Undecidable word problem in subshift automorphism groups

Pierre Guillon[1], Emmanuel Jeandel[2], Jarkko Kari[3], and Pascal Vanier[4]

[1] Université d'Aix-Marseille, CNRS, Centrale Marseille
I2M, UMR 7373 – 13453 Marseille, France
pierre.guillon@math.cnrs.fr
[2] Université de Lorraine, CNRS, Inria
LORIA – F 54000 Nancy, France
emmanuel.jeandel@loria.fr
[3] Department of Mathematics and Statistics
FI-20014 University of Turku, Finland
jkari@utu.fi
[4] Laboratoire d'Algorithmique, Complexité et Logique
Université de Paris-Est, LACL, UPEC, France
pascal.vanier@lacl.fr

Abstract. This article studies the complexity of the word problem in groups of automorphisms (or reversible cellular automata) of subshifts. We show in particular that for any computably enumerable Turing degree, there exists a (two-dimensional) subshift of finite type whose automorphism group contains a subgroup whose word problem has exactly this degree. In particular, there are such subshifts of finite type where this problem is uncomputable. This remains true in a large setting of subshifts over groups.

Subshifts are sets of colorings of a group G avoiding some family of forbidden finite patterns. They have first been introduced, for $G = \mathbb{Z}$, as a way of discretizing dynamical systems on compact spaces. SFTs correspond to the particular case when only finitely many patterns are forbidden; they are used in information theory to model data streams with coding constraints. When $G = \mathbb{Z}^2$, SFTs turn out to be, up to recoding, the sets of colorings defined by some Wang tiles, and a tool to study decidability questions. When G is the free group, subshifts can be seen as sets of colorings of a tree; the case of the free monoid is known to correspond to the so-called tree languages, and SFTs to tree automata [1,2,3].

Subshifts are hence both a means to model complex systems, and to provide complete problems for a wide range of complexity and computability classes.

An automorphism of a subshift X is a shift-invariant continuous bijection from X onto X, or equivalently a reversible cellular automaton on X. Understanding the automorphism group of a subshift can be seen as a way to understand how constraints over the "physical space" (the possible configurations) restrict the interactions between the cellular automata that act on them.

Little is known about automorphism groups of subshifts in general, besides that they are countable. As an example of our ignorance, it is a long-standing

open problem whether the automorphism groups of the 2-symbol full shift and of the 3-symbol full shift are isomorphic.

Many results have nevertheless been recently reached, for $G = \mathbb{Z}$, in two kinds:

- The automorphism group of some *large* subshifts (positive-entropy SFTs, ...) is rich [4]: it contains all finite groups, finitely generated abelian groups, countable free and free abelian groups, ... This means that when you pick some reversible cellular automata over these subshifts, they can have very complex interactions. In [5], it is proved that periodicity of cellular automata is undecidable, which can be interpreted as the torsion problem for the automorphism group of these subshifts.
- The automorphism group of some *small* subshifts (small complexity function, substitutive, ...) is poor [6,7,8]: in the most extreme case, it is proven to be virtually $\mathbb{Z}$, which means that every reversible cellular automaton is essentially the shift (up to finitely many local permutations).

With $G = \mathbb{Z}^d$ when $d \geq 2$, computability has played a central role in the study of SFTs. From a computability point of view, it is noted in [9] that their automorphism groups have a computably enumerable word problem (which is formalized in a general setting in Theorem 2). The word problem essentially corresponds to picking up a reversible cellular automaton rule over this subshift, and asking whether it is equal to the identity. We show that it can be arbitrarily complex: for any given computably enumerable degree, one can construct an SFT the automorphism group of which has a word problem with this degree (Corollary 2).

1 Preliminaries

By countable set, we mean injectable in $\mathbb{N}$. Let λ denote the empty word. For $\mathcal{A}$ a countable alphabet, we note $\mathcal{A}^* := \bigsqcup_{n\in\mathbb{N}} \mathcal{A}^n$ the set of finite words over $\mathcal{A}$. We also note $\mathcal{A}^{\leq r} := \bigsqcup_{n\leq r} \mathcal{A}^n$ for $r \in \mathbb{N}$.

Let us note X^C the complement of set X. $W \Subset X$ means that $W \subset X$ and W is finite. $V \sqcup W$ means $V \cup W$ assuming that $V \cap W = \emptyset$.

1.1 Computability

Computability problems are naturally defined over $\mathbb{N}$, but can easily be extended through subsets of it, cartesian products or disjoint union (by canonically injecting $\mathbb{N}$ in sets of tuples). For example, if $\mathcal{G} \subset \mathbb{N}$, then the set $\mathcal{G}^*$ of tuples admits a simple injection into $\mathbb{N}$. Let us fix a (computable) countable set I, that we can identify to integers.

