Ergod. Th. & Dynam. Sys. (2008), **28**, 1945–1958
doi:10.1017/S0143385708000096
© *2008 Cambridge University Press*
Printed in the United Kingdom

Module shifts and measure rigidity in linear cellular automata

MARCUS PIVATO

Department of Mathematics, Trent University, 1600 West Bank Drive, Peterborough, Ontario, Canada K9J 7B8
(e-mail: marcuspivato@trentu.ca)

(*Received* 9 *July* 2007 *and accepted in revised form* 22 *January* 2008)

Abstract. Suppose $\mathcal{R}$ is a finite commutative ring of prime characteristic, $\mathcal{A}$ is a finite $\mathcal{R}$-module, $\mathbb{M} := \mathbb{Z}^D \times \mathbb{N}^E$, and Φ is an $\mathcal{R}$-linear cellular automaton on $\mathcal{A}^{\mathbb{M}}$. If μ is a Φ-invariant measure which is multiply σ-mixing in a certain way, then we show that μ must be the Haar measure on a coset of some submodule shift of $\mathcal{A}^{\mathbb{M}}$. Under certain conditions, this means that μ must be the uniform Bernoulli measure on $\mathcal{A}^{\mathbb{M}}$.

1. *Introduction*

Let $\mathcal{A}$ be a finite set. Let $\mathbb{M} := \mathbb{Z}^D \times \mathbb{N}^E$ be a $(D+E)$-dimensional lattice, for some D, $E \in \mathbb{N}$, and let $\mathcal{A}^{\mathbb{M}}$ denote the set of all functions $\mathbf{a} : \mathbb{M} \longrightarrow \mathcal{A}$, which we regard as $\mathbb{M}$-indexed *configurations* of elements in $\mathcal{A}$. We write such a configuration as $\mathbf{a} = [a_{\mathsf{m}}]_{\mathsf{m} \in \mathbb{M}}$, where $a_{\mathsf{m}} \in \mathcal{A}$ for all $\mathsf{m} \in \mathbb{M}$. Treat $\mathcal{A}$ as a discrete topological space; then $\mathcal{A}^{\mathbb{M}}$ is a Cantor space—that is, it is compact, perfect, totally disconnected, and metrizable.

If $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$ and $\mathbb{U} \subset \mathbb{M}$, then we define $\mathbf{a}_{\mathbb{U}} \in \mathcal{A}^{\mathbb{U}}$ by $\mathbf{a}_{\mathbb{U}} := [a_{\mathsf{u}}]_{\mathsf{u} \in \mathbb{U}}$. If $\mathsf{m} \in \mathbb{M}$, then strictly speaking, $\mathbf{a}_{\mathsf{m}+\mathbb{U}} \in \mathcal{A}^{\mathsf{m}+\mathbb{U}}$; however, it will often be convenient to 'abuse notation' and treat $\mathbf{a}_{\mathsf{m}+\mathbb{U}}$ as an element of $\mathcal{A}^{\mathbb{U}}$ in the obvious way. Let $\mathbb{H} \subset \mathbb{M}$ be some finite subset, and let $\phi : \mathcal{A}^{\mathbb{H}} \longrightarrow \mathcal{A}$ be a function (called a *local rule*). The *cellular automaton* (CA) determined by ϕ is the function $\Phi : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ defined by $\Phi(\mathbf{a})_{\mathsf{m}} = \phi(\mathbf{a}_{\mathsf{m}+\mathbb{H}})$ for all $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$ and $\mathsf{m} \in \mathbb{M}$. We refer to $\mathbb{H}$ as the *neighbourhood* of Φ.

We will prove a new 'measure rigidity' result for linear cellular automata: if Φ is a linear CA and μ is a Φ-invariant measure which is multiply σ-mixing in a certain way, then μ must be the Haar measure on a coset of some submodule shift of $\mathcal{A}^{\mathbb{M}}$. In particular, if $\mathcal{A}^{\mathbb{M}}$ admits no proper mixing subgroup shifts (e.g. $D = 1$ and $\mathcal{A} = \mathbb{Z}_{/p}$, for p prime), then μ must be the uniform measure on $\mathcal{A}^{\mathbb{M}}$. This result is complementary to previous rigidity results of [**Sch95b, HMM03, Piv05, Ein05, Sab07**].

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

1.1. *Terminology and notation.* Throughout, lowercase bold-faced letters ($\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, ...) denote elements of $\mathcal{A}^{\mathbb{M}}$, and Roman letters (a, b, c, ...) are elements of $\mathcal{A}$ or ordinary numbers. Lowercase sans-serif letters (..., m, n, p) denote elements of $\mathbb{M}$, and uppercase hollow font ($\mathbb{U}$, $\mathbb{V}$, $\mathbb{W}$, ...) are subsets of $\mathbb{M}$. For any $\mathsf{v} \in \mathbb{M}$, let $\sigma^{\mathsf{v}} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ be the *shift map* defined by $\sigma^{\mathsf{v}}(\mathbf{a})_{\mathsf{m}} = a_{\mathsf{m}+\mathsf{v}}$ for all $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$ and $\mathsf{m} \in \mathbb{M}$. Let $\mathsf{CA}(\mathcal{A}^{\mathbb{M}})$ denote the set of cellular automata on $\mathcal{A}^{\mathbb{M}}$; then $\mathsf{CA}(\mathcal{A}^{\mathbb{M}})$ is also the set of continuous transformations of $\mathcal{A}^{\mathbb{M}}$ which commute with all shifts [**Hed69**, Theorem 3.4]. A *subshift* is a closed subset $\mathbf{S} \subseteq \mathcal{A}^{\mathbb{M}}$ which is invariant under all shifts. Let $\mathsf{CA}(\mathbf{S}) := \{\Phi \in \mathsf{CA}(\mathcal{A}^{\mathbb{M}}) \; ; \; \Phi(\mathbf{S}) \subseteq \mathbf{S}\}$.

