Groups and Monoids of Cellular Automata

Ville Salo

Groups and monoids of cellular automata*

Ville Salo
vosalo@utu.fi

Center for Mathematical Modeling,
University of Chile

Abstract. We discuss groups and monoids defined by cellular automata on full shifts, sofic shifts, minimal subshifts, countable subshifts and coded and synchronized systems. Both purely group-theoretic properties and issues of decidability are considered.

Keywords: automorphism groups, cellular automata, subshifts

1 Motivation

1.1 From CA to monoid actions

Consider a system (X, f) with a (discrete) time-evolution rule $f : X \to X$. The set X is thought of as the set of all possible states of the system, and f tells us how the system evolves as time progresses. If the system is currently in state $x \in X$, it will be in state $f(x)$ after one time step. Systems that fit this general picture are studied in physics as models of the real world, in computer science as models of computation, and in mathematics for their intrinsic interest. In the world of cellular automata (CA), X is typically the set of bi-infinite sequences over a finite alphabet, and f is a cellular automaton on this space.[1]

Questions we ask about such systems can be both dynamical and computational (or a combination of the two). When X has a topological or measurable structure, often the motivating question on the side of dynamics is how 'chaotic' the system is. Trying to understand what is chaotic about a system leads to the study of properties such as transitivity, mixing and entropy. The study of what is not chaotic about it leads to the study of periodicity, almost periodicity, equicontinuous factors and spectral theory. For cellular automata, a range of different behaviors are known to be possible. Another common motivating question on the side of both dynamics and computation is whether the system is 'universal'. We wish to understand which other systems our system can simulate, in one sense or another.

A particularly interesting case in all these considerations is when f is reversible, that is, no information is lost when f is applied. Typically, we are

* The author was supported by FONDECYT Grant 3150552.

[1] Later, we will instead fix f to be the left shift map on X, and see cellular automata in another way.

interested in a strong, structural kind of reversibility where there is a concrete inverse time-evolution rule $g : X \to X$ such that $f \circ g$ and $g \circ f$ are identity maps on X. The importance of reversibility in physics is that the laws of nature seem to be reversible, and thus it makes sense to make such an assumption on our models. In computer science, reversible computation is an interesting programming paradigm promising challenges for theoreticians, but also allows more energy-efficient computation. In mathematics, reversibility often makes systems more malleable to the development of theory.

Now, what happens if we have two rules? Suppose $f : X \to X$ and $g : X \to X$ are two evolution rules on X, that is, we have two transformations on X which we be applied in any order. This can model many situations. For example, we can apply f and g at random, so that X has two ways to evolve at each time step, and we want to understand what the limit behavior is likely to be. This is a very simple example of a (discrete) random dynamical system. In parallel computing, we can think of f and g as two computations that are happening in parallel, and we need to understand their interaction to know the good or legal orders to apply them in. In this case, the order in which the maps are applied might be chosen by an adversary. The reversibility of a system with two evolution rules can be defined as simply f and g being reversible: it automatically follows that every finite composition of f and g is reversible, as one can apply the inverses of f and g in the reverse order to undo their actions.[2]

Abstracting from this, in the not necessarily reversible case we obtain the mathematical concept of a monoid action, where instead of a single function on X, we have a countable discrete monoid M acting on X by functions. More precisely, we associate to each $m \in M$ a function $\phi_m : X \to X$, and write $m \cdot x = \phi_m(x)$ for short. We require that the obvious compatibility conditions $m \cdot m' \cdot x = mm' \cdot x$ and $1 \cdot x = x$ hold. The systems (X, f) with a single time-evolution rule are modeled by setting $M = \mathbb{N}$, and $n \cdot x = f^n(x)$ for all $n \in \mathbb{N}$. The systems with two evolution rules are most generally modeled by setting M to be the free monoid[3] with two generators a, b and defining the action of M on X by $a \cdot x = f(x)$ and $b \cdot x = g(x)$.

When the operations are reversible, we usually consider group actions instead,[4] that is, we choose the monoid M to have multiplicative inverses (so that it is a group). A group action should of course have the additional compatibility condition that the inverse g^{-1} of $g \in G$ undoes the action of g on every element. This is automatic: if $a \in M$ and $a^{-1} \in M$ is its inverse (that is,

[2] Note that if f and g have been applied to x, the resulting state does *not* carry information in which order, and how many times, f and g have been applied. We can only reverse their action if we know in which order they have been applied.

[3] This is just the set of all words over the alphabet $\{a, b\}$ with concatenation as the multiplication operation

[4] However, no-one forces us to: for example, from a reversible CA, we obtain both an $\mathbb{N}$-action and a $\mathbb{Z}$-action. While these systems may look the same, their properties may be different. For example, many $\mathbb{N}$-actions of CA are expansive (that is, there are *positively expansive* CA). A reversible CA cannot be expansive as an $\mathbb{N}$-action, but $\mathbb{Z}$-actions by reversible CA can be expansive.

$aa^{-1} = a^{-1}a = 1$), then the action of $a^{-1} \in M$ is automatically the inverse of the action $a \in M$ by the compatibility condition for the monoid action:

$$a \cdot (a^{-1} \cdot x) = aa^{-1} \cdot x = 1 \cdot x = x = a^{-1}a \cdot x = a^{-1} \cdot (a \cdot x).$$

Thus, the natural compatibility conditions for a group action are the same as for a monoid action. If we have a single reversible time-evolution rule f, we obtain a natural action of $\mathbb{Z}$ by the same formula as in the non-reversible case, but extending to negative powers in the obvious way. In the case of two reversible actions, we obtain an action of the free group on two generators (see Section 2), again by the same formula. Considering the element $1 \in \mathbb{N}$ or $1 \in \mathbb{Z}$, the same formula shows that actions of $\mathbb{N}$ and $\mathbb{Z}$ are in one-to-one correspondence with systems with a time-evolution rule, and ones with a reversible time-evolution rule, respectively.

For most of the notions for $\mathbb{N}$-actions and $\mathbb{Z}$-actions, such as expansivity, transitivity, entropy and almost equicontinuity, there exist one or more corresponding notions that apply more generally to monoid or group actions. For example, one-dimensional expansivity for $\mathbb{Z}$-actions is defined by the formula $\exists \epsilon > 0 : \forall x, y \in X : \exists n \in \mathbb{Z} : d(f^n(x), f^n(y)) > \epsilon$. The formula defining expansivity for a general monoid is obtained by replacing $\mathbb{Z}$ by the monoid and f^n by the action of n. Sometimes additional conditions are needed on the monoid for the definition to work. For example, the entropy of a group action is measured along a Følner sequence, and thus requires amenability.[5]

The generalization allows us to ask what the dynamics of a finite (or even infinite) set of cellular automata looks like. We can choose a set of cellular automata F, let them generate a free monoid or group, and investigate the properties of the corresponding action. We can also fix the monoid to be M, and ask what M-actions of cellular automata look like. For example, it is known that the entropies of $\mathbb{N}$-actions by cellular automata on one-dimensional full shifts are precisely the class Π_1 of positive real numbers [GZ12]. What is the corresponding class for $\mathbb{N}^2$-actions of cellular automata (given by two CA f and g satisfying $f \circ g = g \circ f$)? For $\mathbb{Z}$-actions?[6]

1.2 From monoid actions to the endomorphism monoid

Now, let us return to the simple systems (X, σ) with a single time-evolution rule and suppose now that X is a compact Hausdorff space, and $\sigma : X \to X$ is continuous. It turns out that there is a monoid that one can attach to any such system: let $\mathrm{End}(X)$[7] be the set of all continuous functions $f : X \to X$ such that $\sigma \circ f = f \circ \sigma$ (as functions). Then $\mathrm{End}(X)$ becomes a monoid, called the *endomorphism monoid*, under function composition. We define $\mathrm{Aut}(X)$, the

[5] *Sofic entropy* applies more generally to sofic groups.[Bow10]

[6] The entropies of $\mathbb{Z}$-actions are just the entropies of reversible cellular automata. Characterizing the set of entropies in this case (on full shifts) seems to be essentially harder than in the non-reversible case.

[7] We omit σ from the notation $\mathrm{End}(X)$ since we consider it an intrinsic part of X.

automorphism group, as the restriction of $\mathrm{End}(X)$ to the elements which are bijective. From the assumption that X is compact and Hausdorff, it follows that every bijective continuous function on X has a continuous inverse. Since the inverse is easily seen to also commute with σ, $\mathrm{Aut}(X)$ is indeed a group under function composition. The endomorphism monoid and the automorphism group act on X in the obvious way: $f \cdot x = f(x)$.

This gives another way to see the set of cellular automata on a full shift: Let $X = S^{\mathbb{Z}}$ and let $\sigma : X \to X$ be the left shift map defined by $\sigma(x)_i = x_{i+1}$. Then $\mathrm{End}(X)$ is precisely the set of cellular automata on X: the continuous shift-commuting maps are precisely the ones admitting a spatially uniform local rule. Thinking of cellular automata as elements of the endomorphism monoid, and considering its action on X, we get a more global way to look at cellular automata, as this point of view encompasses not only the possible dynamics and computational power of individual cellular automata, but also their possible interactions.

In this paper we take a very simplified approach to this interaction, by forgetting the action of $\mathrm{End}(X)$ on X. Thus, we are interested in the abstract structure of the monoid $\mathrm{End}(X)$, and in particular the group $\mathrm{Aut}(X)$. This omits many interesting questions – for example, chaoticity or universality of a cellular automaton or a family of cellular automata does not (to our knowledge) in any way differentiate it among the other elements of $\mathrm{End}(X)$.[8] All that matters is which equalities $f_n \circ f_{n-1} \circ \cdots \circ f_1 = g_m \circ g_{m-1} \circ \cdots \circ g_1$ hold, when f_i and g_i are cellular automata. In the case of groups, it only matters which compositions of cellular automata are equal to the identity map on X.

While dynamical properties are out of the question, there are many things we can ask: For any property of groups (of which there are many), we can ask if $\mathrm{Aut}(X)$ has this property. Is it abelian? Is it amenable? For many group-theoretic decidability questions (of which there are many) we can ask if the question is decidable for $\mathrm{Aut}(X)$. Is the word problem decidable? What about the torsion problem? We can also ask if there are alternative descriptions of $\mathrm{Aut}(X)$, or connections with previously known groups.

It turns out that many interesting things can be said when X is a full shift over an alphabet S of size at least 2: For example, every finite group can be embedded in $\mathrm{Aut}(X)$, as can $\mathbb{Z}$ and free groups with a countable number of generators [Hed69,BLR88]. On the other hand, this group is residually finite and has a decidable word problem.

