Cellular automata over groups with finite parts and decidability of the invertibility problem

Silvio Capobianco
Dipartimento di Matematica "Guido Castelnuovo"
Università degli Studi di Roma "La Sapienza"
Email: capobian@mat.uniroma1.it

October 9, 2003

Abstract

We show that, for every cellular automaton over a group of the form $H \ltimes_\tau K$ with H finitely generated and K finite, there is a conjugate cellular automaton over H. From this we find an extension of Amoroso and Patt's result on the decidability of the invertibility problem.

1 Introduction

Cellular automata are uniform lattices of devices, whose global evolution is determined by local interactions. They are very well suited for simulations of large systems in physics, biology, and economics.

The classical definition of a cellular automaton involves a finite set of states Q, a dimension d, a finite set $\mathcal{N} \subset \mathbb{Z}^d$, and a local transition function $f : Q^{|\mathcal{N}|} \to Q$, such that the future state of a point i on the lattice $\mathbb{Z}^d$ is the value of f on the present states of the points $j \in i + \mathcal{N}$. There is a more general definition, as in [10] and [3], where the lattice is the Cayley graph of a finitely generated group. This group is called the *tessellation group* of the cellular automaton. The local evolution function of a cellular automaton induces a global evolution function on the space of the configurations of the automaton.

A *conjugacy* from a cellular automaton to another is a homeomorphism of

their configuration spaces such that the image of the successor of a configuration of the first automaton is the successor of its image in the second automaton. The properties of cellular automata that are not changed by conjugacies are called *invariants*; they are very important in the study of dynamics.
It is expecially interesting to determine whether a given cellular automaton is invertible, that is, if its global evolution function is bijective. Invertibility is of course an invariant, because conjugacies are bijections.
We show that the finite part of the tessellation group is unessential to the dynamics: that is, if the tessellation group is a semi-direct product $H \ltimes_\tau K$ with H finitely generated and K finite and normal, then there is a conjugate cellular automaton whose tessellation group is H. This allows us to translate some cellular automata into other cellular automata with a simpler tessellation group, thus giving a tool that can be used in solving problems where the structure of the tessellation group is of fundamental importance. Moreover, the fact that this transformation is computable allows us to obtain an extension of the classical results of [1] and [7] about the decidability of the invertibility problem.

2 Cellular automata over finitely generated groups

Definition 2.1 *Let G be a group. A* set of generators *for G is a set S such that any element of G can be written as a finite product of elements of S and their inverses. G is* finitely generated *if it admits a finite set of generators.*

Every finite group is finitely generated. For every $d > 0$, the group $\mathbb{Z}^d$ is finitely generated, the standard base $S = \{\bar{e}_1 \dots \bar{e}_d\}$ being a finite set of generators.
The *Cayley graph* of a finitely generated group G with respect to a finite set of generators S is the graph whose nodes are the elements of the group, and such that there is an edge from node g to node h if and only if $h = gt$ for some $t \in S \cup S^{-1}$. For example, the Cayley graph of $\mathbb{Z}^2$ is the square grid on the plane.
It is possible to define a metric on a finitely generated group G by fixing a finite set of generators S for G, putting $S^{-1} = \{x^{-1},\ x \in S\}$, and defining $\|g\|_S^G$, the *length* of g in G with respect to S, as the minimum number

of elements in $S \cup S^{-1}$ needed to obtain g as a product of these elements, that is, the length of the shortest path from 1 to g in the Cayley graph of G w.r.t. S. Then the *distance* between a and b in G w.r.t. S is the quantity $d_S^G(a,b) = \|a^{-1}b\|_S^G$, and $D_{r,S}^G(g)$ is the set of those $h \in G$ such that $d_S^G(g,h) \leq r$. We write $D_{r,S}^G$ for $D_{r,S}^G(1)$.
For example, if $G = \mathbb{Z}^2$ and $S = \{\bar{e}_1, \bar{e}_2\}$, then $\|x\|_S^G = |x_1| + |x_2|$ and $d_S^G(x,y) = \|y-x\|_1 = |y_1 - x_1| + |y_2 - x_2|$; the disk $D_{r,S}^G(x)$ is called the *von Neumann neighborhood of range* r of point x.
If G and/or S are clear from the context, we will sometimes omit them. Observe that, since S is finite, $D_{r,S}^G(g)$ is finite for any $g \in G$, $r \geq 0$.

An *alphabet* is a finite set with 2 or more elements. Any alphabet A is a discrete topological space. Elements of A^G are called *configurations of A over G*, or simply *configurations* where the context is clear. If c is a configuration, then the value of c over $g \in G$ is denoted by c_g; the restriction of c to $X \subseteq G$ is denoted by $c_{|X}$
For any alphabet A and finitely generated G, A^G is compact by Tychonoff's theorem. The product topology on A^G is induced by many distances, such as:

$$d_S(c_1, c_2) = 2^{-\min\left\{r : c_{1|D_{r,S}^G} \neq c_{2|D_{r,S}^G}\right\}} \tag{1}$$

with the conventions $\min \emptyset = +\infty$, $2^{-\infty} = 0$.
We observe that all these distances induce the same topology regardless of S: indeed the projections, being in this case evaluations at a point, are obviously continuous with respect to d_S; moreover, by definition of product space and product topology, any topology that makes the projections continuous must contain all the sets made of all the configurations c' that agree with a given configuration c over a finite set of elements of G, and in particular must contain all the disks of d_S, since the $D_{r,S}^G$ are finite by construction.
It is then easy to understand that continuity for a function $\varphi : A^G \to (A')^{G'}$ is defined in the following way: for every $N > 0$ there exists $K > 0$ such that, if c_1 and c_2 are equal over D_K^G, then $\varphi(c_1)$ and $\varphi(c_2)$ are equal over $D_N^{G'}$.

