Topological rigidity of linear cellular automaton shifts

Journal Item

TOPOLOGICAL RIGIDITY OF LINEAR CELLULAR AUTOMATON SHIFTS

ROBBERT FOKKINK AND REEM YASSAWI

Abstract. We prove that topologically isomorphic linear cellular automaton shifts are algebraically isomorphic. Using this, we show that two distinct such shifts cannot be isomorphic. We conclude that the automorphism group of a linear cellular automaton shift is a finitely generated abelian group.

1. Introduction

A full shift consists of a space, the set of doubly infinite sequences $\{1, 2, \ldots, q\}^{\mathbb{Z}}$, and the transformation σ acting on points in that space, defined by $\sigma(x)_n = x_{n+1}$. A multi-dimensional shift is defined analagously, where the space $\{1, 2, \ldots, q\}^{\mathbb{Z}^d}$ is acted on by d shifts, defined by

$$\sigma_i(x)_{(n_1,\ldots,n_i,\ldots,n_d)} = x_{(n_1,\ldots,n_i+1,\ldots,n_d)}$$

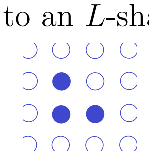
for transformations $\sigma_1, \sigma_2, \ldots, \sigma_d$. A *subshift* is a closed, shift-invariant subset of a full shift. It is *Markov* if it is a shift of finite type. We refer to [LM95] for definitions and the basic topological set-up.

In symbolic dynamics $\{1, \ldots, q\}$ is a finite set with no additional structure. In algebraic dynamics $\{1, \ldots, q\}$ is a finite abelian group or a finite field. In this paper, we limit ourselves to the simplest case, when q is prime. To emphasize this, we write p from now on, instead of q, and we denote the finite field by $\mathbb{F}_p$. Thus $\{1, 2, \ldots, p\}^{\mathbb{Z}^d}$ becomes a compact abelian group under coordinatewise addition $\mathbb{F}_p^{\mathbb{Z}^d}$. A *Markov subgroup* is a subshift that is also an additive subgroup of $\mathbb{F}_p^{\mathbb{Z}^d}$. Any such group is a shift of finite type. A very nice survey of Markov groups is given in [Kit97]. One motivation of our paper is to try and find topological analogues of the metric results in that survey.

The standard example of a Markov subgroup is the *Ledrappier shift* [Led79] defined by

$$\Lambda = \{(x)_{(m,n)} \colon x_{(m,n)} + x_{(m+1,n)} + x_{(m,n+1)} = 0 \text{ for each } i, j \in \mathbb{Z}^2\} \subset \{0, 1\}^{\mathbb{Z}^2}.$$

The defining relation of Λ corresponds to an L-shape in the lattice $\mathbb{Z}^2$:



1991 *Mathematics Subject Classification.* Primary 37B10, Secondary 37B05, 37B15.

Key words and phrases. Algebraic dynamics, endomorphisms and automorphisms of compact abelian $\mathbb{Z}^d$ actions, Automorphism groups.

It is convenient to identify $(c_{(i_1,\ldots,i_d)}) \in \mathbb{F}_p^{\mathbb{Z}^d}$ with the formal Laurent series

$$\sum_{(i_1,\ldots,i_d)\in\mathbb{Z}^d} c_{i_1,\cdots,i_d} X_1^{i_1}\cdots X_d^{i_d}.$$

The shift σ_i is given by the multiplication by X_i^{-1}. We denote the set of all Laurent series by $\mathbb{F}_p[[X_1^{\pm 1},\ldots,X_d^{\pm 1}]]$. A *Laurent polynomial* is a Laurent series in which all but finitely many coefficients are zero. We denote the set of Laurent polynomials by $\mathbb{F}_p[X_1^{\pm 1},\ldots,X_d^{\pm 1}]$. It is a unique factorization domain and the set of Laurent series $\mathbb{F}_p[[X_1^{\pm 1},\ldots,X_d^{\pm 1}]]$ is a module over this domain. A Markov subgroup is a subgroup of $\mathbb{F}_p[[X_1^{\pm 1},\ldots,X_d^{\pm 1}]]$ which is invariant under multiplication by X_i, i.e., it is a submodule. The annihilator of a Markov subgroup M is the ideal of all polynomials P such that $Px = 0$ for each $x \in M$. Annihilator are finitely generated since $\mathbb{F}_p[[X_1^{\pm 1},\ldots,X_d^{\pm 1}]]$ is Noetherian. We will be interested in particular in submodules $P^\perp$ that have an annihilator that is generated by a single polynomial P. For example, with this notation, the Ledrappier shift is equal to $\left(1 + X_1^{-1} + X_2^{-1}\right)^\perp$.