If $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, and $\mathbb{K} \subset \mathbb{M}$, recall that $\mathbf{a}_{\mathbb{K}} := [a_{\mathsf{k}}]_{\mathsf{k} \in \mathbb{K}} \in \mathcal{A}^{\mathbb{K}}$. If $\mathbf{S} \subseteq \mathcal{A}^{\mathbb{M}}$ is a subshift, let $\mathbf{S}_{\mathbb{K}} := \{\mathbf{s}_{\mathbb{K}} \; ; \; \mathbf{s} \in \mathbf{S}\} \subseteq \mathcal{A}^{\mathbb{K}}$. If $\mathbf{k} \in \mathcal{A}^{\mathbb{K}}$, then let $\langle \mathbf{k} \rangle := \{\mathbf{a} \in \mathcal{A}^{\mathbb{M}} \; ; \; \mathbf{a}_{\mathbb{K}} = \mathbf{k}\}$ be the *cylinder set* defined by $\mathbf{k}$. The topology (and hence, the Borel sigma-algebra) of $\mathcal{A}^{\mathbb{M}}$ is generated by the collection of all such cylinder sets for all finite $\mathbb{K} \subset \mathbb{M}$. Let $\mathfrak{M}_{\mathsf{erg}}(\mathcal{A}^{\mathbb{M}})$ ($\mathfrak{M}_{\mathsf{erg}}(\mathbf{S})$)] be the set of Borel probability measures on $\mathcal{A}^{\mathbb{M}}$ ($\mathbf{S}$), and let $\mathfrak{M}_{\mathsf{erg}}(\mathcal{A}^{\mathbb{M}}, \sigma)$ ($\mathfrak{M}_{\mathsf{erg}}(\mathbf{S}, \sigma)$) be the shift-invariant measures on $\mathcal{A}^{\mathbb{M}}$ ($\mathbf{S}$). If $\Phi \in \mathsf{CA}(\mathbf{S})$, let $\mathfrak{M}_{\mathsf{erg}}(\mathbf{S}, \Phi)$ be the Φ-invariant measures on $\mathbf{S}$.

2. *Linear cellular automata*

Let $(\mathcal{R}, +, \cdot)$ be a finite ring with unity $1_{\mathcal{R}}$, and let $(\mathcal{A}, +, \cdot)$ be a finite $\mathcal{R}$-module. If $\Phi \in \mathsf{CA}(\mathcal{A}^{\mathbb{M}})$, then Φ is an *$\mathcal{R}$-linear* CA ($\mathcal{R}$-LCA) if the local rule $\phi : \mathcal{A}^{\mathbb{H}} \longrightarrow \mathcal{A}$ has the form

$$\phi(\mathbf{a}_{\mathbb{H}}) := \sum_{\mathsf{h} \in \mathbb{H}} \varphi_{\mathsf{h}} a_{\mathsf{h}} \quad \text{for all } \mathbf{a}_{\mathbb{H}} \in \mathcal{A}^{\mathbb{H}}, \tag{1}$$

where $\varphi_{\mathsf{h}} \in \mathcal{R} \setminus \{0\}$ for each $\mathsf{h} \in \mathbb{H}$. Let $\mathcal{R}\text{-}\mathsf{LCA}(\mathcal{A}^{\mathbb{M}})$ be the set of all $\mathcal{R}$-linear cellular automata on $\mathcal{A}^{\mathbb{M}}$.

Example 1. (a) If $(\mathcal{A}, +)$ is a finite abelian group, and $\mathcal{A}^{\mathbb{M}}$ is treated as a Cartesian product and endowed with componentwise addition, then $(\mathcal{A}^{\mathbb{M}}, +)$ is a compact abelian group. If $\Phi \in \mathsf{CA}(\mathcal{A}^{\mathbb{M}})$, then Φ is an *endomorphic cellular automaton* (ECA) if Φ is also a group homomorphism of $(\mathcal{A}^{\mathbb{M}}, +)$. Let $\mathcal{E}$ be the (non-commutative) ring of all group endomorphisms of $(\mathcal{A}, +)$. Then $\mathcal{A}$ is an $\mathcal{E}$-module, and any ECA on $\mathcal{A}^{\mathbb{M}}$ is an $\mathcal{E}$-linear CA. (In the literature, these are often just called *linear* cellular automata.)

(b) In particular, let $m \in \mathbb{N}$ and let $\mathcal{A} = (\mathbb{Z}_{/m}, +)$, with addition modulo m. Then $\mathcal{E} = (\mathbb{Z}_{/m}, +, \cdot)$ (with multiplication modulo m), so equation (1) becomes $\phi(\mathbf{a}_{\mathbb{H}}) = \sum_{\mathsf{h} \in \mathbb{H}} \varphi_{\mathsf{h}} a_{\mathsf{h}} \mod m$, where $\varphi_{\mathsf{h}} \in [1 \ldots m)$ for each $\mathsf{h} \in \mathbb{H}$.

(c) Let $k \in \mathbb{N}$, and let $\mathcal{R} := \mathbb{F}_{p^k}$ be the unique finite field of order p^k (in particular, if $k = 1$ then $\mathbb{F}_{p^k} = \mathbb{Z}_{/p}$ as in (b)). Let $\mathcal{A}$ be any finite-dimensional $\mathbb{F}_{p^k}$-vector space (e.g. $\mathcal{A} := (\mathbb{F}_{p^k})^m$, for some $m \in \mathbb{N}$); then $\mathcal{A}^{\mathbb{M}}$ is an (infinite-dimensional) $\mathbb{F}_{p^k}$-vector space, and Φ is an $\mathbb{F}_{p^k}$-LCA if and only if Φ is a linear endomorphism of $\mathcal{A}^{\mathbb{M}}$.