Definition 2.2 *Let $\mathcal{C} = A^G$, A alphabet, G finitely generated group. A* shift subspace*, or briefly* subshift*, of $\mathcal{C}$ is a compact subset $X \subseteq \mathcal{C}$ that is stable under the natural action of G over $\mathcal{C}$ defined by:*

$$(c^g)_i = c_{gi} \quad \forall i \in G \quad \forall g \in G \tag{2}$$

The shift subspace $X = \mathcal{C}$ is called the full shift *over G.*

For a non-trivial example, consider $G = \mathbb{Z}$, $A = \{0, 1\}$, and let X be the set of those $c \in A^{\mathbb{Z}}$ such that $c_i c_{i+1} \neq 11$ for every $i \in \mathbb{Z}$: then X is a shift subspace, because it is clearly stable under the action of $\mathbb{Z}$ and because no configuration with two consecutive 1s can be the limit of a sequence in X.
Observe that, for every $g \in G$, the map $\Phi_g : \mathcal{C} \to \mathcal{C}$ defined by $\Phi_g(c) = c^g$ is continuous: so $(\mathcal{C}, \Phi_g)$ is a dynamical system for every $g \in G$. Hence, a subshift is a subset $X \subseteq \mathcal{C}$ such that, for every $g \in G$, (X, Φ_g) is a dynamical subsystem of $(\mathcal{C}, \Phi_g)$.

Definition 2.3 *A* pattern of range r *is a function $p \in A^{D_r^G}$. A pattern p of range r* occurs *in a configuration c if there exists $g \in G$ such that, for every $i \in D_r^G$, $(c^g)_i = p_i$. A pattern p is* forbidden *for a set X of configurations if it does not occur in any of the elements of X. For a set $\mathcal{F}$ of patterns, $\mathsf{X}_{\mathcal{F}}$ is the set of all the configurations such that no element of $\mathcal{F}$ occurs in any of the elements of $\mathsf{X}_{\mathcal{F}}$.*

It is a well known result (see [3] and [8]) that $\mathsf{X}_{\mathcal{F}}$ is a shift subspace for every set $\mathcal{F}$ of patterns and that every shift subspace X has a *characterizing set of forbidden patterns* $\mathcal{F}$ such that $X = \mathsf{X}_{\mathcal{F}}$.
If $X = \mathsf{X}_{\mathcal{F}}$ for a finite set $\mathcal{F}$, we say that X is *of finite type*: in this case, it is not restrictive to suppose $\mathcal{F} \subseteq A^{D_M^G}$ for some $M \geq 0$. The shift X of the example above is obviously of finite type: indeed, if xyz is the pattern $p \in A^{D_1^{\mathbb{Z}}}$ such that $p_{-1} = x$, $p_0 = y$ and $p_1 = z$, then $X = \mathsf{X}_{\{011,110,111\}}$.

Definition 2.4 *Let $\mathcal{C} = A^G$, A alphabet, G finitely generated group. A function $F : \mathcal{C} \to \mathcal{C}$ is* local *if there exist a number $r \in \mathbb{N}$ and a function $f : A^{|D_r^G|} \to A$ such that, for any $g \in G$,*

$$(F(c))_g = f\left(\langle c_h \rangle_{h \in D_r^G(g)}\right) \tag{3}$$

The number r is called the range *of the local function F.*

Of course, if F is local of range r, then F is local of range r' for every $r' \geq r$.
The well known *Hedlund's Theorem* (see [4], [8], or [3]) states that F is local if and only if F is continuous and commutes with the "natural" action (2).
Observe that Φ_g is local if and only if g commutes with every other element of G.
If F is local and *invertible*, then F^{-1} is local too. This fact, known as

Richardson's Lemma in the classical case (see [9]), depends on Hedlund's Theorem and the easily proven fact that a continuous invertible function between compact metric spaces has a continuous inverse.

Definition 2.5 *Let $\mathcal{C} = A^G$, A alphabet, G finitely generated group. A* cellular automaton over *G is a triple $\langle X, r, f\rangle$ where $X \subseteq \mathcal{C}$ is a shift subspace, $r \geq 0$ an integer, f a function from $A^{|D_r^G|}$ into A such that the function F defined by (3) satisfies $F(X) \subseteq X$.*
A is called the alphabet *of the cellular automaton. G is called the* tessellation group *of the cellular automaton. f is called the* local evolution function *of the cellular automaton. The function $F : X \to X$ defined by (3) is called the* global evolution function *of the cellular automaton.*

Roughly speaking, a cellular automaton can be seen as a network of identical devices placed on the nodes of the Cayley graph of its tessellation group, each one outputting signals in the alphabet at integer time steps in a way such that output of a device at a given time depends only on the output of "neighboring" devices at the previous time.
If X is of finite type, we will say that $\langle X, r, f\rangle$ is of finite type.

