product), e.g. by Lemma 15.

4.5 Modifying just one track

The proof of Lemma 6 implements the maps $\phi|_F$ by elements of $\mathrm{PAut}[B;C]$ which only modify the second track, making R an interesting example of a finitely-generated subgroup of $\mathrm{PAut}(A)$, for any alphabet $A \notin \mathbb{P} \cup \{4\}$. Out of general interest, we take a brief look at its structure.

This provides a new proof of the two-sided case of [43].

Proposition 1. *Let $|B|, |C| \geq 2$ and let $R[B;C] \leq \mathrm{PAut}[B;C]$ be the (finitely-generated) subgroup generated by the partial shift on the second track, and symbol permutations that only modify the second track. Then $R[B;C] \cong P(B^{\mathbb{Z}}, \mathrm{Sym}(C))$.*

Proof. Since there is a homomorphism that tracks the movement of the second track [27], the group does not change if we replace the partial shift on the second track by the one on the first track. Observe also that every cell on the second track behaves independently. The isomorphism simply tracks what happens at the origin. □

This motivates the study of the groups $P(B^{\mathbb{Z}}, H)$, especially when H is a symmetric group.

Proposition 2. *Let $|B| \geq 2$, let $H \leq \mathrm{Sym}(C)$ be a finite permutation group, and let $G = P(B^{\mathbb{Z}}, H)$. If H has derived length ℓ, then G has derived length $\ell + 1$. If H is not solvable, G is not virtually solvable.*

Proof. Let ϕ be the homomorphism that tracks the movement of the first track. Then G is $\ker\phi$-by-cyclic. Let $K = \ker\phi$, and observe that $[G,G] \leq K$ since $\mathbb{Z}$ is abelian.

Elements $g \in K$ do not modify the "controlling configuration" $B^{\mathbb{Z}}$ and only perform permutations on C depending on the controlling word. Thus, K is a subgroup of the uncountable direct product $H^{\beth_1}$ where $\beth_1 = 2^{\aleph_0}$. Whenever every element of $[H,H]$ can be expressed as a bounded product of commutators, we have $[H^X, H^X] = [H,H]^X$ for any set X. It follows that when H is finite, the derived length of $H^{\beth_1}$ is the same as that of H, so the derived length of G is at most one more than the derived length of H.

On the other hand, $[G,G] \leq K$ contains a subgroup mapping homomorphically onto H: consider the elements $[\sigma, g|_{[1]_0}]$ where g runs over G. If $x = ...0000.10000...$, then $[\sigma, g|_{[1]_0}]$ acts as g on C, so the homomorphism that maps elements of K to their action under the controlling configuration x is indeed surjective onto H. It follows that the derived length of G is at least one more than that of H.

If H is not solvable, G is not virtually solvable since it has H^n as a subquotient for all n, which can be seen by conjugating elements $g|_{[1]_0}$ by shifts and considering the action on elements of the form $(\sigma^i(x), a)$ with again $x = ...0000.10000....$ See [43] for a more detailed version of this argument. □

Corollary 1. *Let $|B|, |C| \geq 2$. Then $G = P(B^{\mathbb{Z}}, \mathrm{Sym}(C))$ is (locally finite)-by-cyclic. If $|C| \in \{2,3,4\}$, the group has derived length $|C|$. If $|C| \geq 5$, it is not virtually solvable.*

Proof. In the previous proof, it was observed that G is $\ker\phi$-by-cyclic, and the kernel of ϕ is clearly locally finite when H is finite since $H^{\supset_1}$ is locally finite. Thus G is (locally finite)-by-cyclic. For the claims about derived length, observe that S_2 is abelian, S_3 is metabelian and S_4 has derived length three, while S_n for $n \neq 5$ is non-solvable. □

Proposition 3. *If $|B| \geq 2, |C| \geq 3$, then $R[B;C]$ is not linear.*

Proof. The group is easily seen to contain copies of $\mathbb{Z}_2^n$ and $\mathbb{Z}_3^n$ for arbitrarily large n, since conjugating $g|_{[1]_0}$ where g is a generator of $\mathbb{Z}_k$ by the shift, we obtain a commuting set of maps which generate an internal direct product of copies of $\mathbb{Z}_k$, and the action is faithful, by considering the points $(\sigma^i(x), a)$ with $x = ...0000.10000....$ □

The group is never nilpotent: let $g \in \mathrm{Sym}(C)$ be arbitrary and let $g_0 = g|_{[1]_0}$ and $g_{i+1} = [\sigma, g_i]$. Then $g_i({}^\infty 010^\infty, a) = ({}^\infty 010^\infty, ga)$ for all i (and of course if $|C| \geq 3$ already $\mathrm{Sym}(C)$ is not nilpotent).

We recover the two-sided case of [43].

Proposition 4. *If $|B| \geq 2, |C| \geq 5$, then $R[B;C]$ does not satisfy Tits' alternative.*

Proof. When $|B| \geq 2, |C| \geq 5$, $P(B^{\mathbb{Z}}, \mathrm{Sym}(C))$ is elementary amenable and non-solvable by Corollary 1. □

Note that the group $R[B;C]$ in Proposition 1 is not equal to the group $\mathrm{RAut}(B^{\mathbb{Z}} \times C^{\mathbb{Z}}) \cap \mathrm{PAut}[B;C]$ in general. We do not any non-trivial cases where $\mathrm{RAut}(B^{\mathbb{Z}} \times C^{\mathbb{Z}}) \cap \mathrm{PAut}[B;C]$ is solvable, and the universality proofs in fact build copies of f.g. cellular automata groups precisely inside $\mathrm{RAut}(B^{\mathbb{Z}} \times C^{\mathbb{Z}}) \cap \mathrm{PAut}[B;C]$.