Fixing the action σ on $S^{\mathbb{Z}}$ makes it natural to consider also subshifts $X \subset S^{\mathbb{Z}}$, where we forbid a possibly infinite set of finite words from appearing in points of $S^{\mathbb{Z}}$. There are uncountably many subshifts X, and to each we associate the monoid $\mathrm{End}(X)$ and the group $\mathrm{Aut}(X)$, which act on X by function application. On each subshift X, $\mathrm{End}(X)$ still corresponds to the usual cellular automata,

[8] It is a very interesting question which properties have such algebraic definitions. Equicontinuity corresponds to eventual periodicity and by *Ryan's theorem* the shift maps are precisely the center of $\mathrm{Aut}(X)$ [Rya72] and more generally of $\mathrm{End}(X)$ [Sal14b] on mixing SFTs, but we don't know much more.

defined by a local rule; of course, it may be hard or impossible to tell which local rules give a well-defined map on X.

It turns out that the known constructions on full shifts can be carried out in many subshift X under some chaoticity assumptions on the action of the shift map on X. In fact, we show in Section 3 that we can embed the automorphism group of a full shift in many subshifts, such as all positive entropy sofic shifts [BLR88]. In Section 6, we show that similar constructions, and much more, can be carried out on the larger classes of synchronized and coded systems – in particular on coded systems we obtain a large set of groups as automorphism groups [FF96].

We also show examples of subshifts on which the automorphism group is essentially smaller, and some ways to control this. In Section 5 we discuss some interesting recent results in the case where either the word complexity grows slowly or recurrence times are short. In particular, in the case of subshifts with linear word complexity (for example, ones generated by primitive substitutions), we seem to be very close to a full understanding of the set of automorphism groups. In the case of countable sofic shifts, the author is working on the characterization of the automorphism groups, and we give an example of such a computation in Section 4.

Remark 1. Since, on the full shift, Ryan's theorem guarantees that there is an algebraic way to separate the shift map from the others (as it is the center of the group), we have no need to carry it in the structure $\mathrm{Aut}(X)$ explicitly. However, this is not true in general, as for example in minimal and coded systems we can have large abelian automorphism groups (so the group is its own center). In this case, it makes sense to think of σ as part of the algebraic structure, and consider for example the group $\mathrm{Aut}(X)/\langle\sigma\rangle$ instead of $\mathrm{Aut}(X)$. This simplifies many problems, as for example the characterization of these groups is known in the linear word complexity case.

2 Definitions and basic results

We give basic definitions of dynamical systems. In particular for the case of subshifts with $\mathbb{Z}$-actions, some standard references are [Kůr03,LM95,Kit98].

By a *dynamical (M-)system* we mean a pair (X, M, ϕ) where X is a compact metric zero-dimensional space, M is a countable discrete monoid, and M acts on X by $\phi_m : X \to X$ for $m \in M$, that is,

$$\phi_1(x) = x \text{ and } \forall m, m' \in M : \phi_{m\cdot m'}(x) = \phi_m(\phi_{m'}(x)).$$

Usually, the action is left implicit, and we write simply (X, M) for the system and $m \cdot x$ for $\phi_m(x)$. Of particular interest to us are the *subshifts* $(X, \mathbb{Z}^d, \sigma)$, topologically closed sets $X \subset S^{\mathbb{Z}^d}$ which are invariant under the *shifts* $\sigma_{\boldsymbol{v}}$ defined by $\sigma_{\boldsymbol{v}}(x)_{\boldsymbol{w}} = x_{\boldsymbol{w}+\boldsymbol{v}}$, where S is some finite alphabet. The subshift $S^{\mathbb{Z}^d}$ is called

the *full shift (over S)*. A subshift $X \subset S^{\mathbb{Z}^d}$ is a dynamical system with a $\mathbb{Z}^d$-action given by the shifts. If d is not specified, we by default study the *one-dimensional* setting where $d = 1$, that is, the set $S^{\mathbb{Z}}$ of two-way infinite sequences, and explicitly state when studying the *multidimensional* case $d > 1$.

In the one-dimensional case,[9] subshifts are characterized as sets of sequences in a full shift where none of a (possibly infinity) set of *forbidden words* occurs. Yet another characterization is the following: Let $L \subset S^*$ be a set of words over S. We say L is *extendable* if $\forall w \in L : \exists a, b \in S : awb \in L$. The *factor-closure* of L is the set $F(L) = \{u \in S^* \mid \exists v, v' \in S^* : vuv' \in L\}$. Subshifts are precisely the sets of infinite words whose finite subwords belong to the factor-closure of a fixed extendable language. Thus, if L is extendable, we define

$$\mathcal{L}^{-1}(L) = \{x \in S^{\mathbb{Z}} \mid \forall a, b : x_{[a,b]} \in F(L)\}.$$

We write $\mathcal{L}(X)$ for the *language* of X, that is, the set of words occurring in X. It is always factor closed, and $\mathcal{L}(\mathcal{L}^{-1}(L)) = F(L)$ and $\mathcal{L}^{-1}(\mathcal{L}(X)) = X$ for an extendable language L and a subshift X. We write $\mathcal{L}_n(X) = \mathcal{L}(X) \cap S^n$.

A *sofic shift* is a subshift that can be defined by a regular language of forbidden words, or alternatively as $\mathcal{L}^{-1}(L)$ for an extendable regular language L. An *SFT* is a subshift that can be defined by a finite set of forbidden words.

The *endomorphism monoid* of a subshift consists of the continuous functions on X which commute with the translations:

$$\mathrm{End}(X) = \{f : X \to X \mid f \text{ continuous and } \forall \boldsymbol{v} \in \mathbb{Z}^k : \sigma_{\boldsymbol{v}} \circ f = f \circ \sigma_{\boldsymbol{v}}\}.$$

We give $\mathrm{End}(X)$ the structure of a monoid by function composition $(f, g) \mapsto f \circ g$. The monoid $\mathrm{End}(X)$ acts on X from the left by $f \cdot x = f(x)$, and thus $(X, \mathrm{End}(X))$ is itself a dynamical system. We are interested in the following family of questions:

Question 1. What can we say about $\mathrm{End}(X)$ as a monoid and $\mathrm{Aut}(X)$ as a group by looking at properties of X? What can we say about X by looking at properties of $\mathrm{End}(X)$ (or $\mathrm{Aut}(X)$)?

We emphasize in particular the automorphism group, since it is often easier to understand than the endomorphism monoid, and since there is more literature on it. For any property of groups, and any subshift X, we can ask if $\mathrm{Aut}(X)$ has the property.

Some notions we need, mainly for $\mathbb{Z}$-subshifts, are the following: (X, σ) is *transitive* if there exists a *transitive point*, that is, a point $x \in X$ such that $\overline{\bigcup_{n\in\mathbb{Z}} \sigma^n(x)} = X$. If every point is transitive, the system is *minimal*, equivalently, it has no proper subsystems except the empty one.

In terms of words, a minimal subshift is one where every word occurs with bounded gaps, that is, in every long enough word that occurs in a point of

[9] And in more dimensions with an obvious generalization.

the subshift. Transitivity means $\forall u, v \in \mathcal{L}(X) : \exists w : uwv \in \mathcal{L}(X)$. A subshift $X \subset S^{\mathbb{Z}}$ is *mixing* if

$$\forall u, v \in \mathcal{L}(X) : \exists n : \forall m \geq n : \exists w \in \mathcal{L}_m(X) : uwv \in \mathcal{L}(X).$$

The *entropy* of a subshift X is $\lim_{n\to\infty} \frac{\log |\mathcal{L}_n(X)|}{n}$.

2.1 Properties and examples of groups

For a group G, we can ask which kind of subshifts (if any) can have it as an automorphism group, or can have an embedded copy of it in the automorphism group. Similarly, each property of groups gives a family of questions about automorphism groups subshifts: Does there exist a subshift whose automorphism group has that property? Does one exist in a particular class such as the class of SFTs or minimal subshifts? What closure properties do automorphism groups have when restricting to particular classes of subshifts? Can we characterize the automorphism groups of some families of subshifts? A group is not determined by its subgroups, and thus it is also interesting to ask what kind of subgroups automorphism groups have. In this section, we give basic group theoretical definitions needed in later sections. The notation and definitions in this section are mostly standard, but we give them for completeness. For more details, the reader may consult any standard reference [Rot95].

In this section, and usually also in other sections a 'group' is a countable (discrete) group. Thus, a group is a countable set of objects called *elements*, where a mapping $(\cdot) : G \times G \to G$ satisfying a particular set of axioms is defined. The axioms are associativity $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, the existence of an identity element $\exists 1 \in G : a \cdot 1 = 1 \cdot a = a$ (which is automatically unique) and the existence of inverses $\forall a : \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1$ (which are automatically unique), where a, b, c are arbitrary elements of the group. We often drop the symbol '$\cdot$' and write $ab = a \cdot b$. Groups are usually denoted by G and H. If $g_1, g_2, \cdots, g_k \in G$, the products of g_i and g_i^{-1} generate a subgroup of G, and we write this group as $\langle g_1, g_2, \cdots, g_k \rangle$. This is the *subgroup of G generated by* $g_1, g_2, \cdots, g_k$. This naturally generalizes to infinite sets of generators.

A group that has a finite set of generators is *finitely generated*. A group is *cyclic* if it has only one generator, that is, $G = \langle g \rangle$ for some $g \in G$. The only infinite cyclic group is the additive group of integers $\mathbb{Z}$ with the operation $a \cdot b = a + b$.[10] The finite cyclic groups are the groups $\mathbb{Z}_n$ with elements $[0, n-1]$ and group operation $a \cdot b = ((a + b) \bmod n)$.[11] A group is *locally finite* if its finitely generated subgroups are finite.

There are many ways to build new groups from existing ones. If G is a group, a *subgroup* $H \leq G$ of G is a subset of G which is closed under products and

[10] Of course, $\mathbb{Z}$ has a natural multiplication operation as well, the multiplication of integers, but it does not yield a group.

[11] Again, multiplication could be defined on $\mathbb{Z}_n$ by integer multiplication modulo n, but this does not form a group. However, if 0 is omitted, we *do* obtain a group when n is a prime.

inverses, that is, $g, h \in H \implies gh \in H \wedge g^{-1} \in H$. When H is a subgroup, the sets $gH = \{gh \mid h \in H\}$ for $g \in G$ are called *cosets*, and they form a partition of G (that is, $gH \cap g'H \neq \emptyset \implies gH = g'H$). The set of cosets is denoted by G/H. We say H is *normal* and write $H \trianglelefteq G$ if $gH = Hg$ for all $g \in G$, and then the cosets G/H have a natural group structure given by $gH \cdot g'H = gg'H$. The cardinality of G/H is denoted by $[G : H]$, and is called the *index* of H in G. If the index is finite, H is called a *finite-index subgroup*. If H has a particular group property P and H is a finite-index subgroup of G, then we say G is *virtually P*.