Local evolution functions of cellular automata must not be confused with local functions over configurations: indeed, the global evolution function of a cellular automaton is local because it is defined from a local evolution function.

3 Semi-direct products of groups and conjugate cellular automata

Definition 3.1 *Let H and K be groups. Let τ be a homeomorphism of H into the group* $\mathrm{Aut}(K)$ *of automorphisms of K. The* semi-direct product of H by K with respect to *τ is the group $H \ltimes_\tau K$ of the ordered pairs (h, k), $h \in H$, $k \in K$, with the operation $(h_1, k_1)(h_2, k_2) = (h_1 h_2, \tau_{h_2}(k_1)k_2)$. If $\tau_h = \mathrm{id}_K$ for every $h \in H$, we speak of* direct product of H and K *and simply write $H \times K$.*

It is not hard to prove that $H \ltimes_\tau K$ is a group, just remember that for homomorphisms the product of α and β is $\beta \circ \alpha$, hence $\tau_{h_1 h_2} = \tau_{h_2} \circ \tau_{h_1}$. Definition 3.1 easily extends to products with a finite number of factors.

It is well known that every finitely generated Abelian group is isomorphic to a finite direct product of cyclic groups; that is, for every finitely generated Abelian group G there exist $N, n_1, \ldots, n_k$ such that $G \cong \mathbb{Z}^N \times \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$. The number N is called the *rank* of the finitely generated Abelian group G; isomorphic finitely generated Abelian groups have the same rank.
If H is generated by S and K is generated by T, then $H \times K$ is generated by $(S \times \{1_K\}) \cup (\{1_H\} \times T)$. This is still true for semi-direct products because of:

Lemma 3.2 *Let H, K be groups. Let $\tau : H \to \mathrm{Aut}(K)$ be a homomorphism. Then in $H \ltimes_\tau K$, for every $h, i \in H$, $k, j \in K$, we have:*

1. $(h, 1_K)(i, j) = (hi, j) = (h, k)(i, \tau_i(k^{-1})j)$
2. $(h, k)(i, j) = (h, 1_K)(i, \tau_i(k)j)$
3. $(h, k)(1_H, j) = (h, kj)$

Proof:
Immediate consequence of the definition and of the fact that τ is a homomorphism, so in particular $\tau_{1_H} = \mathrm{id}_K$ and $\tau_h(1_K) = 1_K$ for all $h \in H$. $\square$
From Lemma 3.2 follows that, if $h = s_1 s_2 \ldots s_n$ and $k = t_1 t_2 \ldots t_m$, then $(h, k) = (s_1, 1_K)(s_2, 1_K) \ldots (s_n, 1_K)(1_H, t_1)(1_H, t_2) \ldots (1_H, t_m)$. From now on, given a set S of generators for H and a set T of generators for K, we will always consider the semi-direct product $H \ltimes_\tau K$ as generated by $(S \times \{1_K\}) \cup (\{1_H\} \times T)$.

Definition 3.3 *Let $\langle X, r, f\rangle$ be a cellular automaton with alphabet A and tessellation group G, and $\langle X', r', f'\rangle$ be a cellular automaton with alphabet A' and tessellation group G'. Let F and F' be the global evolution functions of $\langle X, r, f\rangle$ and $\langle X', r', f'\rangle$ respectively. We say that $\langle X, r, f\rangle$ and $\langle X', r', f'\rangle$ are* conjugate *if there exists a homeomorphism $\varphi : X \to X'$ such that $\varphi \circ F = F' \circ \varphi$. The map φ is called a* conjugacy *between $\langle X, r, f\rangle$ and $\langle X', r', f'\rangle$.*

Our goal is, given a cellular automaton of a certain kind, to find a conjugate cellular automaton with a less complicated tessellation group. To do this, we plan to transfer some of the complexity of the structure from the tessellation group to the alphabet. This is possible if the tessellation group has a *finite*