5 Corollaries

5.1 The result in terms of $\mathrm{PAut}(A)$

Theorem 10. *Let A be a finite alphabet with cardinality n.*

- *If $n \in \mathbb{P}$, then $\mathrm{PAut}(A) \cong \langle\sigma\rangle \times \mathrm{Sym}(A)$.*
- *If $n = 4$, then $\mathrm{PAut}(A)$ is linear, thus not f.g.-universal in $\mathrm{Aut}(A^{\mathbb{Z}})$.*
- *If $n \in \{6, 8, 9\}$, then $\mathrm{PAut}(A)$ is not a subdirect product of linear groups.*
- *If $n \notin \mathbb{P} \cup \{4, 6, 8, 9\}$, then $\mathrm{PAut}(A)$ is f.g.-universal in $\mathrm{Aut}(A^{\mathbb{Z}})$.*

The group is virtually cyclic if and only if it is amenable if and only if $n \in \mathbb{P}$.

Proof. This follows from Theorem 1 by a bit of numerology: When n is prime, $\mathrm{PAut}(A) = \mathrm{PAut}[A]$ by definition. When $n = 4$, $\mathrm{PAut}(A) \cong \mathrm{PAut}[B;C]$ where $|B| = |C| = 2$. When $n \in \{6, 8, 9\}$, we can write $n = k\ell$ where $k \geq 2, \ell \geq 3$. When $n \notin \mathbb{P} \cup \{4, 6, 8, 9\}$, we can write $n = k\ell$ where $k \geq 2, \ell \geq 5$. □

5.2 The optimal radius for an f.g.-universal set of CA

Let $N \subset \mathbb{Z}$ be a finite neighborhood and A an alphabet. Let $\mathrm{RCA}_N(A^{\mathbb{Z}})$ be the set of RCA with bineighborhood (the union of neighborhoods of the RCA and its inverse) contained in N. One interesting class of naturally occurring RCA groups is obtained by varying $(|A|, N)$ and studying the group $\langle \mathrm{RCA}_N(A^{\mathbb{Z}})\rangle$ they generate. The case $N = \{-r, ..., r\}$, that is, biradius r, and more generally cases where N is a contiguous interval, are of particular interest.

In the context of the present paper, one could concretely ask, for example, which of these groups are linear and which contain all finitely-generated groups of cellular automata. As an immediate corollary of the main theorem, we obtain the minimal contiguous bineighborhood size for f.g.-universality, for all but finitely many alphabets.

Theorem 11. *Let $n \geq 2$ and let $G_n = \langle \mathrm{RCA}_1(n)\rangle$. The group G_2 is virtually cyclic, while $G_n \leq \mathrm{RCA}(n)$ is f.g.-universal whenever $n \geq 6$ is composite or $n \geq 36$. If $N = \{a, a+1\}$ for some a then $\langle \mathrm{RCA}_N(n)\rangle$ is not f.g.-universal for any n.*

Proof. In the case $|A| = 2$, $N = \{-1, 0, 1\}$ we obtain the so-called elementary cellular automata. It is known that the group generated by reversible elementary cellular automata is $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, generated by the shift and the bit flip.

Let now U be the set of all numbers n such that $\langle \mathrm{RCA}_1(n)\rangle$ is f.g.-universal in $\mathrm{RCA}(n)$. By Theorem 8, U contains all composite numbers $n \geq 6$.

Let now $k, m \in \mathbb{N}$ be arbitrary. Then if $|A| = n = k^2 + m$, we can decompose the alphabet A as $A = B^2 \sqcup C$ where $|B| = k$. A radius-1 cellular automaton can treat elements of C as walls (which are never modified), and use the elements of B^2 as two B-tracks, wrapping into a conveyor belt next to elements of C. From this we obtain an embedding of the group $\langle \mathrm{RCA}_1(k)\rangle$ in $\langle \mathrm{RCA}_1(n)\rangle$. Since $\mathrm{RCA}(k)$ has the same subgroups as $\mathrm{RCA}(n)$, the f.g.-universality of $\langle \mathrm{RCA}_1(k)\rangle$ in $\mathrm{RCA}(k)$ then implies f.g.-universality of $\langle \mathrm{RCA}_1(n)\rangle$ in $\mathrm{RCA}(n)$. Thus, $U^2 + \mathbb{N} \subset U$, so $6 \in U$ implies $[36, \infty) \subset U$.

For the last claim, consider a contiguous neighborhood of size 2. Such a neighborhood is either entirely in $\mathbb{N}$ or in $-\mathbb{N}$, so if f and f^{-1} both have such neighborhood for all generators, they can be seen as elements of $\mathrm{Aut}(A^{\mathbb{N}})$. No subgroup of $\mathrm{Aut}(A^{\mathbb{N}})$ contains every finite group [8], so such a group cannot be f.g.-universal. □

In general, as $|A|$ grows the subgroups of $\mathrm{RCA}_{\{0,1\}}(A^{\mathbb{Z}})$ range over all finitely-generated groups of one-sided cellular automata by standard blocking arguments, so these groups can be very interesting, even though they are never f.g.-universal in $\mathrm{Aut}(A^{\mathbb{Z}})$.