A function $\pi : G \to H$ satisfying $\pi(gh) = \pi(g)\pi(h)$ is called a *group homomorphism* from G to H. We say H is a *quotient* of the group G if there is a surjective group homomorphism $\pi : G \to H$. A bijective group homomorphism is called an *isomorphism*, and we write $G \cong H$ if there is an isomorphism between G and H. We say G and H are *isomorphic*, and consider them the same group for most purposes. The *kernel* $\ker(\pi) \subset G$ of a homomorphism π consists of the elements $g \in G$ such that $\pi(g) = 1_H$. It is always a normal subgroup, and $G/\ker(f) \cong \pi(G)$. The group G is *residually finite* if for all $g \in G$ with $g \neq 1$ there exists a finite group H and a homomorphism $\phi : G \to H$ such that $\phi(g) \neq 1_H$.

Given two groups G, H, one can construct larger groups in multiple ways. The *direct product* of G and H is the group $G \times H$ whose elements are the elements of the Cartesian product $G \times H$ and the operation is $(g, h) \cdot (g', h') = (gg', hh')$. Generalizing this, we define the *semidirect product* of G and H as follows. Write $\mathrm{Aut}(G)$ for the group of bijective group homomorphisms from G to itself. Let $\psi : H \to \mathrm{Aut}(G)$ be a group homomorphism, and define $G \rtimes_\psi H$ (or just $G \rtimes H$) as the group with the Cartesian product $G \times H$ as elements, and

$$(g, h)(g', h') = (g\psi_h(g'), hh')$$

as the operation. The idea is that H is 'acting' on G. We show only associativity:

$$\begin{aligned}(a, b)((c, d)(e, f)) &= (a, b)(c\psi_d(e), df) \\ &= (a\psi_b(c\psi_d(e)), bdf) \\ &= (a\psi_b(c)\psi_{bd}(e)), bdf)) \\ &= (a\psi_b(c), bd)(e, f) \\ &= ((a, b)(c, d))(e, f).\end{aligned}$$

Both the direct and semidirect product have G and H as subgroups in a natural way: $G \cong G \times \{1\}$ and $H \cong \{1\} \times H$. Both subgroups are normal in $G \times H$, but (a priori) only G is normal in $G \rtimes H$.

A more general 'construction' is the following: suppose $N \trianglelefteq G$, and $\phi : G \to H$ is a homomorphism with $\ker(\phi) = N$. Then G is a *group extension* of H by N. If G is a direct product of N and H, then it can be seen as a group extension of N by H, and of H by N. The semidirect product $N \rtimes H$ is a group extension of H by N. However, there are not the only possible extensions, and even among finite groups, there is no full understanding of group extensions: the problem of characterizing them is called the *extension problem*, and it is still a major open

problem in group theory. Nevertheless, many properties of groups are closed under group extensions, in the sense that if N and H have the property, then also every group extension of H by N has this property.

We can also construct groups by combining infinitely many smaller groups. We present (simplified versions of) two of the most basic constructions. If $G_1 \subset G_2 \subset G_3 \subset \cdots$ is an increasing sequence of groups (by which we mean that the elements of G_i are elements of G_{i+1} for all i and the group operations are compatible), then $\bigcup G_i$ has an obvious group structure by $g \cdot h = g \cdot_i h$, where $\cdot_i$ is the group operation of any G_i with $g, h \in G_i$. This is called the *direct union* of the groups G_i. For an arbitrary countable family of groups $G_1, G_2, G_3, \cdots$, their *direct sum* is the group $\bigoplus_i G_i$ whose elements are functions $f : \mathbb{N} \to \bigcup_i G_i$ with $f(i) \in G_i$ for all i and $f(i) = 1_{G_i}$ for all but finitely many i, and whose group operation is pointwise product: $(f \cdot g)(i) = f(i) \cdot_i g(i)$.

We say G is *abelian* if $ab = ba$ for all $a, b \in G$. The finitely generated abelian groups are of the form $\mathbb{Z}^d \times \mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_n}$ for some $k_1, \ldots, k_n \in \mathbb{N}$. General countable abelian groups are *not* obtained by extending this to infinite products of this – in fact there is no full characterization of them. The best-known example of a non-finitely generated abelian group is probably the additive group of rational numbers $\mathbb{Q}$ with operation $a \cdot b = a + b$.[12]

A notion generalizing abelianity is nilpotency. For a group G and $g, h \in G$, define the *commutator* of g and h as $[g, h] = ghg^{-1}h^{-1}$ and the *commutator subgroup* $[A, B]$ generated by $A, B \subset G$ as the one genenerated by $[a, b]$ where $a \in A, b \in B$. The *lower central series* of G is defined inductively by $G_1 = G$ and $G_{i+1} = [G_i, G]$. If G_i is the trivial group $\{1\}$ for some $i \in \mathbb{N}$, then G is said to be *nilpotent*, and the smallest i such that $G_i = \{1\}$ is the *step* of G. Every abelian group is nilpotent, but the converse does not hold.

For a set S, the *free group* F_S generated by S is defined as the group whose elements are all words over the alphabet $\{s, s^{-1} \mid s \in S\}$ where the subwords of the form ss^{-1} and $s^{-1}s$ do not occur, and $u \cdot v$ is the word obtained from uv by repeatedly erasing subwords of the form ss^{-1} and $s^{-1}s$ until none occur. For $n \in \mathbb{N}$, we write F_n for the free group with any n generators, as they are all isomorphic. The free group F_∞ with countably many generators is defined in the obvious way, as a direct union of the F_n.

Generalizing the definition of the free group, a group presentation is a combinatorial way to describe a group. Given a list of generators $g_1, g_2, g_3, \ldots$ (considered as formal symbols) and a list of words

$$w_1, w_2, w_3, \ldots \in \{g_1, g_1^{-1}, g_2, g_2^{-1}, g_3, g_3^{-1}, \cdots\}^*$$

(either list of may also be finite), we define the group $\langle g_1, g_2, g_3 \ldots \mid w_1, w_2, w_3, \ldots \rangle$ as the group whose elements are equivalence classes of words over the symbols g_i and g_i^{-1} under the equivalence relation $\sim$ generated as follows: $\lambda \sim 1$, $gg^{-1} \sim g^{-1}g = \lambda$ where λ is the empty word, and $uw_iv \sim uv$ for all $i \in \mathbb{N}$. If

[12] The usual multiplication of $\mathbb{Q}$ is again not a group, but if 0 is omitted we obtain another non-finitely generated group, namely the free abelian group on countably many generators, by the unique factorization theorem of rational numbers.

$G \cong \{g_1, g_2, \dots \mid w_1, w_2, \dots\}$, then $\{g_1, g_2, \dots \mid w_1, w_2, \dots\}$ is a *group presentation* of G. A group presentation for F_n is $\langle a_1, a_2, \cdots, a_n \mid \emptyset\rangle$ and one for $\mathbb{Z}^d$ is

$$\langle a_1, a_2, \cdots, a_d \mid \{a_i a_j a_i^{-1} a_j^{-1} \mid 1 \le i, j \le d\}\rangle.$$

Every (countable) group G has a group presentation $\{g_1, g_2, \dots \mid w_1, w_2, \dots\}$ where the g_i are an enumeration of elements of G and w_i are all words in $\{g_1, g^{-1}, g_2, g^{-2}, g_3, g_3^{-1}, \cdots\}^*$ which present the identity element of G.

Using group presentations, we can define another product of G and H, namely their *free product*. Choose presentations for the groups G and H, $G \cong \langle g_1, g_2, \dots \mid w_1, w_2, \dots\rangle$ and $H \cong \langle h_1, h_2, \dots \mid u_1, u_2, \dots\rangle$, and define

$$G * H = \langle g_1, h_1, g_2, h_2, g_3, h_3, \cdots \mid w_1, u_1, w_2, u_2, w_3, u_3, \dots\rangle.$$

This group is defined by G and H up to isomorphism, no matter which presentations are chosen. Its elements can be thought of as words $w \in (G \cup H)^*$ such that $w_i \in G \iff w_{i+1} \in H$, that is, elements of G and H alternate, where neither 1_G nor 1_H occurs in w. The product of $u, v \in G * H$ is obtained from the word uv by repeatedly combining two adjancent elements of G into a single element of G using the group operation of G, and symmetrically for H, and removing 1_G and 1_H whenever they occur. The free product of finite groups can be infinite. For example, the $\mathbb{Z}_2 * \mathbb{Z}_2$ is virtually $\mathbb{Z}$ and $\mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2$ is virtually F_2.

A group G *acts* on a set X as explained already in the introduction, for each $g \in G$, $x \mapsto g \cdot x$ is a bijection on X satisfying $1 \cdot x = x$ and $g \cdot h \cdot x = gh \cdot x$. The *orbit* of x under the action is the set $G \cdot x = \{g \cdot x \mid g \in G\}$, and the *stabilizer* of x is the subgroup $G_x \le G$ of elements $g \in G$ such that $g \cdot x = x$.

The group S_n is the one acting maximally transitively on the set $[1, n]$, that is, it contains exactly the permutations of $[1, n]$. For $f, g \in S_n$, we define $f \circ g$ by $(f \circ g)(a) = f(g(a))$ where $a \in [1, n]$. The direct union of all such groups is called S_∞. Every finite group embeds in S_n for some $n \in \mathbb{N}$ by Cayley's theorem.

2.2 Amenability, Cayley graphs and growth

Amenability is a notion which is extremely important in group theory.[13] We say G is *amenable* if it admits a *Følner sequence*, that is, a sequence $A_1 \subset A_2 \subset A_3 \subset \cdots$ such that each $A_i \subset G$ is finite, $G = \bigcup_i A_i$ and

$$\forall g \in G : \frac{|gA_i \Delta A_i|}{|A_i|} \underset{i \to \infty}{\longrightarrow} 0.$$

Amenability is equivalent to (and often defined as) the existence of a *left-invariant mean* on G, that is, a functional $\nu : \ell^\infty(G) \to \mathbb{R}$ (where $\ell^\infty(G)$ are the bounded real-valued functions on G) satisfying $\nu(1_G) = 1$ (where 1_G is the constant-1 function on G) and

$$\forall f \in \ell^\infty(G) : (\forall g \in G : f(g) \ge 0) \implies \nu(f) \ge 0.$$

[13] It is also very important in dynamics: as noted in the introduction, it is needed in the direct generalization of entropy to group actions.

All finite groups are amenable, as we can choose $A_i = G$ for all i, and $\mathbb{Z}^d$ is amenable because we can choose $A_i = [-i, i]^d$ as a Følner sequence.[14] More generally, every abelian group is amenable. Amenable groups also have various closure properties: they are closed under subgroups, quotients, group extensions and direct unions. Thus, it is natural to define *elementary amenable groups* as the smallest class of groups which contains the finite and abelian ones, and is closed under subgroups, quotients, group extensions and direct unions (and isomorphism, naturally).