Two Markov shifts M_1 and M_2 are *isomorphic* if there exists an invertible map $\phi\colon M_1 \to M_2$ which is shift commuting, i.e., $\phi\circ\sigma_i = \sigma_i\circ\phi$ for all i. If ϕ is a homeomorphism, then it is a *topological isomorphism.* If ϕ is measure preserving, then it is a *measurable isomorphism.* If M_1 and M_2 are Markov subgroups and ϕ is an isomorphism between modules, then it is an *algebraic isomorphism.* An algebraic isomorphism is continuous and preserves the Haar probability measure, which is the only measure we consider. Kitchens conjectured that if $P^\perp$ and $Q^\perp$ are measurably isomorphic, then they are algebraically isomorphic [Kit97]. This conjecture has been proved for irreducible and strongly mixing $P^\perp$ and $Q^\perp$:

Theorem 1 (Kitchens-Schmidt, [KS00])**.** *Suppose that P and Q are irreducible elements of $\mathbb{F}_p[X_1^{\pm 1},\ldots,X_d^{\pm 1}]$. If $P^\perp$ and $Q^\perp$ are measurably isomorphic and strongly mixing, then they are algebraically isomorphic.*

We are interested in the topological version of Kitchens's conjecture. We were unable to settle this topological version in full generality, and restrict our attention to polynomials of the following form: if

$$P = X_d - \Phi(X_1,\ldots,X_{d-1})$$

then we say that $P^\perp$ is a *linear cellular automaton shift.* Points of a linear cellular automaton shift, that is specific two dimensional configurations in these shifts, have been studied by many, for example by Martin, Odlyzko and Wolfram in [MOW84]. To our knowledge it is Ledrappier who first studied a particular such Markov group, and Kitchens and Schmidt who first studied these shifts in full generality. We require that Φ contains at least two non-zero terms, otherwise the shift would be trivial. For cellular automaton shifts it is customary to decompose the module $\mathbb{F}_p[[X_1^{\pm 1},\ldots,X_d^{\pm 1}]]$ into layers which are indexed by powers of X_d. The powers of X_d form the *time axis.* One imagines layers to be changing over time. An individual time step from one layer to the next corresponds to a multiplication by $\Phi(X_1,\ldots,X_{d-1})$.

In this article, we show in Theorem 13 that topologically isomorphic linear cellular automaton shifts are algebraically isomorphic. We apply this result to deduce, in Corollary 14, that distinct linear cellular automaton shifts cannot be topological factors of one another. We also show in Corollary 15 that the automorphism group of a linear cellular automaton shift is finitely generated and abelian.

2. Mixing

A probability measure preserving system $(X, \mathcal{B}, \mu, T)$ is $k+1$-*mixing* if for all measurable sets $A_0, \ldots, A_k$

$$\mu(A_0 \cap T^{-n_1} A_1 \cap \cdots \cap T^{-n_k} A_k) \longrightarrow \mu(A_0) \cdots \mu(A_k)$$

as $n_1, n_2 - n_1, \ldots, n_k - n_{k-1} \longrightarrow \infty$. The term strongly mixing is used to refer to 2-mixing. It has been an open problem for some time, due to Rokhlin [Rok49], whether strong mixing implies mixing of all orders.

Let G be a countable abelian group. A G-*system* $(X, \mathcal{B}, \mu, (T_g)_{g \in G})$ is a probability space with a measure preserving G-action. It is $k+1$-mixing if for all measurable sets $A_0, \ldots, A_k$

$$\mu(A_0 \cap T_{-g_1} A_1 \cap \cdots \cap T_{-g_k} A_k) \longrightarrow \mu(A_0) \cdots \mu(A_k)$$

as $g_i \longrightarrow \infty$ and $g_j - g_i \longrightarrow \infty$ for all $i \neq j$. We often abbreviate the notation and denote a G-system simply by X. Let μ be the Haar measure on $P^{\perp}$ and let $\mathcal{B}$ be the Borel σ-algebra. Ledrappier's shift is a $\mathbb{Z}^2$-system which is 2-mixing but not 3-mixing. Another way to define $k+1$-mixing would be that

$$\mu(T_{-g_0} A_0 \cap T_{-g_1} A_1 \cap \cdots \cap T_{-g_k} A_k) \longrightarrow \mu(A_0) \cdots \mu(A_k)$$

as $g_j - g_i \longrightarrow \infty$ for all $i \neq j$. The two definitions are equivalent because T_{g_0} is a measure preserving automorphism.