5.3 Sofic shifts and the perfect core

Lemma 17. *Suppose $m, n \geq 2$, $2|\binom{m}{2}n^2$, $2|\binom{n}{2}m^2$. Then $\mathrm{PAut}[m; n; m; n]$ has a perfect subgroup G generated by six involutions, such that $\mathrm{PAut}[m; n] \hookrightarrow G$.*

Proof. Let $|B| = m, |C| = n$ and $A = B \times C \times B \times C$. The map $\updownarrow_B$ defined by $\updownarrow_B(x, x', y, y') = (y, x', x, y')$ is in $\mathrm{Alt}(A)$ under the conditions by a similar proof as that of Lemma 3. Similarly the symbol permutation $\updownarrow_C(x, x', y, y') =$

(x, y', y, x') is even. Define $\swarrow\!\!\nearrow_B = \updownarrow_B^{\sigma_1 \circ \sigma_2} = \updownarrow_B^{\sigma_1} \in \mathrm{PAut}[B; C; B; C]$ and $\swarrow\!\!\nearrow_C = \updownarrow_C^{\sigma_1 \circ \sigma_2} = \updownarrow_C^{\sigma_2} \in \mathrm{PAut}[B; C; B; C]$. Define also

$$\sigma_B = [\updownarrow_B, \swarrow\!\!\nearrow_B] = \sigma_1^2 \circ \sigma_3^{-2} \in \mathrm{PAut}[B; C; B; C]$$

$$\sigma_C = [\updownarrow_C, \swarrow\!\!\nearrow_C] = \sigma_2^2 \circ \sigma_4^{-2} \in \mathrm{PAut}[B; C; B; C]$$

For every symbol permutation $\pi \in \mathrm{Sym}(B \times C)$, the diagonal permutation $\pi \times \pi : A \to A$ is even.

It is well-known that $\mathrm{Alt}(A)$ is generated by three involutions, so let $|F| = 3$ be any set of symbol permutations corresponding to such a generating set. Then $F \cup F^{\sigma_1 \circ \sigma_2}$ generates all of $\updownarrow_B$, $\updownarrow_C$, $\swarrow\!\!\nearrow_B$ and $\swarrow\!\!\nearrow_B$, thus it generates σ_B and σ_C.

Now, it is easy to see that σ_B and σ_C and the symbol permutations $\pi \times \pi$ simulate four independent copies of $\mathrm{PAut}[B; C]$ in $\mathrm{PAut}[B; C; B; C]$, so the group $G = \langle F \cup F^{\sigma_1 \circ \sigma_2} \rangle$ contains an embedded copy of $\mathrm{PAut}[B; C]$. Since $\mathrm{Alt}(A)$ is perfect, all the generators of G can be written as a product of commutators of the generators, so also G is perfect. □

Theorem 12. *Let X be a sofic shift. Then the following are equivalent:*

- *The group $\mathrm{Aut}(X)$ has a perfect subgroup generated by six involutions containing every finitely-generated subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$ for any A.*
- *The group $\mathrm{Aut}(X)$ is not elementarily amenable.*
- *X has uncountable cardinality.*

Proof. Suppose first that X is uncountable. Standard embedding theorems [30, 42] show that $\mathrm{Aut}(A^{\mathbb{Z}}) \hookrightarrow \mathrm{Aut}(X)$ for any alphabet A. Let $|B| \geq 2, |C| \geq 5$ satisfy the assumptions of Lemma 17 and let $A = B \times C \times B \times C$ (e.g. $|B| = 2, |C| = 6$ so $|A| = 144$), so that $\mathrm{PAut}[B; C]$ is f.g.-universal and contained in $\mathrm{PAut}(A)$. Let G be the group provided by Lemma 17. Then G is a finitely-generated perfect subgroup of $\mathrm{PAut}(A)$, generated by six involutions, which contains every group of cellular automata on any alphabet. We have $G \hookrightarrow \mathrm{PAut}(A) \leq \mathrm{Aut}(A^{\mathbb{Z}}) \hookrightarrow \mathrm{Aut}(X)$.

If X is countable, then $\mathrm{Aut}(X)$ is elementarily amenable by [46], thus cannot contain a free group, thus cannot contain every finitely-generated subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$ for any nontrivial alphabet A. □

The *perfect core* $c(G)$ of a group G is the largest subgroup H such that $H = [H, H]$. The group $c(G)$ is contained in the commutator subgroup of G and (by definition) contains every perfect subgroup of G. Note that the conclusion of the previous theorem is stronger than simply finding an f.g.-universal f.g. subgroup of the perfect core, since a perfect group can contain non-perfect subgroups.

5.4 The abstract statement and the decidability of the word problem

Theorem 13. *There exists a finitely-generated residually finite perfect group G such that, letting $\mathcal{G}$ be the class of subgroups of G:*

- *G has decidable word problem and undecidable torsion problem, and does not satisfy the Tits alternative, and*

- *$\mathcal{G}$ is closed under finite extensions, direct products and free products, and contains all graph groups.*

Proof. Pick $G = \mathrm{PAut}(144)$ as in the proof of Theorem 12, so G is finitely-generated and perfect, and contains every finitely-generated group of cellular automata on every alphabet.

