Universal groups of cellular automata

Ville Salo
vosalo@utu.fi

February 5, 2019

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 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. For non-prime non-four alphabets, it 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 [43, 54, 51, 18, 14, 16, 21, 20, 15, 23, 48, 52, 3], 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 [10], 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 [31] 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 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 $m \geq 2, n \geq 3$, then $\mathrm{PAut}[m; n]$ is f.g.-universal in $\mathrm{RCA}(mn)$.*

This is proved in Section 4.1. The embeddings of finitely-generated subgroups are dynamical, in the sense that we concretely simulate cellular automata on encoded configurations.

The set of finitely-generated subgroups of $\mathrm{RCA}(A)$ does not depend on A as long as $|A| \geq 2$ by [35], 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).

The group $\mathrm{RCA}(A)$ is neither amenable nor locally linear when $|A| \geq 2$, so the following result shows that Theorem 1 is optimal.

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

- $\mathrm{PAut}[m] \cong \mathrm{PAut}[1; m] \cong \mathbb{Z} \times S_m$, *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.*

Both nonamenability and nonlinearity for $\mathrm{PAut}[m; n]$ for $m \geq 2, n \geq 3$ follow directly from f.g.-universality, but we give instead a uniform natural construction that proves the second and fourth item simultaneously by embedding groups of the form $\mathbb{Z}_k^\omega * \mathbb{Z}_\ell^\omega$, in Section 4.4. Linearity of $\mathrm{PAut}[2; 2]$ is proved in Section 4.3, where we show that $\mathrm{PAut}(4) \cong \mathbb{Z}_2^2 \rtimes \mathrm{GL}(2, \mathbb{Z}_2[\boldsymbol{x}, \boldsymbol{x}^{-1}])$.

Table 1 gives the characterizations of f.g. subgroups of $\mathrm{PAut}[m; n]$, by giving, in each case, a well-known group whose f.g. subgroups are the same as those of $\mathrm{PAut}[m; n]$. The number $k \geq 2$ in the table is arbitrary.

$m \geq 3$	$\mathbb{Z} \times S_n$	RCA(k)	RCA(k)
$m = 2$	$\mathbb{Z} \times S_n$	$\mathbb{Z}_2^2 \rtimes \mathrm{GL}(2, \mathbb{Z}_2[\boldsymbol{x}, \boldsymbol{x}^{-1}])$	RCA(k)
$m = 1$	1	$\mathbb{Z} \times S_n$	$\mathbb{Z} \times S_n$
	$n = 1$	$n = 2$	$n \geq 3$

Table 1: F.g. subgroups of PAut$[m; n]$ are precisely the f.g. subgroups of ...

We can also state the result in terms of alphabet size alone. Write PAut(A) for the group 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 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 PAut(n) for the group PAut(A) where $|A| = n$.

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

- *If $n \in \mathbb{P}$, then* PAut(n) $\cong \mathbb{Z} \times S_n$.
- *If $n = 4$, then* PAut(n) $\cong \mathbb{Z}_2^2 \rtimes \mathrm{GL}(2, \mathbb{Z}_2[\boldsymbol{x}, \boldsymbol{x}^{-1}])$.
- *If $n \notin \mathbb{P} \cup \{4\}$, then* PAut($n$) *is f.g.-universal in* RCA(n).

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

Finally, we obtain a corollary about the group $\langle \mathrm{RCA}_1(n) \rangle$ of RCA generated by those with biradius one. 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.*

This is proved in Theorem 9.

As mentioned above, one motivation for the result is that the groups Aut($A^{\mathbb{Z}}$), and more generally 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, in cases where we do not obtain universality, such study provides new examples of "naturally occurring" finitely-generated RCA groups.

The set of finitely-generated subgroups of Aut($A^{\mathbb{Z}}$) is relatively big: It is closed under direct and free products and finite extensions [48], contains the graph groups (a.k.a. right-angled Artin groups) [35], and contains a group not satisfying the Tits alternative [50] (we give another proof in Proposition 5). In the planned extended version of [3] 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 [33] provides a new proof of this.[1]

We state one corollary obtained in the symbolic dynamics setting (other embedding theorems are surveyed in [50]). 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.

[1]Though the extended version of [3] 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.

Theorem 5. *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 f.g. subgroup of* $\mathrm{Aut}(A^{\mathbb{Z}})$ *for any alphabet A.*
- *X has uncountable cardinality.*

This is proved in Theorem 10

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 finitely-generated 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 f.g. graph groups (that is, right-angled Artin 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 [36, 22], and having all finite groups as subgroups rules out automata groups.

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 [3], 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 [45], symbolic dynamics [38] 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 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 self-homeomorphisms of X that commute with the shift σ, 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.

[2] It is not known whether all hyperbolic groups are residually finite [26].

Words over an alphabet A [39] form a monoid A^* under concatenation, which is denoted $u \cdot v$ or uv. A word u is *m-unbordered* if $vu = uv' \implies |v| = 0 \vee |v| \geq m$, and *unbordered* if it is $|u|$-unbordered. 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 ${}^{\omega}u$ and a right tail as u^{ω}. 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.

The clopen sets in $A^{\mathbb{Z}}$ are precisely the Boolean algebra generated by basic cylinders. We say a clopen set F is *m-unbordered* if $F \cap \sigma^i(F) = \emptyset$ for $i \in [1, m-1]$. Clearly u is m-unbordered if and only if $[u]_i$ is an m-unbordered clopen set in the full shift.

For two words u, v of the same length, write $D(u, v)$ for $\{i \in [0, |u|-1] \mid u_i \neq v_i\}$. 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 $w_i^T = w_{|w|-1-i}$. We also reverse other things such as subshifts, by reversing points in the sense $x_i^T = x_{-i}$, 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 X-track is also referred to as the *top* track, and the Y-track the *bottom* 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 *neighborhoods* are sets N such that $f(x)_0$ depends only on $x|_N$, and *bineighborhoods* are defined in the obvious way.

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 $n \in \mathbb{N}$.

The commutator conventions are

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

For g, h elements of the same group, write $g^h = h^{-1}gh$. If $\phi : X \to Y$ is bijection, we also use 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 *subdirect product* of groups $G_1, ..., G_k$ is a subgroup of $G_1 \times \cdots \times G_k$. A *subquotient* of a group G is a quotient of a subgroup.