(d) Let $\mathcal{A}$ be a finite-dimensional $\mathbb{F}_{p^k}$-vector space, and let $\mathsf{End}(\mathcal{A})$ be the (non-commutative) ring of all $\mathbb{F}_{p^k}$-linear endomorphisms of $\mathcal{A}$. Suppose that $\{\varphi_{\mathsf{h}}\}_{\mathsf{h} \in \mathbb{H}} \subset \mathsf{End}(\mathcal{A})$ is a collection of endomorphisms which commute with one another, and let $\mathcal{R}$ be the subring of $\mathsf{End}(\mathcal{A})$ generated by $\{\varphi_{\mathsf{h}}\}_{\mathsf{h} \in \mathbb{H}}$; then $\mathcal{R}$ is a commutative ring, $\mathcal{A}$ is an $\mathcal{R}$-module, and if Φ is as in equation (1), then Φ is an $\mathcal{R}$-LCA. ◇

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

Example 1(a) is 'universal' in the following sense: any $\mathcal{R}$-module is also an abelian group, and any $\mathcal{R}$-linear CA is automatically an ECA. However, in a general ECA, the coefficients $\{\varphi_{\mathsf{h}}\}_{\mathsf{h}\in\mathbb{H}} \subset \mathcal{E}$ do not commute, because the endomorphism ring $\mathcal{E}$ is not commutative unless $\mathcal{A} = \mathbb{Z}_{/m}$, as in Example 1(b). If $\mathcal{R}$ is commutative, then $\mathcal{R}$-linear cellular automata are much easier to analyze than general endomorphic cellular automata.

If $r \in \mathcal{R}$, then the *characteristic* of r is the smallest $m \in \mathbb{N}$ such that $m \cdot r = 0$ (or it is 0 if there is no such m). The *characteristic* of $\mathcal{R}$ is the characteristic of the unity element $1_{\mathcal{R}}$. (For example, $\mathcal{R} = \mathbb{Z}_{/m}$ has characteristic m.) If $\mathcal{R}$ has characteristic m, then $m \cdot r = 0$ for all $r \in \mathcal{R}$; hence the characteristic of r divides m. We will be mainly interested in the case where $\mathcal{R}$ is a *commutative* ring of prime characteristic, as in Examples 1(c,d).

3. *Subgroup shifts and submodule shifts*

Suppose $(\mathcal{A}, +)$ is a finite abelian group, so that $(\mathcal{A}^{\mathbb{M}}, +)$ is compact abelian. A *subgroup shift* is a closed, shift-invariant subgroup $\mathbf{G} \subset \mathcal{A}^{\mathbb{M}}$ (i.e. $\mathbf{G}$ is both a subshift and a subgroup); see [**Kit87, Kit00, KS89, KS92, Sch95a**]. If $\mathcal{A}$ is an $\mathcal{R}$-module, then $\mathcal{A}^{\mathbb{M}}$ is also an $\mathcal{R}$-module under componentwise $\mathcal{R}$-multiplication. An *$\mathcal{R}$-submodule shift* is a subgroup shift which is also an $\mathcal{R}$-submodule. For example, if $\Phi \in \mathcal{R}\text{-}\mathsf{LCA}(\mathcal{A}^{\mathbb{M}})$, then $\Phi(\mathcal{A}^{\mathbb{M}})$ and $\ker(\Phi) := \Phi^{-1}\{\mathbf{0}\}$ are submodule shifts (here $\mathbf{0} \in \mathcal{A}^{\mathbb{M}}$ is the constant zero element). Also $\mathsf{Fix}[\Phi] := \{\mathbf{a} \in \mathcal{A}^{\mathbb{M}} \,;\; \Phi(\mathbf{a}) = \mathbf{a}\}$ is a submodule shift (because $\mathsf{Fix}[\Phi] = \ker(\Phi - \mathbf{Id})$). If $\mathcal{A} = \mathcal{R} = \mathbb{Z}_{/m}$, then every subgroup shift is a submodule shift, and vice versa. However, in general the $\mathcal{R}$-submodule shifts form a more restricted class.

To study the ergodic theory of $\mathcal{R}$-linear cellular automata, it is first necessary to characterize their invariant measures. If $\mathbf{G} \subseteq \mathcal{A}^{\mathbb{M}}$ is a subgroup shift, then the *Haar measure* of $\mathbf{G}$ is the unique $\eta_{\mathbf{G}} \in \mathfrak{M}_{\text{ces}}(\mathbf{G})$ which is invariant under translation by all elements of $\mathbf{G}$. That is, if $\mathbf{g} \in \mathbf{G}$, and $\mathbf{U} \subset \mathbf{G}$ is any measurable subset, and $\mathbf{U} + \mathbf{g} := \{\mathbf{u} + \mathbf{g} \,;\; \mathbf{u} \in \mathbf{U}\}$, then $\eta_{\mathbf{G}}[\mathbf{U} + \mathbf{g}] = \eta_{\mathbf{G}}[\mathbf{U}]$. In particular, if $\mathbf{G} = \mathcal{A}^{\mathbb{M}}$, then $\eta_{\mathbf{G}}$ is just the uniform Bernoulli measure on $\mathcal{A}^{\mathbb{M}}$. Let $\mathsf{ECA}(\mathbf{G}) := \{\Phi \in \mathsf{CA}(\mathcal{A}^{\mathbb{M}}) \,;\; \Phi \text{ is an ECA and } \Phi(\mathbf{G}) \subseteq \mathbf{G}\}$.