In our case the probability space is a Markov shift $P^{\perp} \subset \mathbb{F}_p[[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]]$ endowed with the Haar measure and G is equal to $\mathbb{Z}^d$. For $\mathbf{n} \in \mathbb{Z}^d$ the transformation $T_{\mathbf{n}}$ is the group automorphism

$$\sum c_{i_1, \cdots, i_d} X_1^{i_1} \cdots X_d^{i_d} \longrightarrow \sum c_{i_1, \cdots, i_d} X^{i_1 + n_1} \cdots X^{i_d + n_d}$$

if $\mathbf{n} = (n_1, \ldots, n_d)$. In other words, $T_{\mathbf{n}}$ is the multiplication by the monomial with exponent $\mathbf{n}$, which we denote by $X^{\mathbf{n}} = X_1^{n_1} \cdots X_d^{n_d}$.

It is convenient to describe Markov subgroups as modules, but they are also compact abelian groups. We recall Halmos's classical result [Hal43], [Wal82, Theorems 1.10 and 1.28], which is that a continuous automorphism T of a compact abelian group Γ is 2-mixing if and only if the induced automorphism on the character group $\widehat{\Gamma}$ has no finite orbits. Kitchens and Schmidt finesse this characterisation of 2-mixing for algebraic shifts.

Lemma 2. [KS92, Proposition 2.11] *Let $P = P_1 \ldots P_\ell$ for irreducible Laurent polynomials P_i. Then $(P^{\perp}, \mathcal{B}, \mu, T_{\mathbf{n}})$ is not 2-mixing if and only if one of the factors P_i is a polynomial in $X^{\mathbf{m}}$ for some $\mathbf{m} \in \mathbb{Z}^d$.*

Theorem 3. [KS89, Theorem 2.4] *If the algebraic shift $(P^\perp, \mathcal{B}, \mu, T_{\mathbf{n}})$ is 2-mixing for every $\mathbf{n} \in \mathbb{Z}^d$, then the $\mathbb{Z}^d$-system $(P^\perp, \mathcal{B}, \mu, \mathbb{Z}^d)$ is 2-mixing.*

Lemma 2 and Theorem 3 combined with the following lemma imply that a cellular automaton shift $P^\perp$ is 2-mixing.

Lemma 4. *A Laurent polynomial $X_d - \Phi(X_1, \ldots, X_{d-1}) \in \mathbb{F}_p[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]$ is irreducible.*

Proof. We denote the ring of Laurent polynomials in $d-1$ variables by $\mathfrak{R}_{d-1}$. The polynomial $X_d + r$ has degree one and therefore is irreducible in $\mathfrak{R}_{d-1}[X_d]$ for any $r \in \mathfrak{R}_{d-1}$. It remains irreducible in the localization of $\mathfrak{R}_{d-1}[X_d]$ by the multiplicative set $S = \{X_d^n \colon n \in \mathbb{N}\}$. The ring of fractions $S^{-1}\mathfrak{R}_{d-1}$ is equal to $\mathfrak{R}_d$. Therefore $X_d + r$ is irreducible in $\mathfrak{R}_d$. $\square$

If a monomial $X^{\mathbf{n}}$ has a non-zero coefficient in P, then we say that it *occurs* in P. We say that the set

$$S(P) = \{\mathbf{n} \colon X^{\mathbf{n}} \text{ occurs in } P\}$$

is the *shape* of the polynomial. For instance, the shape of the Ledrappier polynomial is equal to $\{(0,0), (-1,0), (0,-1)\}$.

We say that a finite subset $S = \{\mathbf{n}_0, \ldots, \mathbf{n}_k\} \subset \mathbb{Z}^d$ is *mixing* (for the particular action we are considering) if for all measurable sets $A_0, \ldots, A_k$

$$\mu(T_{-m\mathbf{n}_0} A_0 \cap T_{-m\mathbf{n}_1} A_1 \cap \cdots \cap T_{-m\mathbf{n}_k} A_k) \longrightarrow \mu(A_0) \cdots \mu(A_k)$$

as $m \longrightarrow \infty$. Note that S is mixing if and only if any of its translates $\mathbf{n} + S$ is mixing, since $T_{\mathbf{n}}$ is a measure preserving automorphism. Therefore, we may translate S so that it contains 0. We say that S is *primitive* if $0 \in S$. Similarly, we say that P is *primitive* if 0 occurs in P.

