The group of reversible Turing machines

Sebastián Barbieri[1], Jarkko Kari[2] and Ville Salo[3]

[1] LIP, ENS de Lyon – CNRS – INRIA – UCBL – Université de Lyon,
[2] University of Turku
[3] Center for Mathematical Modeling, University of Chile
sebastian.barbieri@ens-lyon.fr, jkari@utu.fi, vosalo@utu.fi

Abstract. We consider Turing machines as actions over configurations in $\Sigma^{\mathbb{Z}^d}$ which only change them locally around a marked position that can move and carry a particular state. In this setting we study the monoid of Turing machines and the group of reversible Turing machines. We also study two natural subgroups, namely the group of finite-state automata, which generalizes the topological full groups studied in the theory of orbit-equivalence, and the group of oblivious Turing machines whose movement is independent of tape contents, which generalizes lamplighter groups and has connections to the study of universal reversible logical gates. Our main results are that the group of Turing machines in one dimension is neither amenable nor residually finite, but is locally embeddable in finite groups, and that the torsion problem is decidable for finite-state automata in dimension one, but not in dimension two.

1 Introduction

1.1 Turing machines and their generalization

Turing machines have been studied since the 30s as the standard formalization of the abstract concept of computation. However, more recently, Turing machines have also been studied in the context of dynamical systems. In [22], two dynamical systems were associated to a Turing machine, one with a 'moving tape' and one with a 'moving head'. After that, there has been a lot of study of dynamics of Turing machines, see for example [16,30,21,13,12,17,1]. Another connection between Turing machines and dynamics is that they can be used to define subshifts. Subshifts whose forbidden patterns are given by a Turing machine are called effectively closed, computable, or Π_1^0 subshifts, and especially in multiple dimensions, they are central to the topic due to the strong links known between SFTs, sofic shifts and Π_1^0-subshifts, see for example [10,4]. An intrinsic notion of Turing machine computation for these subshifts on general groups was proposed in [3], and a similar study was performed with finite state machines in [29,28].

In all these papers, the definition of a Turing machine is (up to notational differences and switching between the moving tape and moving head model) the following: A Turing machine is a function $T : \Sigma^{\mathbb{Z}} \times Q \to \Sigma^{\mathbb{Z}} \times Q$ defined by a local rule $f_T : \Sigma \times Q \to \Sigma \times Q \times \{-1, 0, 1\}$ by the formula

$$T(x, q) = (\sigma_{-d}(\tilde{x}), q') \text{ if } f_T(x_0, q) = (a, q', d),$$

where $\sigma : \Sigma^{\mathbb{Z}} \to \Sigma^{\mathbb{Z}}$ is the shift action given by $\sigma_d(x)_z = x_{z-d}$, $\tilde{x}_0 = a$ and $\tilde{x}|_{\mathbb{Z}\setminus\{0\}} = x|_{\mathbb{Z}\setminus\{0\}}$. In this paper, such Turing machines are called *classical Turing machines*. This definition (as far as we know) certainly suffices to capture all computational and dynamical properties of interest, but it also has some undesirable properties: The composition of two classical Turing machines – and even the square of a classical Turing machine – is typically not a classical Turing machine, and the reverse of a reversible classical Turing machine is not always a classical Turing machine.

In this paper, we give a more general definition of a Turing machine, by allowing it to move the head and modify cells at an arbitrary (but bounded) distance on each timestep. With the new definition, we get rid of both issues: With our definition,

- Turing machines are closed under composition, forming a monoid, and
- reversible Turing machines are closed under inversion, forming a group.

We also characterize reversibility of classical Turing machines in combinatorial terms, and show what their inverses look like. Our definition of a Turing machine originated in the yet unpublished work [27], where the group of such machines was studied on general $\mathbb{Z}$-subshifts (with somewhat different objectives).

These benefits of the definition should be compared to the benefits of allowing arbitrary radii in the definition of a cellular automaton: If we define cellular automata as having a fixed radius of, say, 3, then the inverse map of a reversible cellular automaton is not always a cellular automaton, as the inverse of a cellular automaton may have a much larger radius [9]. Similarly, with a fixed radius, the composition of two cellular automata is not necessarily a cellular automaton.

We give our Turing machine definitions in two ways, with a moving tape and with a moving head, as done in [22]. The moving tape point of view is often the more useful one when studying one-step behavior and invariant measures, whereas we find the moving head point of view easier for constructing examples, and when we need to track the movement of multiple heads. The moving head Turing machines are in fact a subset of cellular automata on a particular kind of subshift. The moving tape machine on the other hand is a generalization of the topological full group of a subshift, which is an important concept in particular in the theory of orbit equivalence. For topological full groups of minimal subshifts, see for example [14,15,18]. The (one-sided) SFT case is studied in [26].

1.2 Our results and comparisons with other groups

In Section 2, we define our basic models and prove basic results about them. In Section 2.3, we define the uniform measure and show as a simple application of it that injectivity and surjectivity are both equal to reversibility.

Our results have interesting counterparts in the theory of cellular automata: One of the main theorems in the theory of cellular automata is that injectivity implies surjectivity, and (global) bijectivity is equivalent to having a cellular automaton inverse map. Furthermore, one can attach to a reversible one- or

two-dimensional cellular automaton its 'average drift', that is, the speed at which information moves when the map is applied, and this is a homomorphism from the group of cellular automata to a sublattice of $\mathbb{Q}^d$ (where d is the corresponding dimension), see [19]. In Section 3 we use the uniform measure to define an analog, the 'average movement' homomorphism for Turing machines.

In Section 3, we define some interesting subgroups of the group of Turing machines. First, we define the local permutations – Turing machines that never move the head at all –, and their generalization to oblivious Turing machines where movement is allowed, but is independent of the tape contents. The group of oblivious Turing machines can be seen as a kind of generalization of lamplighter groups. It is easy to show that these groups are amenable but not residually finite. What makes them interesting is that the group of oblivious Turing machines is finitely generated, due to the existence of universal reversible logical gates. It turns out that strong enough universality for reversible gates was proved only recently [2].

We also define the group of (reversible) finite-state machines – Turing machines that never modify the tape. Here, we show how to embed a free group with a similar technique as used in [11], proving that this group is non-amenable. By considering the action of Turing machines on periodic points,[4] we show that the group of finite-state automata is residually finite, and the group of Turing machines is locally embeddable in finite groups (in particular sofic).

Our definition of a Turing machine can be seen as a generalization of the topological full group, and in particular finite-state machines with a single state exactly correspond to this group. Thus, it is interesting to compare the results of Section 3 to known results about topological full groups. In [15,18] it is shown that the topological full group of a minimal subshift is locally embeddable in finite groups and amenable, while we show that on full shifts, this group is non-amenable, but the whole group of Turing machines is LEF.[5]

Our original motivation for defining these subgroups – finite-state machines and local permutations – was to study the question of whether they generate all reversible Turing machines. Namely, a reversible Turing machine changes the tape contents at the position of the head and then moves, in a globally reversible way. Thus, it is a natural question whether every reversible Turing machine can actually be split into reversible tape changes (actions by local permutations) and reversible moves (finite-state automata). We show that this is not the case, by showing that Turing machines can have arbitrarily small average movement, but that elementary ones have only a discrete sublattice of possible average movements. We do not know whether this is the only restriction.

In Section 4, we show that the group of Turing machines is recursively presented and has a decidable word problem, but that its torsion problem (the

[4] The idea is similar as that in [25] for showing that automorphism groups of mixing SFTs are residually finite, but we do not actually look at subsystems, but the periodic points of an enlarged system, where we allow infinitely many heads to occur.

[5] In [27] it is shown that on minimal subshifts, the group of Turing machines coincides with the group of finite-state automata.

problem of deciding if a given element has finite order) is undecidable in all dimensions. For finite-state machines, we show that the torsion problem is decidable in dimension one, but is undecidable in higher dimensions, even when we restrict to a finitely generated subgroup. We note a similar situation with Thompson's group V: its torsion problem is decidable in one-dimension, but undecidable in higher dimensions. [6,5]

1.3 Preliminaries

In this section we present general definitions and settle the notation which is used throughout the article. The review of these concepts will be brief and focused on the dynamical aspects. For a more complete introduction the reader may refer to [24] or [8] for the group theoretic aspects. Let $\mathcal{A}$ be a finite alphabet. The set $\mathcal{A}^{\mathbb{Z}^d} = \{x : \mathbb{Z}^d \to \mathcal{A}\}$ equipped with the left group action $\sigma : \mathbb{Z}^d \times \mathcal{A}^{\mathbb{Z}^d} \to \mathcal{A}^{\mathbb{Z}^d}$ defined by $(\sigma_{\boldsymbol{v}}(x))_{\boldsymbol{u}} = x_{\boldsymbol{u}-\boldsymbol{v}}$ is a *full shift*. The elements $a \in \mathcal{A}$ and $x \in \mathcal{A}^{\mathbb{Z}^d}$ are called *symbols* and *configurations* respectively. With the discrete topology on $\mathcal{A}$ the set of configurations $\mathcal{A}^{\mathbb{Z}^d}$ is compact and given by the metric $d(x, y) = 2^{-\inf(\{|\boldsymbol{v}| \in \mathbb{N} |\ x_{\boldsymbol{v}} \neq y_{\boldsymbol{v}}\})}$ where $|\boldsymbol{v}|$ is a norm on $\mathbb{Z}^d$ (we settle here for the $||\cdot||_\infty$ norm). This topology has the *cylinders* $[a]_{\boldsymbol{v}} = \{x \in \mathcal{A}^{\mathbb{Z}^d} | x_{\boldsymbol{v}} = a \in \mathcal{A}\}$ as a subbasis. A *support* is a finite subset $F \subset \mathbb{Z}^d$. Given a support F, a *pattern with support* F is an element p of $\mathcal{A}^F$. We also denote the cylinder generated by p in position $\boldsymbol{v}$ as $[p]_{\boldsymbol{v}} = \bigcap_{\boldsymbol{u} \in F} [p_{\boldsymbol{u}}]_{\boldsymbol{v}+\boldsymbol{u}}$, and $[p] = [p]_{\mathbf{0}}$.

Definition 1. *A subset X of $\mathcal{A}^{\mathbb{Z}^d}$ is a* subshift *if it is σ-invariant – $\sigma(X) \subset X$ – and closed for the cylinder topology. Equivalently, X is a subshift if and only if there exists a set of forbidden patterns $\mathcal{F}$ that defines it.*

$$X = \bigcap_{p \in \mathcal{F}, \boldsymbol{v} \in \mathbb{Z}^d} \mathcal{A}^{\mathbb{Z}^d} \setminus [p]_{\boldsymbol{v}}.$$

Let X, Y be subshifts over alphabets $\mathcal{A}$ and $\mathcal{B}$ respectively. A continuous $\mathbb{Z}^d$-equivariant map $\phi : X \to Y$ between subshifts is called a morphism. A well-known Theorem of Curtis, Lyndon and Hedlund which can be found in full generality in [8] asserts that morphisms are equivalent to maps defined by local rules as follows: There exists a finite $F \subset \mathbb{Z}^d$ and $\Phi : \mathcal{A}^F \to \mathcal{B}$ such that $\forall x \in X : \phi(x)_{\boldsymbol{v}} = \Phi(\sigma_{-\boldsymbol{v}}(x)|_F)$. If ϕ is an endomorphism then we refer to it as a cellular automaton. A cellular automaton is said to be reversible if there exists a cellular automaton ϕ^{-1} such that $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = \mathrm{id}$. It is well known that reversibility is equivalent to bijectivity.

Throughout this article we use the following notation inspired by Turing machines. We denote by $\Sigma = \{0, \ldots, n-1\}$ the set of tape symbols and $Q = \{1, \ldots, k\}$ the set of states. We also use exclusively the symbols $n = |\Sigma|$ for the size of the alphabet and $k = |Q|$ for the number of states. Given a function $f : \Omega \to \prod_{i \in I} A_i$ we denote by f_i the projection of f to the i-th coordinate.