Definition 1. *Let us define the following reducibility notions, for $X, Y \subset I$:*

1. *X is* Turing-reducible *to Y, $X \leq_T Y$, if: one can compute X with oracle Y.*

2. X *is* enumeration-reducible *to* Y, $X \leq_e Y$, *if: from any* x *and any integer* $i \in \mathbb{N}$, *one can compute a finite set* $Y_i(x)$ *such that* $x \in X$ *if and only if* $\exists i \in \mathbb{N}, Y_i(x) \subset Y$.
3. X *is* positive-reducible *to* Y, $X \leq_p Y$, *if: from any* x, *one can compute finitely many finite sets* $Y_0(x), \ldots, Y_{n-1}(x)$ *such that* $x \in X$ *if and only if* $\exists i < n, Y_i(x) \subset Y$.
4. X *is* many-one-reducible *to* Y, $X \leq_m Y$, *if: from any* x, *one can compute some* $\phi(x)$ *such that* $x \in X$ *if and only if* $\phi(x) \in Y$.
5. X *is* one-one-reducible *to* Y, $X \leq_1 Y$, *if,* $X \leq_m Y$ *and the corresponding* ϕ *is one-to-one.*

One-one reducibility implies many-one reducibility, which in turns implies positive-reducibility, which implies both Turing-reducibility and enumeration-reducibility.

Each reducibility $\leq_r$ induces a notion of equivalence $\equiv_r$: $A \equiv_r B$ iff $A \leq_r B$ and $B \leq_r A$. And each notion of equivalence $\equiv_r$ induces a notion of degree $\deg_r$: the *degree of a set* A is its equivalence class for $\equiv_r$.

The *join* $A \oplus B$ of A and B is the set C such that $2n+1 \in C$ iff $n \in A$ and $2n \in C$ iff $n \in B$. It has the property that $A \leq_r A \oplus B$ and $B \leq_r A \oplus B$ for any reducibility $\leq_r$ previously defined.

See [10] for a reference on computability-theoretical reductions.

1.2 Monoids and groups

We will deal with countable monoids $\mathbb{M} = \mathcal{G}^*/R$, where $\mathcal{G} \subset \mathbb{N}$, $\mathcal{G}^*$ is the free monoid generated by symbols from $\mathcal{G}$ and R is a monoid congruence[5]. The monoid is always implicitly endowed with its generating set $\mathcal{G}$ (later, some problems may depend on the presentation). Each element of the monoid is represented by a word $u \in \mathcal{G}^*$, but the representation is not one-to-one (except for the free monoid itself). We note $i =_{\mathbb{M}} j$ if $\pi(i) = \pi(j)$ and $\pi : \mathcal{G}^* \to \mathbb{M}$ is the natural quotient map.

It is also clear that the concatenation map, which from any two words $i, j \in \mathcal{G}^*$ outputs $i \cdot j$, which is one representative of the corresponding product, is computable. We say that $\mathbb{M}$ is an *effective group* if, additionally, there is a computable map $\psi : \mathcal{G}^* \to \mathcal{G}^*$ such that $i \cdot \psi(i) =_{\mathbb{M}} \psi(i) \cdot i =_{\mathbb{M}} \lambda$.

The *equality problem* of $\mathbb{M}$, endowed with generating family $\mathcal{G}$, is the set of pairs $\left\{ (i,j) \in (\mathcal{G}^*)^2 \middle| i =_{\mathbb{M}} j \right\}$, endowed with a natural enumeration so that we can consider it as a computability problem.

Remark 1.

1. It is clear that the *word problem* $\{ i \in \mathcal{G}^* | \, i =_{\mathbb{M}} \lambda \}$ is one-one-reducible to the equality problem.
2. If $\mathbb{M}$ is an effective group, then the word problem is actually many-one-equivalent to the equality problem.

[5] We could deal in the same way with semigroups, by prohibiting the empty word.

3. The equality problems for $\mathbb{M}$ endowed with two distinct finite generating sets are one-one-equivalent.
4. If $\mathbb{M}'$ is a submonoid of $\mathbb{M}$ endowed with a generating set which is included in that of $\mathbb{M}$, then the equality problem in $\mathbb{M}'$ is one-one-reducible to that of $\mathbb{M}$.
5. In particular, the equality problem in any finitely generated submonoid is one-one-reducible to that of $\mathbb{M}$.

Nevertheless, there are countable groups whose word problem is computable when endowed with one generating family, and uncomputable when endowed with another one.

The word problem is known to be decidable if and only if the group is *computable* (see [11] for a proof in the finitely generated case), that is, it can be seen as a computable subset of $\mathbb{N}$ over which the composition rule is a computable function (this implies that inversion is also a computable map).