If a $\mathbb{Z}^d$-system is $k+1$-mixing, then all primitive sets of cardinality $k+1$ are mixing. The converse is also true but this is not obvious. In fact, this remained an open problem for quite some time, until it was solved by Masser [Mas04]. Ledrappier's shift is 2-mixing but not mixing on $S = \{(0,0), (-1,0), (0,-1)\}$, as follows from the following lemma.

Lemma 5. *$S(P)$ is a non-mixing set of $P^\perp$. More generally, $S(Q)$ is non-mixing for any $Q \in \langle P \rangle$.*

Proof. Without loss of generality we may assume that P is primitive. Consider the cylinder set A of all Laurent series $\sum_{\mathbf{n}} c_{\mathbf{n}} X^{\mathbf{n}}$ which have constant coefficient $c_{\mathbf{0}} = 1$. Similarly, let B be the cylinder set of Laurent series in $P^\perp$ such that $c_{\mathbf{0}} = 0$. Let $\{\mathbf{0}, \mathbf{n}_1, \ldots, \mathbf{n}_k\}$ be the shape of P. The elements of

$$A \cap T_{-\mathbf{n}_1} B \cap \cdots \cap T_{-\mathbf{n}_k} B$$

are exactly those Laurent series L which have constant coefficient 1 and coefficient zero at all other monomials $X^{-\mathbf{n}}$ which occur in P. Therefore $P \cdot L$ has constant coefficient 1. In particular, L is not annihilated by P.

Observe that the shape of P^p is equal to $pS(P)$ and more generally $S(P^{p^n}) = p^n S(P)$. By the same argument as above, the elements of

$$A \cap T_{-p^n \mathbf{n}_1} B \cap \cdots \cap T_{-p^n \mathbf{n}_k} B$$

are not annihilated by P^{p^n} and therefore this intersection is empty in $P^\perp$. We conclude that

$$\mu(T_{-m\mathbf{n}_0}A \cap T_{-m\mathbf{n}_1}B \cap \cdots \cap T_{-m\mathbf{n}_k}B) = 0$$

if $m = p^n$. It follows that $S(P)$ is non-mixing. We have only used that P annihilates $P^\perp$ in this argument. The same proof applies to any $Q \in \langle P \rangle$ since $\langle P \rangle$ is the annihilator of $P^\perp$. ☐

The following deep result of Masser can be found in [KS93, Cor 3.9].

Theorem 6. *Let P be an irreducible Laurent polynomial. A primitive set E is non-mixing for $P^\perp$ if and only if there exist $a, b, \ell \in \mathbb{N}$ and a Laurent polynomial $Q \in \mathbb{F}_{p^\ell}[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]$ with $S(Q) \subset E$, such that $P^{(a)}$ and $Q^{(b)}$ have a common factor.*

Corollary 7. *Let $P^\perp$ be a linear cellular automaton shift with $P = X_d - \Phi(X_1, \ldots, X_{d-1})$. If all elements $(n_1, \ldots, n_d) \in S$ have zero final coordinate $n_d = 0$ then S is mixing.*

Proof. By contradiction. Suppose that S is not mixing. Then $S - \mathbf{n}$ is not mixing for any $\mathbf{n} \in S$. Since $S - \mathbf{n}$ is primitive, there exists a Q with shape $S(Q) \subset S - \mathbf{n}$ such that $Q^{(b)}$ and $P^{(a)}$ have a common factor R for some a, b. Q is a polynomial with indeterminates $X_1, \ldots, X_{d-1}$. Multiplying by a monomial, if necessary, we may assume that R is also a polynomial with indeterminates $X_1, \ldots, X_{d-1}$. Since R divides $P^{(a)}$, which has unit coefficient at X_d^a, we conclude that R divides 1: it is a unit. Therefore $Q^{(b)}$ and $P^{(a)}$ have no common factor. We conclude that S is mixing. ☐

3. Topological rigidity of linear cellular automaton shifts

We study equivariant maps between linear cellular automaton shifts. An equivariant map ϕ between G-systems does not necessarily preserve 0. However, for the systems that we consider here, it is possible to replace an equivariant map that does not preserve 0 by one that does, as follows. Since 0 is fixed so is $\phi(0)$. Therefore the coordinates of $\phi(0)$ are a constant $c \in \mathbb{F}_p \setminus \{0\}$. In other words, $\phi(0) = (c)$, the Laurent series which has coefficient c at every monomial. Since Q annihilates (c), we conclude $Q^\perp$ is closed under subtraction of (c). The map $\bar{\phi}(x) = \phi(x) - (c)$ is equivariant and preserves 0. This shows that the following definition is not restrictive.