2 Two models for Turing machine groups

In this section we define our generalized Turing machine model, and the group of Turing machines. In fact, we give two definitions for this group, one with a moving head and one with a moving tape as in [22]. We show that – except in the case of a trivial alphabet – these groups are isomorphic.[6] Furthermore, both can be defined both by local rules and 'dynamically', that is, in terms of continuity and the shift. In the moving tape model we characterize reversibility as preservation of the uniform measure. Finally we conclude this section by characterizing reversibility for classical Turing machines in our setting.

2.1 The moving head model

Consider $Q = \{1, \dots, k\}$ and let X_k be the subshift with alphabet $Q \cup \{0\}$ such that in each configuration the number of non-zero symbols is at most one.

$$X_k = \{x \in \{0, 1, \dots, k\}^{\mathbb{Z}^d} \mid 0 \notin \{x_{\boldsymbol{u}}, x_{\boldsymbol{v}}\} \implies \boldsymbol{u} = \boldsymbol{v}\}.$$

In particular $X_0 = \{0^{\mathbb{Z}^d}\}$ and $i < j \implies X_i \subsetneq X_j$. Let also $\Sigma = \{0, \dots, n-1\}$ and $X_{n,k} = \Sigma^{\mathbb{Z}^d} \times X_k$. For the case $d = 1$, configurations in $X_{n,k}$ represent a bi-infinite tape filled with symbols in Σ possibly containing a head that has a state in Q. Note that there might be no head in a configuration.

Definition 2. *Given a function*

$$f : \Sigma^F \times Q \to \Sigma^{F'} \times Q \times \mathbb{Z}^d,$$

where F, F' are finite subsets of $\mathbb{Z}^d$, we can define a map $T_f : X_{n,k} \to X_{n,k}$ as follows: Let $(x, y) \in X_{n,k}$. If there is no $\boldsymbol{v} \in \mathbb{Z}^d$ such that $y_{\boldsymbol{v}} \neq 0$ then $T(x, y) = (x, y)$. Otherwise let $p = \sigma_{-\boldsymbol{v}}(x)|_F$, $q = y_{\boldsymbol{v}} \neq 0$ and $f(p, q) = (p', q', \boldsymbol{d})$. Then $T(x, y) = (\tilde{x}, \tilde{y})$ where:

$$\tilde{x}_{\boldsymbol{t}} = \begin{cases} x_{\boldsymbol{t}} & \text{if } \boldsymbol{t} - \boldsymbol{v} \notin F' \\ p'_{\boldsymbol{t}-\boldsymbol{v}} & \text{if } \boldsymbol{t} - \boldsymbol{v} \in F' \end{cases}, \qquad \tilde{y}_{\boldsymbol{t}} = \begin{cases} q' & \text{if } \boldsymbol{t} = \boldsymbol{v} + \boldsymbol{d} \\ 0 & \text{otherwise} \end{cases}$$

Such $T = T_f$ is called a (moving head) (d, n, k)-Turing machine*, and f is its* local rule*. If there exists a (d, n, k)-Turing machine T^{-1} such that $T \circ T^{-1} = T^{-1} \circ T = \mathrm{id}$, we say T is* reversible*.*

Note that $\sigma_{-\boldsymbol{v}}(x)|_F$ is the F-shaped pattern 'at' $\boldsymbol{v}$, but we do not write $x|_{F+\boldsymbol{v}}$ because we want the pattern we read from x to have F as its domain.

This definition corresponds to classical Turing machines with the moving head model when $d = 1$, $F = F' = \{0\}$ and $f(x, q)_3 \in \{-1, 0, 1\}$ for all x, q. By possibly changing the local rule f, we can always choose $F = [-r_i, r_i]^d$ and

[6] Note that the *dynamics* obtained from these two definitions are in fact quite different, as shown in [22,23].

$F' = [-r_o, r_o]^d$ for some $r_i, r_o \in \mathbb{N}$, without changing the Turing machine T_f it defines. The minimal such r_i is called the *in-radius* of T, and the minimal r_o is called the *out-radius* of T. We say the in-radius of a Turing machine is -1 if there is no dependence on input, that is, the neighborhood $[-r_i, r_i]$ can be replaced by the empty set. Since $\Sigma^F \times Q$ is finite, the third component of $f(p, q)$ takes only finitely many values $\boldsymbol{v} \in \mathbb{Z}^d$. The maximum of $|\boldsymbol{v}|$ for such $\boldsymbol{v}$ is called the *move-radius* of T. Finally, the maximum of all these three radii is called the *radius* of T. In this terminology, classical Turing machines are those with in- and out-radius 0, and move-radius 1.

Definition 3. *Define* $\mathrm{TM}(\mathbb{Z}^d, n, k)$ *as the set of* (d, n, k)*-Turing machines and* $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ *the set of reversible* (d, n, k)*-Turing machines.*

In some parts of this article we just consider $d = 1$. In this case we simplify the notation and just write $\mathrm{RTM}(n, k) := \mathrm{RTM}(\mathbb{Z}, n, k)$.

Of course, we want $\mathrm{TM}(\mathbb{Z}^d, n, k)$ to be a monoid and $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ a group under function composition. This is indeed the case, and one can prove this directly by constructing local rules for the inverse of a reversible Turing machine and composition of two Turing machines. However, it is much easier to extract this from the following characterization of Turing machines as a particular kind of cellular automaton.

For a subshift X, we denote by $\mathrm{End}(X)$ the monoid of endomorphisms of X and $\mathrm{Aut}(X)$ the group of automorphisms of X.

Proposition 1. *Let* n, k *be positive integers and* $Y = X_{n,0}$*. Then:*

$$\mathrm{TM}(\mathbb{Z}^d, n, k) = \{\phi \in \mathrm{End}(X_{n,k}) \mid \phi|_Y = \mathrm{id}, \phi^{-1}(Y) = Y\}$$
$$\mathrm{RTM}(\mathbb{Z}^d, n, k) = \{\phi \in \mathrm{Aut}(X_{n,k}) \mid \phi|_Y = \mathrm{id}\}$$

Corollary 1. *We have* $\phi \in \mathrm{RTM}(\mathbb{Z}^d, n, k)$ *if and only if* $\phi \in \mathrm{TM}(\mathbb{Z}^d, n, k)$ *and* ϕ *is bijective.*

Clearly, the conditions of Proposition 1 are preserved under function composition and inversion. Thus:

Corollary 2. *Under function composition,* $(\mathrm{TM}(\mathbb{Z}^d, n, k), \circ)$ *is a submonoid of* $\mathrm{End}(X_{n,k})$ *and* $(\mathrm{RTM}(\mathbb{Z}^d, n, k), \circ)$ *is a group.*

We usually omit the function composition symbol, and use the notations $\mathrm{TM}(\mathbb{Z}^d, n, k)$ and $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ to refer to the corresponding monoids and groups.

2.2 The moving tape model

It's also possible to consider the position of the Turing machine as fixed at 0, and move the tape instead, to obtain the moving tape Turing machine model. In [22], where Turing machines are studied as dynamical systems, the moving head

model and moving tape model give non-conjugate dynamical systems. However, the abstract monoids defined by the two points of view turn out to be equal, and we obtain an equivalent definition of the group of Turing machines.

As in the previous section, we begin with a definition using local rules.

Definition 4. *Given a function $f : \Sigma^F \times Q \to \Sigma^{F'} \times Q \times \mathbb{Z}^d$, where F, F' are finite subsets of $\mathbb{Z}^d$, we can define a map $T_f : \Sigma^{\mathbb{Z}^d} \times Q \to \Sigma^{\mathbb{Z}^d} \times Q$ as follows: If $f(x|_F, q) = (p, q', \boldsymbol{d})$, then $T_f(x, q) = (\sigma_{\boldsymbol{d}}(y), q')$ where*

$$y_{\boldsymbol{u}} = \begin{cases} x_{\boldsymbol{u}}, \text{ if } \boldsymbol{u} \notin F' \\ p_{\boldsymbol{u}}, \text{ if } \boldsymbol{u} \in F', \end{cases}$$

is called the moving tape Turing machine *defined by f.*

These machines also have the following characterization with a slightly more dynamical feel to it. Say that x and y are *asymptotic*, and write $x \sim y$, if $d(\sigma_{\boldsymbol{v}}(x), \sigma_{\boldsymbol{v}}(y)) \to 0$ as $|\boldsymbol{v}| \to \infty$. We write $x \sim_m y$ if $x_{\boldsymbol{v}} = y_{\boldsymbol{v}}$ for all $|\boldsymbol{v}| \geq m$, and clearly $x \sim y \iff \exists m : x \sim_m y$.

Lemma 1. *Let $T : \Sigma^{\mathbb{Z}^d} \times Q \to \Sigma^{\mathbb{Z}^d} \times Q$ be a function. Then T is a moving tape Turing machine if and only if it is continuous, and for a continuous function $s : \Sigma^{\mathbb{Z}^d} \times Q \to \mathbb{Z}^d$ and $a \in \mathbb{N}$ we have $T(x, q)_1 \sim_a \sigma_{s(x,q)}(x)$ for all $(x, q) \in \Sigma^{\mathbb{Z}^d} \times Q$.*

Note that in place of a we could allow a continuous $\mathbb{N}$-valued function of (x, q) – the definition obtained would be equivalent, as the a of the present definition can be taken as the maximum of such a function.

We call the function s in the definition of these machines the *shift indicator* of T, as it indicates how much the tape is shifted depending on the local configuration around 0. In the theory of orbit equivalence and topological full groups, the analogs of s are usually called *cocycles*. We also define in-, out- and move-radii of moving tape Turing machines similarly as in the moving head case.

We note that it is not enough that $T(x, q)_1 \sim \sigma_{s(x,q)}(x)$ for all $(x, q) \in \Sigma^{\mathbb{Z}^d} \times Q$: Let $Q = \{1\}$ and consider the function $T : \Sigma^{\mathbb{Z}} \times Q \to \Sigma^{\mathbb{Z}} \times Q$ defined by $(T(x, 1)_1)_i = x_{-i}$ if $x_{[-|i|+1,|i|-1]} = 0^{2i-1}$ and $\{x_i, x_{-i}\} \neq \{0\}$, and $(T(x, 1)_1)_i = x_i$ otherwise. Clearly this map is continuous, and the constant-$\mathbf{0}$ map $s(x, q) = \mathbf{0}$ gives a shift-indicator for it. However, T is not defined by any local rule since it can modify the tape arbitrarily far from the origin.

As for moving head machines, it is easy to see (either by constructing local rules or by applying the dynamical definition) that the composition of two moving tape Turing machines is again a moving tape Turing machine. This allows us to proceed as before and define their monoid and group.

Definition 5. *We denote by $\mathrm{TM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k)$ and $\mathrm{RTM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k)$ the monoid of moving tape (d, n, k)-Turing machines and the group of reversible moving tape (d, n, k)-Turing machines respectively.*

Now, let us show that the moving head and moving tape models are equivalent. First, there is a natural epimorphism $\Psi : \mathrm{TM}(\mathbb{Z}^d, n, k) \to \mathrm{TM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k)$. Namely, let $T \in \mathrm{TM}(\mathbb{Z}^d, n, k)$. We define $\Psi(T)$ as follows: Let $(x, q) \in \Sigma^{\mathbb{Z}^d} \times Q$. Letting y be the configuration such that $y_{\mathbf{0}} = q$ and 0 everywhere else and $T(x, y) = (x', y')$ such that $y'_{\boldsymbol{v}} = q'$ we define $\Psi(T)(x, q) = (\sigma_{-\boldsymbol{v}}(x'), q')$. This is clearly an epimorphism but it's not necessarily injective if $n = 1$. Indeed, we have that $\mathrm{RTM}_{\mathrm{fix}}(\mathbb{Z}^d, 1, k) \cong S_k$ and $\mathrm{TM}_{\mathrm{fix}}(\mathbb{Z}^d, 1, k)$ is isomorphic to the monoid of all functions from $\{1, \dots, k\}$ to itself while $\mathbb{Z}^d \leq \mathrm{RTM}(\mathbb{Z}^d, 1, k) \leq \mathrm{TM}(\mathbb{Z}^d, 1, k)$. Nevertheless, if $n \geq 2$ this mapping is an isomorphism.