Groups of RCA on full shifts are residually finite and f.g. groups of RCA have decidable word problems [9], so G has these properties. Given an RCA, its periodicity is undecidable [28]. The f.g.-universality of G, together with the fact our proofs are algorithmic, then implies that it has an undecidable torsion problem.

Since the Tits alternative does not hold in $\mathrm{Aut}(A^{\mathbb{Z}})$ [43] and all graph groups are subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$ [30], the same results hold for $\mathcal{G}$. The set $\mathcal{G}$ has the same closure properties as the set of f.g. subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$, which by [30] include finite extensions and by [42] include direct products and free products. □

Let us say a few words about the (mainly expositional) implications of $\mathrm{PAut}(A)$ having a decidable word problem.

It is well-known that the group of RCA (over any alphabet) "has decidable word problem", in the sense that if one uses the standard recursive presentation by local rules, then one can check if a given composition of RCA evaluates to the identity map. Unfortunately, it is possible for group that is not finitely-generated to have several recursive presentations, such that the word problem is decidable in some of them, and is undecidable in others, see Example 5.3 in [33]. Thus the decidability of the word problem depends on the a priori "cultural" fact that the abstract group $\mathrm{Aut}(A^{\mathbb{Z}})$ is represented by local rules, so to get a precise statement, one needs to state the theorem either about the *presentation* of $\mathrm{Aut}(A^{\mathbb{Z}})$ (or the group together with its presentation) rather than about the abstract group, or alternatively one needs to quantify over all possible presentations and say that one of them has a decidable word problem.

In [9], this issue is circumvented by stating that for every finitely-generated subgroup, the word problem is decidable, but this result is essentially weaker: it is possible for a recursively presented group to have no recursive presentation with decidable word problem, such that all finitely-generated subgroups have a decidable word problem, see Example 5.4 in [33].

By Theorem 1, the fact $\mathrm{PAut}(A)$ has a decidable word problem is, as a statement, somehow the best of both worlds if one does not wish to explicitly refer to recursive presentations, yet wants to reap the benefits of decidability: The decidability of $\mathrm{PAut}(A)$, and the fact it is f.g.-universal, directly imply the decidability of the word problem for all finitely-generated subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$. Since our proofs are effective, in the sense that we explicitly show how to build elements of $\mathrm{PAut}(A)$ given elements of the standard presentation, i.e. local rules of RCA, it follows that $\mathrm{Aut}(A^{\mathbb{Z}})$ has a decidable word problem when using the standard presentation.

6 Questions

6.1 Automorphism groups of full $\mathbb{Z}$-shifts

The following question was mentioned in the introduction.

Question 1. *Let A be a nontrivial finite alphabet. Does* $\mathrm{Aut}(A^{\mathbb{Z}})$ *have a finitely-generated subgroup containing* $\mathrm{Aut}(A^{\mathbb{Z}})$ *as a subgroup? Is the commutator subgroup* $[\mathrm{Aut}(A^{\mathbb{Z}}), \mathrm{Aut}(A^{\mathbb{Z}})]$ *such a group?*

The latter question is two questions in one: the author does not know whether the commutator subgroup is finitely-generated, and does not know whether it has the first property. The question is also open at least for all transitive SFTs, but outside full shifts we do not even know when $\mathrm{Aut}(X)$ and $\mathrm{Aut}(Y)$ have the same subgroups (or even finitely-generated subgroups).

$m \geq 5$	$\approx \mathbb{Z}$	f.g.-univ.	f.g.-univ.	f.g.-univ.	f.g.-univ.
$m = 4$	$\approx \mathbb{Z}$	?	?	?	f.g.-univ.
$m = 3$	$\approx \mathbb{Z}$	?	?	?	f.g.-univ.
$m = 2$	$\approx \mathbb{Z}$	linear	?	?	f.g.-univ.
$m = 1$	trivial	$\approx \mathbb{Z}$	$\approx \mathbb{Z}$	$\approx \mathbb{Z}$	$\approx \mathbb{Z}$
	$n = 1$	$n = 2$	$n = 3$	$n = 4$	$n \geq 5$

Table 1: The structure of $\mathrm{PAut}[m; n]$.

Table 1 contains a partial summary of Theorem 1 and Theorem 2 in terms of what can be said about the set of f.g. subgroups. In the virtually cyclic cases, denoted by $\approx \mathbb{Z}$, it is easy to give a full description of the subgroup lattice. In the linear case $\mathrm{PAut}[2; 2]$, the group still seems quite difficult to understand, but linearity does give strong restrictions on subgroups. For example it follows that $\mathrm{PAut}[2; 2]$ satisfies the Tits alternative and does not contain copies of all finite groups (both of which imply that it is not f.g.-universal by [9, 43]). See below for more implications of linearity.

In the "?"-cases, we can find some interesting subgroups, and obtained that these groups are not subdirect products of linear groups. However, these groups remain mysterious, since we cannot really do any precise word-manipulation typical for cellular automata, yet do not have any upper bounds on subgroups.