Definition 8. We say that a $\mathbb{Z}^d$-equivariant map $\phi\colon P^\perp \to Q^\perp$ is a *homomorphism* if $\phi(0) = 0$. If ϕ is continuous, then we say that it is a *topological homomorphism.* If ϕ is a module homomorphism, then we say that it is an *algebraic homomorphism.*

Let S be a shape. We say that a map $f\colon S \to \mathbb{F}_p$ is a *configuration*, or, more specifically, an *S-configuration.* Configurations are a higher-dimensional analogue of words in shift dynamical systems. If $x \in P^\perp$, then $x|_S$ represents the configuration defined by $s \mapsto x_s$. We say that this configuration *occurs* in $P^\perp$. Let $\mathcal{L}_S(P^\perp)$ be the set of all S-configurations which occur in $P^\perp$. Since $P^\perp$ is a group, $\mathcal{L}_S(P^\perp)$ is a group. A map $\gamma\colon \mathcal{L}_S(P^\perp) \to \mathbb{F}_p$ is called a *coding*, or also a *local rule.* The map

$$(x)_{\mathbf{n}\in\mathbb{Z}^d} \to (\gamma(x|_{\mathbf{n}+S}))_{\mathbf{n}\in\mathbb{Z}^d}$$

is called a *sliding block code*. It is customary to select a shape of the form $\{0,\ldots,m\}^d \subset \mathbb{Z}^d$, i.e., a block, hence the name. Let 0_S denote the zero configuration. A topological homomorphism corresponds to a sliding block code such that $\gamma(0_S) = 0$. The topological homomorphism is a group homomorphism if and only if $\gamma\colon \mathcal{L}_S(P^\perp) \to \mathbb{F}_p$ is a group homomorphism.

Lemma 9. *Let $P^\perp$ be a linear cellular automaton shift on a finite field $\mathbb{F}_p$. Suppose that $\{\mathbf{n}_1,\ldots,\mathbf{n}_k\} \subset \mathbb{Z}^d$ all have final coordinate equal to zero, and that $C_1,\ldots,C_k \in \mathcal{L}_S(P^\perp)$ for some shape S. Then there exists $x \in P^\perp$ and $m \in \mathbb{N}$ such that $x|_{S+p^m\mathbf{n}_i} = C_i$ for $1 \le i \le k$.*

Proof. Let $A_i \subset P^\perp$ be the cylinder set of all elements such that $x_S = C_i$. By Corollary 7, the shift is mixing on $\{\mathbf{n}_1,\ldots,\mathbf{n}_k\}$. Therefore, for large enough $n \in \mathbb{N}$

$$T_{-n\mathbf{n}_1}A_1 \cap \cdots \cap T_{-n\mathbf{n}_k}A_k$$

has non-zero measure, which implies that this intersection is non-empty. Any element in this intersection satisfies $x|_{S+n\mathbf{n}_i} = C_i$. We can choose n to be a power of p. □

Lemma 10. *Let $P^\perp$ and $Q^\perp$ be linear cellular automaton shifts. If $S(P) \not\subset S(Q)$, then the trivial homomorphism is the only topological homomorphism between $P^\perp$ and $Q^\perp$.*

Proof. Let $\phi\colon P^\perp \to Q^\perp$ be a homomorphism with local rule $\gamma\colon \mathcal{L}_S(P^\perp) \to \mathbb{F}_p$ for some shape S. Let $P = X_d - \Phi$ and $Q = X_d - \Psi$ and let $S(\Phi) \cup S(\Psi) = \{\mathbf{n}_1,\ldots,\mathbf{n}_k\}$. By Corollary 7, $\{-\mathbf{n}_1,\ldots,-\mathbf{n}_k\}$ is a mixing set for $P^\perp$. By Lemma 9, for any k configurations $C_i \in \mathcal{L}_S(P^\perp)$ there exists an $x \in P^\perp$ such that $x|_{S-p^m\mathbf{n}_i} = C_i$. Since $S(P) \not\subset S(Q)$, there exists an $\mathbf{n}_j$ which is in $S(\Phi)$ but not in $S(\Psi)$. For all $i \neq j$ we take C_i to be the zero configuration. For C_j we take an arbitrary configuration.