1.3 Subshifts

Let $\mathcal{A}$ be a finite alphabet with at least two letters, and $\mathbb{M}$ a group (most of the following should be true if $\mathbb{M}$ is a cancellative monoid though). In a first reading, the reader is encouraged to think of $\mathbb{M}$ as being $\mathbb{Z}$: the results are not significantly simpler in that specific setting (except those that mention 1D SFT). A finite *pattern* w over $\mathcal{A}$ with *support* $W = \mathcal{S}(w) \Subset \mathcal{G}^*$ is a map $w = (w_i)_{i \in W} \in \mathcal{A}^W$. An element of $\mathcal{A}^{\mathbb{M}}$ is called a *configuration*. Configurations can be seen as colorings of the Cayley graph by the letters of $\mathcal{A}$ and patterns can be seen as finite configurations. Depending on the context, note that, for $g \in \mathcal{S}(w)$, w_g may either be an element of $\mathcal{A}$ or a subpattern with support $\{g\}$. If $g \in \mathcal{G}^*$ and w is a pattern, we will denote by $\sigma^g(w)$ the pattern with support $W \cdot g$ such that $\sigma^g(w)_{i \cdot g^{-1}} = w_i$ for all $i \in \mathcal{S}(w)$.

We are interested in $\mathcal{A}^{\mathbb{M}}$, which is a Cantor set, when endowed with the prodiscrete topology, on which $\mathbb{M}$ acts continuously by (left) shift: we note $\sigma^i(x)_j = x_{i.j}$ for $i, j \in \mathbb{M}$ and $x \in \mathcal{A}^{\mathbb{M}}$. $\mathcal{A}^{\mathbb{M}}$ is thus called the *full shift* on alphabet $\mathcal{A}$. A *subshift* is a closed σ-invariant subset $X \subset \mathcal{A}^{\mathbb{M}}$. Equivalently, X can be defined as the set $X_{\mathcal{F}} := \left\{ x \in \mathcal{A}^{\mathbb{M}} \middle| \forall i \in \mathbb{M}, \forall w \in \mathcal{F}, \exists j \in \mathcal{S}(w), x_{i \cdot j} \neq w_j \right\}$ avoiding a language $\mathcal{F} \subset \bigsqcup_{W \Subset \mathcal{G}^*} \mathcal{A}^W$, which is then called a (defining) *forbidden language*. If $\mathcal{F}$ can be chosen finite, the subshift is called *of finite type* (SFT); if it can be chosen computably enumerable, it is called *effective*. Figure 1 shows an example of forbidden language and configuration of the associated subshift.

The *language* with *support* $W \Subset \mathcal{G}^*$ of subshift X is the set $\mathcal{L}_W(X) := \left\{ (x_{\pi(i)})_{i \in W} \middle| x \in X \right\}$; the *language* of X is $\mathcal{L}(X) = \bigsqcup_{W \Subset \mathcal{G}^*} \mathcal{L}_W(X)$, and its *colanguage* is the complement of it. The latter is a possible defining forbidden language. If $u \in \mathcal{L}_W(X)$, we define the corresponding *cylinder*

$$[u] = \left\{ x \in X \middle| \forall i \in W, x_{\pi(i)} = u_i \right\}.$$

Remark 2. π induces a natural covering $\Pi : \mathcal{A}^{\mathbb{M}} \to \mathcal{A}^{\mathcal{G}^*}$ by $\Pi(x)_i = x_{\pi(i)}$. Its image set $\Pi(\mathcal{A}^{\mathbb{M}})$ is a subshift over the free monoid. One can note the following.

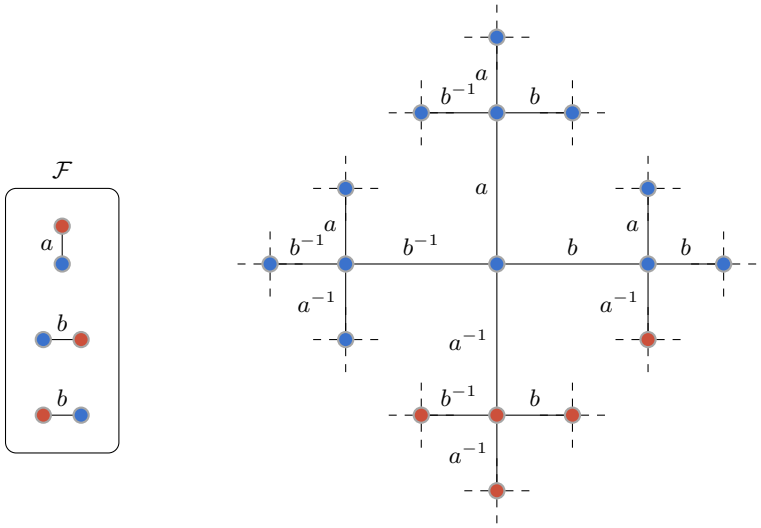

Fig. 1. If $\mathbb{M}$ is the free group on two elements $\{a, b\}$ and the set of forbidden patterns is on the left, then the configuration on the right is in $X_{\mathcal{F}}$.