We usually explicitly discuss neither Følner sequences nor means: the following theorem summarizes our typical way to prove amenability or non-amenability.

Theorem 1. *An elementary amenability group is amenable, and a group containing a free group on two or more generators is not amenable.*

In general, an amenable group need not be elementary amenable [Gri85], and a non-amenable group need not contain a free group [Ols83].

Let $A = \{g_1, g_2, \ldots, g_k\}$ be a finite set of elements generating a group G, where $A^{-1} = A$. The *Cayley graph* of G with respect to the generators A is the directed edge-labeled countable graph with nodes G and for each $a \in A$ an edge (g, ga, a), where by (a, b, c) we mean an edge from a to b with label c. In a graph, a natural notion of distance between nodes is the length of the shortest path between them. We write $d_{G,A}$ for the distance function of G in its Cayley graph with respect to generators A. We write $B_{G,A}(n)$ for the corresponding *Cayley ball* of radius n, defined as

$$B_{G,A}(n) = \{g \in G \mid d_{G,A}(1, g) \leq n\}.$$

Changing the generators of G only changes distances by a multiplicative constant, that is, if $\langle A \rangle = \langle B \rangle = G$ then

$$\exists C > 1 : \forall g, h \in G : d_{G,B}(g, h)/C \leq d_{G,A}(g, h) \leq C d_{G,B}(g, h).$$

Thus, the growth rate of balls in all Cayley graphs of G is similar. For finitely generated groups, we define some notions giving a rough classification of this growth rate. We say a (finitely generated) group G has *polynomial growth rate* if

$$\exists k \in \mathbb{N} : \forall n : |B_{G,A}(n)| \leq n^k + k$$

for some – and thus any – set of generators A. We say it has *exponential growth rate* if

$$\exists a > 1 : \forall n : |B_{G,A}(n)| \geq a^n$$

and say it is *subexponential growth rate* if it does not have exponential growth rate. By Gromov's theorem, a group with polynomial growth is virtually nilpotent. A group of subexponential growth is amenable.

[14] That is, the Cayley balls are a Følner sequence in the abelian case – we note that this is *not* how Følner sequences look in general. For example, if the size of balls grows exponentially, then the balls are never a Følner sequence.

2.3 Decidability

Definitional issues In this section, we discuss mainly decidability questions regarding the relationship between a CA and its local rule, for example the decidability of reversibility. See [Kar12] for a survey of decidability in the theory of cellular automata.

To ask decidability questions about a group or a monoid, we need to fix a computational presentation of the elements. Let us choose such presentations for endomorphisms of subshifts: A *cellular automaton* on a subshift $X \subset S^{\mathbb{Z}^k}$ is a function $f : X \to X$ which has a *radius* $r \in \mathbb{N}$ and a *local rule* $F : S^{[-r,r]^k} \to S$ such that $f(x)_{\boldsymbol{v}} = F(x_{\boldsymbol{v}+[-r,r]^k})$. It is well-known that cellular automata are precisely the functions $\mathrm{End}(X)$. The local rule of a cellular automaton gives a computational presentation of the function, and thus a way to give a finite list of elements of the endomorphism monoid to an algorithm. This allows us to ask algorithmic questions about the monoid $\mathrm{End}(X)$, *on any subshift* X, even a highly uncomputable one. Note that from the local rules of $f, g : X \to X$, we can easily form *a* local rule for the composition of two cellular automata by composing the local rules in an obvious way, again no matter what the subshift is.

We make a few (mostly obvious) remarks about the canonicality and caveats of this presentation of cellular automata. Every cellular automaton, on every subshift, has an infinite family of presentations by local rules, as we can always increase its radius. However, there is always a smallest possible radius.[15] By also using a local rule $F : \mathcal{L}_{2r+1}(X) \to S$ instead of $F : S^{[-r,r]^k} \to S$ (so that we only define the cellular automaton on the words it actually sees), we obtain a unique presentation. If the language of X is decidable, that is, given $w \in S^*$ we can algorithmically check whether $w \in \mathcal{L}(X)$, then this minimization process can be done algorithmically:

Lemma 1. *Let $X \subset S^{\mathbb{Z}}$ be a subshift such that $\mathcal{L}(X)$ is a decidable language. Then, given $F : S^{[-r,r]} \to S$ defining a CA $f : X \to X$, we can compute $r' \leq r$ and $G : L \to S$ where $L \subset S^{[-r',r']}$ such that G defines the same CA f and both r' and L are minimal.*

We mainly study decidability questions on subshifts with decidable languages, so the presentations can be thought of as unique, but when the subshift is not a priori decidable, we feel it is more natural to assume the local rule given as input is not minimized.

A more subtle issue is which local rules are actually endomorphisms or automorphisms of a particular subshift X. More precisely, given a rule $F : S^{[-r,r]^k} \to S$, a CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ is defined, and we call the *well-definedness problem* the question of whether $f(X) \subset X$ holds (that is, whether f restricts to a CA on X), and the *reversibility problem* the question of whether $f|X \in \mathrm{Aut}(X)$, where

[15] We note that, except on full shifts, there is in general no minimal neighborhood, as easy examples show – nevertheless, there must be a minimal radius simply because the natural numbers are well-ordered.

$f|X$ is the restriction of f to X. The following simple example shows that neither problem is in general decidable even if the language of X is decidable, for somewhat uninteresting reasons.

Example 1. Define the CA f_n on the full shift $\{0,1,1',2,3\}^{\mathbb{Z}}$ which exhanges 10^n2 and $1'0^n2$ and otherwise behaves as the identity map. Take the subshift X of $\mathcal{L}^{-1}(0^*10^*20^*30^* + 0^*1'0^*20^*30^*)$ where additionally $1'0^n20^k3$ is forbidden if the nth Turing machine halts on the kth step. Then f_n restricts to an automorphism on X if the nth Turing machine never halts, and otherwise it is not well-defined on X – thus, both the well-definedness problem and the reversibility problem are undecidable. The language of X is clearly decidable. △

We mainly study decidability questions for cellular automata on sofic shifts in dimension one, and in this case both the well-definedness problem and the reversibility problem are decidable by basic automata theory [LM95,HMU06]. We note that the picture is different in the case of multidimensional full shifts, as checking whether a local rule corresponds to a reversible cellular automaton is undecidable [Kar90]. Since every effective subshift – in particular the example above – is a sofic shift in the next dimension [AS13,DRS12], checking well-definedness of a CA on a multidimensional sofic shift with a decidable language is undecidable. On multidimensional SFTs, a simple construction based on the undecidability of the domino problem with a seed tile, or an application of the result of [Gui11], shows that the well-definedness problem is undecidable on general SFTs. We do not know if the language can be made decidable.

Question 2. Is there a two-dimensional SFT with a decidable language where the well-definedness problem is undecidable?

Another basic issue is whether two given local rules are the same. As mentioned above, if the language of X is decidable, we can compute a canonical local rule for each CA from any given local rule. Thus, to check whether two CA are the same, we can simply compute their minimal local rules and compare them. In particular the *word problem* of $\mathrm{Aut}(X)$ – the problem of checking whether the product of a given list of automorphisms is the identity map, is decidable for all subshifts X with a decidable language.

Again, this applies in particular to one-dimensional sofic shifts. In two dimensions, SFTs need not have a decidable language, and indeed, using the undecidability of the domino problem with a seed tile, one can easily build a two-dimensional SFT X where the problem of deciding whether a given local rule represents the identity element is undecidable, even when restricted to local rules that represent reversible CA. Nevertheless we do not know whether there are two-dimensional SFTs on which the word problem of a finitely generated subgroup of the automorphism group is undecidable. See [Hoc10] for a related discussion.

Group-related issues Sofar, we have mainly discussed definitional issues, which, while necessary background information, have little to do with the actual automorphism groups. The list of possible group-theoretical questions about

automorphism groups is pretty much endless: for any subshift X and any family of groups $\mathcal{G}$, we can ask whether a given finitely generated subgroup G of $\mathrm{Aut}(X)$ is in $\mathcal{G}$. For example, we are interested in the decidability of abelianity, cyclicity, finiteness and freeness of such groups. We can also ask whether the subgroup generated by them has a particular property in the larger group, such as normality or centrality.

There are also many well-known computational problems in pure group theory, which we also discuss. We already discussed the word problem.

Remark 2. Note that we defined the word problem of the automorphism group of a subshift in terms of local rules. For a finitely generated group, one can define the word problem can be defined without actually knowing what the elements of the group are: We choose a set of generators, and ask for the decidability of the word problem over those generators. The decidability of the word problem will be independent of the generators. Usually, it will be clear from context which problem we mean, and in fact they are equivalent in the situations we consider.

A question related to the word problem is the *geodesics problem*, where given a word w over a finite set of generators, we want to find the minimal word u over the same generators which represents the same group element. While the geodesics problem may take an exponentially longer time to solve than the word problem, in the sense of decidability the questions are equivalent. There are many variants of this problem, but as we do not address computational complexity in this paper, all of these questions may be thought of as restatements of the word problem. The *conjugacy problem* is the problem of, given two elements g, g' of the group, deciding whether $g = hg'h^{-1}$ for some group element h.

A common question to ask about a group, and one that turns out quite interesting in the case of automorphism groups, is the *torsion problem* of deciding, given an element of the group, whether it generates an infinite group. For example, it is known that the two-dimensional generalization $2V$ of Thompson's group V has an undecidable torsion problem [BB14], while Thompson's group V itself has a decidable torsion problem [BB14,BM14].

As noted in the introduction, many of the existing algorithmic questions about cellular automata do not fit into our framework. Namely, the usual approach to cellular automata is the study of the dynamics of the $\mathbb{N}$-action (or $\mathbb{Z}$-action) of a CA f given by $n \cdot x = f^n(x)$. A variety of dynamical and computational behaviors is observed in these systems, yet the groups and monoids generated by a single cellular automaton are not particularly interesting: they are cyclic, and thus the groups obtained are isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}_n$ for some $n \in \mathbb{N}$ (and the monoids are equally simple).

2.4 Showing finiteness of a group of CA

It is useful to note that a group of cellular automata is finite if and only if the orbits under its action are finite (even bounded). We will use this result in Section 3 to prove some undecidability results for the automorphism group of a full shift.

Lemma 2. *Let X be a transitive subshift, and let $x \in X$ be a transitive point. Then the stabilizer of x in the action of $\mathrm{Aut}(X)$ is trivial, that is, if $f, g \in \mathrm{Aut}(X)$ and $f(x) = g(x)$, then $f = g$.*

Proof. If $f \neq g$, then $f(y)_0 \neq g(y)_0$ for some $y \in X$. Since x is transitive, $f(y)_0 = f(\sigma^n(x))_0 = g(\sigma^n(x))_0 = g(y)_0$ for some $n \in \mathbb{Z}$. □

In other words:

Theorem 2. *Let X be a transitive subshift and let G be any subgroup of $\mathrm{Aut}(X)$. Then the following are equivalent:*

- *G is infinite,*
- *$G \cdot x$ is infinite for some $x \in X$,*
- *$G \cdot x$ can be arbitrarily large for $x \in X$.*

In particular, it follows that if G is an infinite subgroup of $\mathrm{Aut}(X)$ for a transitive subshift X, then G is infinite if and only if it has an infinite orbit. In our main application, X is a full shift, and thus certainly transitive. The result is true in much more generality, but we omit the discussion of this.