Since $x|_{S-p^m\mathbf{n}_i} = C_i$, by the local rule $\phi(x)|_{-p^m\mathbf{n}_i} = \gamma(C_i)$. All of these configurations except at C_j are zero. In particular $\gamma(C_i) = 0$ for all i such that $\mathbf{n}_i$ occurs in Ψ. Since $\phi(x)$ is annihilated by $Q^{p^m} = X_d^{p^m} - \Phi^{p^m}$, and since $S(\Phi^{p^m}) = p^m S(\Phi)$, we have that

$$\phi(x)_{(0,\ldots,0,-p^m)} = 0.$$

In other words, if all of the coefficients that correspond to Ψ are zero, then Q^{p^m} can only annihilate $\phi(x)$ if the remaining coefficient corresponding to $X_d^{p^m}$ is zero as well. A similar argument applies to P^{p^m}, but here we have that the coefficient corresponding to $\mathbf{n}_j$ is not zero. So here the coefficient corresponding to $X_d^{p^m}$ is non-zero. The configuration at $x|_{S+(0,\ldots,0,-p^m)}$ has to match up against C_j. More specifically, if c is the coefficient of Ψ at $X^{\mathbf{n}_j}$, then

$$x_{S+(0,\ldots,0,-p^m)} = cC_j$$

By the local rule $\gamma(cC_j) = 0$ and since C_j is arbitrary and c is non-zero, the local rule is trivial. □

A Laurent polynomial is a series

$$\sum_{\mathbf{n}\in\mathbb{Z}^d} c_P(\mathbf{n})X^{\mathbf{n}}$$

in which all but finitely many coefficients $c_P(\mathbf{n})$ are zero. Now think of c_P as a map of $\mathbf{Z}^d$ into the 1-configurations. Extending this, for a shape S let $C_{P,S}$ be a map of $\mathbf{Z}^d$ into $\mathcal{L}_S(P^\perp)$. For a Laurent polynomial Q we denote

$$Q \cdot C_{P,S} = \sum_{\mathbf{n}\in\mathbb{Z}^d} c_Q(\mathbf{n}) C_{P,S}(\mathbf{n}).$$

Since $\mathcal{L}_S(P^\perp)$ is a group and since this is a finite sum, $Q\cdot C_{P,S}$ is a well-defined configuration. If $\gamma\colon \mathcal{L}_S(P^\perp) \to \mathbb{F}_p$ is a local rule, then $\gamma \circ C_{P,S}$ is a map $\mathbb{Z}^d \to \mathbb{F}_p$, which we denote by $\gamma(C_{P,S})$.

Lemma 11. *Let $P^\perp, Q^\perp$ be linear cellular automaton shifts such that $S(P) \subset S(Q)$ and such that $P = X_d - \Phi$ and $Q = X_d - \Psi$. A topological homomorphism between $P^\perp$ and $Q^\perp$ with local rule γ satisfies the functional equation*

$$\gamma(\Phi \cdot C_{P,S}) = \Psi \cdot \gamma(C_{P,S})$$

Proof. Since $S(\Psi)$ is a mixing set there exists $x \in P^\perp$ and $m \in \mathbb{N}$ such that $x|_{S-p^m\mathbf{n}} = C_{P,S}(\mathbf{n})$ for $\mathbf{n} \in S(\Psi)$. Since $P^{p^m} \cdot x = 0$ we have

$$x|_{S-(0,\dots,0,p^m)} = \Phi \cdot C_{P,S}.$$

If ϕ is the topological homomorphism with local rule γ, then $\phi(x)(-\mathbf{n}) = \gamma(C_{P,S}(\mathbf{n}))$ for $\mathbf{n} \in S(\Psi)$ and $\phi(x)(0,\dots,0,-p^m) = \gamma(\Phi \cdot C_{P,S})$. Since $Q^{p^m} \cdot \phi(x) = 0$ we also have

$$\phi(x)|_{(0,\dots,0,-p^m)} = \Psi \cdot \gamma(C_{P,S}).$$

□

Lemma 12. *Let $P^\perp, Q^\perp$ be linear cellular automaton shifts such that $S(P) \subset S(Q)$. A topological homomorphism between $P^\perp$ and $Q^\perp$ is an algebraic homomorphism.*