PROPOSITION 2. *Let $(\mathcal{A}, +)$ be a finite abelian group, let $\mathbf{G} \subseteq \mathcal{A}^{\mathbb{M}}$ be a subgroup shift, and let $\Phi \in \mathsf{ECA}(\mathbf{G})$. Then $(\Phi(\eta_{\mathbf{G}}) = \eta_{\mathbf{G}}) \Longleftrightarrow (\Phi(\mathbf{G}) = \mathbf{G})$.*

Proof. '$\Longrightarrow$' is because $\mathbf{G} = \mathsf{supp}(\eta_{\mathbf{G}})$. To see '$\Longleftarrow$', note that $\Phi(\eta_{\mathbf{G}}) \in \mathfrak{M}_{\text{ces}}(\mathbf{G})$. Thus, it suffices to show that $\Phi(\eta_{\mathbf{G}})$ is invariant under all $\mathbf{G}$-translations. Let $\mathbf{g} \in \mathbf{G}$, and let $\tau^{\mathbf{g}} : \mathbf{G} \longrightarrow \mathbf{G}$ be the translation map (i.e. $\tau^{\mathbf{g}}(\mathbf{h}) := \mathbf{g} + \mathbf{h}$). Find $\mathbf{h} \in \mathbf{G}$ such that $\Phi(\mathbf{h}) = \mathbf{g}$ (this $\mathbf{h}$ exists because $\Phi(\mathbf{G}) = \mathbf{G}$). Then $\tau^{\mathbf{g}}[\Phi(\eta_{\mathbf{G}})] \underset{(*)}{=} \Phi[\tau^{\mathbf{h}}(\eta_{\mathbf{G}})] \underset{(\dagger)}{=} \Phi(\eta_{\mathbf{G}})$, where $(*)$ is because $\tau^{\mathbf{g}} \circ \Phi = \Phi \circ \tau^{\mathbf{h}}$, and $(\dagger)$ is because $\eta_{\mathbf{G}}$ is the Haar measure. This holds for all $\mathbf{g} \in \mathbf{G}$. But $\eta_{\mathbf{G}}$ is the unique probability measure on $\mathbf{G}$ such that $\tau^{\mathbf{g}}(\eta_{\mathbf{G}}) = \eta_{\mathbf{G}}$ for all $\mathbf{g} \in \mathbf{G}$; thus $\Phi(\eta_{\mathbf{G}}) = \eta_{\mathbf{G}}$. □

Some endomorphic cellular automata exhibit a great deal of *measure rigidity*, meaning that the Haar measures of Φ-invariant subgroup shifts are the *only* Φ-invariant measures satisfying certain 'non-degeneracy' conditions. For example, Host, Maass and Martínez showed that, if p is prime and $\mathcal{A} = \mathbb{Z}_{/p}$, and Φ is a nearest neighbour $\mathbb{Z}_{/p}$-LCA on $\mathcal{A}^{\mathbb{Z}}$, then the only positive-entropy, σ-ergodic, Φ-invariant measure is the Haar measure

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

on $\mathcal{A}^{\mathbb{Z}}$—that is, the uniform Bernoulli measure [**HMM03**, Theorem 12]. This result was vastly generalized by Sablik, who showed that, if $\mathbf{G} \subseteq \mathcal{A}^{\mathbb{Z}}$ is any subgroup shift and $\Phi \in \mathsf{ECA}(\mathbf{G})$, then the only positive-entropy, Φ-invariant measure satisfying certain ergodicity conditions is the Haar measure on $\mathbf{G}$ [**Sab07**, Theorems 3.3 and 3.4]. (Actually, Sablik's result is even more general, since it allows any abelian group shift structure on $\mathcal{A}^{\mathbb{Z}}$.) See also [**Piv05**] for similar results concerning endomorphic cellular automata in the case where $\mathcal{A}^{\mathbb{Z}}$ is a *non-abelian* group shift, as well as *multiplicative* cellular automata (in the case where $(\mathcal{A}, \cdot)$ is a non-abelian group).

All of these results are for *one*-dimensional endomorphic cellular automata. Einsiedler [**Ein05**, Corollary 2.3] has a similar rigidity result for automorphic $\mathbb{Z}^D$-actions on compact abelian groups (e.g. the $\mathbb{Z}^D$-shift action on a subgroup shift $\mathbf{G} \subseteq \mathcal{A}^{\mathbb{Z}^D}$). This theorem can easily be translated into equivalent rigidity results for endomorphic cellular automata in $\mathcal{A}^{\mathbb{Z}^{D-1}}$. Like [**HMM03**] and [**Sab07**], Einsiedler requires both an entropy condition and fairly strong ergodicity hypotheses.

Let $\mathcal{R}$ be a commutative ring of characteristic p. We will prove a measure rigidity result for multidimensional $\mathcal{R}$-linear cellular automata whose only requirement on the measure is a limited form of multiple mixing. Our result is philosophically similar to the rigidity results in [**Sch95b**] or [**Sch95a**, §29], but it is applicable to much larger class of cellular automata.