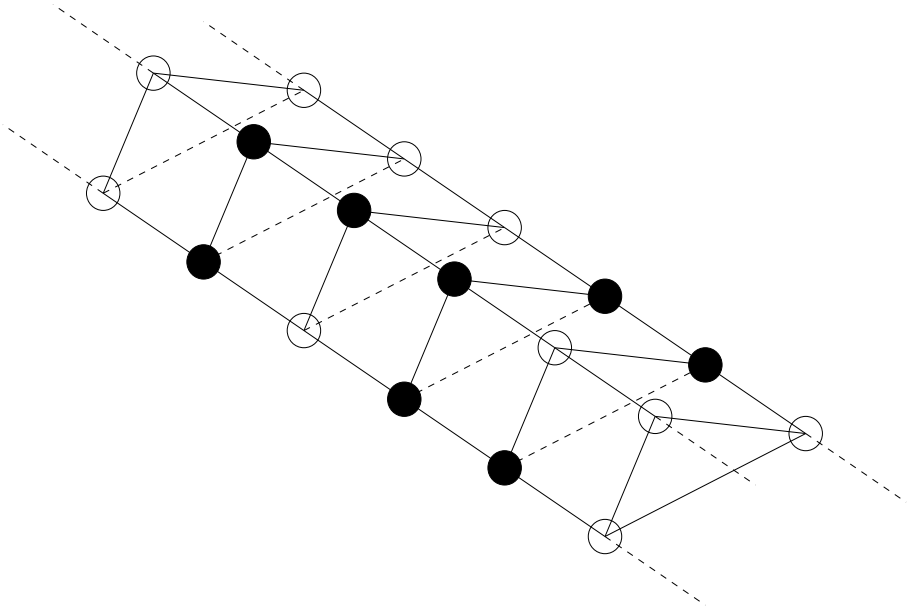

Figure 1: A configuration of a cellular automaton with tessellation group $\mathbb{Z} \times \mathbb{Z}_3$ and alphabet $\{0, 1\}$. White represents 0 and black 1.

part, in the sense that it is isomorphic to a product $H \ltimes_\tau K$ with H finitely generated and K finite.
We start by observing an intuitive but interesting property.

Proposition 3.4 *Let $\mathcal{C} = A^G$, A alphabet, G finitely generated group. Suppose $G \cong H \ltimes_\tau K$ with H finitely generated and K finite. Put $\mathcal{C} = A^G = A^{H \ltimes_\tau K}$, $\mathcal{C}' = \left(A^K\right)^H$. Then the map $\varphi : \mathcal{C} \to \mathcal{C}'$ given by:*

$$((\varphi(c))_h)_k = c_{(h,k)} \quad \forall h \in H \; \forall k \in K \tag{4}$$

is a homeomorphism.

Proof:
We observe that, since K is finite, A^K is an alphabet and the product topology is actually the discrete one.
The map φ is invertible, its inverse ψ being given by:

$$(\psi(c'))_{(h,k)} = ((c')_h)_k \quad \forall k \in K \; \forall h \in H \tag{5}$$

Suppose that c_1 and c_2 agree on $D^{H \ltimes_\tau K}_{r+|K|}$. Let $h \in D^H_r$: there is a writing of h as product of elements of S having at most length r. Let $k \in K$: every

writing of k as a product of elements of T having minimal length cannot have more than $|K|$ elements, because if $k = t_1 t_2 \dots t_n$ with $n > |K|$, then there exist i and $j > i$ such that $t_1 \dots t_i = t_1 \dots t_j$, so that $k = t_1 \dots t_i t_{j+1} \dots t_n$ is a shorter writing; but this implies that (h,k) has a writing of length at most $r + |K|$ as a product of elements of $(S \times \{1_K\}) \cup (\{1_H\} \times T)$. Hence, for all $k \in K$,

$$((\varphi(c_1))_h)_k = (c_1)_{(h,k)} = (c_2)_{(h,k)} = ((\varphi(c_2))_h)_k$$

and so $(\varphi(c_1))_h = (\varphi(c_2))_h$. This proves that, if c_1 and c_2 agree on $D^{H \ltimes_\tau K}_{r+|K|}$, then $\varphi(c_1)$ and $\varphi(c_2)$ agree on D^H_r: hence φ is continuous.
Now, suppose that c'_1 and c'_2 agree over D^H_r. Let $(h,k) \in D^{H \ltimes_\tau K}_r$. Let $(h,k) = (h_1,k_1) \dots (h_n,k_n)$ be a writing of (h,k) as product of elements of $(S \times \{1_K\}) \cup (\{1_H\} \times T)$ of minimal length n: then $h = h_1 \dots h_n$ is a writing of h as a product of elements of $S \cup \{1_H\}$ of length $n \leq r$, so there must exist a writing of k as a product of elements of S of length $m \leq n \leq r$. Hence $h \in D^H_r$ and so:

$$(\psi(c'_1))_{(h,k)} = ((c'_1)_h)_k = ((c'_2)_h)_k = (\psi(c'_2))_{(h,k)}$$

This proves that, if c'_1 and c'_2 agree on D^H_r, then $\psi(c'_1)$ and $\psi(c'_2)$ agree on $D^{H \ltimes_\tau K}_r$: hence ψ is continuous. $\square$
The homeomorphism of Proposition 3.4 has an important property.

Proposition 3.5 *Let $\mathcal{C}$, $\mathcal{C}'$ and φ as in Proposition 3.4. Let $X \subseteq \mathcal{C}$.*

1. *If X is a shift subspace, then $\varphi(X) \subseteq \mathcal{C}'$ is a shift subspace.*
2. *If X is a shift of finite type, then $\varphi(X)$ is a shift of finite type.*

To prove this, we make use of

Lemma 3.6 *Let H, K, $\mathcal{C}$, $\mathcal{C}'$, φ and ψ as in Proposition 3.4. Let $h \in H$.*

1. *For every $c \in \mathcal{C}$, $(\varphi(c))^h = \varphi(c^{(h,1_K)})$.*
2. *For every $c' \in \mathcal{C}'$, $(\psi(c'))^{(h,1_K)} = \psi((c')^h)$.*