3 Full shifts and transitive sofic shifts

We now look at full shifts and transitive sofic shifts, perhaps the most natural habitat of cellular automata. If the alphabet S is not explicitly specified, we assume $|S| > 1$.

One of the main tools in the positive entropy case is Lemma 3 below. It shows that it is usually enough to prove undecidability results and to perform constructions of subgroups on full shifts. A proof in the mixing SFT case, and restricted to automorphisms, appeared in [KR90]. The general proof for X a positive entropy (equivalently, uncountable) sofic shift is also easy, and outlines the idea of *marker constructions* (our version of the marker being the word u in the proof). We sketch a proof.

An *unbordered word* u is one that does not overlap itself, that is, $uw = vu \implies |v| \geq |u|$.

Lemma 3 (essentially [KR90]). *If X is a positive entropy sofic shift, then $\mathrm{End}(X)$ contains a copy of $\mathrm{End}(S^{\mathbb{Z}})$ for any alphabet S.*

Proof (Proof sketch). Every infinite aperiodic word contains arbitrarily long unbordered words, by Theorem 8.3.9 in [Lot02].[16] Choose a positive entropy transitive sofic Y subshift inside the X, and a long unbordered word u that occurs in Y. If u is taken long enough, there are many words uvu where v is of length $\lfloor |u|/2 \rfloor$,[17] and by the pigeonhole principle (and long enough u), many such words

[16] A stronger version of this is shown in Lemma 2.2 of [BLR88].

[17] This follows because every transitive sofic shift has a uniform distance k such that if u and v occur in the language, then uwv occurs for some w of length at most k. This is a direct application of the pigeonhole principle.

which correspond to the same element of the *syntactic monoid*[18] of $\mathcal{L}(X)$. Since u is unbordered, a local rule can safely change the word v between two occurrences of u, that is, compute a local transformation $uvu \mapsto uv'u$.

More precisely, let V with $|V| = |S|^2$ be the a set of words v of length $\lfloor |u|/2 \rfloor$ such that uvu is a word of X, and the words uvu for $v \in V$ correspond to the same element of the syntactic monoid. Choose a bijection $\pi : V \to S^2$. Now, we map each $f \in \mathrm{End}(S^{\mathbb{Z}})$ to a CA $g \in \mathrm{End}(X)$ with the following behavior: on the points $\cdots uv_{-2}uv_{-1}uv_0uv_1uv_2u\cdots$ where $v_i \in V$ for all i, we apply $f \times f^R$ to the point $\cdots \pi(v_{-2})\pi(v_{-1})\pi(v_0)\pi(v_1)\pi(v_2)\cdots \in (S^2)^{\mathbb{Z}}$ (which we think of as two separate tracks each containing a point over the full shift $S^{\mathbb{Z}}$), where $y^R = \cdots y_2y_1.y_0y_{-1}y_{-2}\cdots$ and $f^R(y) = f(y^R)^R$. On points where no such sequence appears, g is the identity map. When a partial such sequence occurs, we glue the two tracks together like a conveyor belt at the end of the sequence, and think of the first track turning 180 degrees and continuing backwards on the second track. It is easy to check that this gives a consistent embedding of the endomorphism monoid $\mathrm{End}(S^{\mathbb{Z}})$ to $\mathrm{End}(X)$. □

We note that we do *not* claim that $\mathrm{Aut}(X)$ embeds in $\mathrm{Aut}(Y)$ when X and Y are general mixing SFTs. We suspect this to be the case, but subtle problems seem to arise when attempting to generalize the proof above. See [KR90] for an example of this.

3.1 Subgroups of $\mathrm{Aut}(X)$ for a transitive sofic shift X

In this section, we give some examples of what kind of subgroups can be created with the marker construction, and end the section with a complete characterization of the locally finite subgroups that appear in the automorphism group [KR90]. Most of the results in this section were essentially proved in [BLR88] or [KR90].

While we know no restrictions on the groups $\mathrm{Aut}(X)$ for general subshifts X, there are some restrictions when X has suitable dynamical properties.

Lemma 4 ([BLR88]). *Let X be a subshift where periodic points are dense (for example, a transitive sofic shift). Then $\mathrm{Aut}(X)$ is residually finite.*

Since the class of residually finite groups is closed under taking subgroups, we obtain nontrivial restrictions on the possible subgroups that can occur in $\mathrm{Aut}(X)$ when X has periodic points dense. For example, $\mathrm{Aut}(X)$ cannot contain a nontrivial divisible subgroup such as $(\mathbb{Q}, +)$, and cannot contain the infinite permutation group S_∞.

The decidability of the word problem restricts the possible subgroups further, as we have already seen:

[18] We omit the definition, but u and v corresponding to the same element of this monoid means exactly that they occur in the same contexts, so we may exchange them. See [HMU06].

Lemma 5. *If X is a subshift with a decidable language (for example, a sofic shift), then every finitely generated subgroup of* $\mathrm{Aut}(X)$ *has a decidable word problem.*

Note that in the proof of Lemma 3, the CA in the image of the embedding only change the points in subwords of the form $\cdots uv_{-1}uv_0uv_1u\cdots$. Since u can be taken arbitrarily long, the CA thus change only points in a subshift of strictly smaller entropy. Using standard techniques, we can make sure that the complement of this subshift still contains a positive entropy sofic shift. Using this idea, we obtain the following generalization.

Lemma 6 (Essentially Theorem 2.6 in [BLR88]). *If X is a positive entropy sofic shift (equivalently, uncountable), then* $\mathrm{End}(X)$ *contains a copy of the countable direct sum* $\bigoplus_{i\in\mathbb{N}} \mathrm{End}(S^{\mathbb{Z}})$ *for any alphabet S.*

Equivalently, we can have countably many distinct alphabets, by Lemma 3. As a direct corollary, we obtain two closure properties for subgroups of automorphism groups of full shifts.

Theorem 3. *The set of subgroups of* $\mathrm{Aut}(S^{\mathbb{Z}})$ *is closed under countable direct sums for any alphabet S.*

Of course, for this to be interesting, we need to have some subgroups to begin with. A trivial observation is that σ generates a copy of $\mathbb{Z}$ on any infinite subshift. Another observation, essentially Theorem 6.13 in [Hed69], is that every finite group embeds in $\mathrm{Aut}(X)$ for a positive entropy sofic shift. Using Lemma 3, this is very easy to show: a finite group G embeds in the permutation group S_k for some k, and thus into $\mathrm{Aut}([1,k]^{\mathbb{Z}})$ by symbol permutations.

Proposition 1. *If X is a positive entropy sofic shift, then* $\mathrm{Aut}(X)$ *contains every countable direct sum of finite groups and copies of* $\mathbb{Z}$.

In [BLR88], it is shown that the free group with infinitely many generators embeds in the automorphism group of a mixing SFT. Applying Lemma 3, we obtain the same result for the automorphism group of a positive entropy sofic shift.

Theorem 4. *If X is a positive entropy sofic shift, then* $\mathrm{Aut}(X)$ *contains* F_∞.

Corollary 1. *If X is a positive entropy sofic shift, then* $\mathrm{Aut}(X)$ *is not amenable.*

To prove Theorem 4, one embeds the free group $\mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2$ in the automorphism group using a marker construction. In [KR90], it is attributed to R. C. Alperin that more generally any free product of finitely many finite groups embeds in the automorphism groups. We make a slightly bolder conjecture:

Conjecture 1. If X is a positive entropy sofic shift, $\mathrm{End}(X)$ contains the copy of the free product of countably many copies of $\mathrm{End}(S^{\mathbb{Z}})$ for any alphabet S.

Restricted to locally finite groups G, a full characterization of the subgroups of $\mathrm{Aut}(X)$ is known. As observed in the beginning of this section, the automorphism group of a transitive sofic shift is residually finite. This is the only requirement:

Theorem 5 ([KR90]). *Let X be a positive entropy sofic shift. Then a locally finite group G is isomorphic to a subgroup of the automorphism group of X if and only if G is residually finite and countable.*

The paper [KR90] contains many more examples of subgroups that can be embedded (for example, fundamental groups of 2-manifolds), and proves that the set of subgroups of $\mathrm{Aut}(X)$ is closed under finite extensions when X is a full shift. That is, if $H \leq \mathrm{Aut}(X)$ where X is a full shift, and $[G : H] < \infty$, then $G \leq \mathrm{Aut}(X)$.

Note that by Lemma 3, the groups $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$ and $\mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$ embed into each other, and thus have the same subgroups. However, we do not know whether there is an isomorphism between them.[19] This is one of the open problems in symbolic dynamics listed in [Boy08].

Question 3. Are $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$ and $\mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$ isomorphic?

It follows from Ryan's theorem that $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$ and $\mathrm{Aut}(\{0,1,2,3\}^{\mathbb{Z}})$ are not isomorphic, because in $\mathrm{Aut}(\{0,1,2,3\}^{\mathbb{Z}})$ that shift map has a square root, while it does not have one in $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}})$.

3.2 Decidability on positive entropy sofic shifts

Most decidability problems for cellular automata are about their dynamical properties, such as mixing, transitivity, sensitivity and expansivity. These questions are, at least a priori, outside our scope, as there is no known algebraic property satisfied by, for example, the mixing CA, but not the rest.

However, the dynamical notion of *equicontinuity* turns out to be equivalent to eventual periodicity on all subshifts. For automorphisms $f \in \mathrm{Aut}(S^{\mathbb{Z}})$, this is the question of whether $f^k = \mathrm{id}_X$ for some $k \geq 1$, that is, the torsion problem. Though the result is not stated in group-theoretic terms, in [KO08], this problem is shown undecidable on full shifts. Using Lemma 3,[20] we obtain the result for all positive entropy sofic shifts.

Theorem 6 ([KO08]). *Let X be a positive entropy sofic shift. Then the group $\mathrm{Aut}(X)$ has an undecidable torsion problem.*

This trivially implies many undecidability problems, such as whether a given finite set of elements generates an infinite group, or whether it generates a torsion group. We now prove some slightly more interesting corollaries.

[19] There certainly are non-isomorphic groups that embed into each other, for example the free groups F_2 and F_3 are such a pair.

[20] We also need to note that the embedding is explicitly computable – clearly it is.