The *(transfinite) derived series* of a group G is $G^{(0)} = G$, $G^{(\alpha+1)} = [G^{(\alpha)}, G^{(\alpha)}]$ for successor ordinals and $G^{(\alpha)} = \bigcap_{\beta<\alpha} G^{(\beta)}$ for limit ordinals. If this stabilizes at $G^{(k)} = 1$ for a finite ordinal k (i.e. G is solvable), then k is called the the *derived length* of G. This series terminates at some ordinal α, and $G^{(\alpha)}$ is called the *perfect core* of G. The *(transfinite) lower central series* is $G_0 = G$, $G_{\alpha+1} = [G, G_\alpha]$ for successor ordinals and $G_\alpha = \bigcap_{\beta<\alpha} G_\beta$. This always stabilizer at some ordinal α, and we call G_α the *hypocenter*.

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 a proposition P, eventually writes the answer "yes" if $P \in \mathcal{P}$, 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

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

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, but 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. □

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 $[g, h]$ are a generating set for the 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 ring of sets generated by $\mathcal{E}$, i.e. unions, intersections and relative complements of events. The Boolean algebra where the events live is typically the algebra of clopen sets in some space.

The same idea can be used with S_3 and S_4, using the fact that they are not nilpotent, and their hypocenters are A_3 and A_4, respectively. Concretely, using for example the formula $[(0\ 1\ 2), (0\ 1)] = (0\ 1\ 2)$, we can condition an even permutation on the intersection of two events, assuming one is a "primitive event" (so we can apply an arbitrary permutation conditioned on it), and the other is any "composite event" (so by induction we can apply an even permutation conditioned on it). See for example Lemma 4 for a formal result to this effect.

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 or conditioned actions*, and use terms such as "increase the control" to refer to the tricks described above. The main application is to subshifts, whose Boolean algebra of clopen sets is generated by basic cylinders $[a]_i$.

3.2 Alternating groups and 3-hypergraphs

The following lemma is from [7], 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 $G = \mathrm{Alt}(V(\mathcal{G}))$.*

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 3 which strengthens a result of

[7]. Many results like this are known, see e.g. [1, 6, 55], 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. (The swap of two wires is directly among the generators only if $|A| \equiv 0, 1 \bmod 4$.)

Lemma 3. *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. It is enough to show that the 3-cycles $(u;\ v;\ w)$ where for some j, $|\{u_j, v_j, w_j\}| = 3$, and $u_i = v_i = w_i$ for $i \neq j$, are generated. Namely, the result then follows by applying Lemma 2 to the hypergraph with vertices A^n and edges (u, v, w) that only differ in one position.

It is enough to show that the permutation that applies the cycle (0 1 2) in coordinate j if all other coordinates contain 0, and is the identity otherwise, is generated. Namely, the other generators are conjugate to it or its inverse by even symbol permutations. Let us fix the coordinate j, and for a set of coordinates $N \not\ni j$ and permutation π, write π^N for the permutation that applies π in coordinate j if all coordinates in N contain 0, and is the identity otherwise. We need to construct $(0\ 1\ 2)^{[0,j-1]\cup[j+1,n-1]}$.

By induction, we can assume that the map $(0\ 1\ 2)^{[j-\ell,\ldots,j-1]\cup[j+1,\ldots,j+r]}$, which applies (0 1 2) at j if and and only if the ℓ symbols to the left and r symbols to the right are all 0, is generated. By symmetry, it is enough to show that also $(0\ 1\ 2)^{[j-\ell,\ldots,j-1]\cup[j+1,\ldots,j+r+1]}$ is generated.

If $|A|$ is odd, define

$$\pi = (01;\ 11)(02;\ 12)\cdots(0(|A|-1);\ 1(|A|-1)) \in \mathrm{Alt}(A^2),$$

and if $|A|$ is even, define

$$\pi = (01;\ 11)(02;\ 12)\cdots(0(|A|-1);\ 1(|A|-1))(20;\ 21) \in \mathrm{Alt}(A^2).$$

In each case, π has the property that, when applied to a word ab, if $a = 0$ then the value of a changes if and only if $b \neq 0$, and it always changes to 1 in this case.

Let ψ be the map that applies π successively in the subwords

$$[j+r, j+r+1], [j+r-1, j+r], ..., [j+1, j+2].$$

Observe that if $w_{j-\ell,\ldots,j-1} w_{j+1,\ldots,j+r} = 0^{\ell+r}$, then $\psi(w)_{j+1} \in \{0, 1\}$ and we have $\psi(w)_{j+1} = 1 \iff w_{j+r+1} \neq 0$.

Let β apply the permutation $(00;\ 10)(02;\ 12)$ at $[j, j+1]$. Note that β^ψ does not modify any coordinate other than j. Now, since $(0\ 1\ 2) = [(0\ 1\ 2), (0\ 1)]$, we have

$$[(0\ 1\ 2)^{[j-\ell,j-1]\cup[j+1,\ldots,j+r]}, \beta^\psi] = (0\ 1\ 2)^{[j-\ell,j-1]\cup[j+1,j+r+1]},$$

and we conclude. □

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 [19], 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 natural linear structure of A^2, so they will also give only affine maps with respect to the natural linear structure of 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 $(a, b, c) \mapsto (a, b, c + ab)$ are even as permutations of A^4), and a quick search in GAP [24] shows that the set of all even permutations of A^4 is generated by 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

We prove Theorem 1 in Section 4.1. Theorem 2 is a combination of Lemma 8, Theorem 7 and Theorem 8, which are proved in sections 4.2, 4.3 and 4.4, respectively. In addition to the results mentioned, we discuss some basic structural properties of subgroups which arise in the course of the proof.

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.

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

$$\pi^F(x, y)_j = \begin{cases} (x_j, \pi(y_{[j-i,j-i+n-1]})_i) & \text{if } i \in [0, n-1], \sigma^{j-i}(x) \in F \\ (x_j, y_j) & \text{if } \forall i \in [0, n-1] : \sigma^{j-i}(x) \notin F. \end{cases}$$

The map π^F performs the permutation π on the bottom track under every occurrence of F on the top track. One should think of this as a conditional application of π on the bottom track, where the condition is that the top 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.