1. $X = X_{\mathcal{L}(X)^C}$.
2. The colanguage of the full shift $\mathcal{A}^{\mathbb{M}}$ is the same as that of the subshift $\Pi(\mathcal{A}^{\mathbb{M}})$: the set
$$\mathcal{L}(\mathcal{A}^{\mathbb{M}})^C = \bigsqcup_{W \Subset \mathcal{G}^*} \left\{ w \in \mathcal{A}^W \,\middle|\, \exists i, j \in W, i =_{\mathbb{M}} j, w_i \neq w_j \right\}$$
of patterns that do not respect the monoid congruence.
3. Nevertheless, $\emptyset$ is a forbidden language defining $\mathcal{A}^{\mathbb{M}}$.
4. The colanguage of every subshift $X_{\mathcal{F}} \subset \mathcal{A}^{\mathbb{M}}$ is the set of patterns $w \in \mathcal{A}^W$, $W \Subset \mathcal{G}^*$, whose all extensions to configurations $x \in [w]$ involve as a subpattern a pattern of either $\mathcal{F}$, or $\mathcal{L}(\mathcal{A}^{\mathbb{M}})^C$. In that case, by compactness, there exists $V \supset W$ (which depends only on W) such that $w \in \mathcal{A}^W$ is in the colanguage iff every $v \in \mathcal{A}^V$ such that $v_{|W} = u$ involves a subpattern from $\mathcal{F}$ or $\mathcal{L}(\mathcal{A}^{\mathbb{M}})^C$.

Remark 3. Let $\mathbb{M}$ be a monoid.

1. The equality problem in $\mathbb{M}$ is positive-equivalent (and one-one-reducible) to the colanguage of the full shift.
2. The colanguage of any subshift X is enumeration-reducible to the join of any defining forbidden language for X and the equality problem of $\mathbb{M}$.

Proof.

1. one-one-reducibility: one can computably map each word $(i,j) \in (\mathcal{G}^*)^2$ to a unique pattern over $\{i,j\}$ involving two different symbols. By Point 2 of Remark 2, this pattern is in the colanguage of the full shift if and only if $i =_{\mathbb{M}} j$.
   positive-reducibility (with all Y_is being singletons): from each pattern $w \in \mathcal{A}^{\mathcal{G}^*}$, one can compute the set of pairs $(i,j) \in \mathcal{S}(w)^2$ such that $w_i \neq w_j$. By Point 2 of Remark 2, w is in the colanguage if and only if one of these pairs is an equality pair in $\mathbb{M}$.
2. Consider the set Z of *locally inadmissible* patterns, that involve a subpattern either from the forbidden language or from $\mathcal{L}(\mathcal{A}^{\mathbb{M}})^C$. From any pattern w, one can enumerate all of its subpatterns and all of their shifts, *i.e.* all patterns v such that there exists $i \in \mathcal{G}^*$ with $\mathcal{S}(v) \cdot i \subset \mathcal{S}(w)$ and $w_{j \cdot i} = v_j$ for every $j \in \mathcal{S}(v)$. This shows that Z is enumeration-reducible to the join of the forbidden language and $\mathcal{L}(A^{\mathbb{M}})^C$, the latter being equivalent to the equality problem, by the previous point. It remains to show that the colanguage of X is enumeration-reducible to Z.
   From any pattern $w \in \mathcal{A}^{\mathcal{G}^*}$ and any $i \in \mathbb{N}$, one can compute some $V_i \Subset \mathcal{G}^*$ including $\mathcal{S}(w)$, in a way that $V_{i+1} \supset V_i$ and $\bigcup_{i \in \mathbb{N}} V_i = \mathcal{G}^*$ (for example take the union of $\mathcal{S}(w)$ with balls in the Cayley graph). Then, one can compute the set Y_i of extensions of w to V_i, *i.e.* patterns with support V_i whose restriction over $\mathcal{S}(w)$ is w. By Point 4 of Remark 2, $w \in \mathcal{L}(X)^C$ if and only if there exists $V \Subset \mathcal{G}^*$ with $V \supset \mathcal{S}(w)$ such that all extensions of w to V are in Z; and in particular this should happen for some V_i, which precisely means that $Y_i \subset Z$. □

It results that, in some sense, one expects most subshifts to have a colanguage at least as complex as the equality problem in the underlying monoid.