The notion of time-symmetry was introduced for cellular automata in [GKM12]. We give this definition for an arbitrary subshift: a CA is *time-symmetric* if it is the composition of two *involutions*, where an involution is a CA $g \in \mathrm{Aut}(X)$ satisfying $g^2 = \mathrm{id}_X$. That is, $f \in \mathrm{Aut}(X)$ is time-symmetric $f = g \circ h$ for some $g, h \in \mathrm{Aut}(X)$ satisfying $f^2 = g^2 = \mathrm{id}_X$. The name comes from the equivalent condition that $g \circ f \circ g = f^{-1}$ for some involution $g \in \mathrm{Aut}(X)$. It is shown in [GKM12] that time-symmetric CA are *intrinsically universal* among the reversible cellular automata, that is, every reversible automaton can be simulated by a time-symmetric one. The proof of this claim gives the following theorem:[21]

Theorem 7. *Given a finite set of finite order automorphisms of a positive entropy sofic shift X, it is undecidable whether they generate a finite group.*

Proof. Again, it is enough to prove the result for full shifts by Lemma 3. We show that an algorithm for this problem would give an algorithm for the torsion problem as well. Let $f \in \mathrm{Aut}(S^{\mathbb{Z}})$ be given. Consider the full shift $(S \times S)^{\mathbb{Z}}$, and define $g, h \in \mathrm{Aut}((S \times S)^{\mathbb{Z}})$ by $g(x, y) = (f(y), f^{-1}(x))$ and $h(x, y) = (y, x)$. Then $(g \circ h)(x, y) = (f(x), f^{-1}(y))$. If $\langle f \rangle$ is infinite, then the orbit of some point x is infinite by Theorem 2, and thus the orbit of (x, y) is of infinite order by Theorem 2 for any $y \in S^{\mathbb{Z}}$. Let then $|\langle f \rangle| = k$, and consider a point (x, y). Clearly the orbit of (x, y) under the action of $\langle g, h \rangle$ is contained in the finite set $\{(f^i(x), f^j(y)), (f^i(y), f^j(x)) \mid i, j \in \mathbb{Z}\}$. Since every orbit is finite, $\langle g, h \rangle$ is finite, again by Theorem 2. □

The proof shows more precisely that given two automorphisms of order 2, it is undecidable whether they generate a finite or an infinite group. More precisely, in the construction, depending on whether f halts, we obtain either a finite dihedral group D_n, or the infinite dihedral group $D_\infty = \mathbb{Z}_2 * \mathbb{Z}_2$. One can easily perform a similar proof to for example show that the finiteness of a group generated by automorphisms of order 3 is undecidable. We prove a more general result of this form.

Theorem 8. *Let X be a positive entropy sofic, and let G be an arbitrary nonempty finite group. Then, given two finite subgroups $F, F' \leq \mathrm{Aut}(X)$ with $F \cong F' \cong G$, it is undecidable whether $\langle F \cup F' \rangle$ is finite.*

Proof. Again, we only need to prove the claim on full shifts. Let $f \in \mathrm{Aut}(S^{\mathbb{Z}})$ be arbitrary. We again show that an algorithm for the problem in the statement also decides whether $\langle f \rangle$ is finite. Without loss of generality, we may assume G is a subgroup of a symmetric group S_k, so that G acts nontrivially on $[1, k]$. Let $F = \{f_g \mid g \in G\}$ be the subgroup of $\mathrm{Aut}((S^k)^{\mathbb{Z}})$ permuting the tracks according to this embedding:

$$f_g(x_1, \ldots, x_k) = (x_{g^{-1}(1)}, x_{g^{-1}(2)}, \ldots, x_{g^{-1}(k)}).$$

[21] In fact, the CA constructed in [KO08] are already time-symmetric, but the idea on permuting tracks illustrates Theorem 2 better.

We now give another embedding, F', where in addition to permuting the tracks, we apply a power of f to the tracks when they are moved. For this, choose a function $c : [1, k] \to \mathbb{Z}$. The idea is that if track i is moved to track j by a permutation $g \in G$, the corresponding CA f'_g will apply $f^{c(j)-c(i)}$ to the ith track x_i before moving it. Thus, the jth track will always be $c(j) - c(i)$ steps ahead in time compared to the track i. This gives another embedding of G to $\mathrm{Aut}((S^k)^{\mathbb{Z}})$, since if $g_1 \cdot g_2 \cdots g_\ell = 1$ for $g_i \in G$, then $f'_{g_1} \circ f'_{g_2} \circ \cdots \circ f'_{g_\ell}$ permutes every track to its starting position, and naturally the movements in time cancel out, so that $f'_{g_1} \circ f'_{g_2} \circ \cdots \circ f'_{g_k} = \mathrm{id}_{(S^k)^{\mathbb{Z}}}$.

More precisely, take a function $c : G \to \mathbb{Z}$ and define $C : G \times [1, k] \to \mathbb{Z}$ by

$$C(g, i) = c(g \cdot i) - c(i).$$

Define $F' = \{f'_g \mid g \in G\}$ by

$$f'_g(x_1, \ldots, x_k) = (f^{C(g,g^{-1}\cdot 1)}(x_{g^{-1}\cdot 1}), \ldots, f^{C(g,g^{-1}\cdot k)}(x_{g^{-1}\cdot k})).$$

It is easy to check that $g \mapsto f'_g$ gives an embedding of G into $\mathrm{Aut}((S^k)^{\mathbb{Z}})$.[22]

We claim that if c is injective, then $\langle F \cup F' \rangle$ is finite if and only if $\langle f \rangle$ is. Consider thus an arbitrary point $(x_1, x_2, \ldots, x_k) \in (S^k)^{\mathbb{Z}}$. First, if $\langle f \rangle$ is finite, we are done: every point in the orbit of $(x_1, x_2, \ldots, x_k)$ has a point from the orbit of one of the points x_i on each track, which gives a finite upper bound on the size of orbits. Conversely, suppose x has an infinite orbit in the action of f. Let $g \cdot i = j$ for $g \in G$ and $i, j \in [1, k]$ with $i \neq j$ (the action of G is nontrivial on $[1, k]$). Since c is injective, $C(g, i) = c(g \cdot i) - c(i) = n \neq 0$. For notational simplicity, suppose $i = 1$ and $j = 2$. Then

$$(x, y, \cdots) \overset{f'_g}{\mapsto} (y', f^n(x), \cdots) \overset{f_{g^{-1}}}{\mapsto} (f^n(x), y'', \cdots)$$

for some points $y, y', y'' \in S^{\mathbb{Z}}$. Clearly, this shows that the orbit of any point $(x, \cdots)$ is infinite.

Again, the alphabet S^k can be changed by applying Lemma 3. □

There are many open questions about automorphism groups, even on full shifts. For example, the decidability of time-symmetry is open in one dimension (in two dimensions, it is undecidable [GKM12]).

Question 4. Is it decidable whether a given CA $f \in \mathrm{Aut}(S^{\mathbb{Z}})$ is time-symmetric?

More generally, we do not know whether it is decidable if a given CA is generated by involutions, or elements of finite order. For a more general question in the same spirit, see the FOG conjecture (not true in general [KR91]) and virtual FOG conjecture in [Boy08]. Another question whose solution we do not

[22] Readers familiar with cohomology will notice that c is just an arbitrary 0-cochain $c \in \mathrm{Hom}(C(G, [1, k]), \mathbb{Z})$ for the action of G on $[1, k]$ and C is the corresponding 1-coboundary – in particular, C is a 1-cocycle, from which it follows that the action of F' is well-defined.

know is the conjugacy problem: is it decidable in $\mathrm{Aut}(S^{\mathbb{Z}})$ whether two given elements f, g are conjugate?

More in line with Theorem 8 and our constructions in this section, we state the following conjecture.

Conjecture 2. It is undecidable whether two given automata generate a (non-abelian) free group.

If Conjecture 1 is true, and the embedding is computable, then the previous conjecture is true as well: given $f \in \mathrm{Aut}(S^{\mathbb{Z}})$, consider the CA $g, h \in \mathrm{Aut}(S^{\mathbb{Z}})$ given by the embedding of $\mathrm{Aut}(S^{\mathbb{Z}}) * \mathrm{Aut}(S^{\mathbb{Z}})$ into $\mathrm{Aut}(S^{\mathbb{Z}})$, so that $\langle f \rangle \cong \langle g \rangle \cong \langle h \rangle$ and g and h generate the product $\langle g \rangle * \langle h \rangle$ in $\mathrm{Aut}(S^{\mathbb{Z}})$. Then clearly g and h generate a group isomorphic to F_2 if and only if f has infinite order.

A simple decidable property is abelianness: to check whether a finite set F of cellular automata generate an abelian group, we only need to check whether the identity $f \circ g = g \circ f$ holds for all pairs $f, g \in F$.

4 Countable subshifts

The simplest countable subshifts (and the simplest subshifts in general) are probably the finite ones. A finite subshift is always an SFT, and the automorhism groups of such SFTs are simply the centralizers of permutations on finite sets. The following characterization was given in [CK14]: Let S_n act on $\mathbb{Z}_m^n$ by $\phi(g)(i_1, i_2, \ldots, i_n) = (i_{g^{-1}(1)}, i_{g^{-1}(2)}, \ldots, i_{g^{-1}(n)})$ for $g \in S_n$.[23] Define the semidirect product $S(m, n) = \mathbb{Z}_m^n \rtimes S_n$ with respect to the action ϕ. For future purposes, similarly define $S(\infty, n) = \mathbb{Z}^n \rtimes S_n$.

Theorem 9. *A group G is the automorphism group of some finite subshift if and only if*

$$G \cong S(m_1, n_1) \times S(m_2, n_2) \times \cdots \times S(m_s, n_s)$$

for some $m_1 < m_2 < \cdots < m_s$ and $n_1 < n_2 < \cdots < n_s$.

Equivalently, these are precisely the finite groups that occur as automorphism groups of subshifts, since σ generates an infinite subgroup of $\mathrm{Aut}(X)$ if X is infinite.

In [ST12], cellular automata on countable sofic shifts were discussed from the point of view of computability. Unlike in the case of full shifts, many dynamical behaviors (though not all!) of such automata are decidable. In particular, the following is proved:

Theorem 10 ([ST12]). *Let X be a countable sofic shift. Then the torsion problem is decidable for* $\mathrm{Aut}(X)$.

[23] In [CK14], the dual definition is used. Our definition must be used to obtain a homomorphism when the composition of permutations is defined by $(\pi \circ \pi')(a) = \pi(\pi'(a))$ (but also the dual definition is used by some authors).

While undecidability results about the *dynamics* of cellular automata on countable sofic shifts are shown in [ST12], we do not know any interesting undecidability results about the automorphism group in the countable case.

This suggests that the automorphism group might be essentially simpler in the countable case, and in a way it is: While Corollary 1 shows that the automorphism group of an uncountable sofic shift is never amenable, the author and Michael Schraudner are working on the proof that the automorphism group of a countable sofic shift always is. We prove this for a simple example.