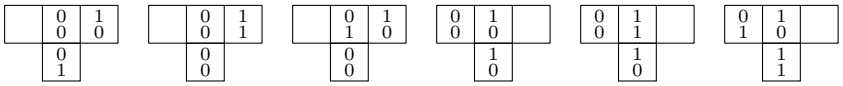
Example 1: Let $f = (00; 10; 01)^{[01]_0}$. To apply f, locate occurrences of 01 on the top track, and permute the words under the occurrences according to the

permutation $(00;10;01)$:

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

where we write occurrences of the controlling clopen set $[01]_0$ 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*

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

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 4. *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 hypocenter 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 hypocenter, then $h = [h_1, g_1][h_2, g_2]...[h_k, g_j]$ for some h_i in the hypocenter and g_i in G. It is thus enough to show that $[h_i, g_i]^{[wa]_m} \in P(X,G)$. 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 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 5. *Let $|B|, |C| \geq 2$. Then for every even permutation ϕ of C and any clopen $F \subset B^{\mathbb{Z}}$, ϕ^F is in* $\mathrm{PAut}[B; C]$.

Proof. For every n, the hypocenter 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 bottom 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. □

Lemma 6. *Let $|B| \geq 2, |C| \geq 3$. Then for any n-unbordered clopen set $F \subset B^{\mathbb{Z}}$, $\pi^F \in \mathrm{PAut}[B; C]$ for every $\pi \in \mathrm{Alt}(C^{|u|})$.*

Proof. We may assume $|B| \geq 2, |C| \geq 3$. Any clopen set F is a union of disjoint basic cylinders $[u]_i$, and it follows from the assumption that the word u is necessarily n-unbordered for each u appearing in this decomposition of F. We can take each i and the lengths $|u|$ to be equal, and if $F = \bigcup_{j=1}^{\ell} [u_j]_i$ for a finite set of words $u_j \in B^m$, then the union is disjoint and

$$\pi^F = \pi^{[u_\ell]_i} \circ \cdots \circ \pi^{[u_1]_i}$$

for any $\pi \in \mathrm{Alt}(C^n)$, because by the assumption that F is n-unbordered, each coordinate can be affected by at most one of these ℓ applications of π. By conjugation with the shift, it is enough to show that $\pi^{[u]_0} \in \mathrm{PAut}[B; C]$ for any n-unbordered word u and any $\pi \in \mathrm{Alt}(C^{|u|})$.

We may suppose $B = \{0, ..., |B| - 1\}, C = \{0, ..., |C| - 1\}$. Let (x, y) stand for some configuration in $(B \times C)^{\mathbb{Z}}$. By Lemma 5, $\pi^{[u]_i} \in \mathrm{PAut}[B; C]$ for all $\pi \in \mathrm{Alt}(C)$. Since u is n-unbordered, it follows that the maps $\psi^{[u]_0}$, where $\psi = \pi_1 \times \pi_2 \times \cdots \times \pi_{|u|}$ is a Cartesian product of n even symbol permutations, are in $\mathrm{PAut}[B; C]$.

We claim that it is enough to show $(00;\ 10;\ 20)^{[u]_0}$ is in $\mathrm{PAut}[B; C]$. To see this, observe that then also $(00;\ 10;\ 20)^{[u]_j} \in \mathrm{PAut}[B; C]$ by conjugation by partial shifts. By symmetry, also $(00;\ 01;\ 02)^{[u]_j} \in \mathrm{PAut}[B; C]$. Since we can perform even symbol permutations in any coordinate under occurrences of u, it is easy to see that the set of 3-tuples $(v_1,\ v_2,\ v_3)$, $v_i \in C^2$, such that $(v_1;\ v_2;\ v_3)^{[u]_j} \in \mathrm{PAut}[B; C]$, is weakly connected as a hypergraph. Thus, we can perform any even permutation of C^2 in any two consecutive symbols under each occurrence of u by Lemma 2. By Lemma 3, we can then perform any even permutation in each segment of length n under every occurrence of u. Note that by n-unborderedness, these permutations indeed happen in disjoint segments of y, for distinct occurrences of u in x.

Suppose first that $|B|$ is even. Then we claim that the map f_k defined by $f_k(x, y)_i = (x_i, y_i)$ if $y_{i+k} \neq 0$, $f_k(x, y)_i = (x_i, \pi(y_i))$ if $y_{i+k} = 0$, is in $\mathrm{PAut}[B; C]$ where $\pi = (1\ 2)$.

We claim that

$$f_k = (\sigma_1^{-k} \circ (1\ 2)^{[E]_0} \circ \sigma_1^k \circ (\psi^{[0]_0})^{\updownarrow})^2,$$

where $\psi = (0\ 1)(2\ 3) \cdots ((|B| - 2)\ (|B| - 1))$, $E = \{0, 2, 4, ..., |B| - 2\} \subset B$, and $\updownarrow : (B \times C)^{\mathbb{Z}} \to (C \times B)^{\mathbb{Z}}$ exchanges the tracks. Conjugation by $\updownarrow$ is performed in the groupoid sense, and means that we modify the top track conditioned on the bottom track. To see that the formula holds, observe that since the set of positions where 0 occurs in y never changes, the effect on x is cancelled. If $y_{i+k} = 0$, then the symbol at x_i will be even during exactly one of the two

applications, while otherwise it is even either zero times or two times, and the flip cancels out.

Then consider $[f_k, (0\ 1\ 2)^{[u]_0}]^2$. Since $[(0,1),(0,1,2)]^2 = (0,1,2)$, it does $(0\ 1\ 2)$ at y_i at least if $x_{[i,i+|u|-1]} = u$ and $y_{i+k} = 0$, which is what we want (for $k = 1$). Let us analyze its side-effects. If $x_{[i,i+|u|-1]} = u$ and $y_{i+k} \neq 0$, then as long as $k < n$, y_{i+k} is nonzero after all partial applications (since u is n-unbordered and f_k does not modify the set of coordinates where 0 occurs), so in this case the rotation $(0\ 1\ 2)$ cancels, and y_i retains its value. In fact, one quickly sees that the only danger is the coordinate y_{i-k}, when $x_{[i,i+|u|-1]} = u$. In this coordinate, we apply the flip $(1\ 2)$ if and only if $y_{i+k} = 0$ and $y_i \in \{0,1\}$ (if $y_{i+k} \neq 0$, then since $[f_k, (0\ 1\ 2)^{[u]_0}]$ was applied twice, the flip cancels).

To account for these problematic coordinates y_{i-k} where $x_{[i,i+|u|-1]} = u$, let us continue by applying

$$([f_k, (0\ 1\ 2)^{[u]_0}]^2)^{(0\ 2\ 1)^{[u]_0}},$$

i.e. rotate y_i backward if $x_{[i,i+|u|-1]} = u$, apply the above map, and rotate back. The effect on y_i is as above, namely rotation by $(0\ 1\ 2)$, since rotations form an abelian group. Thus, in total we do $(0\ 2\ 1)$ at y_i whenever $y_{i+k} = 0$, $x_{[i,i+|u|-1]} = u$. But now at y_{i-k} we actually perform the flip $(1\ 2)$ under the precise same condition on the original value of y_i, i.e. $y_i \in \{1,2\}$, since before the second application, we rotated it back to its original value. Thus this undesired flip is undone.