1.4 Homomorphisms

Let $X \subset \mathcal{A}^{\mathbb{M}}$ and $Y \subset \mathcal{B}^{\mathbb{M}}$ be subshifts. Denote $\mathcal{E}nd(X,Y)$ the set of *homomorphisms* (continuous shift-commuting maps) from X to Y, and $\mathcal{A}ut(X,Y)$ the set of bijective ones (*conjugacies*). We also note $\mathcal{E}nd(X) = \mathcal{E}nd(X,X)$ the monoid of *endomorphisms* of X, and $\mathcal{A}ut(X) = \mathcal{A}ut(X,X)$ the group of its *automorphisms*.

If $\mathbb{M}$ is finitely generated, then homomorphisms correspond to block maps (and endomorphisms to cellular automata), thanks to a variant of the Curtis-Hedlund-Lyndon theorem [12].

Theorem 1. *Let $\mathbb{M}$ be finitely generated. A map Φ from subshift $X \subset \mathcal{A}^{\mathbb{M}}$ into subshift $Y \subset \mathcal{B}^{\mathbb{M}}$ is a homomorphism if and only if there exist a* radius $r \in \mathbb{N}$ *and a* block map $\phi : \mathcal{A}^{\mathcal{G}^{\leq r}} \to \mathcal{B}$ *such that for every $x \in \mathcal{A}^{\mathbb{M}}$ and $i \in \mathcal{G}^*$, $\Phi(x)_{\pi(i)} = \phi(x_{|\pi(i \cdot \mathcal{G}^{\leq r})})$ (where the latter has to be understood with the obvious reindexing of the argument).*

See Figure 2 for an example of block map and associated homomorphism. Let

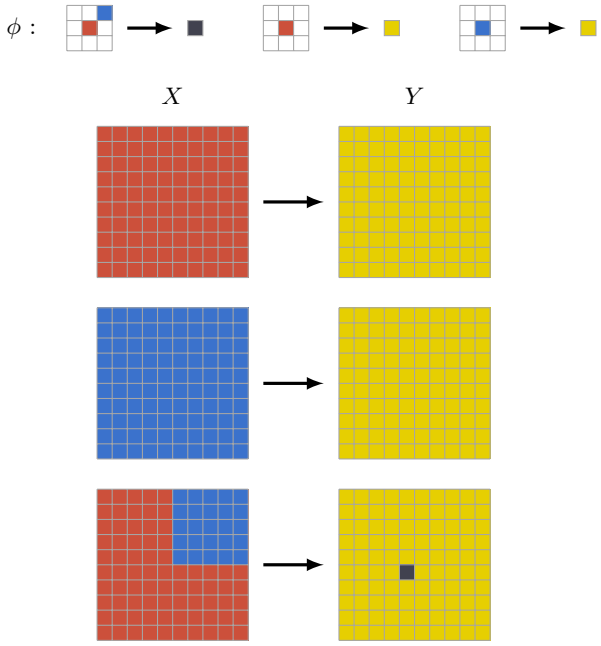

Fig. 2. The block map ϕ takes the $\mathbb{Z}^2$ subshift X to the $\mathbb{Z}^2$ subshift Y by applying it locally at each position.

us order the block maps $\phi : \mathcal{A}^{\mathcal{G}^{\leq r}} \to \mathcal{B}$ by increasing radius $r \in \mathbb{N}$, and then by lexicographic order, so that we have a natural bijective enumeration $\mathbb{N} \to \bigsqcup_{r\in\mathbb{N}} \mathcal{B}^{\mathcal{A}^{\mathcal{G}^{\leq r}}}$ (because $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{G}$ are finite). This gives in particular a surjective enumeration $\mathbb{N} \to \mathcal{E}nd(\mathcal{A}^{\mathcal{G}^*}, \mathcal{B}^{\mathcal{G}^*})$ and in general, a partial surjective enumeration $\mathbb{N}' \subset \mathbb{N} \to \mathcal{E}nd(X, Y)$.

Let us discuss briefly the situation of this enumeration, which is not the main topic of the present paper, but sheds light on the difficulties for an effective representation of homomorphisms. In general, $\mathbb{N}' \neq \mathbb{N}$. It is a nontrivial problem to ask whether $\mathbb{N}'$ is computable (this would mean that we can decide whether a block map sends X into Y), like for the full shift. Similarly, the domain $\mathbb{N}'$ of an enumeration of $\mathcal{A}ut(X, Y)$ need not be computable: it is already uncomputable for $\mathcal{A}ut(\mathcal{A}^{\mathbb{Z}^2})$, because it corresponds to the reversibility problem for two-dimensional cellular automata (over the full shift) [13].