Question 2. *Let* $|A| \in \{6, 8, 9\}$. *Does* $\mathrm{PAut}(A)$ *contain every finitely-generated group of reversible cellular automata? Does it satisfy the Tits alternative? What about* $\mathrm{PAut}[3; 4]$ *and* $\mathrm{PAut}[4; 4]$*?*

Recall that on all non-prime non-four alphabets we identified a single $f \in \mathrm{Aut}_1(A^{\mathbb{Z}})$ such that if $f \in \mathrm{PAut}(A)$, then $\mathrm{PAut}(A)$ is f.g.-universal, and when $|A| \notin \mathbb{P} \cup \{4, 6, 8, 9\}$, we showed $f \in \mathrm{PAut}(A)$, which yields the universality results. For alphabet sizes $6, 8, 9$, we are not able to prove that $f \notin \mathrm{PAut}(A)$.

Such questions can be studied algorithmically, to the following extent: Of course $f \in \mathrm{PAut}(A)$ is semidecidable. We do not know whether $f \notin \mathrm{PAut}(A)$ can be semidecided. However, write $\overline{\mathrm{PAut}(A)}$ for the properiodic completion of the group $\mathrm{PAut}(A)$, i.e. the (locally compact) group of permutations of periodic points of $A^{\mathbb{Z}}$ which can be approximated arbitrarily well by the action

of $\mathrm{PAut}(A)$. Now, $f \notin \overline{\mathrm{PAut}(A)}$ implies $f \notin \mathrm{PAut}(A)$, and the statement $f \notin \overline{\mathrm{PAut}(A)}$ is semidecidable. (But we do not know whether $f \in \overline{\mathrm{PAut}(A)}$ is semidecidable.)

Our brief studies in GAP and Python suggest (but did not prove) that for $|A| = 6$, $f \notin \overline{\mathrm{PAut}(A)}$, and that for $|A| \in \{8, 9\}$, $f \in \overline{\mathrm{PAut}(A)}$.

We have not looked at $\mathrm{PAut}[3; 4]$ and $\mathrm{PAut}[4; 4]$ in depth, as our original interest was in understanding the groups $\mathrm{PAut}(n)$, and $\mathrm{PAut}[3; 4]$ and $\mathrm{PAut}[4; 4]$ give no new information from this point of view since $\mathrm{PAut}(12)$ and $\mathrm{PAut}(16)$ are universal by using the decompositions $\mathrm{PAut}[2; 6]$ and $\mathrm{PAut}[2; 8]$. On the other hand, these groups are interesting from the point of view of trying to understanding naturally occurring f.g.-groups of cellular automata.

The homomorphism of [27] shows that $\mathrm{PAut}[3; 4]$ and $\mathrm{PAut}[4; 4]$, respectively, do not contain the partial shifts with respect to the decompositions $\mathrm{PAut}[2; 6]$ and $\mathrm{PAut}[2; 8]$, respectively, so at least as sets these groups are different.

A similar set of finitely many open cases comes from Theorem 4, where we do not know the f.g.-universality status of $\langle \mathrm{RCA}_1(n) \rangle$ for

$$n \in \{3, 4, 5, 7, 11, 13, 17, 19, 23, 29, 31\}.$$

We have not looked at these groups in detail.

Throughout the article, we have allowed the use of any symbol permutation. One obtains a large class of RCA groups by varying the permutation group allowed.

Question 3. *Let $G \leq \mathrm{Sym}(B_1 \times B_2 \times ... \times B_k)$ be a permutation group. What can be said about the group $\mathrm{PAut}_G[B_1; B_2; \cdots ; B_k]$ generated by partial shifts and symbol permutations in G?*

It is clear that most of the proofs would go through if only even permutations are allowed, and we have mainly chosen to include all permutations to allow uniform treatment of also the alphabet sizes $6, 8, 9$: In Theorem 8 we only needed to add a single element to $\mathrm{PAut}(A)$ in the end, to obtain universality. For these three alphabet sizes, it is not clear that the arguments go through with only even symbol permutations.

It is an open question whether $\mathrm{Aut}(\{0, 1\})$ is generated by the shift map and involutions [9]. By Theorem 12, the assumption that a group of cellular automata is generated by involutions does not put any restrictions on at least its set of subgroups. Two involutions are not enough, as $\mathbb{Z}_2 * \mathbb{Z}_2$ is the dihedral group which is virtually cyclic. We conjecture that three involutions can generate an f.g.-universal group of RCA.

For a finitely-generated group $G = \langle g_1, ..., g_k \rangle$, we say $f \in G$ is *distorted* if $\langle f \rangle$ is infinite and satisfies $\mathrm{wn}(f^n) = O(n)$ where

$$\mathrm{wn}(g) = \min\{\ell \mid \exists i_1, i_2, ..., i_\ell : g = g_{i_1} g_{i_2} ... g_{i_\ell}\}$$

It is open whether $\mathrm{Aut}(A^{\mathbb{Z}})$ contains elements which are distorted in some finitely-generated subgroup. Note that if G is finitely generated and $f \in G$ is distorted in a subgroup $f \in H \leq G$, then f is also distorted in G. Thus, by our main result, we can use $\mathrm{PAut}(A)$ as the canonical subgroup, and state the problem equivalently without quantification over f.g. subgroups:

Question 4. *Does $\mathrm{PAut}(A)$ contain distortion elements for some alphabet A?*

By the universality result, the question stays equivalent if we fix $|A| = 10$.