Let $\mu \in \mathfrak{M}_{\mathrm{acs}}(\mathcal{A}^{\mathbb{M}}; \sigma)$. For any $H \in \mathbb{N}$, we say $(\mathcal{A}^{\mathbb{M}}, \mu; \sigma)$ is (σ, H)-*mixing* if, for any Borel measurable $\mathbf{B}_0, \mathbf{B}_1, \ldots, \mathbf{B}_H \subseteq \mathcal{A}^{\mathbb{M}}$,

$$\lim_{\substack{\mathsf{m}_0, \mathsf{m}_1, \ldots, \mathsf{m}_H \in \mathbb{M} \\ |\mathsf{m}_h - \mathsf{m}_i| \to \infty \\ \text{for all } h \neq i \in [0 \ldots H]}} \mu\left[\bigcap_{h=0}^{H} \sigma^{-\mathsf{m}_h}(\mathbf{B}_h) \right] = \prod_{h=0}^{H} \mu[\mathbf{B}_h].$$

If $\mathbb{H} \subset \mathbb{M}$ is a finite subset, then μ is $\mathbb{H}$-*mixing* if, for any finite subset $\mathbb{B} \subset \mathbb{M}$ and any $\mathbb{H}$-indexed collection of $\mathbb{B}$-words $\{\mathbf{b}_{\mathsf{h}}\}_{\mathsf{h} \in \mathbb{H}} \subset \mathcal{A}^{\mathbb{B}}$, with cylinder sets $\mathbf{B}_{\mathsf{h}} := \langle \mathbf{b}_{\mathsf{h}} \rangle \subset \mathcal{A}^{\mathbb{M}}$ for all $\mathsf{h} \in \mathbb{H}$,

$$\lim_{n \to \infty} \mu\left[\bigcap_{\mathsf{h} \in \mathbb{H}} \sigma^{-n\mathsf{h}}(\mathbf{B}_{\mathsf{h}}) \right] = \prod_{\mathsf{h} \in \mathbb{H}} \mu[\mathbf{B}_{\mathsf{h}}].$$

This property was introduced by [**Led78**], and has been studied extensively; see [**KS93, Mas04**] or [**Sch95a**, §§27–29]. We will actually require a slightly weaker (albeit more technical) condition. For any finite $\mathbb{H} \subset \mathbb{M}$ and any prime p, we say that μ is $(p, \mathbb{H})$-*mixing* if, for any finite $\mathbb{B} \subset \mathbb{M}$, if $\{\mathbf{b}_{\mathsf{h}}\}_{\mathsf{h} \in \mathbb{H}} \subset \mathcal{A}^{\mathbb{B}}$, and $\mathbf{B}_{\mathsf{h}} := \langle \mathbf{b}_{\mathsf{h}} \rangle \subset \mathcal{A}^{\mathbb{M}}$ are as above, then

$$\lim_{k \to \infty} \mu\left[\bigcap_{\mathsf{h} \in \mathbb{H}} \sigma^{-p^k \mathsf{h}}(\mathbf{B}_{\mathsf{h}}) \right] = \prod_{\mathsf{h} \in \mathbb{H}} \mu[\mathbf{B}_{\mathsf{h}}]. \tag{2}$$

For example, if $|\mathbb{H}| = H$, then any (σ, H)-mixing measure is $\mathbb{H}$-mixing. In turn, any $\mathbb{H}$-mixing measure is clearly $(p, \mathbb{H})$-mixing. In particular, any non-trivial Bernoulli measure in $\mathcal{A}^{\mathbb{M}}$ is $(p, \mathbb{H})$-mixing, and any mixing Markov measure in $\mathcal{A}^{\mathbb{Z}}$ or $\mathcal{A}^{\mathbb{N}}$ is $(p, \mathbb{H})$-mixing.

If $\mathbf{S} \subseteq \mathcal{A}^{\mathbb{M}}$ is a subshift, then $\mathbf{S}$ is *topologically* $(p, \mathbb{H})$-*mixing* if, for any finite $\mathbb{B} \subset \mathbb{M}$ and $\mathbb{H}$-indexed collection of $\mathbb{B}$-words $\{\mathbf{b}_{\mathsf{h}}\}_{\mathsf{h} \in \mathbb{H}} \subseteq \mathbf{S}_{\mathbb{B}}$, with $\mathbf{B}_{\mathsf{h}} := \langle \mathbf{b}_{\mathsf{h}} \rangle$ as above, there is some $N \in \mathbb{N}$ such that, for all $n > N$, we have $\bigcap_{\mathsf{h} \in \mathbb{H}} \sigma^{-p^k \mathsf{h}}(\mathbf{B}_{\mathsf{h}}) \neq \emptyset$. For example, if μ

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

is a $(p, \mathbb{H})$-mixing measure, then $\mathbf{S} = \mathsf{supp}(\mu)$ is a topologically $(p, \mathbb{H})$-mixing subshift. In particular, any irreducible Markov subshift of $\mathcal{A}^{\mathbb{Z}}$ or $\mathcal{A}^{\mathbb{N}}$ is topologically $(p, \mathbb{H})$-mixing.

A *coset shift* is a subshift $\mathbf{C}$ which is a coset of some submodule shift $\mathbf{S} \subset \mathcal{A}^{\mathbb{M}}$. For example, for any $c \in \mathcal{A}$, let $c^{\mathbb{M}} \in \mathcal{A}^{\mathbb{M}}$ denote the constant configuration equal to c everywhere. Then $c^{\mathbb{M}} + \mathbf{S}$ is a coset shift. If $\mathbf{C} \subseteq \mathcal{A}^{\mathbb{M}}$ is any subshift, and $\mathbf{C} - \mathbf{C} := \{\mathbf{c} - \mathbf{c}' \,;\ \mathbf{c}, \mathbf{c}' \in \mathbf{C}\}$, then it is easy to see that

$$(\mathbf{C} \text{ is a coset shift}) \Longleftrightarrow (\mathbf{C} - \mathbf{C} \text{ is a submodule shift}). \tag{3}$$

Let $\mathbf{c} \in \mathcal{A}^{\mathbb{M}}$, and suppose $\mathbf{C} := \mathbf{c} + \mathbf{S}$ is a coset shift. If $\tau^{\mathbf{c}} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ is the translation map $\tau^{\mathbf{c}}(\mathbf{a}) := \mathbf{a} + \mathbf{c}$, then the *Haar measure* of $\mathbf{C}$ is defined then $\eta_{\mathbf{C}} := \tau^{\mathbf{c}}(\eta_{\mathbf{S}})$, where $\eta_{\mathbf{S}}$ is the Haar measure of $\mathbf{S}$. (This definition is independent of the choice of $\mathbf{c} \in \mathbf{C}$.)