Proposition 2. *For $k \in \mathbb{N}$, let $X_k \subset \{0,1\}^{\mathbb{Z}}$ be the (countable sofic) subshift whose forbidden words form the regular language $(10^*)^k1$. Then $\mathrm{Aut}(X_k)$ is elementarily amenable.*

Proof. We prove this by induction on k. The base case is the one-point subshift X_0 whose automorphism group is the trivial group, which is certainly elementary amenable. Now, let $k > 0$. The isolated points of X_k are exactly the ones containing k 1-symbols. A homeomorphism must map isolated points to isolated points, so if $f \in \mathrm{Aut}(X_k)$, then the restriction $f|X_{k-1}$ is well-defined. The map $\phi : f \mapsto f|X_{k-1}$ is a homomorphism from $\mathrm{Aut}(X_k)$ to $\mathrm{Aut}(X_{k-1})$. Its image is elementary amenable by induction, so we only need to show that $\ker(\phi)$ is as well.

For this, let r be the common radius of $f, f^{-1} \in \ker(\phi)$. Let Y_r be the set of points y in X that contain k 1-symbols, which all occur in a single subword of y of length $2r+1$. We claim that if $x \notin Y_r$, then $f(x) = x$. Otherwise, $x_i \neq f(x)_i$ for some i. If x contains less than k 1-symbols, then f is not in the kernel of ϕ. Otherwise, because $x \notin Y_r$, $x_{[i-r,i+r]}$ cannot contain all the 1-symbols. In particular,the point y with $y_{[i-r,i+r]} = x_{[i-r,i+r]}$ and $y_j = 0$ for $j \notin [i-r, i+r]$ is in X_{k-1}. But $f(y)_i \neq y_i$, so again f cannot be in the kernel. This contradiction shows that only points in Y_r can be changed. The same reasoning applies to f^{-1}, so the set Y_r is invariant under the action of f. In other words, the action of f permutes Y_r and leaves every point in $X \setminus Y_r$ invariant.[24]

Now, let F_r be the subgroup of $\ker(\phi)$ that only permutes the points in Y_r. This is clearly a subgroup, and $\ker(\phi) = \bigcup_{r\in\mathbb{N}} F_r$. Thus, it is enough to show that F_r is elementary amenable. For this, observe that the set Y_r consists of finitely many orbits: $Y_r = \mathcal{O}(x_1) \cup \mathcal{O}(x_2) \cup \cdots \mathcal{O}(x_n)$ for some n and $x_i \in X$. A permutation of Y_r can, by shift-commutation, only permute the tracks and shift them around. It is then easy to show that F_r embeds in the group $\mathbb{Z}^n \rtimes S_n$, which is elementary amenable as a semidirect product of amenable groups. □

On the other hand, unlike the automorphism group of a transitive sofic shift, the automorphism group of a countable one need not be residually finite:

Proposition 3. *There exists a countable sofic shift X with $S_\infty \leq \mathrm{Aut}(X)$. In particular, $\mathrm{Aut}(X)$ is not be residually finite.*

[24] It is a general fact that if a group action on A maps $B \subset A$ to $C \subset B$, then it maps B exactly onto itself, and also $A \setminus B$ onto itself.

Proof. An example is $X_2 = \mathcal{L}^{-1}(0^*10^*10^*)$. If $g \in S_\infty$, define $f_g : X_2 \to X_2$ by

$$f_g(^\infty 0.10^n 10^\infty) = {}^\infty 0.10^{g(n)} 10^\infty.$$

Since g has finite support, f_g simply permutes finitely many (orbits of) isolated points and leaves everything else invariant. Continuity and shift-commutation are clear, and it is easily verified that $g \mapsto f_g$ embeds S_∞ into $\mathrm{Aut}(X_2)$. □

Every countable subshift has zero entropy, and it seems likely that this puts severe restrictions on the automorphism group. For example, the only ways to embed free groups into automorphism groups that the author is aware of generate entropy. Nevertheless, from just the assumption that X is countable, we are not able to prove any properties for $\mathrm{Aut}(X)$.

Question 5. If G is the automorphism group of a subshift, is it also the automorphism group of a countable subshift? Are automorphism groups of countable subshifts amenable? Can they contain a copy of F_2?

5 Minimal subshifts and subshifts of low complexity

A *substitution* is a function $\tau : S \to S^+$. We can apply such a map τ also to finite words by $\tau(w) = \tau(w_0)\tau(w_1)\cdots\tau(w_{|w|-1})$. Suppose τ is *primitive*, that is, $\exists n : \forall a, b \in S : \exists i : \tau^n(b)_i = a$. For $a \in S$ let $L_a = \{\tau^n(a) \mid n \in \mathbb{N}\}$. Then

$$X_\tau = \mathcal{L}^{-1}(L_a),$$

for any a, is the subshift generated by τ. The substitution τ is *binary* if $S = \{0, 1\}$ and *constant-length* if $\exists n : \forall a \in S : |\tau(a)| = n$. We say τ has a *coincidence* if $\exists i : \tau(a)_i = \tau(b)_i$ for all $a, b \in S$.

The subshifts X_τ for primitive τ are always minimal. Due to their rigid self-similar structure, one can often precisely compute their automorphism groups. To our knowledge, the first explicit result was the following.

Theorem 11 ([Cov71]). *Let τ be a binary primitive constant-length substitution. If τ has a coincidence, then* $\mathrm{Aut}(X_\tau) = \langle\sigma\rangle$. *Otherwise,* $\mathrm{Aut}(X_\tau) = \langle\sigma\rangle \times f$, *where f is the* binary flip CA *defined by $f(x)_i = 1 - x_i$.*

This was generalized in [HP89] to the non-binary case. We state only a weak form of the theorem.

Theorem 12 ([HP89]). *Let τ be a primitive constant-length substitution. Then* $\mathrm{Aut}(X_\tau)$ *is virtually* $\mathbb{Z}$.

It is also shown in [HP89] that this is close to optimal, as $\mathrm{Aut}(X_\tau)$ can be of the form $G \times \mathbb{Z}$ for any finite group G. (This construction can also be found in [DDMP14].) In [ST13], we generalized this result to all balanced substitutions – ones where $|\tau^n(a)| = a^n + d(n)$ where $a > 1$ and d is a bounded function.

A further generalization is the class of linearly recurrent minimal subshifts, and even more general are the minimal subshifts with *linear (factor) complexity*: the *word complexity* of X is the function $n \mapsto p_n(X) = |\mathcal{L}_n(X)|$, and X has linear factor complexity if $\exists C : \forall n : p_n(X) \leq Cn + C$. We asked in [ST14] whether it is true in general that linear factor complexity on a minimal subshift implies virtually $\mathbb{Z}$. It quickly turned out that the answer is 'yes':

Theorem 13 ([CY14,CK14,DDMP14]). *The automorphism group of an infinite minimal subshift with linear factor complexity is virtually $\mathbb{Z}$.*

In fact the result turned out to be, in some sense, folklore, though not explicitly published before. It can be proved quite quickly by using known properties of the fibers of the maximal equicontinuous factor in the linear complexity case.

The result of [CK14] is stated more generally for transitive subshifts, and all papers show more general results, in different directions. For cellular automata, we obtain in particular that for some k, every reversible CA $f : X \to X$ on an infinite minimal subshift with linear factor complexity satisfies $f^k = \sigma^n$ for some $n \in \mathbb{Z}$. It is quite easy to see that a virtually $\mathbb{Z}$ group has a decidable word problem and a decidable torsion problem in the purely group-theoretical sense. Using the folklore result that a Π_1^0 minimal subshift has a decidable language (see [Sal14b]), we see that these problems are even uniformly decidable in the following sense.

Theorem 14. *Given a Turing machine T enumerating the forbidden patterns of an infinite minimal subshift X and a cellular automaton $f : X \to X$, we can decide whether $f = \mathrm{id}_X$. If X has linear factor complexity, whether $\exists n \geq 1 : f^n = \mathrm{id}_X$ is decidable as well.*

Proof. An algorithm for checking $f = \mathrm{id}_X$ follows directly from the decidability of the language of x, so in particular the word problem is decidable. As for the torsion problem, iterating f, we obtain local rules for f^n for all n. By the assumption, $f^n = \sigma^m$ for some n, m. Since the word problem is decidable, it is easy to find such n and m algorithmically.[25] If $m = 0$, the answer is 'yes'. Otherwise it is 'no'. □

A result analogous to Theorem 13 can be shown for the endomorphism monoid when the subshift is also *linearly recurrent*, that is, there exists n such that every word $u \in \mathcal{L}(X)$ that appears in every word of $\mathcal{L}_{n|u|}(X)$ (see [DHS99] for more on this concept). Namely, it is known that in this case the subshift is *coalescent*, that is, $\mathrm{Aut}(X) = \mathrm{End}(X)$ [Dur00].

We note that while it is known that the automorphism group is virtually $\mathbb{Z}$ for a linear growth minimal subshift (in fact [CK14] shows the subtly stronger result, that it is a semidirect product of a finite group and $\mathbb{Z}$), and groups of the form $G \times \mathbb{Z}$ all occur as automorphism groups, we do not know what the precise class of automorphism groups is even in the linear growth case. The answer is presumably right around the corner, but we don't know it:

[25] For this, the assumption that f is indeed a cellular automaton on X is crucial. Given a local rule not defining such a CA, it is not clear what can be said.

Question 6. Which groups appear as $\mathrm{Aut}(X)$ for minimal subshifts X with linear factor complexity?

Another class of subshifts that has been studied are the ones with subquadratic factor complexity (for all $C > 0$, we have $p_n(X) < Cn^2$ for large enough n):

Theorem 15 ([CK14]). *Every cellular automaton on a transitive subshift of subquadratic complexity is a root of a shift map.*

In other words, if $f : X \to X$ is a CA and X is transitive and of subquadratic complexity, then $f^k = \sigma^n$ for some $k > 0, n \in \mathbb{Z}$. Unlike in the case of linear complexity, there is no uniform bound on the k, that is, for a transitive subshift X of subquadratic complexity, if $k(f)$ is the least positive integer such that $f^{k(f)} \in \{\sigma^n \mid n \in \mathbb{Z}\}$, then $k : \mathrm{End}(X) \to \mathbb{N}$ may be unbounded. An explicit example of such a subshift is given in [Sal14a].

Theorem 16 ([Sal14a]). *There exists a minimal Toeplitz subshift X with subquadratic complexity whose automorphism group is not finitely generated:*

$$\mathrm{Aut}(X) \cong \left\langle \left(\frac{2}{5}\right)^i \mid i \in \mathbb{N} \right\rangle \leq (\mathbb{Q}, +).$$

Of course, Theorem 14 extends to the subquadratic minimal case by the same proof. Presumably it does not generalize to all minimal subshifts, but we have no examples.