Repeating all of the above twice, we perform $(0\ 1\ 2)$ at y_i under the same condition $y_{i+1} = 0$, $x_{[i,i+|u|-1]} = u$. In other words,

$$(([f_1, (0\ 1\ 2)^{[u]_0}]^2)^{(0\ 2\ 1)^{[u]_0}} \circ [f_1, (0\ 1\ 2)^{[u]_0}]^2)^2 = (00;\ 10;\ 20)^{[u]_0}$$

is in $\mathrm{PAut}[B;C]$, and the result follows from Lemma 3 as explained above.

Next, suppose $|B|$ is odd, let $a \neq [u]_k$ and consider the definition

$$f'_k = (\sigma_1^{-k} \circ (1\ 2)^{[a]_0} \circ \sigma_1^k \circ (\psi^{[0]_0})^{\updownarrow})^{|B|-1}$$

where again $k < n$, and $\psi = (0\ 1\ 2\ \cdots\ (|B|-1))$. This map applies $(1\ 2)$ at y_i iff $y_{i+k} = 0$ or $x_{i+k} = a$. We can in fact repeat the previous argument almost verbatim.

Consider $[f'_k, (0\ 1\ 2)^{[u]_0}]^2$. It does $(0\ 1\ 2)$ at y_i if $x_{[i,i+|u|-1]} = u$ and $y_{i+k} = 0$. If $x_{[i,i+|u|-1]} = u$ and $y_{i+k} \neq 0$, then as long as $k < n$, y_{i+k} is nonzero after all partial applications (since u is n-unbordered and f'_k does not modify the set of coordinates where 0 occurs), so in this case y_i retains its value. Again the only danger are the coordinates y_{i-k} such that $x_{[i,i+|u|-1]} = u$. In this coordinate, we apply the flip $(1\ 2)$ if and only if either $y_{i+k} = 0$ and $y_i \in \{0,1\}$, or if $u_0 = a$.

Whether or not $u_0 = a$, as in the case when $|B|$ is even,

$$(([f'_1, (0\ 1\ 2)^{[u]_0}]^2)^{(0\ 2\ 1)^{[u]_0}} \circ [f'_1, (0\ 1\ 2)^{[u]_0}]^2)^2$$

is precisely the desired map $(00;\ 10;\ 20)^{[u]_0}$ □

Remark 1. *The two cases depending on the parity of $|B|$ are really about the two cases $(|B|,|C|) \in \{(2,3),(3,3)\}$, which were solved last. For larger $|C|$, we can separate data and control, and for example for $|C| \geq 6$ (and any $|B| \geq 2$),*

since $\mathrm{Alt}(C \setminus \{0\})$ *is perfect, one can rather directly write a formula for an arbitrary even permutation of* $C \setminus \{0\}$ *at* y_i *controlled by* $x_{[i,i+|u|-1]} = u$ *and* $y_{i+1} = 0$*, without side effects. After this, one again concludes by Lemma 5 and Lemma 3.*

Lemma 7. *Let* $|B|, |C| \geq 2$ *and* $A = B \times C$*, and let* $G \leq \mathrm{Aut}(A^{\mathbb{Z}})$*. Suppose that for unbordered words* w *of any large enough length* ℓ*, the maps* $\pi^{[w]_i}$ *and* $\pi^{[ww]_i}$ *are in* G *for all* $\pi \in \mathrm{Alt}(C^\ell)$ *and* $i \in \mathbb{Z}$*. Then* G *contains an embedded copy of every finitely-generated group of cellular automata.*

Proof. Let $r \geq 1$ be arbitrary and large enough, let $\ell = 24r$ and pick a corresponding unbordered word w.

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 w^m in x with m finite (points x with this property are dense since $|w| \geq 2$ and w is unbordered). We split the subword of y under the occurrence of w^m into $u_1 v_1 u_1' v_1' \cdot u_2 v_2 u_2' v_2' \cdots u_m v_m u_m' v_m'$ 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 $u_i v_i$ 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 $u_i v_i$, 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 $(u_1 u_2 \cdots u_m (v_m)^T (v_{m-1})^T \cdots (v_1)^T)^{\mathbb{Z}}$ and decode the contents of $[0, 12rm]$ into the new contents below the occurrence of w^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 $4r' + \ell$ 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 ℓ is needed because we need to know whether the sequence of ws continues. 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 w^m can appear in x for arbitrarily large m, this is an embedding of $\mathrm{Aut}(C^{\mathbb{Z}})$ into $\mathrm{Aut}(A^{\mathbb{Z}})$. See [48] 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 $\mathrm{Aut}(C^{\mathbb{Z}})$ [35].

We now recall the concept of stairs from [31]. Define $L \subset C^{4r}$ as the left stairs of f, i.e. the possible contents $\boxed{\begin{smallmatrix}\mathrm{u}\\ \mathrm{v}\end{smallmatrix}}$ 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 [31], 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 any bijections.

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 bottom track, conditioned on having w on the top track. To see that this permutation is even, observe that the first permutation is diagonal (i.e. of the form $\pi \times \pi$ for a permutation π) 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" consecutive occurrences of w for $1 \leq i < m$, i.e. in the middle of each occurrence of ww, 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 ℓ on the bottom track, conditioned on $[ww]_{-12r}$ on the top track. Note that the permutation is applied with an offset, and an individual application under an occurrence of ww 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 w^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 [31] for the detailed argument.

Now, we deal with the remaining $12r$ coordinates under left corners of maximal occurrences w^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 bottom track, conditioned on $[w]^c_{-\ell} \cap [w]_0 = [w]_0 \setminus [ww]_{-\ell}$ on the top track (the latter form shows that we have this controlled application in G). 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 w^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 w. □

Theorem 1. *If $m \geq 2, n \geq 3$, then* $\mathrm{PAut}[m; n]$ *is f.g.-universal in* $\mathrm{RCA}(mn)$.