Finitely-generated linear groups can contain distorted elements, as for example the discrete Heisenberg group (of invertible unitriangular 3×3 matrices over $\mathbb{Z}$) has distorted cyclic center. However, distortion cannot happen in linear groups over fields with positive characteristic by [39, Lemma 2.10], so $\mathrm{PAut}(A)$ with $|A| = 4$ does not contain distortion elements. We do not know the answer for any other composite alphabet size.

Two other questions we do not know the answer to are whether $\mathrm{PAut}(A)$ contains torsion (i.e. periodic) finitely-generated infinite subgroups, or whether $\mathrm{PAut}(A)$ contains subgroups of intermediate growth. Again $\mathrm{PAut}[2;2]$ cannot have such subgroups by linearity.

Another natural direction to take is to further study the poset $\mathcal{P}$ of finitely-generated subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$ up to the algebraic simulation equivalence $G \approx H \iff G \leq H \leq G$. For example, this poset contains all finitely-generated free groups as one element. This poset embeds in a natural way in the lattice $\mathcal{L}$ of subgroup-closed sets of subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$. The lattice $\mathcal{L}$ obviously has a maximal element, namely the family of all f.g. subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$. Our main result states that this top element is actually in $\mathcal{P}$.

6.2 First-order theory

The existence of a universal subgroup implies that some types of questions turn into questions about a fixed finitely-generated group. Not all do – global properties such as homomorphic images need not behave well under passing to universal subgroups, see Example 1 for an example of a universal subgroup with a different abelianization. Another class of questions which a priori need not behave well under passing to universal subgroups is the first-order theory of $\mathrm{Aut}(A^{\mathbb{Z}})$, and one of the motivations for the search for universal subgroups was to understand this theory better. When viewed in this framework, our universality result is very weak, and in the end the conclusion is somewhat orthogonal.

In model-theoretic terms, our main result finds in $\mathrm{Aut}(A^{\mathbb{Z}})$ a substructure which is finitely-generated and contains every finitely-generated substructure of $\mathrm{Aut}(A^{\mathbb{Z}})$ as a substructure. This model-theoretic point of view leads to several questions.

Recall that a subgroup H of a group G is *elementary* if every true first-order sentence in G with parameters in H is also true directly in H. Here, first-order sentences have quantifies over elements of the group, and the language is that of group theory, that is, multiplication, identity and inverses.[3] For example the free group F_m (on m free generators) is an elementary subgroup of F_n when $2 \leq m < n < \infty$ [29].

Question 5. *Is there a finitely-generated group H of cellular automata which contains $\mathrm{Aut}(A^{\mathbb{Z}})$ (or at least every finitely-generated group of cellular automata) as an elementary subgroup? Can we take $H = \mathrm{PAut}(A)$?*

Question 6. *Does $\mathrm{Aut}(A^{\mathbb{Z}})$ have any finitely-generated elementary subgroups, and can the subgroup H in the previous question be taken to be elementary?*

[3] Identity and inverses are first-order definable, but in order for all substructures to be subgroups we need to include at least inverses in the language. Elementary subgroups will mean the same thing no matter which convention is used, again since inverses can be defined.

These questions are related to the problem of understanding the first-order theory of the groups $\mathrm{Aut}(A^{\mathbb{Z}})$. One motivation is that it is not known whether $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}}) \cong \mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$ [7], and we have not proved that the groups $\mathrm{PAut}(A)$ are all distinct either, for distinct alphabets A. If these groups had a different first-order theory, then of course they would not be isomorphic. An elementary embedding $H \leq G$ in particular implies equality of the first-order theories, which is called *elementary equivalence* (while a non-elementary embedding between two groups does not directly imply any inclusion relation between their first-order theories). The author does not know whether $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$ and $\mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$ are elementarily equivalent.

Any elementary embedding of $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$ into $\mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$ would necessarily map $\sigma \mapsto \sigma$ or $\sigma \mapsto \sigma^{-1}$, since any non-shift can be identified by Ryan's theorem [41], and for any fixed $|k| \neq 1$, a first-order sentence can separate σ and σ^k since σ does not have any roots in these two groups [24]. The author is not aware of any embedding of $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$ into $\mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$ which maps σ into $\{\sigma, \sigma^{-1}\}$.

The universal fragments of the first-order theories of $\mathrm{PAut}(A)$ (for composite $|A| \geq 10$) and $\mathrm{Aut}(A^{\mathbb{Z}})$ (for any $|A| \geq 2$) coincide with the corresponding fragment of the family of all finite groups, since every finite group can be embedded in these groups, and they are residually finite. It follows from a theorem of Tarski that these fragments are undecidable,[4] and thus also the existential fragment is undecidable.[5] To obtain this result, it is enough to show that $\mathrm{PAut}(A)$ has all finite groups as subgroups, which is much weaker than f.g.-universality.

It would be of interest to find first-order (or higher-order) statements that single out (classes or orbits of) infinite order RCA other than the shift, as this would connect the algebra to the dynamics. In other words, can one find definable sets of RCA with interesting properties? Is there a definable f.g.-universal f.g. subgroup?

One interesting first-order statement about $\mathrm{Aut}(A^{\mathbb{Z}})$ is Kopra's finitary version [32] of Ryan's theorem [41] which states that there exist two automorphisms whose centralizers intersect to the center of the group, i.e.

$$\exists a, b : \forall c : (ac = ca \wedge bc = cb \implies \forall d : dc = cd).$$

The center of the group is $\langle \sigma \rangle$ [41], so the orbit of the shift map is definable. It is not clear to the author whether the shift map itself, i.e. the set $\{\sigma, \sigma^{-1}\}$, is first-order definable.