Proof:
Let $i \in H$, $j \in K$. Then by part 1 of Lemma 3.2:

$$(((\varphi(c))^h)_i)_j \;=\; ((\varphi(c))_{hi})_j$$

$$
\begin{aligned}
&= c_{(hi,j)} \\
&= c_{(h,1_K)(i,j)} \\
&= \left(c^{(h,1_K)}\right)_{(i,j)} \\
&= \left(\left(\varphi(c^{(h,1_K)})\right)_i\right)_j
\end{aligned}
$$

and:

$$
\begin{aligned}
\left(\left(\psi(c')\right)^{(h,1_K)}\right)_{(i,j)} &= \left(\psi(c')\right)_{(h,1_K)(i,j)} \\
&= \left(\psi(c')\right)_{(hi,j)} \\
&= \left((c')_{hi}\right)_j \\
&= \left(\left((c')^h\right)_i\right)_j \\
&= \left(\psi\left((c')^h\right)\right)_{(i,j)}
\end{aligned}
$$

From the arbitrariness of i and j the thesis follows. $\square$

Proof of Proposition 3.5:

Since φ is a homeomorphism, $Y = \varphi(X)$ is compact in $\mathcal{C}'$.

Let $c' \in Y$: then $c' = \varphi(c)$ for one and only one $c \in X$. Let $h \in H$: by Lemma 3.6 we have $(c')^h = (\varphi(c))^h = \varphi(c^{(h,1_K)})$. But $c^{(h,1_K)} \in X$ because $c \in X$ and X is a subshift: hence $(c')^h \in Y$. From the arbitrariness of $c' \in Y$, $h \in H$ follows that $Y \subseteq \mathcal{C}'$ is a shift subspace.

This proves point 1.

Suppose $X = \mathsf{X}_{\mathcal{F}}$ for a finite set $\mathcal{F}$: we can suppose $\mathcal{F} \subseteq A^{D_M^G}$ for some $M \geq 0$. Put:

$$
\begin{aligned}
\mathcal{F}' = \Big\{ & p' \in (A^K)^{D_M^H} : \exists p \in \mathcal{F} : \exists k \in K : \\
& \forall i \in H : \forall j \in K : (i,j) \in D_M^G \rightarrow (p'_i)_{\tau_i(k)j} = p_{(i,j)} \Big\}
\end{aligned}
$$

$\mathcal{F}' \subseteq (A^K)^{D_M^H}$ is clearly finite; we want to show that $\varphi(X) = \mathsf{X}_{\mathcal{F}'}$.

Suppose $c' \notin \varphi(X)$. Then $\psi(c') \notin X$, so there are $g = (h,k) \in G$, $p \in \mathcal{F}$ such that $\left((\psi(c'))^g\right)_{|D_M^G} = p$. Put $(p'_i)_j = \left(\left(\psi(c')\right)^{(h,1_K)}\right)_{(i,j)}$ for $i \in D_M^H$, $j \in K$: from point 2 of Lemma 3.2 follows that if $(i,j) \in D_M^G$ then $(p'_i)_{\tau_i(k)j} = \left(\left(\psi(c')\right)^{(h,1_K)}\right)_{(i,\tau_i(k)j)} = \left(\left(\psi(c')\right)^{(h,k)}\right)_{(i,j)} = p_{(i,j)}$ so that $p' \in \mathcal{F}'$; moreover, for all $i \in D_M^H$, $j \in K$ we have $\left(\left((c')^h\right)_i\right)_j = \left(\left(\psi(c')\right)^{(h,1_K)}\right)_{(i,j)} = (p'_i)_j$, so the pattern $p' \in \mathcal{F}'$ occurs in c'.

Suppose that a pattern $p' \in \mathcal{F}'$ occurs in c'. Then there is $h \in H$ such that, for every $i \in D_M^H$, $j \in K$ we have $\left(\left((c')^h\right)_i\right)_j = (p'_i)_j$. In particular, given the structure of $\mathcal{F}'$, there are $p \in \mathcal{F}$, $k \in K$ such that, for every $i \in H$, $j \in K$

such that $(i,j) \in D_M^G$, we have $((\psi(c'))^{(h,1_K)})_{(i,\tau_i(k)j)} = p_{(i,j)}$. But then by point 2 of Lemma 3.2 $((\psi(c'))^{(h,k)})_{(i,j)} = p_{(i,j)}$ for every $i \in H$, $j \in K$ such that $(i,j) \in D_M^G$: thus $\psi(c') \notin \mathsf{X}_{\mathcal{F}} = X$ and so $c' \notin \varphi(X)$.
This proves point 2. $\square$
We observe that Proposition 3.5 cannot be reversed, because $\psi(Y)$ can possibly not be a shift subspace of $\mathcal{C}$, even if $Y \subseteq \mathcal{C}'$ is a shift of finite type and the product is direct. (This is not surprising, because a less complicated tessellation group means less restrictive conditions for commutation with the group action.)
To prove this, take $H = \mathbb{Z}$, $K = \mathbb{Z}_2$, $A = \{a,b\}$. Let $f_{xy} : \mathbb{Z}_2 \to A$ be the function such that $f_{xy}(0) = x$, $f_{xy}(1) = y$: then $A^{\mathbb{Z}_2} = \{f_{aa}, f_{ab}, f_{ba}, f_{bb}\}$. Let $Y = \{c' \in (A^{\mathbb{Z}_2})^{\mathbb{Z}} : ((c')_h)_1 = b \ \forall h \in \mathbb{Z}\}$: then $Y = \mathsf{X}_{\{0 \mapsto f_{aa}, 0 \mapsto f_{ba}\}}$ is a shift of finite type. But $\psi(Y) = \{c \in A^{\mathbb{Z} \times \mathbb{Z}_2} : c_{(h,1)} = b \ \forall h \in \mathbb{Z}\}$ is not a shift subspace, because if $\bar{c} \in A^{\mathbb{Z} \times \mathbb{Z}_2}$ is such that $\bar{c}_{(h,k)} = a$ if $k = 0$ and $\bar{c}_{(h,k)} = b$ if $k = 1$, then $\bar{c} \in \psi(Y)$ but $\bar{c}^{(0,1)} \notin \psi(Y)$.