Proof. Lemma 6 implies that for any unbordered u, any $\pi \in \mathrm{Alt}(C^{|u|})$ can be performed controlled by any $|u|$-unbordered clopen set, in particular $[u]_i$ and $[uu]_i$ for any i. We conclude by Lemma 7. □

Lemma 7 also directly applies to the commutator subgroup of $\mathrm{RCA}(B \times C)$ (since large enough alternating groups are perfect), so we also obtain that the commutator subgroup (even the perfect core) of $\mathrm{RCA}(B \times C)$, for any $|B|, |C| \geq 2$, is f.g.-universal. See Theorem 10 for a stronger result.

4.2 The prime case

Lemma 8. *If $n \in \mathbb{P}$, then* $\mathrm{PAut}(n) \cong \langle\sigma\rangle \times S_n$.

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

4.3 The linear case

By Lemma 8, $\mathrm{PAut}(A)$ 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".

Write $\mathbb{Z}_2[\boldsymbol{x}, \boldsymbol{x}^{-1}]$ for the ring of Laurent polynomials over the two-element field $\mathbb{Z}_2$. Write $\mathbb{Z}_2((\boldsymbol{x}))$ for the field of formal Laurent series over $\mathbb{Z}_2$ (with only finitely many negative powers of $\boldsymbol{x}$), which contains the ring $\mathbb{Z}_2[\boldsymbol{x}, \boldsymbol{x}^{-1}]$. For any (commutative unital) ring R, write $\mathrm{GL}(n, R)$ for the group of invertible n-by-n matrices over R.

Theorem 7. *The group* $\mathrm{PAut}(4)$ *is linear, and has an* 8*-dimensional representation over* $\mathbb{Z}_2((\boldsymbol{x}))$*. In fact,*

$$\mathrm{PAut}(4) \cong \mathbb{Z}_2^2 \rtimes \mathrm{GL}(2, \mathbb{Z}_2[\boldsymbol{x}, \boldsymbol{x}^{-1}]).$$

Proof. We begin with the second claim. 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. Give also $A^{\mathbb{Z}}$ the structure of an abelian group, by cellwise addition.

Consider maps of the form $x \mapsto f(x) + a^{\mathbb{Z}}$, where $a \in A$ and f is a reversible linear cellular automaton in the sense that $f(x + y) = f(x) + f(y)$ for all $x, y \in A^{\mathbb{Z}}$. A straightforward computation shows that such maps form a subgroup G of $\mathrm{Aut}(A^{\mathbb{Z}})$. The subgroup K of maps $x \mapsto x + a^{\mathbb{Z}}$ for $a \in A$ is isomorphic to $\mathbb{Z}_2^2$, and a direct computation shows that it is normal in G. The subgroup H of reversible linear cellular automata is also a subgroup, and we have $KH = G$, $K \cap H = 1$. It follows that $G = K \rtimes H$ is an internal semidirect product.

We can in a standard way see H as the group $\mathrm{GL}(2, \mathbb{Z}_2[\boldsymbol{x}, \boldsymbol{x}^{-1}])$, by writing the local rule of a cellular automaton f satisfying $f(x + y) = f(x) + f(y)$ as a matrix, so $G \cong \mathbb{Z}_2^2 \rtimes \mathrm{GL}(2, \mathbb{Z}_2[\boldsymbol{x}, \boldsymbol{x}^{-1}])$.

The generators of $\mathrm{PAut}(4)$ are contained in G since all symbol permutations of A are affine, and conversely it is straightforward to show that linear symbol permutations and partial shifts are a generating set for H, see e.g. [32], and the maps $x \mapsto x + a^{\mathbb{Z}}$ are among generators of $\mathrm{PAut}(4)$ as well. It follows that $\mathrm{PAut}(4) = G$.

For the first claim, since $[G : H] = 4$ and H is a 2-dimensional matrix group, where the entries can be seen to be in the field $\mathbb{Z}_2((\boldsymbol{x}))$, the induced representation of G is 8-dimensional over the same field. □

The action ϕ of $\mathrm{GL}(2, \mathbb{Z}_2[\boldsymbol{x}, \boldsymbol{x}^{-1}])$ on $\mathbb{Z}_2^2$ is the following: Let

$$h : \mathrm{GL}(2, \mathbb{Z}_2[\boldsymbol{x}, \boldsymbol{x}^{-1}]) \to \mathrm{GL}(2, \mathbb{Z}_2)$$

be the group homomorphism obtained by applying the ring homomorphism extending $\boldsymbol{x}^i \mapsto 1$ in each entry. The action ϕ is the pullback of the natural action of $\mathrm{GL}(2, \mathbb{Z}_2)$ on $\mathbb{Z}_2^2$ through h.

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 $\mathbb{Z}_2 \wr \mathbb{Z}$ (actually two natural embeddings of it, one acting on the top track and one on the bottom).

4.4 Non-linearity and non-amenability

We prove that apart from trivial cases (where the group is virtually cyclic and thus linear over any field admitting invertible matrices of infinite order), none of $\mathrm{PAut}[B;C]$ are amenable, and $\mathrm{PAut}[2;2]$ is the only linear case. This follows from natural embeddings of groups of the form $(\mathbb{Z}/m\mathbb{Z})^\omega * (\mathbb{Z}/k\mathbb{Z})^\omega$, where $m \leq |B|, k \leq |C|$.

In all cases $|B|, |C| \geq 2$ except $\mathrm{PAut}[2;2]$, *all* groups of the form $G^\omega * H^\omega$ are in $\mathrm{PAut}[B;C]$ for finite groups G, H, by f.g.-universality and by closure properties by Theorem 11, but we give the simple direct argument and explain why the groups $(\mathbb{Z}/m\mathbb{Z})^\omega * (\mathbb{Z}/k\mathbb{Z})^\omega$ are indeed typically not even subdirect products of linear groups. The embedding is by RCA with one-sided bineighborhoods, thus we also obtain these subgroups in $\mathrm{Aut}((B \times C)^{\mathbb{N}})$.

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 9. *Let $|B| = m, |C| = k$. Let G, H be abelian groups with $|G| \leq m$, $H \leq k$. Then $G^\omega * H^\omega \leq \mathrm{PAut}[B;C]$.*

Proof. Let $B = \{0, ..., m-1\}, C = \{0, ..., k-1\}$. The assumption $|G| \leq m$, $H \leq k$ is equivalent to the assumption that G and H act on B and C, respectively, with at least one free orbit. Fix such an action. 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

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

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 $(0^\mathbb{Z}, {}^\omega 0.10^\omega)$ 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:

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

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

Proof. A stronger fact is true: 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 cyclic. 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 by the normal form theorem of free products [40]. □

The following lemma is classical. We give a direct proof mimicking [45, Theorem 8.1.11] as suggested by user Panurge on the MathOverflow website [30].