On the other hand, obtaining a bijective enumeration for $\mathcal{E}nd(\mathcal{A}^{\mathcal{G}^*}, \mathcal{B}^{\mathcal{G}^*})$ would be easily achieved by representing each block map only for its smallest possible radius. Nevertheless, trying to achieve a bijective enumeration in general for $\mathcal{E}nd(X, Y)$, or even for $\mathcal{E}nd(\mathcal{A}^{\mathbb{M}}, \mathcal{B}^{\mathbb{M}})$, is a process that would depend on the colanguage of the subshift (we want to avoid two block maps that differ only over the colanguage), which may be uncomputable.

For the rest of the paper, let us assume that $\mathbb{M}$ is an effective group. More precisely, all results could be interpreted as reductions to a join with a problem representing the composition map of the group, and sometimes to an additional join with a problem representing the inversion.

2 Equality problem is not too hard

Remark 4. Two distinct block maps $\phi, \psi : \mathcal{A}^{\mathcal{G}^{\leq r}} \to \mathcal{A}$ representing endomorphisms of X actually represent the same endomorphism if and only if for every pattern $u \in \mathcal{A}^{\mathcal{G}^{\leq r}}$, $\phi(u) \neq \psi(u) \Rightarrow u \in \mathcal{L}(X)^C$.

This remark allows to establish that the equality problem is at most as complex as knowing whether a pattern is in the colanguage.

Theorem 2. *The equality problem in $\mathcal{E}nd(X)$ is positive-reducible to $\mathcal{L}(X)^C$.*

Proof. One can directly apply Remark 4, by noting that it is easy to transform each block map into an equivalent one, so that the resulting two block maps have the same radius (the original maximal one, by ignoring extra symbols). □

Of course, this remains true for the equality problem in $\mathcal{A}ut(X)$. Since positive-reducibility implies both Turing-reducibility and enumeration-reducibility, we get the following for the lowest classes of the arithmetic hierarchy (which was already known; see [9]).

Corollary 1.

1. *The equality problem is decidable, in the endomorphism monoid of any subshift with computable language (for instance 1D sofic subshift, 1D substitutive subshift, minimal effective subshift, two-way space-time diagrams of a surjective cellular automaton...).*
2. *The equality problem is computably enumerable, in the endomorphism monoid of any effective subshift (for instance multidimensional sofic subshift, substitutive subshift, limit set of cellular automaton...).*

3 Automorphism groups with hard equality problem

The purpose of this section is to prove a partial converse to Theorem 2: we can build a subshift X for which the two problems involved are equivalent, however complex they are.

Let $X \subset \mathcal{A}^{\mathbb{M}}$ and $Y \subset \mathcal{B}^{\mathbb{M}}$ be subshifts. For $\alpha : \mathcal{B} \to \mathcal{B}$ and $u \in \mathcal{A}^{\mathbb{M}}$, let us define the *controlled map* $C_{u,\alpha}$ as the homomorphism over $X \times Y$ such that $C_{u,\alpha}(x,y)_0 = (x_0, \alpha(y_0))$ if $x \in [u]$; (x_0, y_0) otherwise. Informally, $C_{u,\alpha}(x,y)$ applies α somewhere in y iff it sees u at the corresponding position in x. Denote also π_1 the projection to the first component, and σ_1^g the shift of the first component with respect to element $g \in \mathbb{M}$: $\sigma_1^g(x,y)_0 = (x_g, y_0)$ for every $(x,y) \in X \times Y$.

Remark 5.

1. $\pi_1 C_{u,\alpha} = \pi_1$.
2. If $\mathbb{M}$ is a group and $g \in \mathbb{M}$, then $C_{u,\alpha} = \sigma_1^g C_{\sigma^{g^{-1}}(u),\alpha} \sigma_1^{-g}$.
3. $C_{u,\alpha} \in \mathcal{E}nd(X \times Y, X \times \mathcal{B}^{\mathbb{M}})$.
4. $C_{u,\alpha}$ is injective if and only if α is a permutation.
5. $C_{u,\alpha} \in \mathcal{E}nd(X \times Y)$ if Y is (locally) α-*permutable*, *i.e.* for all $y \in Y$, if we define z by $z_0 = \alpha(y_0)$, $z_i = y_i$ for $i \neq 0$, then $z \in Y$.
6. From Remark 4, $C_{u,\alpha}$ is the identity over $X \times Y$ if and only if $u \notin \mathcal{L}(X)$, or α is the trivial permutation over letters appearing in Y.

Example 1. Examples of α-permutable subshifts are the full shift on $\mathcal{B}$ or, if $\mathcal{B} = \mathcal{B}' \sqcup \{\perp\}$ and $\alpha(\perp) = \perp$, the $\mathcal{B}'$-*sunny-side-up* defined by forbidding every pattern which involves two occurences of $\mathcal{B}'$. We have seen that the colanguage of the former is positive-equivalent to the word problem in $\mathbb{M}$. The language of the latter can be easily proven to be many-one-equivalent to the word problem in $\mathbb{M}$ (as essentially noted in [14, Prop 2.11]), hence yielding a kind of jump for the colanguage.