The way to the main result of this paper is now paved.

Theorem 3.7 *Let G be a finitely generated group. If $G \cong H \ltimes_\tau K$ with H finitely generated and K finite, then every cellular automaton $\langle X, r, f\rangle$ over G is conjugate to a cellular automaton $\langle X', r', f'\rangle$ over H in a way such that, if $\langle X, r, f\rangle$ is of finite type, then $\langle X', r', f'\rangle$ is of finite type too.*

Proof:
Let $\langle X, r, f\rangle$ be a cellular automaton over $G \cong H \ltimes_\tau K$. Let F be its global evolution function. Let $\mathcal{C}$, $\mathcal{C}'$, φ and ψ as in Proposition 3.4.
By Proposition 3.5, $\varphi(X)$ is a shift subspace of $\mathcal{C}'$ and is of finite type if X is of finite type. We define $F' : \mathcal{C}' \to \mathcal{C}'$ by $F' = \varphi \circ F \circ \psi$. Since F sends X into X, F' sends $\varphi(X)$ into $\varphi(X)$;
Suppose we know c'_i for every $i \in D^H_{r+|K|}(h)$.
Then, for every $k \in K$ we know the value of $(c'_i)_k \in A$ for every $i \in D^H_{r+|K|}(h)$.
Then, *a fortiori*, we know the value of $\psi(c')_{(i,k)}$ for every $i \in H$, $k \in K$ such that $(i,k) \in D^{H \ltimes_\tau K}_{r+|K|}((h, 1_K))$.
This is sufficient to compute $(F(\psi(c')))_{(h,k)}$ for every $k \in K$.
This means that $(\varphi(F(\psi(c')))_h)_k$ is determined for every $k \in K$.
As a consequence, if we know c'_u for every $u \in D^H_{r+|K|}(h)$, then we know

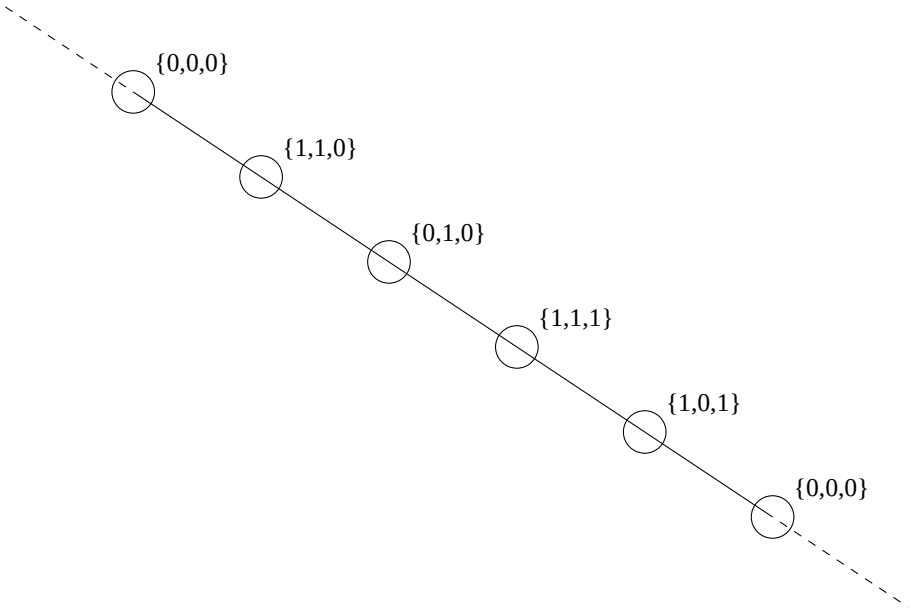

Figure 2: The cellular automaton with tessellation group $\mathbb{Z}$ and alphabet $\{0,1\}^{\mathbb{Z}_3}$ conjugate to the cellular automaton of Figure 1 constructed with the technique of Theorem 3.7. The configuration corresponds to that of Figure 1 too.