Lemma 2. *If $n \geq 2$ then:*

$$\mathrm{TM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k) \cong \mathrm{TM}(\mathbb{Z}^d, n, k)$$
$$\mathrm{RTM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k) \cong \mathrm{RTM}(\mathbb{Z}^d, n, k).$$

The previous result means that besides the trivial case $n = 1$ where the tape plays no role, we can study the properties of these groups using any model.

2.3 The uniform measure and reversibility.

Consider the space $\Sigma^{\mathbb{Z}^d} \times Q$. We define a measure μ on $\mathcal{B}(\Sigma^{\mathbb{Z}^d} \times Q)$ as the product measure of the uniform Bernoulli measure and the uniform discrete measure. That is, if F is a finite subset of $\mathbb{Z}^d$ and $p \in \Sigma^F$, then:

$$\mu([p] \times \{q\}) = \frac{1}{kn^{|F|}}.$$

With this measure in hand we can prove the following:

Theorem 1. *Let $T \in \mathrm{TM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k)$. Then the following are equivalent:*

1. *T is injective.*
2. *T is surjective.*
3. *$T \in \mathrm{RTM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k)$.*
4. *T preserves the uniform measure ($\mu(T^{-1}(A)) = \mu(A)$ for all Borel sets A).*
5. *$\mu(T(A)) = \mu(A)$ for all Borel sets A.*

Remark 1. The proof is based on showing that every Turing machine is a *local homeomorphism* and preserves the measure of all large-radius cylinders in the forward sense. Note that preserving the measure of large-radius cylinders in the forward sense does not imply preserving the measure of all Borel sets, in general. For example, the machine which turns the symbol in $F = \{\mathbf{0}\}$ to 0 without moving the head satisfies $\mu([p]) = \mu(T[p])$ for any $p \in \Sigma^S$ with $S \supset F$. But $\mu([]) = 1$ and $\mu(T([])) = \mu([0]) = 1/2$, where $[] = \{0, \dots, n\}^{\mathbb{Z}}$ is the cylinder defined by the empty word.

Using the measure, one can define the average movement of a Turing machine.

Definition 6. *Let $T \in \mathrm{TM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k)$ with shift indicator function $s : \Sigma^{\mathbb{Z}^d} \times Q \to \mathbb{Z}^d$. We define the* average movement *$\alpha(T) \in \mathbb{Q}^d$ as*

$$\alpha(T) := \mathbb{E}_\mu(s) = \int_{\Sigma^{\mathbb{Z}^d} \times Q} s(x, q) d\mu,$$

where μ is the uniform measure defined in Subsection 2.3. For T in $\mathrm{TM}(\mathbb{Z}^d, n, k)$ we define α as the application to its image under the canonical epimorphism Ψ, that is, $\alpha(T) := \alpha(\Psi(T))$.

We remark that this integral is actually a finite sum over the cylinders $p \in \Sigma^F$. Nonetheless, its expression as an expected value allows us to show the following: If $T_1, T_2 \in \mathrm{RTM}(\mathbb{Z}^d, n, k)$ then $\alpha(T_1 \circ T_2) = \alpha(T_1) + \alpha(T_2)$. Indeed, as reversibility implies measure-preservation, we have that

$$\mathbb{E}_\mu(s_{T_1 \circ T_2}) = \mathbb{E}_\mu(s_{T_1} \circ T_2 + s_{T_2}) = \mathbb{E}_\mu(s_{T_1}) + \mathbb{E}_\mu(s_{T_2}).$$

This means that α defines an homomorphism from $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ to $\mathbb{Q}^d$.

2.4 Classical Turing machines

As discussed in the introduction, we say a one-dimensional Turing machine is *classical* if its in- and out-radii are 0, and its move-radius is 1. In this section, we characterize reversibility in classical Turing machines. If T_0 has in-, out- and move-radius 0, that is, T_0 only performs a permutation of the set of pairs $(s, q) \in \Sigma \times Q$ at the position of the head, then we say T_0 is a *state-symbol permutation*. If T_1 has in-radius -1, never modifies the tape, and only makes movements by vectors in $\{-1, 0, 1\}$, then T_1 is called a *state-dependent shift*.[7]

Theorem 2. *A classical Turing machine T is reversible if and only if it is of the form $T_1 \circ T_0$ where T_0 is a state-symbol permutation and T_1 is a state-dependent shift.*

It follows that the inverse of a reversible classical Turing machine is always of the form $T_0 \circ T_1$ where T_0 is a state-symbol permutation and T_1 is a state-dependent shift. In the terminology of Section 3, the theorem implies that all reversible classical Turing machines are elementary.

3 Properties of RTM and interesting subgroups

In this section we study some properties of RTM by studying the subgroups it contains. We introduce LP, the group of local permutations where the head does not move and RFA, the group of (reversible) finite-state automata which do not

[7] Note that these machines are slightly different than the groups $\mathrm{SP}(\mathbb{Z}, n, k)$ and $\mathrm{Shift}(\mathbb{Z}, n, k)$ introduced in Section 3, as the permutations in $\mathrm{SP}(\mathbb{Z}, n, k)$ do not modify the tape, and moves in $\mathrm{Shift}(\mathbb{Z}; n, k)$ cannot depend on the state.

change the tape. These groups separately capture the dynamics of changing the tape and moving the head. We also define the group of oblivious Turing machines OB as an extension of LP where arbitrary tape-independent moves are allowed, and EL as the group of elementary Turing machines, which are compositions of finite-state automata and oblivious Turing machines.

First, we observe that $\alpha(\mathrm{RTM}(\mathbb{Z}^d, n, k))$ is not finitely generated, and thus:

Theorem 3. *For $n \geq 2$, the group $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ is not finitely generated.*

Although α is not a homomorphism on $\mathrm{TM}(\mathbb{Z}^d, n, k)$, using Theorem 1, we obtain that $\mathrm{TM}(\mathbb{Z}^d, n, k)$ cannot be finitely generated either.

3.1 Local permutations and oblivious Turing machines

For $\boldsymbol{v} \in \mathbb{Z}^d$, define the machine $T_{\boldsymbol{v}}$ which does not modifies the state or the tape, and moves the head by the vector $\boldsymbol{v}$ on each step. Denote the group of such machines by $\mathrm{Shift}(\mathbb{Z}^d, n, k)$. Clearly $\alpha : \mathrm{Shift}(\mathbb{Z}^d, n, k) \to \mathbb{Z}^d$ is a group isomorphism. Define also $\mathrm{SP}(\mathbb{Z}^d, n, k)$ as the *state-permutations*: Turing machines that never move and only permute their state as a function of the tape.

Definition 7. *We define the group $\mathrm{LP}(\mathbb{Z}^d, n, k)$ of* local permutations *as the subgroup of reversible (d, n, k)-Turing machines whose shift-indicator is the constant-$\mathbf{0}$ function. Define also $\mathrm{OB}(\mathbb{Z}^d, n, k) = \langle \mathrm{Shift}(\mathbb{Z}^d, n, k), \mathrm{LP}(\mathbb{Z}^d, n, k) \rangle$, the group of* oblivious Turing machines.

In other words, $\mathrm{LP}(\mathbb{Z}^d, n, k)$ is the group of reversible machines that do not move the head, and $\mathrm{OB}(\mathbb{Z}^d, n, k)$ is the group of reversible Turing machines whose head movement is independent of the tape contents. Note that in the definition of both groups, we allow changing the state as a function of the tape, and vice versa. Clearly $\mathrm{Shift}(\mathbb{Z}^d, n, k) \leq \mathrm{OB}(\mathbb{Z}^d, n, k)$ and $\mathrm{SP}(\mathbb{Z}^d, n, k) \leq \mathrm{LP}(\mathbb{Z}^d, n, k)$.

Proposition 2. *Let S_∞ be the group of permutations of $\mathbb{N}$ of finite support. Then for $n \geq 2$, $S_\infty \hookrightarrow \mathrm{LP}(\mathbb{Z}^d, n, k)$.*

In particular, $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ is not residually finite. By Cayley's theorem, Proposition 2 also implies that $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ contains all finite groups.

Proposition 3. *The group $\mathrm{OB}(\mathbb{Z}^d, n, k)$ is amenable.*

Write $H \wr G$ for the restricted wreath product.

Proposition 4. *If G is a finite group and $n \geq 2$, then $G \wr \mathbb{Z}^d \hookrightarrow \mathrm{OB}(\mathbb{Z}^d, n, k)$.*

The groups $G \wr \mathbb{Z}^d$ are sometimes called generalized lamplighter groups. In fact, $\mathrm{OB}(\mathbb{Z}^d, n, k)$ can in some sense be seen as a generalized generalized lamplighter group, since the subgroup of $\mathrm{OB}(\mathbb{Z}^d, n, k)$ generated by the local permutations $\mathrm{LP}(\mathbb{Z}^d, n, 1)$ with radius 0 and $\mathrm{Shift}(\mathbb{Z}^d, n, 1)$ is isomorphic to $A \cong S_n \wr \mathbb{Z}^d$.

Interestingly, just like the generalized lamplighter groups, we can show that the whole group $\mathrm{OB}(\mathbb{Z}^d, n, k)$ is finitely generated.

Theorem 4. *$\mathrm{OB}(\mathbb{Z}^d, n, k)$ is finitely generated.*

3.2 Finite-state automata

Definition 8. *We define the* reversible finite-state automata $\mathrm{RFA}(\mathbb{Z}^d, n, k)$ *as the group of reversible* (d, n, k)*-Turing machines that do not change the tape. That is, the local rules are of the form* $f(p, q) = (p, q', z)$ *for all entries* $p \in \Sigma^F, q \in Q$.

This group is orthogonal to $\mathrm{OB}(\mathbb{Z}^d, n, k)$ in the following sense:

Proposition 5.

$$\mathrm{RFA}(\mathbb{Z}^d, n, k) \cap \mathrm{LP}(\mathbb{Z}^d, n, k) = \mathrm{SP}(\mathbb{Z}^d, n, k)$$
$$\mathrm{RFA}(\mathbb{Z}^d, n, k) \cap \mathrm{OB}(\mathbb{Z}^d, n, k) = \langle \mathrm{SP}(\mathbb{Z}^d, n, k), \mathrm{Shift}(\mathbb{Z}^d, n, k) \rangle$$

As usual, the case $n = 1$ is not particularly interesting, and we have that $\mathrm{RFA}(\mathbb{Z}^d, 1, k) \cong \mathrm{RTM}(\mathbb{Z}^d, 1, k)$. In the general case the group is more complex.

We now prove that the $\mathrm{RFA}(\mathbb{Z}^d, n, k)$-groups are non-amenable. In [11], a similar idea is used to prove that there exists a minimal $\mathbb{Z}^2$-subshift whose topological full group is not amenable.

Proposition 6. *Let* $n \geq 2$. *For all* $m \in \mathbb{N}$ *we have that:*

$$\underbrace{\mathbb{Z}/2\mathbb{Z} * \cdots * \mathbb{Z}/2\mathbb{Z}}_{m \text{ times}} \hookrightarrow \mathrm{RFA}(\mathbb{Z}^d, n, k)$$

Corollary 3. *For* $n \geq 2$, $\mathrm{RFA}(\mathbb{Z}^d, n, k)$ *and* $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ *contain the free group on two elements. In particular, they are not amenable.*

By standard marker constructions, one can also embed all finite groups and finitely generated abelian groups in $\mathrm{RFA}(\mathbb{Z}^d, n, k)$ – however, this group is residually finite, and thus does not contain S_∞ or $(\mathbb{Q}, +)$.