If $0 \neq \varphi \in \mathcal{R}$, then an $\mathcal{R}$-module $\mathcal{A}$ is *φ-torsion-free* if $\varphi\, a \neq 0$ for all $a \in \mathcal{A} \setminus \{0\}$. We say that φ is a *unit* if it has a multiplicative inverse in $\mathcal{R}$. This means that the function $\mathcal{A} \ni a \mapsto \varphi a \in \mathcal{A}$ is a group automorphism of $(\mathcal{A}, +)$. If $\mathcal{R} = \mathbb{Z}_{/m}$ (Example 1(b)), then φ is a unit if and only if φ is coprime to m. If $\mathcal{R}$ is a field (Example 1(c)), then every non-zero element of $\mathcal{R}$ is a unit. If φ is a unit, then every $\mathcal{R}$-module is φ-torsion-free.

Suppose that Φ has local rule (1) and $\mathcal{R}$ has characteristic p. For all $j \in \mathbb{N}$, let $\mathcal{R}_j$ be the subring of $\mathcal{R}$ generated by $\{\varphi_{\mathsf{h}}^{p^j}\}_{\mathsf{h} \in \mathbb{H}}$. This yields a descending chain $\mathcal{R} \supseteq \mathcal{R}_1 \supseteq \mathcal{R}_2 \supseteq \cdots$ of finite rings (because $\mathcal{R}$ is finite), so there is some $J \in \mathbb{N}$ such that $\mathcal{R}_J = \mathcal{R}_{J+1} = \cdots = \bigcap_{j=1}^{\infty} \mathcal{R}_j$. Let $\mathcal{R}_\Phi := \mathcal{R}_J$. For any $k \in \mathbb{N}$, let $\overline{\varphi}_k := (\sum_{\mathsf{h} \in \mathbb{H}} \varphi_{\mathsf{h}}^{p^k}) - 1$; this defines a sequence $\{\overline{\varphi}_k\}_{k=1}^{\infty} \subseteq \mathcal{R}$. But $\mathcal{R}$ is finite, so there is a non-empty set $\mathcal{F}_\Phi \subseteq \mathcal{R}$ of elements which appear infinitely often in $\{\overline{\varphi}_k\}_{k=1}^{\infty}$. We now come to our main result.

THEOREM 3. *Let $\mathcal{R}$ be a finite commutative ring of prime characteristic p, let $\mathcal{A}$ be a finite $\mathcal{R}$-module, and let $\Phi \in \mathcal{R}$-LCA $(\mathcal{A}^{\mathbb{M}})$ have local rule (1), with $|\mathbb{H}| \geq 2$.*

(a) *Suppose that φ_{h} is a unit for some $\mathsf{h} \in \mathbb{H}$. If $\mathbf{C}$ is a topologically $(p, \mathbb{H})$-mixing, Φ-invariant subshift of $\mathcal{A}^{\mathbb{M}}$, then $\mathbf{C}$ is a coset shift of some $\mathcal{R}_\Phi$-submodule shift $\mathbf{S}$.*

(b) *If there exist $\overline{\varphi} \in \mathcal{F}_\Phi$ and some finite $\mathbb{B} \subset \mathbb{M}$ such that $\mathcal{A}^{\mathbb{B}}/\mathbf{S}_{\mathbb{B}}$ is $\overline{\varphi}$-torsion-free (e.g. if $\overline{\varphi}$ is a unit), and $\mathbf{C}$ is as in (a), then actually $\mathbf{C} = \mathbf{S}$.*

(c) *Suppose φ_{h} is a unit for every $\mathsf{h} \in \mathbb{H}$. If μ is a (Φ, σ)-invariant, $(p, \mathbb{H})$-mixing measure on $\mathcal{A}^{\mathbb{M}}$, then μ is the Haar measure of a Φ-invariant coset shift $\mathbf{C}$ of some $\mathcal{R}_\Phi$-submodule shift $\mathbf{S}$.*

If the hypothesis of (b) holds, then μ is the Haar measure on $\mathbf{S}$.

Example 4. Let $\mathbb{M} := \mathbb{Z} \times \mathbb{N}$, let $\mathcal{R} = \mathcal{A} := \mathbb{Z}_{/2}$, and let $\mathbb{B} := \{(-1, 0); (0, 0); (0, 1); (1, 0)\}$ (i.e. $\begin{smallmatrix} \circ\bullet\circ \\ \bullet\bullet\bullet \end{smallmatrix}$); then $\mathbf{S} := \{\mathbf{a} \in \mathcal{A}^{\mathbb{M}} \,;\ \sum_{\mathsf{b} \in \mathbb{B}} a_{\mathsf{b}+\mathsf{m}} = 0,\ \forall\, \mathsf{m} \in \mathbb{M}\}$ is a submodule shift.