$(F'(c'))_h$.
This proves that F' is local with range $r' \leq r + |K|$. Let f' be such that $(F'(c'))_h = f'\left(\langle c'_u \rangle_{u \in D^H_{r'}(h)}\right)$: then $\langle X, r, f\rangle$ and $\langle \varphi(X), r', f'\rangle$ are conjugate, $\varphi_{|X}$ being a conjugacy between the two cellular automata. $\square$
Another way to prove that F' is local is by showing that it commutes with the action of H over A^K: since F' is continuous by construction, the thesis follows by Hedlund's Theorem. Indeed, for every $c \in (A^K)^H$, $h \in H$ we have by Lemma 3.6:

$$\begin{aligned} F'(c^h) &= \varphi(F(\psi(c^h))) \\ &= \varphi(F((\psi(c))^{(h,1_K)})) \\ &= \varphi((F(\psi(c)))^{(h,1_K)}) \\ &= (\varphi(F(\psi(c))))^h \\ &= (F'(c))^h \end{aligned}$$

4 The invertibility problem

A cellular automaton is *invertible* if its global evotion function is bijective. Invertible cellular automata represent a vast area of research, and are the subject of the monograph [11].
Let $X \subseteq \mathcal{C}$ be a shift subspace. The *invertibility problem* for X states: given a cellular automaton of the form $\langle X, r, f \rangle$, determine if its global evolution function is bijective. If X is the full shift, we speak of *invertibility problem over G*.
It has been proved by Amoroso and Patt in [1] that this problem is decidable if the tessellation group is $\mathbb{Z}$; [3] contains an extension to the case of shifts of finite type. On the other hand, Kari in [7] proved that the problem is undecidable if the tessellation group is $\mathbb{Z}^2$ (and hence if it has the form $H \times \mathbb{Z}^2$ for some group H: in particular, if it is isomorphic to $\mathbb{Z}^d$ with $d > 1$). Moreover, the problem is obviously decidable if the tessellation group is finite, because in this case the set of possible F's is finite and we only need to check if a finite set of functions contains the inverse of the automaton's.
This almost covers all possible Abelian finitely generated groups, with the exception of those of the form $\mathbb{Z} \times \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$.
We are going to show that, in this last case, the invertibility problem is decidable. To do this, we prove:

Theorem 4.1 *If τ is computable and if the word problem is decidable over H and $H \ltimes_\tau K$, then the construction of f' from f in Theorem 3.7 is computable.*

Before proving the theorem, we make some considerations on its hypotheses. First of all, we observe that the computability of τ is a necessary condition for the product of $H \ltimes_\tau K$ to be computable.
Next, we briefly speak about the *word problem*. Given a finitely generated group G and a finite set S of generators for G, we say that the word problem is decidable over G if the set of all the finite sequences over $S \cup S^{-1}$ that reduce to the empty word is recursive. Equivalently, decidability of the word problem means that an algorithm exists to decide if two finite sequences of symbols over $S \cup S^{-1}$ represent the same element of the group. The list of groups with decidable word problem is not too restricted, since it includes finite groups, free groups, and finite direct products of groups with decidable word problem: in particular, every finitely generated Abelian group has a decidable word problem.
Proof of Theorem 4.1:

The proof of Theorem 3.7 already contains a suggestion for the construction algorithm. We are now going to explain it in detail.
We choose to represent $(F'(c'))_h$ by the sequence of its values $((F'(c'))_h)_k$, for k in K. Our procedure is:

INPUT: the list $\langle (c')_i \rangle_{i \in D^H_{r+|K|}(h)}$
OUTPUT: the value $(F'(c'))_h$

$X =$ an empty list
for k in K:
    $s =$ a list of $|D_r^{H \ltimes_\tau K}|$ elements of A
    for i in $D^H_{r+|K|}(h)$:
        for j in K:
            if (i,j) in $D_r^{H \ltimes_\tau K}((h,k))$:
                replace with $((c')_i)_j$ the element of s
                in the position corresponding to $(h,k)^{-1}(i,j)$
                in the defined ordering of $D_r^{H \ltimes_\tau K}$
            end if
        end for
    end for
    append $f(s)$ to X
end for
return X

First of all, we observe that, since τ is computable, the multiplications are all computable, and because the word problem is decidable over H and over $H \ltimes_\tau K$, the fact that an element appears in a finite subset of one of these groups is obviously decidable; so our procedure is actually an algorithm. We must now show that it correctly computes $(F'(c'))_h$.
We observe that:

$$(F(c))_{(h,k)} = f\left(\left\langle c_{(i,j)} \right\rangle_{(i,j) \in D_r^{H \ltimes_\tau K}((h,k))}\right)$$

thus:

$$\begin{aligned}(F(\psi(c')))_{(h,k)} &= f\left(\left\langle (\psi(c'))_{(i,j)} \right\rangle_{(i,j) \in D_r^{H \ltimes_\tau K}((h,k))}\right) \\ &= f\left(\left\langle (c'_i)_j \right\rangle_{(i,j) \in D_r^{H \ltimes_\tau K}((h,k))}\right)\end{aligned}$$

and so:

$$((F'(c'))_h)_k = f\left(\langle (c'_i)_j \rangle_{(i,j)\in D_r^{H\ltimes_\tau K}((h,k))}\right)$$