Proposition 7. *Let* $n \geq 2$ *and* G *be any finite group or a finitely generated abelian group. Then* $G \leq \mathrm{RFA}(\mathbb{Z}^d, n, k)$.

Theorem 5. *Let* $n \geq 2, k \geq 1, d \geq 1$. *Then the group* $\mathrm{RFA}(\mathbb{Z}^d, n, k)$ *is residually finite and is not finitely generated.*

The proof of this theorem is based on studying the action of the group on finite subshifts where heads are occur periodically. Non-finitely generatedness is obtained by looking at signs of permutations of the finitely many orbits, to obtain the *sign homomorphism* to an infinitely generated abelian group.

3.3 Elementary Turing machines and the LEF property of RTM

Definition 9. *We define the group of elementary Turing machines* $\mathrm{EL}(\mathbb{Z}^d, n, k) := \langle \mathrm{RFA}(\mathbb{Z}^d, n, k), \mathrm{LP}(\mathbb{Z}^d, n, k) \rangle$. *That is, the group generated by machines which only change the tape or move the head.*

Proposition 8. *Let* $\mathbb{Q}_p = \frac{1}{p}\mathbb{Z}$. *Then* $\alpha(\mathrm{RFA}(\mathbb{Z}^d, n, k)) = \alpha(\mathrm{EL}(\mathbb{Z}^d, n, k)) = \mathbb{Q}_k^d$. *In particular,* $\mathrm{EL}(\mathbb{Z}^d, n, k) \subsetneq \mathrm{RTM}(\mathbb{Z}^d, n, k)$.

We do not know whether $\alpha(T) \in \mathbb{Z}^d$ implies $T \in \mathrm{EL}(\mathbb{Z}^d, n, 1)$, nor whether $\mathrm{EL}(\mathbb{Z}^d, n, k)$ is finitely generated – the sign homomorphism we use in the proof of finitely-generatedness of the group of finite-state automata does not extend to it.

By the results of this section, the group $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ is neither amenable nor residually finite. By adapting the proof of Theorem 5, one can show that it is locally embeddable in finite groups. See [31,34,32] for the definitions.

Theorem 6. *The group* $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ *is LEF, and thus sofic, for all* n, k, d.

4 Computability aspects

4.1 Basic decidability results

First, we observe that basic management of local rules is decidable. Note that these results hold, and are easy to prove, even in higher dimensions.

Lemma 3. *Given two local rules* $f, g : \Sigma^F \times Q \to \Sigma^F \times Q \times \mathbb{Z}^d$,

- *it is decidable whether* $T_f = T_g$,
- *we can effectively compute a local rule for* $T_f \circ T_g$,
- *it is decidable whether* T_f *is reversible, and*
- *we can effectively compute a local rule for* T_f^{-1} *when* T_f *is reversible.*

A group is called *recursively presented* if one can algorithmically enumerate its elements, and all identities that hold between them. If one can furthermore decide whether a given identity holds in the group (equivalently, whether a given element is equal to the identity element), we say the group has a *decidable word problem*. The above lemma is the algorithmic content of the following proposition:

Proposition 9. *The groups* $\mathrm{TM}(\mathbb{Z}^d, n, k)$ *and* $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ *are recursively presented and have decidable word problems in the standard presentations.*

4.2 The torsion problem

The *torsion problem* of a recursively presented group G is the set of presentations of elements $g \in G$ such that $g^n = 1_G$ for some $n \geq 1$. Torsion elements are recursively enumerable when the group G is recursively presented, but the torsion problem need not be decidable even when G has decidable word problem.

In the case of $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ the torsion problem is undecidable for $n \geq 2$. This result was shown by Kari and Ollinger in [21] using a reduction from the mortality problem which they also prove to be undecidable.

The question becomes quite interesting if we consider the subgroup $\mathrm{RFA}(\mathbb{Z}^d, n, k)$ for $n \geq 2$, as then the decidability of the torsion problem is dimension-sensitive.

Theorem 7. *The torsion problem of* $\mathrm{RFA}(\mathbb{Z}, n, k)$ *is decidable.*

Theorem 8. *For all* $n \geq 2, k \geq 1, d \geq 2$, *there is a finitely generated subgroup of* $\mathrm{RFA}(\mathbb{Z}^d, n, k)$ *whose torsion problem is undecidable.*

5 Acknowledgements

The third author was supported by FONDECYT grant 3150552.

References

1. N. Ollinger A. Gajardo and R. Torres-Avilés. The transitivity problem of Turing machines. 2015.
2. S. Aaronson, D. Grier, and L. Schaeffer. The classification of reversible bit operations. *ArXiv e-prints*, April 2015.
3. N. Aubrun, S. Barbieri, and M. Sablik. A notion of effectiveness for subshifts on finitely generated groups. *ArXiv e-prints*, December 2014.
4. N. Aubrun and M. Sablik. Simulation of effective subshifts by two-dimensional subshifts of finite type. *Acta applicandae mathematicae*, 126(1):35–63, 2013.
5. J. Belk and C. Bleak. Some undecidability results for asynchronous transducers and the Brin-Thompson group 2V. *ArXiv e-prints*, May 2014.
6. James Belk and Francesco Matucci. Conjugacy and dynamics in Thompson's groups. *Geometriae Dedicata*, 169(1):239–261, 2014.
7. T. Boykett, J. Kari, and V. Salo. Strongly universal reversible gate sets. *submitted*, 2016.
8. T. Ceccherini-Silberstein and M. Coornaert. *Cellular Automata and Groups*. Springer Monographs in Mathematics. Springer-Verlag, 2010.
9. E. Czeizler and J. Kari. A tight linear bound on the synchronization delay of bijective automata. *Theoretical Computer Science*, 380(12):23 – 36, 2007. Automata, Languages and Programming.
10. B. Durand, A. Romashchenko, and A. Shen. Effective closed subshifts in 1d can be implemented in 2d. In *Fields of logic and computation*, pages 208–226. Springer, 2010.
11. G. Elek and N. Monod. On the topological full group of a minimal Cantor Zˆ2-system. *ArXiv e-prints*, December 2012.
12. A. Gajardo and P. Guillon. Zigzags in Turing machines. In *Computer Science–Theory and Applications*, pages 109–119. Springer, 2010.
13. A. Gajardo and J. Mazoyer. One head machines from a symbolic approach. *Theoretical Computer Science*, 370(13):34 – 47, 2007.
14. T. Giordano, I. Putnam, and C. Skau. Full groups of Cantor minimal systems. *Israel Journal of Mathematics*, 111(1):285–320, 1999.
15. R. Grigorchuk and K. Medynets. On algebraic properties of topological full groups. *ArXiv e-prints*, May 2011.
16. P. Kůrka J Delvenne and V. Blondel. Decidability and universality in symbolic dynamical systems. *Fund. Inform.*, 74(4):463–490, 2006.
17. E. Jeandel. Computability of the entropy of one-tape Turing machines. *arXiv preprint arXiv:1302.1170*, 2013.
18. K. Juschenko and N. Monod. Cantor systems, piecewise translations and simple amenable groups. *Annals of Mathematics*, 2012.
19. J. Kari. Representation of reversible cellular automata with block permutations. *Theory of Computing Systems*, 29:47–61, 1996. 10.1007/BF01201813.
20. J. Kari. *Developments in Language Theory: 6th International Conference, DLT 2002 Kyoto, Japan, September 18–21, 2002 Revised Papers*, chapter Infinite Snake Tiling Problems, pages 67–77. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

21. J. Kari and N. 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.
22. P. Kůrka. On topological dynamics of Turing machines. *Theor. Comput. Sci.*, 174(1-2):203–216, March 1997.
23. P. Kůrka. Erratum to: Entropy of Turing machines with moving head. *Theor. Comput. Sci.*, 411(31-33):2999–3000, June 2010.
24. D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, 1995.
25. D. Lind M. Boyle and D. Rudolph. The automorphism group of a shift of finite type. *Transactions of the American Mathematical Society*, 306(1):pp. 71–114, 1988.
26. H. Matui. Topological full groups of one-sided shifts of finite type. *ArXiv e-prints*, October 2012.
27. V. Salo and M. Schraudner. in preparation.
28. V. Salo and I. Törmä. Group-walking automata. In Jarkko Kari, editor, *Cellular Automata and Discrete Complex Systems*, volume 9099 of *Lecture Notes in Computer Science*, pages 224–237. Springer Berlin Heidelberg, 2015.
29. V. Salo and I. Törmä. Plane-walking automata. In Teijiro Isokawa, Katsunobu Imai, Nobuyuki Matsui, Ferdinand Peper, and Hiroshi Umeo, editors, *Cellular Automata and Discrete Complex Systems*, volume 8996 of *Lecture Notes in Computer Science*, pages 135–148. Springer International Publishing, 2015.
30. J. Cassaigne V. Blondel and C. Nichitiu. On the presence of periodic configurations in Turing machines and in counter machines. *Theoretical Computer Science*, 289(1):573–590, 2002.
31. A. Vershik and E Gordon. Groups that are locally embeddable in the class of finite groups. *Algebra i Analiz*, 9(1):71–97, 1997.
32. B. Weiss. Sofic groups and dynamical systems. *Sankhyā: The Indian Journal of Statistics, Series A*, pages 350–359, 2000.
33. S. Xu. Reversible logic synthesis with minimal usage of ancilla bits. Master's thesis, MIT, June 2015.
34. M Ziman et al. On finite approximations of groups and algebras. *Illinois Journal of Mathematics*, 46(3):837–839, 2002.

Appendix: Proofs

Proposition 1. *Let n, k be positive integers and $Y = X_{n,0}$. Then:*

$$\mathrm{TM}(\mathbb{Z}^d, n, k) = \{\phi \in \mathrm{End}(X_{n,k}) \mid \phi|_Y = \mathrm{id}, \phi^{-1}(Y) = Y\}$$
$$\mathrm{RTM}(\mathbb{Z}^d, n, k) = \{\phi \in \mathrm{Aut}(X_{n,k}) \mid \phi|_Y = \mathrm{id}\}$$

Proof. Let $T \in \mathrm{TM}(\mathbb{Z}^d, n, k)$. T is clearly shift invariant and continuous, therefore $T \in \mathrm{End}(X_{n,k})$. Also, T acts trivially on $X_{n,0}$ so $T|_Y = \mathrm{id}$ and if the initial configuration has a head, it can only move by a finite amount and not disappear, thus $T^{-1}(Y) \subset Y$. Moreover, if $T \in \mathrm{RTM}(\mathbb{Z}^d, n, k)$, then T has a Turing machine inverse, thus a cellular automaton inverse, and it follows that $T \in \mathrm{Aut}(X_{n,k})$.

Conversely, let $\phi \in \mathrm{End}(X_{n,k})$, so that $\phi(x, y)_{\boldsymbol{v}} = \Phi(\sigma_{-\boldsymbol{v}}((x, y))|_F)$ for some local rule $\Phi : (\Sigma \times \{0, \dots, k\})^F \to \Sigma \times \{0, \dots, k\}$ and F a finite subset of $\mathbb{Z}^d$.