CLAIM 1. *Let $\mathbb{H} := \{(0, 0); (0, 1); (1, 0)\}$ (i.e. $\begin{smallmatrix} \circ\bullet\circ \\ \circ\bullet\bullet \end{smallmatrix}$). Then $\mathbf{S}$ and $\eta_{\mathbf{S}}$ are $(2, \mathbb{H})$-mixing.*

Proof. One way to see this is to apply the transformation $[\mathbb{N} \times \mathbb{Z} \ni (n, z) \mapsto (z + n, n) \in \mathbb{Z} \times \mathbb{N}]$ to [**Sch95a**, Example 28.10(2) on p. 278]. Another way is to note that $\mathbf{S}$ is the set of all spacetime diagrams of the one-dimensional linear CA $\Psi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ defined by $\Psi := \sigma^{-1} + \sigma^0 + \sigma^1$. This yields a bijection $\Psi^{\mathbb{N}} : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathbf{S}$ (where $\Psi^{\mathbb{N}}(\mathbf{a}) \in \mathcal{A}^{\mathbb{Z} \times \mathbb{N}}$ is just the Ψ-spacetime diagram of $\mathbf{a} \in \mathcal{A}^{\mathbb{Z}}$). It follows that $\eta_{\mathbf{S}} = \Psi^{\mathbb{N}}[\eta]$, where η is the uniform Bernoulli measure on $\mathcal{A}^{\mathbb{Z}}$.

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

Equation (5) says that $\Psi^{2^k} = \sigma^{-2^k} + \sigma^0 + \sigma^{2^k}$. Thus, for any $\mathbb{B} \subset \mathbb{M}$, if k is large enough, then for all $\{\mathbf{b}_\mathsf{h}\}_{\mathsf{h}\in\mathbb{H}} \subset \mathbf{S}_\mathbb{B}$, there is a unique $\mathbf{b}' \in \mathbf{S}_\mathbb{B}$ such that $\langle \mathbf{b}_{(0,0)} \rangle \cap \sigma^{(-2^k,0)}\langle \mathbf{b}_{(1,0)} \rangle \cap \sigma^{(0,-2^k)}\langle \mathbf{b}_{(0,1)} \rangle = \langle \mathbf{b}_{(0,0)} \rangle \cap \sigma^{(-2^k,0)}\langle \mathbf{b}_{(1,0)} \rangle \cap \sigma^{(2^k,0)}\langle \mathbf{b}' \rangle$. Thus,

$$\begin{aligned}
&\eta_\mathbf{S}[\langle \mathbf{b}_{(0,0)} \rangle \cap \sigma^{(-2^k,0)}\langle \mathbf{b}_{(1,0)} \rangle \cap \sigma^{(0,-2^k)}\langle \mathbf{b}_{(0,1)} \rangle] \\
&\quad = \eta_\mathbf{S}[\langle \mathbf{b}_{(0,0)} \rangle \cap \sigma^{(-2^k,0)}\langle \mathbf{b}_{(1,0)} \rangle \cap \sigma^{(2^k,0)}\langle \mathbf{b}' \rangle] \\
&\quad \underset{(*)}{=} \eta_\mathbf{S}\langle \mathbf{b}_{(0,0)} \rangle \cdot \eta_\mathbf{S}\langle \mathbf{b}_{(1,0)} \rangle \cdot \eta_\mathbf{S}\langle \mathbf{b}' \rangle,
\end{aligned}$$

where $(*)$ is because $\eta_\mathbf{S} = \Psi^\mathbb{N}[\eta]$, and η is a (one-dimensional) Bernoulli measure. ◇ [Claim 1]

Let $\Phi : \mathcal{A}^\mathbb{M} \longrightarrow \mathcal{A}^\mathbb{M}$ be the LCA with local rule $\phi(\mathbf{a}_\mathbb{H}) = \sum_{\mathsf{h}\in\mathbb{H}} a_\mathsf{h}$ (i.e. $\varphi_\mathsf{h} = 1$ for all $\mathsf{h} \in \mathbb{H}$). Then $\Phi(\mathbf{S}) = \mathbf{S}$, so $\Phi(\eta_\mathbf{S}) = \eta_\mathbf{S}$, by Proposition 2. However, $\overline{\varphi}_k = |\mathbb{H}| - 1 = 2 \equiv 0 \pmod 2$ for all $k \in \mathbb{N}$, so the 'torsion-free' condition of Theorem 3(b) is never satisfied; thus, non-trivial Φ-invariant coset shifts might exist. Indeed, let $\mathbf{c} \in \mathcal{A}^\mathbb{M}$ be the 'checkerboard' configuration defined by $c_{m,n} := (m+n) \mod 2$, for all $(m, n) \in \mathbb{M}$; then $\mathbf{c} \notin \mathbf{S}$, and $\mathbf{C} := \mathbf{c} + \mathbf{S}$ is a non-trivial coset shift of $\mathbf{S}$ (see Lemma 10). Furthermore, $\Phi(\mathbf{c}) = \mathbf{c}$, so $\Phi(\mathbf{C}) = \mathbf{C}$.

CLAIM 2. *$\mathbf{C}$ and $\eta_\mathbf{C}$ are $(2, \mathbb{H})$-mixing.*

Proof. To see this, let $\mathbb{B} \subset \mathbb{M}$ and let $\{\mathbf{b}_\mathsf{h}\}_{\mathsf{h}\in\mathbb{H}} \subset \mathbf{C}_\mathbb{B}$; then for all $\mathsf{h} \in \mathbb{H}$, there exists $\mathbf{s}_\mathsf{h} \in \mathbf{S}_\mathbb{B}$ with $\mathbf{b}_\mathsf{h} = \mathbf{c}_\mathbb{B} + \mathbf{s}_\mathsf{h}$. Thus, $\langle \mathbf{b}_\mathsf{h} \rangle = \mathbf{c} + \langle \mathbf{s}_\mathsf{h} \rangle$; thus, $\sigma^{-2^k\mathsf{h}}\langle \mathbf{b}_\mathsf{h} \rangle = \sigma^{-2^k\mathsf{h}}\{\mathbf{c}\} + \sigma^{-2^k\mathsf{h}}\langle \mathbf{s}_\mathsf{h} \rangle \underset{(*)}{=} \mathbf{c} + \sigma^{-2^k\mathsf{h}}\langle \mathbf{s}_\mathsf{h} \rangle$, where $(*)$ is because $\sigma^{2^k\mathsf{h}}(\mathbf{c}) = \mathbf{c}$ because $\mathbf{c}$ is a checkerboard. Thus,