Lemma 11. *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 [45, 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 12. *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 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 9). By [42] (see also [56]), 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 8. *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, if $|B| \geq m$ and $|C| \geq k$, then $(\mathbb{Z}/m\mathbb{Z})^\omega * (\mathbb{Z}/k\mathbb{Z})^\omega \leq \mathrm{PAut}[B; C]$ by Lemma 9. If $m = k = 2$, Lemma 10 gives non-amenability. If $m = 2, k = 3$, Lemma 12 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. See Proposition 4.

As a side note, we mention that the embedding in Lemma 9 is by one-sided RCA with one-sided inverses, which, unlike the result for $\mathrm{PAut}[B; C]$, does not follow from closure properties.

Proposition 1. *Let $A = B \times C$, and let G, H be abelian groups with $|G| \leq |B|$ and $|H| \leq |C|$. Then $G^\omega * H^\omega \leq \mathrm{Aut}((B \times C)^{\mathbb{N}})$.*

Proof. In the construction of Lemma 9, the generators are involutions and their neighborhoods are contained in $-\mathbb{N}$. Flipping the neighborhoods does not change the group, and gives reversible maps in $\mathrm{Aut}(A^{\mathbb{N}})$. □

For $|A| \geq 8$, $\mathrm{Aut}(A^{\mathbb{N}})$ is non-linear, as it does not even satisfy the Tits alternative [50]. By the previous proposition, $\mathrm{Aut}(A^{\mathbb{N}})$ is also non-linear for $|A| = 6$.

4.5 Modifying just one track

The proof of Lemma 5 implements the maps ϕ^F by elements of $\mathrm{PAut}[B;C]$ which only modify the bottom track. This is 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, which is much easier to understand than that of $\mathrm{PAut}(A)$.

This provides a new proof of the two-sided case of [50].

Proposition 2. *Let $|B|, |C| \geq 2$ and let $R[B;C] \leq \mathrm{PAut}[B;C]$ be the subgroup generated by the partial shift on the bottom track, and symbol permutations that only modify the bottom 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 bottom track [31], the group does not change if we replace the partial shift on the bottom track by the one on the top track. Observe also that every cell on the bottom 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 3. *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 top track. Then G is $\ker\phi$-by-$\mathbb{Z}$. 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 $x = {}^{\omega}0.10^{\omega}$, 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 $x = {}^{\omega}0.10^{\omega}$. □

Corollary 1. *Let $|B|, |C| \geq 2$. Then $G = P(B^{\mathbb{Z}}, \mathrm{Sym}(C))$ is (locally finite)-by-$\mathbb{Z}$. 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-$\mathbb{Z}$, and the kernel of ϕ is clearly locally finite when H is finite since $H^{\beth_1}$ is locally finite. Thus G is (locally finite)-by-$\mathbb{Z}$. 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 $n \geq 5$ is non-solvable. □

Proposition 4. *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 $x = {}^\omega 0.10^\omega$. □

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 $g_i({}^\omega 010^\omega, a) = ({}^\omega 010^\omega, ga)$ for all i (and of course if $|C| \geq 3$ already $\mathrm{Sym}(C)$ is not nilpotent).

We recover the two-sided case of [50].

Proposition 5. *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 (locally finite)-by-cyclic, thus elementary amenable, thus does not contain a free group in two generators. It is not virtually solvable by Corollary 1. □

Note that the group $R[B;C]$ in Proposition 2 is not equal to the group $\mathrm{RAut}(B^{\mathbb{Z}} \times C^{\mathbb{Z}}) \cap \mathrm{PAut}[B;C]$ in general: the f.g.-universality proofs in fact build copies of f.g.-universal cellular automata groups precisely inside $\mathrm{RAut}(B^{\mathbb{Z}} \times C^{\mathbb{Z}}) \cap \mathrm{PAut}[B;C]$.

5 Corollaries

5.1 The optimal radius for an f.g.-universal group 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 $N = \{-r, \dots, r\}$, 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 and biradius for f.g.-universality, for all but finitely many alphabets.

Theorem 9. *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 1, U contains all composite numbers except possibly 4, since $\mathrm{PAut}(n) \leq \langle \mathrm{RCA}_1(n) \rangle$.

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 a 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 [9], 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 $\mathrm{Aut}(A^{\mathbb{Z}})$.

The last claim is only true for contiguous neighborhoods of size two, and the theorem does not apply to e.g. $N = \{-1, 1\}$. Indeed, for the purpose of group embeddings one can consider the case $N = \{-1, 1\}$ to be the case of "radius-1/2 RCA", and by a standard blocking argument (see [41]) and with a little bit of work one can indeed generate f.g.-universal groups this way (for some alphabets).

5.2 Sofic shifts and the perfect core

Lemma 13. *Let $|B| = m, |C| = n$. Then the maps $(a, a', b, b') \mapsto (b, a', a, b')$ and $(a, a', b, b') \mapsto (a, b', b, a')$ are in $\mathrm{Alt}(B \times C \times B \times C)$ if and only if $2 | \binom{m}{2} n$ and $2 | \binom{n}{2} m$.*

Proof. The permutation $(a, a', b, b') \mapsto (b, a', a, b')$ is even if and only if the number of unordered pairs $\{(a, a', b, b'), (b, a', a, b')\}$ is even. The number of such pairs is $\binom{m}{2} n^2$. Symmetrically $(a, a', b, b') \mapsto (a, b', b, a')$ is even if and only if $2 | \binom{n}{2} m^2$. □

Lemma 14. *Suppose $m, n \geq 2$, $2 | \binom{m}{2} n$ and $2 | \binom{n}{2} m$. 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 symbol permutations $\updownarrow_B, \updownarrow_C$ defined by $\updownarrow_B(x, x', y, y') = (y, x', x, y')$ and $\updownarrow_C(x, x', y, y') = (x, y', y, x')$ are in $\mathrm{Alt}(A)$ under the conditions by the above lemma. 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 $\mathrm{PAut}[B;C;B;C]$: one in the even cells of the top track, one in the odd cells, and similarly two copies on the bottom track. Thus 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 elements in $\mathrm{Alt}(A)$, so also G is perfect. □

Theorem 10. *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 f.g. subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$ for any alphabet A.*
- *The group $\mathrm{Aut}(X)$ is not elementarily amenable.*
- *X has uncountable cardinality.*

Proof. Suppose first that X is uncountable. Standard embedding theorems [35, 48] show that $\mathrm{Aut}(A^{\mathbb{Z}}) \hookrightarrow \mathrm{Aut}(X)$ for any alphabet A. The choice $|B| = 2, |C| = 4$ satisfies the assumptions of Lemma 14. Let $A = B \times C \times B \times C$, so that $\mathrm{PAut}[B;C]$ is f.g.-universal and contained in $\mathrm{PAut}(A)$. Let G be the group provided by Lemma 14. 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 $G \hookrightarrow \mathrm{PAut}(A) \leq \mathrm{Aut}(A^{\mathbb{Z}}) \hookrightarrow \mathrm{Aut}(X)$.