As $\phi|_Y = \mathrm{id}$, when $n \geq 2$ we can deduce that $\mathbf{0} \in F$ and that $\Phi(u, v) = (u_{\mathbf{0}}, v_{\mathbf{0}})$ if $v = 0^F$. Therefore if $(x, y) \in X_{n,k}$, $y_{\boldsymbol{v}} \neq 0$ and we define $W_{\boldsymbol{v}} = \{\boldsymbol{u} \in \mathbb{Z}^d \mid \boldsymbol{v} \in \boldsymbol{u} + F\}$ we get that $\phi(x, y)|_{\mathbb{Z}^d \setminus W_{\boldsymbol{v}}} = (x, y)|_{\mathbb{Z}^d \setminus W_{\boldsymbol{v}}}$. We can thus extend Φ to $\widetilde{\Phi} : (\Sigma \times \{0, \dots, k\})^{W_{\mathbf{0}}+F} \to (\Sigma \times \{0, \dots, k\})^{W_{\mathbf{0}}}$ defined by pointwise application of Φ. We can then define $f_\phi : \Sigma^{W_0+F} \times Q \to \Sigma^{W_0} \times Q \times \mathbb{Z}$ by using $\widetilde{\Phi}$ as follows: We set $f_\phi(p, q) = (p', q', \boldsymbol{u})$ if, after defining $r \in \{0, \dots, k\}^{W_0+F}$ such that $r_{\mathbf{0}} = q$ and 0 elsewhere, we have $\widetilde{\Phi}(p, r) = (p', r')$ and $r' \in \{0, \dots, k\}^{W_0}$ contains the symbol q' in position $\boldsymbol{u}$ (there is always a unique such position $\boldsymbol{u}$ as $\phi^{-1}(Y) \subset Y$).

It can be verified that the Turing machine T_{f_ϕ} is precisely ϕ, therefore $\phi \in \mathrm{TM}(\mathbb{Z}^d, n, k)$. If $\phi \in \mathrm{Aut}(X_{n,k})$ then the $\phi^{-1}(Y) \subset Y$ property is implied by $\phi|_Y = \mathrm{id}$, so such ϕ is also Turing machine. It is easy to see that if ϕ satisfies $\phi|_Y = \mathrm{id}$, then also $\phi^{-1}|_Y = \mathrm{id}$. It follows that the inverse map ϕ^{-1} is also a Turing machine. Thus, $\phi \in \mathrm{RTM}(\mathbb{Z}^d, n, k)$. □

Lemma 1. *Let $T : \Sigma^{\mathbb{Z}^d} \times Q \to \Sigma^{\mathbb{Z}^d} \times Q$ be a function. Then T is a moving tape Turing machine if and only if it is continuous, and for a continuous function $s : \Sigma^{\mathbb{Z}^d} \times Q \to \mathbb{Z}^d$ and $a \in \mathbb{N}$ we have $T(x, q)_1 \sim_a \sigma_{s(x,q)}(x)$ for all $(x, q) \in \Sigma^{\mathbb{Z}^d} \times Q$.*

Proof. It is easy to see that T_f for any local rule $f : \Sigma^F \times Q \to \Sigma^{F'} \times Q \times \mathbb{Z}^d$ is continuous. The projection to the third component of f gives the function s, and one can take the maximal length of a vector in F' as a.

For the converse, since s is a continuous function from a compact space to a discrete one, $s(x, q)$ only depends on a finite set F_0 of coordinates of x and obtains a maximum m. Since T is continuous, $T(x, q)_{[-a-m,a+m]}$ depends only on a finitely set of coordinates F_1 of x. It is then easy to extract a local rule

$$f : \Sigma^{F_0 \cup F_1} \times Q \to \Sigma^{[-a,a]^d} \times Q \times \mathbb{Z}^d,$$

for T. □

Lemma 2. *If $n \geq 2$ then:*

$$\mathrm{TM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k) \cong \mathrm{TM}(\mathbb{Z}^d, n, k)$$
$$\mathrm{RTM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k) \cong \mathrm{RTM}(\mathbb{Z}^d, n, k).$$

Proof. Consider again the epimorphism Ψ and let $X \subset \{0, 1\}^{\mathbb{Z}^d}$ be any strongly aperiodic subshift (that is, for each configuration $x \in X$, $stab_\sigma(x) = \{0\}$). Then if $x \in X$, $x \not\sim \sigma_{\boldsymbol{v}}(x)$ for any $\boldsymbol{v} \in \mathbb{Z}^d \setminus \{\mathbf{0}\}$, otherwise the compactness of X would allow us to construct a periodic point by shifting the finite set of differences to infinity. Let $\widetilde{x} \in X$ and consider $T \neq T'$ in $\mathrm{TM}(\mathbb{Z}^d, n, k)$ and a pair (x, y) such that $T(x, y) \neq T'(x, y)$. As elements of $\mathrm{TM}(\mathbb{Z}^d, n, k)$ act locally around the head, we can modify x outside a finite region such that it is asymptotically equivalent to $\widetilde{x}$ and call this modified version x'. We choose the finite region large enough to ensure $T(x', y) \neq T'(x', y)$. Obviously $x' \not\sim \sigma_{\boldsymbol{v}}(x')$ for non-zero $\boldsymbol{v}$ and thus if the non-zero symbol carried by y is q then $\Psi(T)(x', q) \neq \Psi(T')(x', q)$. □

Theorem 1. *Let $T \in \mathrm{TM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k)$. Then the following are equivalent:*

1. *T is injective.*
2. *T is surjective.*
3. *$T \in \mathrm{RTM}_{\mathrm{fix}}(\mathbb{Z}^d, n, k)$.*
4. *T preserves the uniform measure ($\mu(T^{-1}(A)) = \mu(A)$ for all Borel sets A).*
5. *$\mu(T(A)) = \mu(A)$ for all Borel sets A.*

Proof. Let T be arbitrary, and let $F = F' = [-r, r]^d$ and $\epsilon = \frac{1}{k(2r+1)^d}$, where r is the radius of T. Consider the cylinders $C_i = [p_i] \times \{q\}$ where $p_i \in \Sigma^F, q \in Q$. These cylinders form a clopen partition of $\Sigma^{\mathbb{Z}^d} \times Q$ into $k(2r+1)^d$ cylinders of measure ϵ.

Now, because r is the radius of T, T is a homeomorphism from C_i onto $D_i = T(C_i)$, and D_i is a cylinder set of the form $[p'] \times \{q'\}$ for some $p' \in \Sigma^{\boldsymbol{v}+F}$, $q \in Q$, which must be of the same measure as C_i as the domain $\boldsymbol{v} + F$ of p' has as many coordinates as the domain F of p. Note that D_i is not necessarily a cylinder centered at the origin, and the offset $\boldsymbol{v}$ is given by the shift-indicator. Now, observe that injectivity is equivalent to the cylinders $D_i = T(C_i)$ being disjoint. Namely, they must be disjoint if T is injective, and if they are disjoint then T is injective because $T|_{C_i} : C_i \to D_i$ is a homeomorphism. Surjectivity on the other hand is equal to $\Sigma^{\mathbb{Z}^d} \times Q = \bigcup_i D_i$, since $\bigcup_i D_i = \bigcup_i T(C_i) = T(\Sigma^{\mathbb{Z}^d} \times Q)$.

Now, it is easy to show that injectivity and surjectivity are equivalent: If T is injective, then the D_i are disjoint, and $\mu(\bigcup_i D_i) = \sum_i \mu(D_i) = 1$, so we must have $\bigcup_i D_i = \Sigma^{\mathbb{Z}^d} \times Q$ because $\Sigma^{\mathbb{Z}^d} \times Q$ is the only clopen set of full measure. If T is not injective, then for some $i \neq j$ we have $D_i \cap D_j \neq \emptyset$. Then $D = D_i \cap D_j$ is a nonempty clopen set, and thus has positive measure. It follows that $\mu(\bigcup_i D_i) \leq \sum_i \mu(D_i) - \mu(D) < 1$, so $\bigcup_i D_i \subsetneq \Sigma^{\mathbb{Z}^d} \times Q$. Of course, since injectivity and surjectivity are equivalent, they are both equivalent to bijectivity, and thus reversibility (by compactness).

The proof shows that reversibility is equivalent to preserving the uniform Bernoulli measure in the forward sense – if T is reversible, then $\mu(T_f(A)) = \mu(A)$ for all clopen sets A, and thus for all Borel sets, while if T is not reversible, then there is a disjoint union of cylinders $C \cup D$ such that $\mu(T(C \cup D)) < \mu(C \cup D)$.

For measure-preservation in the usual (backward) sense, observe that the reverse of a reversible Turing machine is reversible and thus measure-preserving in the forward sense, so a reversible Turing machine must itself be measure-preserving in the traditional sense. If T is not reversible, then $\mu(T(C \cup D)) < \mu(C \cup D)$ for some disjoint cylinders C and D large enough that $T|_C$ and $T|_D$ are measure-preserving homeomorphisms. Then for $E = T(C) \cap T(D)$ we have $\mu(T^{-1}(E)) \geq \mu((T^{-1}(E) \cap C) \cup (T^{-1}(E) \cap D)) = 2\mu(E)$. □

Theorem 2. *A classical Turing machine T is reversible if and only if it is of the form $T_1 \circ T_0$ where T_0 is a state-symbol permutation and T_1 is a state-dependent shift.*

Proof. We only need to show that if T is reversible then it is of the stated form. Let $f_T : \Sigma \times Q \to \Sigma \times Q \times \{-1, 0, 1\}$ be a local rule for T in the moving tape

model. We claim that if $f_T(a,q) = (b,r,d)$ and $f_T(a',q') = (b',r,d')$ then $d = d'$. Namely, otherwise one can easily find two configurations with the same image. There are multiple cases to consider, but we only show $d = 0$ and $d' = 1$. In this case

$$T((xb'a.y,q)) = (xb'b.y,r) = T((xa'.by),q').$$

We have shown that the direction of movement is entirely determined by the state we enter. Of course, for T to be injective, also f_T must be injective, so the map $g : \Sigma \times Q \to \Sigma \times Q$ defined by $g(a,q) = (b,r)$ if $f_T(a,q) = (b,r,d)$ is injective, thus a bijection. Now, T_0 is defined as the permutation g, and T_1 as the finite-state automaton with local rule $f_{T_1}(a,q) = (a,q,d)$ if $f_T(b,q') = (b',q,d)$ for some $(b,q) \in \Sigma \times Q$. □

Theorem 3. *For $n \geq 2$, the group $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ is not finitely generated.*

Proof. Consider the $(1,n,k)$-Turing machine $T_{\mathtt{SURF},m}$ given by the local function $f : \Sigma^{\{0,\dots,m\}} \times Q \to \Sigma^{\{0,\dots,m\}} \times Q \times \mathbb{Z}$ given by the following: For $a \in \Sigma$ then $f(0^m a, q) = (a0^m, q, 1)$. Otherwise $f(u,q) = (u,q,0)$. This machine is reversible, and satisfies that $\alpha(T_{\mathtt{SURF},m}) = 1/n^m$. This machine can easily be extended to a (d,n,k)-Turing machine with average movement $(1/n^m, 0, \dots, 0)$. Suppose $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ is generated by a finite set S. Then $\alpha(\mathrm{RTM}(\mathbb{Z}^d, n, k)) = \langle \alpha(S) \rangle$ which is a subgroup of $\mathbb{Q}^d$ of elements which have their denominator bounded by the lowest common multiple of the denominators of $\alpha(T)$ for $T \in S$. As $n \geq 2$ there is $m \in \mathbb{N}$ such that $\alpha(T_{\mathtt{SURF},m}) \notin \alpha(\mathrm{RTM}(\mathbb{Z}^d, n, k))$, thus $T_{\mathtt{SURF},m} \notin \mathrm{RTM}(\mathbb{Z}^d, n, k)$, which yields a contradiction. □

Proposition 2. *Let S_∞ be the group of permutations of $\mathbb{N}$ of finite support. Then for $n \geq 2$, $S_\infty \hookrightarrow \mathrm{LP}(\mathbb{Z}^d, n, k)$.*