Proof. We need to show that the local rule γ satisfies $\gamma(C+D) = \gamma(C) + \gamma(D)$ for $C, D \in \mathcal{L}_S(P^\perp)$. Let $\mathbf{m}, \mathbf{n} \in S(P)$ and let c_m, c_n be the corresponding coefficients in P, while d_m, d_n are the coefficients in Q. By choosing $C_{S,P}(\mathbf{m}) = C$ and $C_{S,P}(\mathbf{n}) = D$ and all other shapes zero, we obtain that

$$\gamma(c_m C + c_n D) = d_m \gamma(C) + d_n \gamma(D)$$

by the functional equation in the previous lemma. Taking the second shape to be zero, we obtain that $\gamma(c_m C) = d_m \gamma(C)$ for any shape C. Taking the first shape to be zero, we obtain $\gamma(c_n D) = d_n \gamma(D)$. Therefore

$$\gamma(c_m C + c_n D) = \gamma(c_m C) + \gamma(c_n D).$$

The homomorphism is algebraic. □

Theorem 13. *A topological homomorphism between linear cellular automata $P^\perp$ and $Q^\perp$ is algebraic. The shifts are topologically isomorphic if and only if $P^\perp = Q^\perp$.*

Proof. By the previous lemma, we already know that a topological homomorphism between cellular automaton shifts is algebraic if $S(P) \subset S(Q)$. We also saw that it is trivial if $S(P) \not\subset S(Q)$. Therefore, topological homomorphisms are necessarily algebraic.

Let $f\colon M \to N$ be a module isomorphism. If r annihilates M, then $rN = rf(M) = f(rM) = 0$ and therefore r annihilates N. Since f is an isomorphism, the same argument applies to f^{-1}. The annihilators are equal, which in our case means that $\langle P\rangle = \langle Q\rangle$. For linear cellular automaton shifts this even implies that $P = Q$. □

Corollary 14. *A homomorphism between linear cellular automata $P^\perp$ and $Q^\perp$ is trivial if $P \neq Q$.*

Proof. We will use that the Pontryagin dual of $P^\perp$ is

$$\widehat{P^\perp} = \mathbb{F}_p[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]/\langle P\rangle.$$

A homomorphism $\phi\colon P^\perp \to Q^\perp$ is algebraic, i.e., it is a module homomorphism. Its Pontryagin dual $\widehat{\phi}\colon \widehat{Q^\perp} \to \widehat{P^\perp}$ is a module homomorphism as well. It follows that $\widehat{\phi}(R) = R\widehat{\phi}(1)$. Therefore, the module homomorphism is determined by the value $\widehat{\phi}(1)$. Now Q represents 0 in $\widehat{Q^\perp}$ and therefore $Q\widehat{\phi}(1)$ represents 0 in $\widehat{P^\perp}$. In other words, P divides $Q\widehat{\phi}(1)$. Since P and Q are irreducible and since $\mathbb{F}_p[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]$ is a unique factorization domain, P divides $\widehat{\phi}(1)$. The homomorphism is trivial. □

The automorphism group of a one-dimensional Markov shift is large. In general, it is non-amenable [BLR88]. In contrast, the automorphism group of a linear cellular automaton shift is small.

Corollary 15. *The automorphism group of a linear cellular automaton shift is a finitely generated abelian group.*

Proof. Again, it is easier to consider automorphisms of the dual module. We found that a module homomorphism is a multiplication by a Laurent polynomial R. In case the homomorphism is an automorphism, there exists a Q such that multiplication by QR is equivalent to multiplication by 1. In other words, R is a unit in $\mathbb{F}_p[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]/\langle P\rangle$, which is the localization of the ring $\mathbb{F}_p[X_1, \ldots, X_d]/\langle P\rangle$ by the multiplicative set generated by $\{X_1, \ldots, X_d\}$. The polynomial P is equal to $X_d - \Phi(X_1, \ldots, X_d)$ and therefore

$$\mathbb{F}_p[X_1, \ldots, X_d]/\langle P\rangle \cong \mathbb{F}_p[X_1, \ldots, X_{d-1}].$$

Under this isomorphism, $\mathbb{F}_p[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]/\langle P\rangle$ is the localization of $\mathbb{F}_p[X_1, \ldots, X_{d-1}]$ by the multiplicative set generated by $\{X_1, \ldots, X_{d-1}, \Phi(X_1, \ldots, X_{d-1})\}$. The units in this ring are of the form U/V for polynomials U, V whose prime factor decomposition contains only X_j for $j = 1, \ldots, d-1$, or primes appearing in Φ. □

The automorphism group of a G-system necessarily includes G. For certain cellular automata, it does not contain much more than that.