For any countable subshift X, $\mathrm{Aut}(X)$ is elementarily amenable by [53], thus cannot contain a free group, thus cannot contain every finitely-generated subgroup of $\mathrm{Aut}(A^{\mathbb{Z}})$ for any nontrivial alphabet A. This paper is unpublished, but the case of countable sofics can be obtained by adapting [47, Proposition 2]. □

Note that we do not claim that $\mathrm{Aut}(X)$ has an f.g.-universal f.g. subgroup for any X other than a full shift. See Question 8.

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.

5.3 The abstract statement

Theorem 6. *There exists a finitely-generated residually finite perfect group G such that, letting $\mathcal{G}$ be the class of finitely-generated 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 f.g. graph groups (that is, right-angled Artin groups).*

Proof. Pick $G \leq \mathrm{PAut}(64)$ as in the proof of Theorem 10, 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 [10], so G has these properties. The periodicity of RCA is undecidable [33]. 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 $\mathrm{Aut}(A^{\mathbb{Z}})$ [50] and all f.g. graph groups are subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$ [35], the same results hold for $\mathcal{G}$. The set $\mathcal{G}$ has the same closure properties as the set of subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$, which by [35] include finite extensions and by [48] include direct products and free products. □

5.4 Finitely subgenerated cellular automata groups

We make some basic observations about which non-finitely-generated subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$ can be embedded in our f.g.-universal f.g. groups based on abstract arguments only.

For any group G, write $\mathrm{S}G$ for its set of subgroups, and write $\mathrm{SF}G$ for its *finitely subgenerated subgroups*, i.e. those subgroups $H \leq G$ such that $H \leq K$ for some finitely-generated subgroup of G. write $\mathcal{G}' = \mathrm{SF\ RCA}(A)$ for some nontrivial alphabet A (recall that this does not depend on A).

Lemma 15. *Let G be a group. We have $\mathrm{S}G = \mathrm{SF}G$ if and only if G has a universal finitely-generated subgroup, i.e. $G \hookrightarrow K \hookrightarrow G$ for some f.g. group K.*

Proof. If $\mathrm{S}G = \mathrm{SF}G$, then since $G \in \mathrm{S}G$ there is a finitely-generated subgroup $K \leq G$ containing G. If $G \hookrightarrow K \leq G$ then also $H \hookrightarrow K$ for all subgroups $H \leq G$. □

Lemma 16. *Suppose G has an f.g.-universal f.g. subgroup. If $\mathrm{S}G$ is closed under countable free products (resp. countable direct products), then so is $\mathrm{SF}G$. If $\mathrm{S}G$ is closed under direct products and finite extensions, then so is $\mathrm{SF}G$.*

Proof. For finite direct and free products, the result follows since K^n and $K * K * \cdots * K$ are finitely-generated for any f.g.-universal f.g. group K. For infinite ones, observe that in particular $K * K \leq K$ and $K \times K \leq K$ for any f.g.-universal f.g. K, which implies that the set of subgroups of K is also closed under countable free and direct products [48].

Every finite extension of a group H is a subgroup of $H \wr S_n$ for large enough n, and conversely $H \wr S_n$ has H^n as a finite-index subgroup. Suppose $H \in \mathrm{SF}G$, i.e. $H \leq K$ for an f.g.-universal f.g. K. Since $\mathrm{S}G$ is closed under direct products and finite extensions, the wreath product of K by any symmetric group S_n is in $\mathrm{SF}G$, thus $H \wr S_n \leq K \wr S_n \leq K$, implying that every virtually-H group is in $\mathrm{SF}G$. □

Theorem 11. *The class $\mathcal{G}'$ is closed under countable free and direct products and finite extensions.*

From these closure properties, we obtain also that the free product of all finite groups, constructed as a CA group in [2], is in $\mathcal{G}'$.

We conjecture that all countable locally finite residually finite groups are in $\mathcal{G}'$, as it seems clear that the construction in [35] can be performed directly. We do not know whether the group constructed in [12] is in $\mathcal{G}'$.

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?*

Lemma 6 says much more about $\mathrm{PAut}[m; n]$ than what is needed for f.g.-universality, and we are optimistic that applied to large enough alphabets it is already enough to prove a positive answer to the former question (thus, combined with the results of this paper, all $\mathrm{PAut}(n)$-groups for $n \notin \mathbb{P} \cup \{4\}$ would be universal). We plan to study its implications in a future work.

The latter question is two questions in one: the author does not know whether the commutator subgroup is finitely-generated (this has been previously asked in [49]), and does not know whether it is a universal one. 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).

In Theorem 4, 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 cases 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 2. *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?*

If we restrict to even permutatations, then for many alphabets, in particular whenever $|B|$ and $|C|$ are large enough, the arguments of the present paper can be used to establish f.g.-universality.

It is an open question whether $\mathrm{Aut}(\{0, 1\}^{\mathbb{Z}})$ is generated by the shift map and involutions [10]. By Theorem 10, 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 [15]. 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 3. *Does* $\mathrm{PAut}(A)$ *contain distortion elements for some alphabet* A*?*

By the universality result, the question stays equivalent if we fix $|A| = 6$. In [17], a notion of *range-distortion* is defined. This notion is implied by distortion, and occurs in automorphism groups of all uncountable sofic shifts [27]. Since our group-embeddings are by simulation, it follows that $\mathrm{PAut}(A)$ also contains range-distorted elements.

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 [44, Lemma 2.10], so $\mathrm{PAut}(A)$ with $|A| = 4$ does not contain distortion elements.