Proof. It suffices to show the result for $d = 1$. Let $\sigma \in S_\infty$ with support $F \subset N$ and let T_σ be given by the local function $f_\sigma : \Sigma^F \times Q \to \Sigma^F \times Q \times \mathbb{Z}$ defined by $f_\sigma(p,q) = (p',q,0)$ where $p'_m = p_{\sigma(m)}$. By definition it's clear that $T_{\sigma_1} \circ T_{\sigma_2} = T_{\sigma_1 \circ \sigma_2}$. Moreover the homomorphism is injective: If $\sigma_1 \neq \sigma_2$ then there exists $m \in \mathbb{N}$ such that $\sigma_1(m) \neq \sigma_2(m)$. As $n \geq 2$, we can consider the configuration $(x,y) \in X_{n,k}$ such that $x_m = y_0 = 1$ and $x_{\mathbb{Z}\setminus\{m\}}$ and $y_{\mathbb{Z}\setminus\{0\}}$ contain only zeroes. Then $T_{\sigma_1}(x,y) \neq T_{\sigma_2}(x,y)$. □

Proposition 3. *The group $\mathrm{OB}(\mathbb{Z}^d, n, k)$ is amenable.*

Proof. Clearly, the image of an element of $\mathrm{OB}(\mathbb{Z}^d, n, k)$ in the average movement homomorphism α simply records the powers of the generators T_{e_i} in the representation of the element. The image $\mathbb{Z}^d$ of this homomorphism is abelian, and thus amenable. The kernel is $\mathrm{Ker}(\alpha) \cap \mathrm{OB}(\mathbb{Z}^d, n, k) = \mathrm{LP}(\mathbb{Z}^d, n, k)$ which is locally finite, thus amenable. Thus, $\mathrm{OB}(\mathbb{Z}^d, n, k)$ is the extension of an amenable group by an amenable group, thus amenable. □

Proposition 4. *If G is a finite group and $n \geq 2$, then $G \wr \mathbb{Z}^d \hookrightarrow \mathrm{OB}(\mathbb{Z}^d, n, k)$.*

Proof. Let $|G| = m$. Let $T_z \in \mathrm{OB}(\mathbb{Z}^d, 2, 1)$ be the machine which always moves the head by z and for $s \in S_m$ let T_s the immersion into $\mathbb{Z}^d$ of the machine defined in Proposition 2. By Cayley's theorem G is isomorphic to a subgroup of S_m generated by some elements $s_1, \dots, s_\ell$. Let $e_1, \dots, e_d$ be the generators of $\mathbb{Z}^d$. Then $G \wr \mathbb{Z}^d$ is isomorphic to $\langle T_{s_1}, \dots, T_{s_\ell}, T_{me_1}, \dots, T_{me_d} \rangle$. Indeed, $\langle T_{me_1}, \dots, T_{me_d} \rangle \cong m\mathbb{Z}^d$ and the action of the first ℓ machines only acts on the coset $\mathbb{Z}^d/m\mathbb{Z}^d$ and is isomorphic to G. □

The proof of Theorem 4 is Appendix B.

Proposition 5.

$$\mathrm{RFA}(\mathbb{Z}^d, n, k) \cap \mathrm{LP}(\mathbb{Z}^d, n, k) = \mathrm{SP}(\mathbb{Z}^d, n, k)$$
$$\mathrm{RFA}(\mathbb{Z}^d, n, k) \cap \mathrm{OB}(\mathbb{Z}^d, n, k) = \langle \mathrm{SP}(\mathbb{Z}^d, n, k), \mathrm{Shift}(\mathbb{Z}^d, n, k) \rangle$$

Proof. The inclusions $\mathrm{SP}(\mathbb{Z}^d, n, k) \subset \mathrm{RFA}(\mathbb{Z}^d, n, k) \cap \mathrm{LP}(\mathbb{Z}^d, n, k)$ and

$$\langle \mathrm{SP}(\mathbb{Z}^d, n, k), \mathrm{Shift}(\mathbb{Z}^d, n, k) \rangle \subset \mathrm{RFA}(\mathbb{Z}^d, n, k) \cap \mathrm{OB}(\mathbb{Z}^d, n, k)$$

follow directly from the definitions. For the converse inclusions, observe that an element of $\mathrm{RFA}(\mathbb{Z}^d, n, k) \cap \mathrm{LP}(\mathbb{Z}^d, n, k)$ cannot modify the tape or move the head, so it can only perform a permutation of the state as a function of the tape. In $\mathrm{RFA}(\mathbb{Z}^d, n, k) \cap \mathrm{OB}(\mathbb{Z}^d, n, k)$, precisely the unconditional shifts have been added.

Proposition 6. *Let $n \geq 2$. For all $m \in \mathbb{N}$ we have that:*

$$\underbrace{\mathbb{Z}/2\mathbb{Z} * \cdots * \mathbb{Z}/2\mathbb{Z}}_{m \text{ times}} \hookrightarrow \mathrm{RFA}(\mathbb{Z}^d, n, k)$$

Proof. We show this result only for $\mathrm{RFA}(\mathbb{Z}, n, k)$ where $n = m$. For $a \in \Sigma$ define $T_a \in \mathrm{RFA}(\mathbb{Z}, m, k)$ with radius 1 by the following rules:

1. if $x_0 = a$ and $x_1 \neq a$ move the head to the right.
2. if $x_{-1} = a$ and $x_0 \neq a$ move the head to the left.
3. Otherwise stay in place.

The machine T_a does not change the tape, so it belongs to $\mathrm{RFA}(\mathbb{Z}, m, k)$. It is clearly reversible as $T_a^2 = \mathrm{id}$. We claim that $\langle T_1, \dots, T_m \rangle$ is isomorphic to the free product of m copies of $\mathbb{Z}/2\mathbb{Z}$. Indeed, every element in $\mathbb{Z}/2\mathbb{Z} * \cdots * \mathbb{Z}/2\mathbb{Z}$ can be represented as a word in $\{a_1, \dots, a_m\}$ where no factor $a_i a_i$ appears. Given a word $w = w_1 \dots w_t$ in that form we can construct a configuration $x(w)$ such that $x(w)_{j-1} = i$ if $w_j = a_i$ for $j \in \{1, \dots, t\}$, $x(w)_t \neq x(w)_{t-1}$ and $x(w)_j = 1$ otherwise. The machine $T_{w_t} \circ \cdots \circ T_{w_1}$ acts on $x(w)$ by moving the head t steps to the right. Therefore it is not the identity. □

Theorem 5. *Let $n \geq 2, k \geq 1, d \geq 1$. Then the group $\mathrm{RFA}(\mathbb{Z}^d, n, k)$ is residually finite and is not finitely generated.*

Proof. Let $Y_m \subset (\Sigma \times (Q \cup \{0\}))^{\mathbb{Z}^d}$ be the finite set of points y such that

- $\sigma_{m\boldsymbol{v}}(y) = y$ for unit vectors $\boldsymbol{v} \in \mathbb{Z}^d$, and
- for some $\boldsymbol{u} \in \mathbb{Z}^d$, $(y_{\boldsymbol{v}})_2 \neq 0 \iff \boldsymbol{v} \in \boldsymbol{u} + m\mathbb{Z}^d$.

In other words, configurations of Y_m have period m in every direction, and have Turing machine heads on a sublattice of the same periods.

Now, to each $T \in \mathrm{RFA}(\mathbb{Z}^d, n, k)$ we associate the map $\phi(T) : Y_m \to Y_m$ that applies the local rule of the Turing machine at each head position, ignoring the other heads. Since T is injective and never modifies the tape, also the map $\phi(T)$ is injective, and thus $\phi : \mathrm{RFA}(\mathbb{Z}^d, n, k) \to \mathrm{Sym}(Y_m)$ is a homomorphism to the permutation group $\mathrm{Sym}(Y_m)$ of Y_m.

To show the group is not finitely generated, consider the signs of the permutations $\phi(T)$ performs on Y_m for different m. It is easy to show that for any vector of signs $s_1, s_2, s_3, \ldots \in \{-1, 1\}^{\mathbb{N}}$ where $s_i = 1$ for all large enough i, we can construct a finite-state automaton T such that for all m, $\phi(T)$ performs a permutation with sign s_m on Y_m. This means that $\mathrm{RFA}(\mathbb{Z}^d, n, k)$ has as a homomorphism image the non-finitely generated group $(\mathbb{Z}/2\mathbb{Z})^\infty$, so $\mathrm{RFA}(\mathbb{Z}^d, n, k)$ itself cannot be finitely generated. □

Proposition 8. *Let* $\mathbb{Q}_p = \frac{1}{p}\mathbb{Z}$. *Then* $\alpha(\mathrm{RFA}(\mathbb{Z}^d, n, k)) = \alpha(\mathrm{EL}(\mathbb{Z}^d, n, k)) = \mathbb{Q}_k^d$. *In particular,* $\mathrm{EL}(\mathbb{Z}^d, n, k) \subsetneq \mathrm{RTM}(\mathbb{Z}^d, n, k)$.

Proof. The machine T_j that increments the state by 1 on each step (modulo the number of states) and walks one step along the jth axis whenever it enters the state 1, has $\alpha(T_j) = (0, \ldots, 0, 1/k, 0, \ldots, 0)$. We obtain

$$\langle \alpha(T_j) \mid j \leq d \rangle = \mathbb{Q}_k^d$$

Next, let us show that for every finite-state machine T, we have $\alpha(T) \in \mathbb{Q}_k^d$. For this, consider the behavior of T on the all-zero configuration. Given a fixed state q, T moves by an integer vector $\boldsymbol{v}_q$, thus contributing $\frac{1}{k}\boldsymbol{v}_q$ to the average movement. Let $\boldsymbol{v} = \sum_{q \in Q} \frac{1}{k}\boldsymbol{v}_q$ be the average movement of T on the all-zero configuration.

We claim that $\alpha(T) = \boldsymbol{v}$. Note that by composing T with a suitable combination of the machines T_j and their inverses, it is enough to prove this in the case $\boldsymbol{v} = \boldsymbol{0}$. Now, for a large m, Let $p \in \Sigma^{[-m,m]^d}$ be a pattern, $\boldsymbol{u} \in [-m, m]^d$ a position and $q \in Q$ a state. Complete p to a configuration $x_p \in \Sigma^{\mathbb{Z}^d}$ by writing 0 in every cell outside $[-m, m]^d$. Write $\alpha_m(T)$ for the average movement of T for the finitely many choices of p, u, q. Formally, if s_T is the shift indicator of T:

$$\alpha_m(T) = \frac{1}{k(2m+1)^d n^{(2m+1)^d}} \sum_{p,u,q} s_T(\sigma_{-\boldsymbol{u}}(x_p), q).$$

As $m \to \infty$, it is easy to show that $\alpha_m(T) \to \alpha(T)$, as the movement vector of T is distributed correctly in all positions except at the border of the hypercube which grows slower than the interior.

On the other hand, it is easy to show that for any fixed $[-m,m]^d$-pattern p, then the average movement of T on x_p started from a random state and a random position is precisely $\mathbf{0}$, that is, $\sum_{u,q} s_T(\sigma_{-\boldsymbol{u}}(x_p), q) = \mathbf{0}$. This follows from the fact that $T \in \mathrm{RFA}(\mathbb{Z}^d, n, k)$ and thus the action is simply a permutation of the set of position-state pairs and the fact that $\boldsymbol{v} = \mathbf{0}$. From here we conclude that the sum restricted to $u \in [-m,m]^d$ is $o(m^d)$. It follows that $\alpha(T) = \lim \alpha_m(T) = \mathbf{0}$. □

Theorem 6. *The group* $\mathrm{RTM}(\mathbb{Z}^d, n, k)$ *is LEF, and thus sofic, for all* n, k, d.

Proof. The proof we give is essentially the same proof as that of residual finiteness of $\mathrm{RFA}(\mathbb{Z}^d, n, k)$, with the difference that we only obtain a 'local' homomorphism with that construction.

Let $M \subset \mathrm{RTM}(\mathbb{Z}^d, n, k)$ be a finite set of Turing machines all of which have radius at most r. Let Y_{8r} be as in the proof of the previous theorem.