If $a, b, c \in \mathcal{B}$, let us denote $\alpha_{abc} : \mathcal{B} \to \mathcal{B}$ the 3-*cycle* that maps a to b, b to c, c to b, and any other symbol to itself. The following lemma corresponds essentially to [15, Lemma 18] and shows that controlled permutations, no matter the size of the control pattern u, can be expressed with a finite number of generators.

Lemma 1. *Suppose $\mathcal{B}$ has at least 5 distinct elements a, b, c, d, e. Let $u \in \mathcal{A}^{\mathcal{S}(u)}$ be a pattern, $g \in \mathcal{S}(u)$, and $v = u_{|\mathcal{S}(u)\setminus\{g\}}$. Then $C_{u,\alpha_{abc}} = (\Psi\Phi)^2$, where $\Phi = \sigma_1^g C_{u_g,\alpha_{ade}} C_{u_g,\alpha_{bad}} \sigma_1^{g^{-1}}$ and $\Psi = C_{v,\alpha_{bde}} C_{v,\alpha_{cbd}}$.*

Proof. If $x_g = u_g$, then $\Phi(x,y)_0 = (x_0, \phi(y_0))$, where ϕ is the involution that swaps a and b on the one hand, d and e on the other hand; otherwise $\Phi(x,y)_0 = (x_0, y_0)$. If $x \in [v]$, then $\Psi(x,y)_0 = (x_0, \psi(y_0))$, where ψ is the involution that swaps b and c on the one hand, d and e on the other hand; otherwise $\Psi(x,y)_0 = (x_0, y_0)$. Since $\phi^2 = \psi^2 = \mathrm{id}$, one can see that if $x \notin [u]$, then $(\Psi\Phi)^2(x,y)_0 = (x_0, y_0)$. Now if $x \in [u]$, then we see that $\Psi\Phi(x,y)_0 = (x_0, \psi\phi(y_0))$, and $\psi\phi = \alpha_{acb}$, so that we get the stated result. □

Theorem 3. *Let $X \subset \mathcal{A}^{\mathbb{M}}$ be a subshift and $Y \subset \mathcal{B}^{\mathbb{M}}$ an α_{abc}-permutable subshift for every $a, b, c \in \mathcal{B}' \subset \mathcal{B}$, where $|\mathcal{B}'| \geq 5$. Then $\mathcal{L}(X)^C$ is one-one-reducible to the word problem in the subgroup of automorphisms of $X \times Y$ generated by σ_1^g and $C_{u_0,\alpha_{abc}}$ for $g \in \mathcal{G}$, $a, b, c \in \mathcal{B}'$ and $u_0 \in \mathcal{A}$.*

Proof. From an induction and Lemma 1, we know that this subgroup includes every $C_{u,\alpha_{abc}}$ for every $a, b, c \in \mathcal{B}'$ and $u \in \mathcal{A}^*$. From Point 6 of Remark 5, an automorphism $C_{u,\alpha_{abc}}$ is equal to the identity if and only if $u \notin \mathcal{L}(X)$. □

Consequently, subshifts can have finitely generated automorphism subgroups with equality problem as complex as their colanguage, as formalized by the following corollary. In that case, the equality problem of the whole automorphism group is as complex also.

Corollary 2.

1. *If X and Y are as in Theorem 3, then $\mathcal{L}(X)^C$ is one-one-equivalent to the word problem in (a finitely generated subgroup of) $\mathcal{A}ut(X \times Y)$.*
2. *For every subshift X over a finitely generated group $\mathbb{M}$, there exists a countable-to-one extension $X \times Y$ such that $\mathcal{L}(X)^C$ is one-one-equivalent to the word problem in (a finitely generated subgroup of) $\mathcal{A}ut(X \times Y)$.*
3. *For every subshift X over a finitely generated group $\mathbb{M}$, there exists a full extension $X \times \mathcal{B}^{\mathbb{M}}$ such that $\mathcal{L}(X)^C$ is one-one-equivalent to the word problem in (a finitely generated subgroup of) $\mathcal{A}ut(X \times \mathcal{B}^{\mathbb{M}})$.*
4. *Every Σ_1^0 Turing degree contains the word problem in (a finitely generated subgroup of) $\mathcal{A}ut(X)$, for some 2D SFT X.*
5. *There exists a 2D SFT X for which the word problem in (a finitely generated subgroup of) $\mathcal{A}ut(X)$ is undecidable.*

Point 5 answers [9, Problem 5].