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, discussed previously in [50]. 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 embeddability (and identifying $G \approx H \iff G \hookrightarrow H \hookrightarrow G$). For example, this poset contains all finitely-generated free groups as one element. This poset embeds in a natural way in the lattice $\mathcal{L}$ whose elements are subgroup- and isomorphism-closed collections of f.g. subgroups of $\mathrm{Aut}(A^{\mathbb{Z}})$, under inclusion. 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 $\mathcal{P}$.

Finally, it would also be of interest to study universality for submonoids of $\mathrm{End}(A^{\mathbb{Z}})$, the endomorphism monoid of $A^{\mathbb{Z}}$ consisting of all cellular automata under composition, taking the identity CA id as the monoid identity. The invertible part of a universal or f.g.-universal submonoid must then be universal or f.g.-universal in $\mathrm{Aut}(A^{\mathbb{Z}})$, so this problem is at least as hard as the problem studied here.

One can also consider the semigroup of cellular automata without fixing an identity element, and define universality and f.g.-universality similarly, allowing any idempotent CA to play the role of the identity CA.

6.2 First-order theory of $\mathrm{RCA}(A)$

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 3 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 $2 \leq m < n < \infty$ [34].

Question 4. *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 5. *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?*

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 $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}}) \cong \mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$ [8], 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 [46], 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 [28]. 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? Is the commutator subgroup $[\mathrm{RCA}(A), \mathrm{RCA}(A)]$ first-order definable?

[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.

[4] This was observed for topological full groups in [25], 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.

One interesting first-order statement about $\mathrm{Aut}(A^{\mathbb{Z}})$ is the finitary version of Ryan's theorem [46] in [37], 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 $\langle \sigma \rangle$ [46], 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.

We begin by noting that there is are some well-known non-finitely generated group that have universal finitely-generated subgroups:

Example 2: The abelian group $(\mathbb{Q}^d, +)$ is not f.g. but $\mathbb{Z}^d$ is an f.g.-universal f.g. subgroup. On the other hand, $(\mathbb{R}^d, +)$ has no f.g.-universal f.g. subgroup or a countable universal subgroup, by Hamel bases. ○

Example 3: The (non-abelian) 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 the examples, 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, or (equivalently) is there one 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 for all we know).

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 [9]. 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. However, for a fixed alphabet we do not see a reason why f.g.-universality would not be possible. (The case $|A| = 2$ is trivial [28].)

Question 6. *Is there an (f.g.-)universal f.g. subgroup of* $\mathrm{Aut}(A^{\mathbb{N}})$ *for some finite alphabet* $|A| \geq 3$*?*

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 $d' > d$, $|A|, |B| \geq 2$, and whether $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}^2}) \leq \mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}^2})$ (see [29]). The following question seems to lead into similar problems.

Question 7. *Let* $d \geq 2$*. Does* $\mathrm{Aut}(A^{\mathbb{Z}^d})$ *have an (f.g.-)universal f.g. subgroup?*

Another obvious direction to look at are sofic shifts. For some simple sofics it is easy to show there are no f.g.-universal subgroups, and some even have finitely-generated automorphism groups, but for most of them we have no idea. In particular, we do not know the answer for any mixing SFT.

Question 8. *Let X be a sofic shift. When does* $\mathrm{Aut}(X)$ *have an (f.g.)-universal f.g. subgroup?*

This problem does not seem feasible at the moment: It is not known when $\mathrm{Aut}(Y)$ embeds into $\mathrm{Aut}(X)$ for mixing SFTs X, Y. Trying to find non-trivial self-embedding of subgroups of $\mathrm{Aut}(X)$ into $\mathrm{Aut}(X)$ runs into similar difficulties.

The author does not know another class of subshifts where such a universality question would be interesting. We note, however, that the non-f.g. automorphism groups of minimal subshifts constructed in [10, 51] both have an f.g.-universal f.g.-subgroups, namely $\langle\sigma\rangle$. In [10], $(\mathbb{Q}, +)$ is constructed, in [51], the dyadic rationals.

It is shown in [5] 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 [4], 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 [3]?*

A large finitely-generated subgroup of "elementary Turing machines" is constructed in the planned extended version of [3], 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 [13] and $2V$ [11], 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 (in the CA sense) of $\mathrm{PAut}(A)$ for $|A| = 4$ with Pierre Guillon and Guillaume Theyssier, and the linear case of Lemma 9 is due to Theyssier. I thank Thibault Godin and Ilkka Törmä for several interesting discussions. Question 2 was suggested by Godin. I thank Ilkka Törmä for spotting some typos. 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] Roger C Alperin. Free products as automorphisms of a shift of finite type. 1988.

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

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

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

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

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

[8] 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.

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

[10] 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.

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

[12] Ezra Brown. Periodic seeded arrays and automorphisms of the shift. *Transactions of the American Mathematical Society*, 339(1):141–161, 1993.

[13] James W. Cannon, William J. Floyd, and Walter R. Parry. Introductory notes on Richard Thompson's groups. *Enseignement Mathématique*, 42:215–256, 1996.

[14] E. Coven and R. Yassawi. Endomorphisms and automorphisms of minimal symbolic systems with sublinear complexity. *ArXiv e-prints*, November 2014. Available at `https://arxiv.org/abs/1412.0080`.

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

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

[17] Van Cyr, John Franks, and Bryna Kra. The spacetime of a shift endomorphism. *Transactions of the American Mathematical Society*, 371(1):461–488, 2019.

[18] 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.

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

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

[21] 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.

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

[23] 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.

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

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

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

[27] Pierre Guillon and Ville Salo. *Distortion in One-Head Machines and Cellular Automata*, pages 120–138. Springer International Publishing, Cham, 2017.

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

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

[30] 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).

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

[32] Jarkko Kari. Linear cellular automata with multiple state variables. In *STACS 2000 (Lille)*, volume 1770 of *Lecture Notes in Comput. Sci.*, pages 110–121. Springer, Berlin, 2000.

[33] 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.

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

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

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

[37] 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.

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

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

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

[41] Cristopher Moore and Timothy Boykett. Commuting cellular automata. *Complex Systems*, 11(1):55–64, 1997.

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

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

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

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

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

[47] Ville Salo. Groups and monoids of cellular automata. In Jarkko Kari, editor, *Cellular Automata and Discrete Complex Systems*, volume 9099 of *Lecture Notes in Computer Science*, pages 17–45. Springer Berlin Heidelberg, 2015.

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

[49] Ville Salo. Transitive action on finite points of a full shift and a finitary Ryan's theorem. *ArXiv e-prints*, October 2016. Accepted in Ergodic Theory and Dynamical Systems.

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

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

[52] 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.

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

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

[55] 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`.

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