Now, to each $T \in M^2$ we associate the map $\phi(T) : Y_{8r} \to Y_{8r}$ that applies the local rule of the Turing machine at each head position. The radius of every Turing machine in M^2 is at most $2r$, so it is easy to see that since T is injective, also $\phi(T)$ is, and thus $\phi : M^2 \to \mathrm{Sym}(Y_{8r})$ is a function from M^2 to the permutation group of Y_{8r}. As the heads do not interact in the first two steps, we have $\phi(T \circ T') = \phi(T) \circ \phi(T')$ for all $T, T' \in M$. □

Lemma 3. *Given two local rules* $f, g : \Sigma^F \times Q \to \Sigma^F \times Q \times \mathbb{Z}^d$,

- *it is decidable whether* $T_f = T_g$,
- *we can effectively compute a local rule for* $T_f \circ T_g$,
- *it is decidable whether* T_f *is reversible, and*
- *we can effectively compute a local rule for* T_f^{-1} *when* T_f *is reversible.*

Proof. For the first claim, simply minimize each rule: iteratively replace F by $F' = F \setminus \{a\}$ as long as f does not depend on the coordinate a in the sense that $f(p,q)_a = p_a$ for all $(p,q) \in \Sigma^F \times Q$. This minimization process ends after at most $|F|$ steps and if $T_f = T_g$ the same local rule is reached from both f and g, while this of course does not happen if $T_f \neq T_g$.

Finding a local rule for the composition of two Turing machines is a simple exercise.

For the decidability of reversibility, we give a semialgorithm for both directions. First, if T_f is reversible, then it has a reverse T_g. We thus only need to enumerate local rules g, and check whether $T_f \circ T_g = \mathrm{id}$, which is decidable by the previous lemmas.

If T_f is not reversible, then $T_f(x,y) = T_f(x',y')$ for some $(x,y),(x',y') \in \Sigma^{\mathbb{Z}^d} \times X_k$ with $y_{\mathbf{0}} \neq 0$. If r is the move-radius of f, then necessarily the nonzero position of y' is at distance at most r from the origin each other and $x_{\boldsymbol{v}} = x'_{\boldsymbol{v}}$ for $|\boldsymbol{v}|$ larger than the radius of T_f. Then we can assume $x_{\boldsymbol{v}} = x'_{\boldsymbol{v}} = 0$ for all such $\boldsymbol{v}$. It follows that if T_f is not injective, it is not injective on the finite set of configurations $(x,y) \in \Sigma^{\mathbb{Z}^d} \times X_k$ where $(x,y)_{\boldsymbol{v}} = 0$ for all $|\boldsymbol{v}|$ larger than the radius of T_f, which we can check algorithmically.

Of course, if T is reversible, we find a reverse for it by enumerating all Turing machines and outputting the first T' such that $T \circ T' = T' \circ T = \mathrm{id}$, which we can check by the decidability of equality of Turing machines. □

Theorem 7. *The torsion problem of* $\mathrm{RFA}(\mathbb{Z}, n, k)$ *is decidable.*

Proof. A semialgorithm for recognizing torsion elements exists in all dimensions, since the word problem is decidable: Given $T \in \mathrm{RFA}(\mathbb{Z}, n, k)$, for $n = 1, 2, 3, \ldots$, check whether $T^n = \mathrm{id}$. If this happens for some n, T is a torsion element.

For the other direction we give a proof with a dynamical flavor. We need to show that there is a spatially periodic point where, from some initial state, the head of T performs an infinite periodic walk either left or right. A semialgorithm can then enumerate periodic points and initial states, and once it finds a point where the head moves to infinity, it has proved that T is not a torsion element. First, observe that by compactness, there must be a point and an initial state where the head walks arbitrarily far from its initial position. We may suppose that T can walk arbitrarily far to the right.

Now, consider a walk of the head of T from position 0 to some position $j >> 0$, given by some configuration (x, y). Because T has finite move-radius, there must be a syndetic set of positions $h \in [0, j]$ that T visits on the way to j, such that there is a maximal ℓ_h such that $(T^{\ell_h}(x, y)_2)_h \neq 0$, and $(T^{\ell}(x, y)_2)_i = 0$ for all $\ell > \ell_h$, $i \leq h$. By the pigeonhole principle,

$$(T^{\ell_h}(x, y)_2)_{h+[-r,r]} = (T^{\ell_{h'}}(x, y)_2)_{h'+[-r,r]}$$

for some $h < h'$, and then $(x_{[h-r,h'-r-1]})^{\mathbb{Z}}$ is a spatially periodic point where, started from the inital state $(T^{\ell_h}(x, y)_2)_h$, the head of T performs a periodic walk to infinity. □

Theorem 8. *For all* $n \geq 2, k \geq 1, d \geq 2$*, there is a finitely generated subgroup of* $\mathrm{RFA}(\mathbb{Z}^d, n, k)$ *whose torsion problem is undecidable.*

Proof. We assume $d = 2$ – in the general case, we simply walk on a 2-dimensional plane of the configuration.

First, let us explain why, for a suitable alphabet Σ and the local rule of an element $f \in \mathrm{RFA}(\mathbb{Z}^2, |\Sigma|, 2)$, it is undecidable whether f is a torsion element in that group. We then prove that the alphabet can be fixed, then that we can restrict to a finitely generated subgroup as long as we have 4 states, and finally we get rid of states altogether.

In [20], it is shown that, given a set of Wang tiles T and a function $d : T \to D$ where $D = \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$, the *snake tiling problem* is undecidable, that is, it is undecidable whether it is possible to find a partial tiling $\tau : \mathbb{Z}^2 \to \{\epsilon\} \cup T$, and a path $p : \mathbb{Z} \to \mathbb{Z}^2$ such that $\tau(p(n)) \in T$ and $p(n + 1) - p(n) = d(\tau(p(n)))$ for all n and all tiles match their non-ϵ neighbors.

Let $\Sigma = T$. We use the state – the *direction bit* – to denote a direction for our element $f \in \mathrm{RFA}(\mathbb{Z}^2, |T|, 2)$. As long as f is on a tile that matches all its four neighbors, it walks along the vectors given by d (or their negations, depending on the direction bit). If the neighbors do not match, the direction bit of f is flipped.

Now, if it is possible to tile an infinite snake, then there is a configuration where f walks to infinity. If it is impossible, then there is a bound on how far f can walk from its starting position before turning back, and f has finite order. This concludes the proof of undecidability when the alphabet can be chosen freely.

To get a fixed alphabet, encode the tiles into binary squares of size $n \times n$. By having the top left corner contain $\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}$ and having no two adjacent 1s elsewhere, we ensure that there is a unique way to 'parse' a given tiling into encodings of squares. Of course, our machine will simply flip its direction bit when it does not locally see a valid coding of a tile.

Next, we want to do the same construction with a finitely generated subgroup. For this, we add a second *auxiliary bit*, or *aux bit* to the state. We also change the alphabet to one allowing us to draw paths on configurations: every tile has zero, one or two incoming arrows from the cardinal directions D, and an outgoing path for each incoming one. This alphabet B can be used to encode tiles into $(n \times n)$-squares as well. We assume that the encoded tiles are connected by a path to their neighbors according to the d-function, so that by following the path for n steps from the central cell of the encoding of a Wang tile, we reach the central cell of the next Wang tile.

In our finite set of generators we take

1. $T_{\texttt{walk}}$ that walks along the path depending on the direction bit,
2. $T_{\boldsymbol{v}}$ that walk in the direction $\boldsymbol{v} \in D$ independently of the configuration,
3. g_s that flips the direction bit if the current cell is $s \in \Sigma$,
4. h_s that flips the aux bit if the current cell is s,
5. $g_{+,s}$ that adds the aux bit to the direction bit if the current cell is s, and
6. $h_{+,s}$ that adds the direction bit to the aux bit if the current cell is s,

Let F be this set of machines.

More generally, for a pattern p write g_p and h_p for the machines that flip the direction bit or the auxiliary bit if they see the pattern p. Observe first that it is enough to construct all such g_p and h_p out of the machines in F. Namely, Let $\mathcal{P}$ be the set of all the $3n \times 3n$ patterns p that are not a legal coding of matching Wang tiles, and apply g_p for all of them to get a machine $g = \prod_{p \in \mathcal{P}} g_p$. Then $T^n_{\texttt{walk}} \circ g$ is a torsion element if and only if the Wang tile set allows no infinite snakes.

To build g_p and h_p, we proceed by induction. Suppose $D(p) = D(p') \cup \{\boldsymbol{v}\}$, $p|_{D(p')} = p'$, $p_{\boldsymbol{v}} = s$ and $g_{p'}$ and $h_{p'}$ can be built from F. Then

$$g_p = (T_{-\boldsymbol{v}} \circ g_{+,s} \circ T_{\boldsymbol{v}} \circ h_{p'})^2, \text{ and } h_p = (T_{-\boldsymbol{v}} \circ h_{+,s} \circ T_{\boldsymbol{v}} \circ g_{p'})^2.$$

Finally, let us get rid of the state. For this, add the symbol 0 to the alphabet B. The head now only moves if it is on a square of the form $\begin{smallmatrix} b & 0 \\ 0 & 0 \end{smallmatrix}$ for $b \in B$ which is surrounded by squares of the same form. It uses the four positions modulo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in this square to denote its state. If the 2×2 period where zeroes and nonzeroes occur breaks, the direction bit is reversed (that is, the head moves to another position modulo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). It is easy to modify the generators F

to obtain such behavior. Again, we obtain that that solving the torsion in the group generated by these finite-state machines requires solving the snake tiling problem for all sets of directed Wang tiles, and is thus undecidable. □

Appendix B: OB is finitely generated

Next we prove that $\mathrm{OB}(\mathbb{Z}^d, n, k)$ is finitely generated. This is based on the existence of strongly universal reversible gates for permutations of A^m, recently proved for the binary alphabet $A = \{0, 1\}$ in [2,33], and generalized to other alphabets in [7]. We need a finite generating set for permutations of $Q \times \Sigma^m$, and hence the proof in [7] has to be adjusted to account for non-homogeneous alphabet sizes (that is, due to possibly having $n \neq k$).

The case $n = 1$ is trivial: Group $\mathrm{LP}(\mathbb{Z}^d, 1, k)$ is finite and $\mathrm{Shift}(\mathbb{Z}^d, 1, k)$ is generated by the single step moves. We hence assume that $n > 1$.

The following lemma was proved in [7] (Lemmas 3 and 5):

Lemma 4. *Let $H = (V, E)$ be a connected undirected graph.*

(a) The transpositions $(s\ t)$ for $\{s, t\} \in E$ generate $\mathrm{Sym}(V)$, the set of permutations of the vertex set.
(b) Let $\Delta \subseteq \mathrm{Sym}(V)$ be a set of permutations of V that contains for each edge $\{s, t\} \in E$ a 3-cycle $(x\ y\ z)$ where $\{s, t\} \subset \{x, y, z\}$. Then Δ generates $\mathrm{Alt}(V)$, the set of even permutations of the vertex set.