6.3 Universality in other groups

In this section, we ask universality questions for some of our favorite groups and make some basic observations. Of course, one can ask about universality in other groups, and we invite the reader to add their favorite groups to the list.

In Example 1 we saw that free groups provide examples of groups that have f.g.-universal f.g. subgroups, but no universal f.g.-subgroups. In the example,

[4] This was observed for topological full groups in [22], though with the LEF property in place of residual finiteness.

[5] To prove this, simply negate propositions, which works since we are working with a single model. As a word of caution we note that the existential first-order theory of finite groups is trivially decidable.

the reason for non-universality was rather trivial (cardinality). Is there a countable group containing an f.g.-universal f.g. subgroup which is not universal? Is there a countable group containing an f.g.-universal f.g. subgroup but no universal f.g. subgroup? We expect that the answers are positive, but do not know such examples (though $\mathrm{Aut}(A^{\mathbb{Z}})$ could an example of both phenomena for all we know).

Question 7. *Is there an (f.g.-)universal f.g. subgroup of* $\mathrm{Aut}(A^{\mathbb{N}})$ *for some finite alphabet* A*?*

The groups $\mathrm{Aut}(A^{\mathbb{N}})$ for different $|A|$ have a different set of subgroups in general, as there are strong restrictions on even the finite subgroups [8]. Thus, we cannot expect a finitely-generated subgroup that contains a copy of every cellular automata group on every alphabet, unlike in the two-sided case.

Very little is known about embeddings between automorphism groups of higher-dimensional subshifts, even two-dimensional full shifts, for example it is not known whether we can have $\mathrm{Aut}(A^{\mathbb{Z}^{d'}}) \leq \mathrm{Aut}(B^{\mathbb{Z}^d})$ for $d' > d$, and whether $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}^2}) \leq \mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}^2})$ (see [25]). The following question seems to lead into similar problems.

Question 8. *Let* $d \geq 2$*. Does* $\mathrm{Aut}(A^{\mathbb{Z}^d})$ *have an (f.g.-)universal f.g. subgroup?*

It is shown in [4] that the asynchronous rational group (consisting of all asynchronous finite-state transductions defining a self-homeomorphism of $A^{\mathbb{N}}$, for a finite alphabet A) is not finitely-generated, so one can ask for universality results. The set of subgroups of the asynchronous rational group does not depend on the alphabet.

As for synchronous automata groups, as with one-sided subshifts, one needs to fix a single alphabet, or even finite groups pose a problem for universality (since there is no boundedly-branching rooted tree where all finite groups act). When one alphabet is fixed, the group of all synchronous automata transductions is not finitely generated, as it has infinite abelianization (consider the signs of permutations performed on different levels or the tree).

Question 9. *Is there an (f.g.-)universal automata group over a finite alphabet* A*? Does the asynchronous rational group have an (f.g.-)universal f.g. subgroup?*

Especially in connection with Theorem 3.3 of [3], one could also ask whether there are universal automata groups within automata groups of bounded activity.

Question 10. *Is there an (f.g.-)universal f.g. subgroup of the group of reversible Turing machines of [2]?*

A large finitely-generated subgroup of "elementary Turing machines" is constructed in the journal version of [2], but the author does not know whether it is f.g.-universal.

Topological full groups are another class where such a question can be asked. It seems plausible that marker arguments can be used to prove universality results at least on full shifts.

Question 11. *Let* X *be a subshift. When does the topological full group of* X *have an (f.g.-)universal f.g. subgroup?*

Some other groups with similar symbolic flavor are Thompson's V [11] and $2V$ [10], but these groups are finitely-generated.

All the groups considered above of course act on Cantor space. The homeomorphism group of Cantor space or any manifold of positive finite dimension is uncountable, and thus not finitely-generated. The homeomorphism group of Cantor space contains uncountably many non-isomorphic f.g. subgroups, and thus cannot contain an f.g.-universal subgroup, but it is not immediately clear to the author what happens with, for example, manifolds of positive finite dimension.

Question 12. *Let X be a topological space. When does the homeomorphism group of X contain an f.g.-universal f.g. subgroup?*

Acknowledgements

I have studied the linear part of $\mathrm{PAut}(A)$ for $|A| = 4$ with Pierre Guillon and Guillaume Theyssier, and the linear case of Lemma 13 is due to Theyssier. I thank Thibault Godin for several interesting discussions, and for suggesting Question 3. Some mistakes were spotted in discussion with Ilkka Törmä. I thank Laurent Bartholdi for pointing out that the automorphism group of a boundedly branching tree cannot contain copies of every finite group. The fact that the group of all synchronous automata transductions is not finitely-generated was shown to the author by Ivan Mitrofanov, by studying orbits of eventually periodic points. I thank Vesa Halava for pointing out some subtleties of first-order theories when working with multiple models.

References

[1] Scott Aaronson, Daniel Grier, and Luke Schaeffer. The classification of reversible bit operations. *Electronic Colloquium on Computational Complexity*, (66), 2015.