Corollary 16. *Suppose that $\Phi(X_1, \ldots, X_{d-1})$ is irreducible. Then an automorphism of the corresponding linear cellular automaton $P^\perp$ is a multiplication by $cX_1^{n_1} \ldots X_d^{n_d}$.*

Proof. This follows from the proof of the previous lemma combined with the fact that $\Phi = X_d$ in $\mathbb{F}_p[X_1^{\pm 1}, \ldots, X_d^{\pm 1}]/\langle P \rangle$. □

4. Concluding remarks

Our topological rigidity result is a weak version of the measure rigidity result in [KS00]. The proof in that paper depends on the relatively straightforward algebraic characterization of 2-mixing. Our proof depends on Masser's algebraic characterization of k-mixing, which is a much deeper result. In our topological setting, we produce a weaker result using stronger machinery.

The proof of Masser's theorem in [Mas04] depends on ideas from algebraic geometry. It has recently been extended in [DM12, DM15], presenting an efficient method to compute minimal non-mixing sets. Another approach to computing non-mixing sets can be found in [ACBB18].

5. Acknowledgement

We would like to thank Michael Baake and Marcus Pivato for useful discussions. Reem Yassawi was supported by STAR travel grant 323600 and by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme, Grant Agreement No 648132. She also thanks IRIF, Université Paris Diderot-Paris 7, for its hospitality and support.

References

[ACBB18] L. Arenas-Carmona, D. Berend, and V. Bergelson. An Almost Mixing of All Orders Property of Algebraic Dynamical Systems. *Ergodic Theory Dynam. Systems*, to appear, 2018.

[BLR88] M. Boyle, D. Lind, and D. Rudolph. The automorphism group of a shift of finite type. *Trans. Amer. Mathem. Soc.*, 306(1):71–113, 1988.

[DM12] H. Derksen and D. Masser. Linear equations over multiplicative groups, recurrences, and mixing I. *Proc. Lond. Math. Soc.*, 104(5):1045–1083, 2012.

[DM15] H. Derksen and D. Masser. Linear equations over multiplicative groups, recurrences, and mixing II. *Indag. Math.*, 26(1):113–136, 2015.

[Hal43] Paul R. Halmos. On automorphisms of compact groups. *Bull. Amer. Math. Soc.*, 49:619–624, 1943.

[MOW84] Olivier Martin, Andrew M. Odlyzko and Stephen Wolfram. Algebraic properties of cellular automata. *Commun.Math.Phys.*, 93:219–258, 1984.

[KS89] Bruce Kitchens and Klaus Schmidt. Automorphisms of compact groups. *Ergodic Theory Dynam. Systems*, 9(4):691–735, 1989.

[KS92] Bruce Kitchens and Klaus Schmidt. Markov subgroups of $(\mathbf{Z}/2\mathbf{Z})^{\mathbf{Z}^2}$. In *Symbolic dynamics and its applications (New Haven, CT, 1991)*, volume 135 of *Contemp. Math.*, pages 265–283. Amer. Math. Soc., Providence, RI, 1992.

[KS93] Bruce Kitchens and Klaus Schmidt. Mixing sets and relative entropies for higher-dimensional Markov shifts. *Ergodic Theory Dynam. Systems*, 13(4):705–735, 1993.

[Kit97] Bruce Kitchens. Dynamics of $\mathbb{Z}^d$ actions on Markov subgroups. In *Topics in symbolic dynamics and its applications (Temuco, 1997)*, volume 279 of *London Math. Soc. Lecture Note Ser.*, pages 89–122. Cambridge University Press, 2000.

[KS00] Bruce Kitchens and Klaus Schmidt. Isomorphism rigidity of irreducible algebraic $\mathbb{Z}^d$-actions Invent. math. 142: 559-577, 2000.

[Led79] F. Ledrappier. Un champ markovien peut être d'entropie nulle et mélangeant. *C. R. Acad. Sci. Paris Sér. A-B* 287(7) A561–A563, 1979.

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

[Mas04] D.W. Masser. Mixing and linear equations over groups in positive characteristic. *Israel J. Math*, 142: 189–204, 2004.

[Rok49] V.A. Rohlin. On endomorphisms of compact commutative groups. (Russian) Izvestiya Akad. Nauk SSSR. Ser. Mat. 13: 329–340, 1949.

[Wal82] Peter Walters. *An introduction to ergodic theory*, volume 79 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982.

TU Delft, Netherlands and, Institut Camille Jordan, Université Lyon-1, France
E-mail address: R.J.Fokkink@tudelft.nl, yassawi@math.univ-lyon1.fr