Question 7. Is there a minimal subshift with a decidable language whose automorphism group does not have a decidable word problem? Can the automorphism group have a finitely generated subgroup whose word problem is undecidable?

In [BLR88], a minimal subshift is constructed whose automorphism group contains a copy of $\mathbb{Q}$. There is much freedom in the construction, and they explain how the group could be made precisely $\mathbb{Q}$.

Theorem 17 ([BLR88]). *There is a minimal subshift X with $\mathrm{Aut}(X) \cong \mathbb{Q}$.*

It seems likely that one can also modify the construction so that the subshift has subquadratic factor complexity. With a similar construction, it seems that one can also obtain for example S_∞ as the automorphism group of a subquadratic growth. Nevertheless, we have no conjecture what the characterization is.

All the examples above are locally virtually cyclic: every finitely generated subgroup is virtually cyclic. This is not always the case on minimal subshifts, as shown by the following example (although the group is still locally virtually abelian):

Proposition 4. *[DDMP14] For any $d \in \mathbb{N}$, there exists a minimal subshift X with $\lim_{n\to\infty} p_X(n)/n^{d+1} = 0$ and $\mathrm{Aut}(X) \cong \mathbb{Z}^d$.*

The following limitation is shown in [DDMP14] in the case that recurrence times of words are polynomial (which is a stronger assumption than polynomial complexity). For a subshift X, define

$$N_X(n) = \inf\{m \mid w \in \mathcal{L}_m(X) \implies \forall u \in \mathcal{L}_n(X) : u \text{ occurs in } w\}.$$

Theorem 18 ([DDMP14]). *Let X be a transitive subshift such that*

$$\sup_{n \geq 1} N_X(n)/n^d < \infty$$

for $d \geq 1$. Then, there is a constant C depending only on d, such that any finitely generated subgroup of $\mathrm{Aut}(X)$ is virtually nilpotent of step at most C.

Like in the case of countable subshifts, we are not aware of any general results about the possible automorphism groups of minimal subshifts.

Question 8. Which groups occur as automorphism groups of minimal subshifts? In particular, if G is the automorphism group of a subshift, is it also the automorphism group of a minimal subshift? Can F_2 occur as a subgroup? Are the automorphism groups of minimal subshifts amenable?

Let $\mathcal{G}_M$ (resp. $\mathcal{G}'_M$) be the family of groups $\mathrm{Aut}(X)$ (resp. $\mathrm{Aut}(X)/\langle\sigma\rangle$) for minimal subshifts X. Especially in conjunction with the case of coded subshifts, the following question is particularly interesting:

Question 9. Is $\mathcal{G}_M$ closed under subgroups? Is $\mathcal{G}'_M$? More generally, what closure properties do they have?

6 Coded and synchronized systems

We briefly describe two of the results shown in [FF96] about automorphism groups of two families of transitive subshifts, namely the coded and synchronized systems. A word $w \sqsubset X$ is *synchronizing* if $uw, wv \sqsubset X \implies uwv \sqsubset X$. This means, in some sense, that no information travels over w. A *synchronized system* is a transitive subshift with a synchronizing word. The following construction of synchronized systems is shown in [FF96]:

Theorem 19 ([FF96]). *Given any subshift X with periodic points dense, there is a synchronized system Y such that $\mathrm{Aut}(Y)$ contains a copy of $\mathrm{Aut}(X)$.*

A *coded system* is a subshift X of the form $X = \mathcal{L}^{-1}(W^*)$, where W is any countable set of words over a finite alphabet. In other words, points of X are the limit points of infinite concatenations of words in W. Every synchronized system is coded, but the converse does not hold.

There is much freedom in the construction of automorphism groups of coded systems, as shown by the following strong result.

Theorem 20 ([FF96]). *If X has dense periodic points and $G \leq \mathrm{Aut}(X)$, then there is a coded system Y with $\mathrm{Aut}(Y) \cong G \times \mathbb{Z}$, where the isomorphism maps σ to $(1_G, 1)$.*

We note that this allows the exact construction of automorphism groups, not only subgroups of them, which separates coded systems from the families discussed in the previous sections (at least when it comes to known results). In particular, all finitely generated abelian groups can be obtained exactly as automorphism groups of coded systems. Since coded systems themselves have periodic points dense, the theorem also gives a kind of closure property for their automorphism groups.

Corollary 2. *Let $\mathcal{G}'_C$ be the set of groups G such that $\mathrm{Aut}(X) \cong G \times \mathbb{Z}$ for some coded subshift X. Then $\mathcal{G}'_C$ is closed under taking subgroups.*

We are not aware of a similar closure property for any other natural class of subshifts.

The family of coded systems contains only subshifts with periodic points dense, and thus they have only residually finite automorphism groups. There are some additional restrictions:

Lemma 7 ([FF96]). *The residually finite group $\mathbb{Z}[1/2]$ is not the automorphism group of any coded system.*

Again, we do not know what the precise class of groups that occur is.

References

[AS13] Nathalie Aubrun and Mathieu Sablik. Simulation of effective subshifts by two-dimensional subshifts of finite type. *Acta Appl. Math.*, 126(1):35–63, August 2013.

[BB14] J. Belk and C. Bleak. Some undecidability results for asynchronous transducers and the Brin-Thompson group 2V. *ArXiv e-prints*, May 2014.

[BLR88] 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.

[BM14] James Belk and Francesco Matucci. Conjugacy and dynamics in thompson's groups. *Geometriae Dedicata*, 169(1):239–261, 2014.

[Bow10] Lewis Bowen. Measure conjugacy invariants for actions of countable sofic groups. *Journal of the American Mathematical Society*, 23(1):217–245, 2010.

[Boy08] 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.

[CK14] V. Cyr and B. Kra. The automorphism group of a shift of subquadratic growth. *ArXiv e-prints*, March 2014.

[Cov71] Ethan M Coven. Endomorphisms of substitution minimal sets. *Probability Theory and Related Fields*, 20(2):129–133, 1971.

[CY14] E. Coven and R. Yassawi. Endomorphisms and automorphisms of minimal symbolic systems with sublinear complexity. *ArXiv e-prints*, November 2014.

[DDMP14] Sebastián Donoso, Fabien Durand, Alejandro Maass, and Samuel Petite. On automorphism groups of low complexity minimal subshifts, 2014.

[DHS99] F. Durand, B. Host, and C. Skau. Substitutional dynamical systems, Bratteli diagrams and dimension groups. *Ergodic Theory Dynam. Systems*, 19(4):953–993, 1999.

[DRS12] Bruno Durand, Andrei Romashchenko, and Alexander Shen. Fixed-point tile sets and their applications. *J. Comput. System Sci.*, 78(3):731–764, 2012.

[Dur00] Fabien Durand. Linearly recurrent subshifts have a finite number of non-periodic subshift factors. *Ergodic Theory and Dynamical Systems*, 20:1061–1078, 7 2000.

[FF96] Doris Fiebig and Ulf-Rainer Fiebig. The automorphism group of a coded system. *Transactions of the American Mathematical Society*, 348(8):3173–3191, 1996.

[GKM12] Anahí Gajardo, Jarkko Kari, and Andrés Moreira. On time-symmetry in cellular automata. *Journal of Computer and System Sciences*, 78(4):1115 – 1126, 2012.

[Gri85] R. I. Grigorchuk. Degrees of growth of finitely generated groups, and the theory of invariant means. *Mathematics of the USSR-Izvestiya*, 25(2):259, 1985.

[Gui11] Pierre Guillon. Projective subdynamics and universal shifts. In *17th International Workshop on Cellular Automata and Discrete Complex Systems, Automata 2011, Center for Mathematical Modeling, University of Chile, Santiago, Chile, November 21-23, 2011*, pages 123–134, 2011.

[GZ12] P. Guillon and C. Zinoviadis. Densities and entropies in cellular automata. *ArXiv e-prints*, April 2012.

[Hed69] Gustav A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory*, 3:320–375, 1969.

[HMU06] John E. Hopcroft, Rajeev Motwani, and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation (3rd Edition)*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2006.

[Hoc10] Michael Hochman. On the automorphism groups of multidimensional shifts of finite type. *Ergodic Theory Dynam. Systems*, 30(3):809–840, 2010.

[HP89] B. Host and F. Parreau. Homomorphismes entre systèmes dynamiques définis par substitutions. *Ergodic Theory and Dynamical Systems*, 9:469–477, 8 1989.

[Kar90] Jarkko Kari. Reversibility of 2d cellular automata is undecidable. *Physica D: Nonlinear Phenomena*, 45(1–3):379 – 385, 1990.

[Kar12] Jarkko Kari. Decidability and undecidability in cellular automata. *Int. J. General Systems*, 41(6):539–554, 2012.

[Kit98] Bruce P. Kitchens. *Symbolic dynamics – One-sided, two-sided and countable state Markov shifts*. Universitext. Springer-Verlag, Berlin, 1998.

[KO08] 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.

[KR90] K. H. Kim and F. W. Roush. On the automorphism groups of subshifts. *Pure Mathematics and Applications*, 1(4):203–230, 1990.

[KR91] K. H. Kim and F. W. Roush. Solution of two conjectures in symbolic dynamics. *Proceedings of the American Mathematical Society*, 112(4):1163–1168, 1991.

[Kůr03] Petr Kůrka. *Topological and symbolic dynamics*, volume 11 of *Cours Spécialisés [Specialized Courses]*. Société Mathématique de France, Paris, 2003.

[LM95] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding*. Cambridge University Press, Cambridge, 1995.

[Lot02] M. Lothaire. *Algebraic combinatorics on words*, volume 90 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2002.

[Ols83] A. Yu. Olshanskii. On a geometric method in the combinatorial group theory. In *International Congress of Mathematicians, Proceedings of the International Congress of Muthematicians*, pages 415–424, 1983.

[Rot95] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148. Springer Science & Business Media, 1995.

[Rya72] J. Patrick Ryan. The shift and commutativity. *Mathematical systems theory*, 6(1-2):82–85, 1972.

[Sal14a] V. Salo. Toeplitz subshift whose automorphism group is not finitely generated. *ArXiv e-prints*, November 2014.

[Sal14b] Ville Salo. *Subshifts with Simple Cellular Automata*. PhD thesis, 2014.

[ST12] Ville Salo and Ilkka Törmä. Computational aspects of cellular automata on countable sofic shifts. *Mathematical Foundations of Computer Science 2012*, pages 777–788, 2012.

[ST13] Ville Salo and Ilkka Törmä. Constructions with countable subshifts of finite type. *Fundam. Inf.*, 126(2-3):263–300, April 2013.

[ST14] Ville Salo and Ilkka Törmä. Block maps between primitive uniform and pisot substitutions. *Ergodic Theory and Dynamical Systems*, FirstView:1–19, 9 2014.