Proof.

1. Just use Point 5 of Remark 1. For the converse reduction in the one-one-equivalence, simply apply Theorem 2 and Point 1 of Remark 1.
2. We use Theorem 3 with Y being the $\{0,1,2,3,4\}$-sunny-side-up.
3. We use Theorem 3 with $Y = \{0,1,2,3,4\}^{\mathbb{M}}$. Remark that $\mathcal{L}(X)^C$ and $\mathcal{L}(X \times \{0,1,2,3,4\}^{\mathbb{M}})^C$ are one-one-equivalent.
4. Every Σ_1^0 degree contains the colanguage of a 2D SFT, thanks to constructions from [16,17]. Then its product with the full shift $\{0,1,2,3,4\}^{\mathbb{Z}^2}$ is still an SFT, and we conclude by the previous point.
5. Apply the previous point with any uncomputable Σ_1^0 degree. □

Note that the number of generators can be decreased if we want to reduce only the language whose support is spanned by a subgroup. For instance 2D SFTs are already known to have (arbitrarily Σ_1^0) uncomputable 1D language. Indeed, our automorphisms do not alter the X layer, so that their parallel applications to all traces with respect to a subgroup is still an automorphism.

Among the open questions, we could wonder whether there is a natural class of SFT (irreducible, with uncomputable language, at least over $\mathbb{Z}^2$) whose colanguage could be proven reducible to the word problem in the automorphism group. This could require to encode the whole cartesian product of Theorem 3 inside such subshifts. Another question would be to adapt our construction while controling the automorphism group completely so that it is finitely generated.

Acknowledgements

This research supported by the Academy of Finland grant 296018.

We thank Ville Salo for some discussions on commutators, on the open questions, and for a careful reading of this preprint.

References

1. Nathalie Aubrun and Marie-Pierre Béal. Decidability of conjugacy of tree-shifts of finite type. In *Automata, Languages and Programming*, pages 132–143. Springer Berlin Heidelberg, 2009.
2. H. Comon, M. Dauchet, R. Gilleron, C. Löding, F. Jacquemard, D. Lugiez, S. Tison, and M. Tommasi. Tree automata techniques and applications. Available on: `http://www.grappa.univ-lille3.fr/tata`, 2007. release October, 12th 2007.
3. Wolfgang THOMAS. Chapter 4 - automata on infinite objects. In JAN VAN LEEUWEN, editor, *Formal Models and Semantics*, Handbook of Theoretical Computer Science, pages 133 – 191. Elsevier, Amsterdam, 1990.
4. Mike Boyle, Douglas A. Lind, and Daniel J. Rudolph. The automorphism group of a shift of finite type. *Transactions of the American Mathematical Society*, 306(1):71–114, 1988.
5. Jarkko Kari and Nicolas Ollinger. Periodicity and immortality in reversible computing. In *MFCS 2008*, LNCS 5162, pages 419–430, apr 2008.
6. Ethan Coven and Reem Yassawi. Endomorphisms and automorphisms of minimal symbolic systems with sublinear complexity.
7. Van Cyr and Bryna Kra. The automorphism group of a shift of linear growth: beyond transitivity.
8. Sebastián Donoso, Fabien Durand, Alejandro Maass, and Samuel Petite. On automorphism groups of low complexity subshifts.
9. Michael Hochman. Groups of automorphisms of SFTs. Open problems ; `http://math.huji.ac.il/~mhochman/problems/automorphisms.pdf`.
10. Hartley Rogers, Jr. *Theory of Recursive Functions and Effective Computability*. MIT Press, Cambridge, MA, USA, 1987.
11. Michael O. Rabin. Computable algebra, general theory and theory of computable fields. *Transactions of the American Mathematical Society*, 95:341–360, 1960.
12. Gustav Arnold Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Mathematical Systems Theory*, 3:320–375, 1969.
13. Jarkko Kari. Reversibility and surjectivity problems of cellular automata. *J. Comput. Syst. Sci.*, 48(1):149–182, 1994.
14. Nathalie Aubrun, Sebastián Barbieri, and Mathieu Sablik. A notion of effectiveness for subshifts on finitely generated groups. *Theoretical Computer Science*, 661:35–55, 2017.
15. Tim Boykett, Jarkko Kari, and Ville Salo. Finite generating sets for reversible gate sets under general conservation laws. *Theoretical Computer Science*, 701:27–39, November 2017.
16. Stephen G. Simpson. Medvedev degrees of 2-dimensional subshifts of finite type. *Ergodic Theory and Dynamical Systems*, 34(November 2012):665–674, 2014.
17. William Hanf and Dale Myers. Non recursive tilings of the plane II. *Journal of Symbolic Logic*, 39(2):286–294, 1974.