But for each k in K, the cycle over i transforms the sequence s in the sequence $\langle (c'_i)_j \rangle_{(i,j)\in D_r^{H\ltimes_\tau K}((h,k))}$, because if $(i,j) \in D_r^{H\ltimes_\tau K}((h,k))$ then surely $i \in D_{r+|K|}^H$ and $j \in K$, so that the double iteration over i and j surely catches all the elements in $D_r^{H\ltimes_\tau K}((h,k))$: hence the next instruction appends to the list X precisely the value $f\left(\langle (c'_i)_j \rangle_{(i,j)\in D_r^{H\ltimes_\tau K}((h,k))}\right) = ((F'(c'))_h)_k$. In the end, the returned list X is precisely the sequence $((F'(c'))_h)_{k_1} \dots ((F'(c'))_h)_{k_{|K|}}$.
□

From Theorems 3.7 and 4.1 we obtain:

Theorem 4.2 *Let $G \cong H \ltimes_\tau K$, with H finitely generated and K finite. Suppose that τ is computable, and the word problem is decidable over H and over $H \ltimes_\tau K$. Then the following are true:*

1. *If invertibility of cellular automata over H is decidable, then invertibility of cellular automata over G is decidable too.*
2. *If invertibility of cellular automata of finite type with tessellation group H is decidable, then invertibility of cellular automata of finite type with tessellation group G is decidable too.*

Theorems 3.7 and 4.1 give us a technique to decide the invertibility of a cellular automaton over a finitely generated Abelian group with rank 1, because in this case the conditions over $\tau \equiv \mathrm{id}_K$, $H = \mathbb{Z}$ and $H \ltimes_\tau K = \mathbb{Z} \times K$ are trivially satisfied.
Consider a cellular automaton whose tessellation group is $\mathbb{Z} \times \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$: by applying Theorem 3.7 with $H = \mathbb{Z}$ and $K = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ we find a conjugate cellular automaton over $\mathbb{Z}$, and the construction is computable because of Theorem 4.1. But because of Amoroso and Patt's theorem, invertibility for the new cellular automaton is decidable, and because of conjugacy, it is equivalent to invertibility of the original cellular automaton.
This, together with Kari's theorem, proves:

Theorem 4.3 *Let G be a finitely generated Abelian group. Then invertibility for cellular automata over G is decidable if and only if G has at most rank 1.*

We remark that our procedure is applicable even if the tessellation group is not Abelian. For example, invertibility of cellular automata with tessellation group $\mathbb{Z} \times S_3$, where S_3 is the group of permutation of three distinct objects, is still decidable. We state this in our last claim, extending those of Section 1.6 of [3].

Theorem 4.4 *Let $G \cong \mathbb{Z} \ltimes_\tau K$ with K finite. Let A be an alphabet. Let $X \subseteq A^G$ be a shift of finite type. Then the invertibility problem for X is decidable.*

5 Conclusions

Theorem 3.7 says that the "finite part" of the tessellation group is unessential to the dynamics, because it can be seen as a component of the alphabet instead of the group. This implies that the Abelian case essentially reduces to the classical case, where the tessellation group is finite or is $\mathbb{Z}^d$ for some $d > 0$: hence, study of "non-classical" cellular automata dynamics should be oriented to the case of non-Abelian tessellation group.
On the other hand, Theorem 4.2 says that the question of the decidability of the invertibility problem has a known answer for cellular automata over Abelian groups: further study of the question should then consider either special subcases of the classical case or cellular automata over non-Abelian groups; in this last case, the most interesting groups are perhaps the free groups with two or more (but still finitely many) generators.

6 Acknowledgements

We thank Francesco Aprea, Tullio Ceccherini-Silberstein, Francesca Fiorenzi, Antonio Machì, Patrizia Mentrasti, and Andrea Sambusetti for the many helpful discussions, suggestions, and encouragement.

References

[1] S. Amoroso, Y. N. Patt, Decision Procedures for Surjectivity and Injectivity of Parallel Maps for Tessellation Structures, *J. Comp. Syst. Sci.* **6** (1972) 448-464

[2] A. Clementi, P. Mentrasti, P. Pierini, Some Results on Invertible Cellular Automata, *Complex Systems* **9** (1995) 235-250

[3] F. Fiorenzi, Cellular Automata and Finitely Generated Groups, *Tesi di Dottorato, Dipartimento di Matematica "Guido Castelnuovo", Università degli Studi di Roma "La Sapienza", 2000*

[4] G. A. Hedlund, Endomorphisms and Automorphisms of the Shift Dynamical System, *Math. Syst. Th.* **3** (1969) 320-375

[5] G. Jacopini, P. Mentrasti, Generation of Invertible Functions, *Theoretical Computer Science* **66** (1989) 289-287

[6] G. Jacopini, P. Mentrasti, G. Sontacchi, Reversible Turing Machines and Polynomial Time Reversibly Computable Functions, *SIAM J. Disc. Math.* **3** (1990) 241-254

[7] J. Kari, Reversibility of 2D Cellular Automata is Undecidable, *Physica D* **45** (1990) 379-385

[8] D. Lind, B. Marcus, An Introduction to Symbolic Dynamics and Coding, Cambridge University Press (1995)

[9] D. Richardson, Tessellations with Local Transformations, *J. Comp. Syst. Sci.* **6** (1972) 373-388

[10] T. Toffoli, Cellular Automata Mechanics, *Ph.D. Thesis, Technical Report No. 208, University of Michigan, 1977*

[11] T. Toffoli, N. Margolus, Invertible Cellular Automata: A Review, *Physica D* **45** (1990) 229-253