Let $m \geq 1$, and consider permutations of $Q \times \Sigma^m$. *Controlled swaps* are transpositions $(s\ t)$ where $s, t \in Q \times \Sigma^m$ have Hamming distance one. *Controlled 3-cycles* are permutations $(s\ t\ u)$ where the Hamming distances between the three pairs are 1, 1 and 2, that is, the vectors s, t and u are of the forms $uavcw$, $uavdw$ and $ubvdw$, where a, b, c and d are single letters. Let us denote by $C_m^{(2)}$ and $C_m^{(3)}$ the sets of controlled swaps and 3-cycles, respectively, in $\mathrm{Sym}(Q \times \Sigma^m)$. Let $H = (V, E)$ be the graph with vertices $V = Q \times \Sigma^m$ and edges $\{s, t\}$ that connect elements s and t having Hamming distance one. This graph is clearly connected, so we get from Lemma 4(b) that the controlled 3-cycles generate all its even permutations:

Lemma 5. *Let $n > 1$ and $m \geq 1$. The group $\mathrm{Alt}(Q \times \Sigma^m)$ is generated by $C_m^{(3)}$.*

Let $\ell \leq m$, and let f be a permutation of $Q \times \Sigma^\ell$. We can apply f on $1 + \ell$ coordinates of $Q \times \Sigma^m$, while leaving the other $m - \ell$ coordinates untouched. More precisely, the *prefix application* $\hat{f}$ of f on $Q \times \Sigma^m$, defined by

$$\hat{f} : (q, s_1, \ldots, s_\ell, \ldots, s_m) \mapsto (f(q, s_1, \ldots, s_\ell)_1, \ldots, f(q, s_1, \ldots, s_\ell)_\ell, s_{\ell+1}, \ldots, s_m),$$

applies f on the first $1 + \ell$ coordinates. To apply it on other choices of coordinates we conjugate $\hat{f}$ using rewirings of symbols. For any permutation $\pi \in \mathrm{Sym}(\{1, \ldots, m\})$ we define the *rewiring* permutation of $Q \times \Sigma^m$ by

$$r_\pi : (q, s_1, \ldots, s_m) \mapsto (q, s_{\pi(1)}, \ldots, s_{\pi(m)}).$$

It permutes the positions of the m tape symbols according to π. Now we can conjugate the prefix application $\hat{f}$ using a rewiring to get $\hat{f}_\pi = r_\pi^{-1} \circ \hat{f} \circ r_\pi$, an *application* of f in selected coordinates. Let us denote by

$$[f]_m = \{\hat{f}_\pi \mid \pi \in \mathrm{Sym}(m)\}$$

the set of permutations of $Q \times \Sigma^m$ that are applications of f. For a set P of permutations we denote by $[P]_m$ the union of $[f]_m$ over all $f \in P$.

Note that if n is even and $f \in \mathrm{Sym}(Q \times \Sigma^\ell)$ for $\ell < m$ then $[f]_m$ only contains even permutations. The reason is that the coordinates not participating in the application of f carry a symbol of the even alphabet Σ. The application $[f]_m$ then consists of an even number of disjoint permutations of equal parity – hence the result is even. In contrast, for the analogous reason, if n is odd then $[f]_m$ only contains odd permutations whenever f is itself is an odd permutation.

Lemma 6. *Let $m \geq 6$, and let $G_m = \langle [C_4^{(2)}]_m \rangle$ be the group generated by the applications of controlled swaps of $Q \times \Sigma^4$ on $Q \times \Sigma^m$. If $n = |\Sigma|$ is odd then $G_m = \mathrm{Sym}(Q \times \Sigma^m)$. If n is even then $G_m = \mathrm{Alt}(Q \times \Sigma^m)$.*

Proof. For even n, by the note above, $[C_4^{(2)}]_m \subseteq \mathrm{Alt}(Q \times \Sigma^m)$, and for odd n there are odd permutations in $[C_4^{(2)}]_m$. So in both cases it is enough to show $\mathrm{Alt}(Q \times \Sigma^m) \subseteq G_m$. We also note that, obviously, $[G_{m-1}]_m \subseteq G_m$.

Based on the decomposition in Figure 1, we first conclude that any controlled 3-cycle f of $Q \times \Sigma^m$ is a composition of four applications of controlled swaps of $Q \times \Sigma^{m-2}$. In the figure, the components of $Q \times \Sigma^m$ have been ordered in parallel horizontal wires, the Q-component being among the topmost three wires. Referring to the symbols in the illustration, the gate on the left is a generic 3-cycle (*pszabcdw ptzabcdw qszabcdw*) where one of the first three wires is the Q-component, $a, b, c, d \in \Sigma$ and $w \in \Sigma^{m-6}$. The proposed decomposition consists of two different controlled swaps p_1 and p_2 applied twice in the order $f = p_1 p_2 p_1 p_2$. Because p_1 and p_2 are involutions, the decomposition amounts to identity unless the input is of the form *xyzabcdw* where $x \in \{p, q\}$ and $y \in \{s, t\}$. When the input is of this form, it is easy to very that the circuit on the right indeed amounts to the required 3-cycle. We conclude that $C_m^{(3)} \subseteq \langle [C_{m-2}^{(2)}]_m \rangle$, for all $m \geq 6$. By Lemma 5,

$$\mathrm{Alt}(Q \times \Sigma^m) = \langle C_m^{(3)} \rangle \subseteq \langle [C_{m-2}^{(2)}]_m \rangle. \tag{1}$$

We proceed by induction on m. The base case $m = 6$ is clear: By (1),

$$\mathrm{Alt}(Q \times \Sigma^6) \subseteq \langle [C_4^{(2)}]_6 \rangle = G_6.$$

Consider then $m > 6$ and suppose that G_{m-1} is as claimed. If n is odd then, by the inductive hypothesis,

$$[C_{m-2}^{(2)}]_m \subseteq [\mathrm{Sym}(Q \times \Sigma^{m-1})]_m \subseteq [G_{m-1}]_m \subseteq G_m.$$

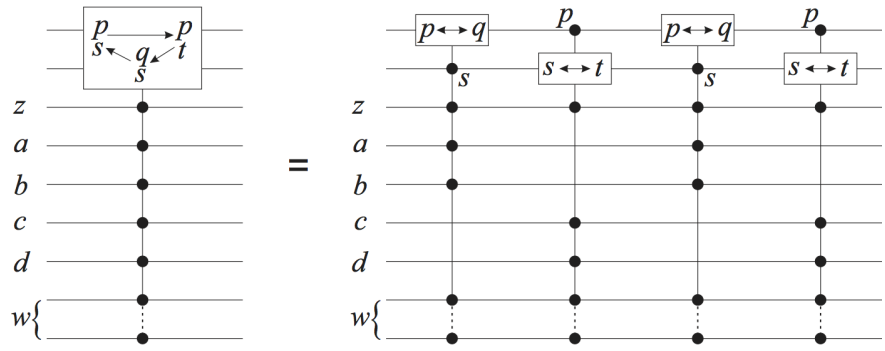

Fig. 1. A decomposition of a controlled 3-cycle of $Q \times \Sigma^m$ on the left into a sequence of four applications of controlled swaps of $Q \times \Sigma^{m-2}$ on the right. The ordering of the wires is such that topmost three wires contain the Q-component and the two wires changed by the 3-cycle (one of which may or may not be the Q-component). Black circles are control points: the gate computes the identity unless the wire carries the symbol indicated at the left of the wire or next to the control point.

By (1) then $\mathrm{Alt}(Q \times \Sigma^m) \subseteq \langle [C^{(2)}_{m-2}]_m \rangle \subseteq G_m$. As pointed out above, G_m contains odd permutations (all elements of $[C^{(2)}_4]_m$ are odd), so $G_m = \mathrm{Sym}(Q \times \Sigma^m)$ as claimed.

If n is even then an application of a permutation of $Q \times \Sigma^{m-2}$ on $Q \times \Sigma^m$ is also an application of an even permutation of $Q \times \Sigma^{m-1}$ on $Q \times \Sigma^m$. (For this reason we left two wires non-controlling for the gates on the right side of Figure 1.) By this and the inductive hypotheses,

$$[C^{(2)}_{m-2}]_m \subseteq [\mathrm{Alt}(Q \times \Sigma^{m-1})]_m \subseteq [G_{m-1}]_m \subseteq G_m,$$

so, by (1), we have the required $\mathrm{Alt}(Q \times \Sigma^m) \subseteq G_m$. □

Corollary 4. $[\mathrm{Sym}(Q \times \Sigma^m)]_{m+1} \subseteq \langle [\mathrm{Sym}(Q \times \Sigma^4)]_{m+1} \rangle$ *for all* $m \geq 5$.

Proof. If n is even then $[\mathrm{Sym}(Q \times \Sigma^m)]_{m+1} \subseteq \mathrm{Alt}(Q \times \Sigma^{m+1})$ and if n is odd then $[\mathrm{Sym}(Q \times \Sigma^m)]_{m+1} \subseteq \mathrm{Sym}(Q \times \Sigma^{m+1})$. In either case, the claim follows from Lemma 6 and $C^{(2)}_4 \subseteq \mathrm{Sym}(Q \times \Sigma^4)$. □

In Corollary 4, arbitrary permutations of $Q \times \Sigma^m$ are obtained as projections of permutations of $Q \times \Sigma^{m+1}$. The extra symbol is an ancilla that can have an arbitrary initial value and is returned back to this value in the end. Such an ancilla is called a "borrowed bit" in [33]. It is needed in the case of even n to facilitate implementing odd permutations of $Q \times \Sigma^m$.

Now we are ready to prove the following theorem.

Theorem 4. $\mathrm{OB}(\mathbb{Z}^d, n, k)$ *is finitely generated.*

Proof. We construct a finite generating set $A_1 \cup A_2 \cup A_3$.

Let A_1 contain the one step moves T_{e_i} for $i = 1, \ldots, d$. These clearly generate $\mathrm{Shift}(\mathbb{Z}^d, n, k)$.

Each $T \in \mathrm{LP}(\mathbb{Z}^d, n, k)$ is defined by a local rule $f : \Sigma^F \times Q \to \Sigma^F \times Q \times \{0\}$ with a finite $F \subseteq \mathbb{Z}^d$. To have injectivity, we clearly need that $\pi : (p, q) \mapsto (f(p, q)_1, f(p, q)_2)$ is a permutation of $\Sigma^F \times Q$. We denote $T = P_\pi$. Let us fix an arbitrary $E \subseteq \mathbb{Z}^d$ of size 4, and let A_2 be the set of all $P_\pi \in \mathrm{LP}(\mathbb{Z}^d, n, k)$ determined by $\pi \in \mathrm{Sym}(\Sigma^E \times Q)$.

For any permutation α of $\mathbb{Z}^d$ with finite support, we define the cell permutation machine $C_\alpha : (p, q) \mapsto (p', q)$, where $p'_{\boldsymbol{v}} = p_{\alpha(\boldsymbol{v})}$ for all $\boldsymbol{v} \in \mathbb{Z}^d$. These are clearly in $\mathrm{LP}(\mathbb{Z}^d, n, k)$. We take A_3 to consist of the cell permutation machines $C_i = C_{(0\ e_i)}$ that, for each $i = 1, \ldots, d$, swaps the contents of the currently scanned cell and its neighbor with offset e_i.

Observe that A_1 and A_3 generate all cell permutation machines C_α. First, conjugating C_i with $T_{\boldsymbol{v}} \in \mathrm{Shift}(\mathbb{Z}^d, n, k)$ gives the cell permutation machine $C_\alpha = T_{\boldsymbol{v}}^{-1} C_i T_{\boldsymbol{v}}$ for the transposition $\alpha = (\boldsymbol{v}\ \boldsymbol{v} + e_i)$. Such transpositions generate all permutations of $\mathbb{Z}^d$ with finite support: This follows from Lemma 4(a) by considering a finite connected grid graph containing the support of the permutation.

Consider then an arbitrary $P_\pi \in \mathrm{OB}(\mathbb{Z}^d, n, k)$, where $\pi \in \mathrm{Sym}(\Sigma^F \times Q)$. We can safely assume $|F| \geq 5$. Let us pick one ancilla $v \in \mathbb{Z}^d \setminus F$ and denote $F' = F \cup \{v\}$. By Corollary 4, P_π is a composition of machines of type P_ρ for $\rho \in \mathrm{Sym}(\Sigma^H \times Q)$ where $H \subseteq F'$ has size $|H| = 4$. It is enough to be able to generate these. Let α be a permutation of $\mathbb{Z}^d$ that exchanges E and H, two sets of cardinality four. Then $C_\alpha^{-1} P_\rho C_\alpha \in A_2$, which implies that P_ρ is generated by $A_1 \cup A_2 \cup A_3$. □