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

[3] Laurent Bartholdi, Vadim A. Kaimanovich, and Volodymyr V. Nekrashevych. On amenability of automata groups. *Duke Math. J.*, 154(3):575–598, 09 2010.

[4] J. Belk, F. Matucci, and J. Hyde. On the asynchronous rational group. *ArXiv e-prints*, November 2017.

[5] Tim Boykett. Closed Systems of Invertible Maps. *ArXiv e-prints*, December 2015. Available at `https://arxiv.org/abs/1512.06813`.

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

[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, John Franks, and Bruce Kitchens. Automorphisms of one-sided subshifts of finite type. *Ergodic Theory Dynam. Systems*, 10(3):421–449, 1990.

[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] Matthew G Brin. Higher dimensional thompson groups. *Geometriae Dedicata*, 108(1):163–192, 2004.

[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] 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`.

[13] V. Cyr, J. Franks, B. Kra, and S. Petite. Distortion and the automorphism group of a shift. *ArXiv e-prints*, November 2016.

[14] V. Cyr and B. Kra. The automorphism group of a minimal shift of stretched exponential growth. *ArXiv e-prints*, September 2015.

[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. The probability of generating the symmetric group. *Mathematische Zeitschrift*, 110(3):199–205, 1969.

[17] S. Donoso, F. Durand, A. Maass, and S. Petite. On automorphism groups of Toeplitz subshifts. *ArXiv e-prints*, January 2017.

[18] 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.

[19] Stefan Friedl. An introduction to 3-manifolds and their fundamental groups. *Preprint*, 2015.

[20] 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.

[21] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.9.2*, 2018.

[22] Rostislav Ivanovich Grigorchuk and Konstantin Medynets. On algebraic properties of topological full groups. *Sbornik: Mathematics*, 205(6):843–861, 2014.

[23] Mikhael Gromov. Hyperbolic groups. *Essays in group theory*, 8(75-263):2, 1987.

[24] Gustav A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory*, 3:320–375, 1969.

[25] Michael Hochman. Groups of automorphisms of SFTs. URL:http://math.huji.ac.il/˜mhochman/problems/automorphisms.pdf (version: 2018-08-07).

[26] Panurge (https://math.stackexchange.com/users/72877/panurge). Does there exist such a subgroup of a linear group? MathOverflow. URL:https://math.stackexchange.com/questions/1891722/does-there-exist-such-a-subgroup-of-a-linear-group (version: 2018-07-06).

[27] Jarkko Kari. Representation of reversible cellular automata with block permutations. *Theory of Computing Systems*, 29:47–61, 1996. 10.1007/BF01201813.

[28] 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.

[29] Olga Kharlampovich and Alexei Myasnikov. Elementary theory of free non-abelian groups. *Journal of Algebra*, 302(2):451–552, 2006.

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

[31] Dessislava H Kochloukova and Pavel A Zalesskii. Tits alternative for 3-manifold groups. *Archiv der Mathematik*, 88(4):364–367, 2007.

[32] Johan Kopra. Glider automorphisms on some shifts of finite type and a finitary ryan's theorem. In Jan M. Baetens and Martin Kutrib, editors, *Cellular Automata and Discrete Complex Systems - 24th IFIP WG 1.5 International Workshop, AUTOMATA 2018, Ghent, Belgium, June 20-22, 2018, Proceedings*, volume 10875 of *Lecture Notes in Computer Science*, pages 88–99. Springer, 2018.

[33] Sebastián Andrés Barbieri Lemp. *Shift spaces on groups: computability and dynamics*. PhD thesis, Université de Lyon, 2017.

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

[35] M. Lothaire. *Algebraic combinatorics on words*, volume 90 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2002.

[36] R.C. Lyndon and P.E. Schupp. *Combinatorial Group Theory*. Classics in Mathematics. Springer Berlin Heidelberg, 2015.

[37] V.L. Nisnewitsch. Über Gruppen, die durch Matrizen über einem kommutativen Feld isomorph darstellbar sind. *Matematicheskii Sbornik*, 50(3):395–403, 1940.

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

[39] Timm von Puttkamer and Xiaolei Wu. Linear groups, conjugacy growth, and classifying spaces for families of subgroups. *International Mathematics Research Notices*, page rnx215, 2017.

[40] D. Robinson. *A Course in the Theory of Groups*. Graduate Texts in Mathematics. Springer New York, 1996.

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

[42] Ville Salo. A note on subgroups of automorphism groups of full shifts. *Ergodic Theory and Dynamical Systems*, page 113, 2016.

[43] Ville Salo. No Tits alternative for cellular automata. *ArXiv e-prints*, September 2017.

[44] Ville Salo. Toeplitz subshift whose automorphism group is not finitely generated. *Colloquium Mathematicum*, 146:53–76, 2017.

[45] Ville Salo. Transitive action on finite points of a full shift and a finitary ryans theorem. *Ergodic Theory and Dynamical Systems*, pages 1–31, 2017.

[46] Ville Salo and Michael Schraudner. Automorphism groups of subshifts through group extensions. Preprint.

[47] Ville Salo and Ilkka Törmä. Block maps between primitive uniform and pisot substitutions. *Ergodic Theory and Dynamical Systems*, FirstView:1–19, 9 2014.

[48] 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`.

[49] B.A.F. Wehrfritz. Generalized free products of linear groups. *Proceedings of the London Mathematical Society*, 3(3):402–424, 1973.