$$\begin{aligned}
\eta_\mathbf{C}\left[\bigcap_{\mathsf{h}\in\mathbb{H}} \sigma^{-2^k\mathsf{h}}\langle \mathbf{b}_\mathsf{h} \rangle\right] \quad &= \quad \eta_\mathbf{C}\left[\mathbf{c} + \bigcap_{\mathsf{h}\in\mathbb{H}} \sigma^{-2^k\mathsf{h}}\langle \mathbf{s}_\mathsf{h} \rangle\right] = \eta_\mathbf{S}\left[\bigcap_{\mathsf{h}\in\mathbb{H}} \sigma^{-2^k\mathsf{h}}\langle \mathbf{s}_\mathsf{h} \rangle\right] \\
&\xrightarrow[k\to\infty]{(*)} \prod_{\mathsf{h}\in\mathbb{H}} \eta_\mathbf{S}\langle \mathbf{s}_\mathsf{h} \rangle = \prod_{\mathsf{h}\in\mathbb{H}} \eta_\mathbf{C}[\mathbf{c} + \langle \mathbf{s}_\mathsf{h} \rangle] = \prod_{\mathsf{h}\in\mathbb{H}} \eta_\mathbf{C}\langle \mathbf{b}_\mathsf{h} \rangle,
\end{aligned}$$

as desired. Here, $(*)$ is because $\eta_\mathbf{S}$ is $(2, \mathbb{H})$-mixing by Claim 1. ◇ [Claim 2]

Thus, $\mathbf{C}$ is a $(2, \mathbb{H})$-mixing, Φ-invariant coset shift, as in Theorem 3(a), while $\eta_\mathbf{C}$ is a $(2, \mathbb{H})$-mixing, Φ-invariant measure, as in Theorem 3(c). ◇

COROLLARY 5. *Let $\mathcal{A} = \mathcal{R} := \mathbb{Z}_{/p}$, where p is prime. Let $\mathbb{M} := \mathbb{Z}^D \times \mathbb{N}^E$, and let $\Phi \in \mathbb{Z}_{/p}$-LCA$(\mathcal{A}^\mathbb{M})$ have a neighbourhood of cardinality $H \geq 2$. Let $\mu \in \mathfrak{M}_{\text{æs}}(\mathcal{A}^\mathbb{M}; \Phi, \sigma)$ be (σ, H)-mixing. Suppose that either*

(i) $D + E = 1$; *or* *(ii)* $h(\mu, \sigma) > 0$ *(and $D + E \geq 1$).*

Then μ is the uniform Bernoulli measure on $\mathcal{A}^\mathbb{M}$.

Proof. Every non-zero element of the field $\mathbb{Z}_{/p}$ is a unit, so we can use Theorem 3(c). Case (i) is because $(\mathbb{Z}_{/p})^\mathbb{Z}$ and $(\mathbb{Z}_{/p})^\mathbb{N}$ have no proper infinite subgroup shifts (because if $\mathbf{S}$ was such a subgroup shift, then $\{a \in \mathbb{Z}_{/p} \,;\, [a, 0] \in \mathbf{S}_{\{0,1\}}\}$ would be a proper non-trivial subgroup of $\mathbb{Z}_{/p}$, which is impossible). Case (ii) is because $(\mathbb{Z}_{/p})^{\mathbb{Z}^D \times \mathbb{N}^E}$ has no proper subgroup shifts of non-zero entropy [**Sch95a**, first paragraph of §25, p. 228]. □

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

Theorem 3(c) is somewhat similar to [**Sch95b**] or [**Sch95a**, Corollary 29.5, p. 289], which characterizes the σ-invariant measures of a subgroup shift $\mathbf{G} \subseteq \mathcal{A}^{\mathbb{M}}$. However, Schmidt requires $\mathbf{G}$ to be 'almost minimal' (i.e. to have no infinite σ-invariant subgroups), whereas we do not.

To prove Theorem 3, we use tools from number theory and harmonic analysis. If $\mathbb{M} := \mathbb{Z}^D \times \mathbb{N}^E$, then any $\mathcal{R}$-linear CA on $\mathcal{A}^{\mathbb{M}}$ can be written as a 'Laurent polynomial of shifts' with $\mathcal{R}$-coefficients. That is, if Φ has local rule (1), then for any $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$,

$$\Phi(\mathbf{a}) := \sum_{\mathsf{h} \in \mathbb{H}} \varphi_{\mathsf{h}}\, \sigma^{\mathsf{h}}(\mathbf{a}) \quad \text{(where we add configurations componentwise).} \tag{4}$$

We indicate this by writing '$\Phi = F(\sigma)$', where $F \in \mathcal{R}[x_1^{\pm 1}, \ldots, x_D^{\pm 1}; y_1, \ldots, y_E]$ is the $(D+E)$-variable Laurent polynomial defined as follows:

$$F(x_1, \ldots, x_D; y_1, \ldots, y_E) \quad := \quad \sum_{(h_1,\ldots,h_D;h'_1,\ldots,h'_E) \in \mathbb{H}} \varphi_{\mathsf{h}}\, x_1^{h_1} \ldots x_D^{h_D} y_1^{h'_1} \ldots y_E^{h'_E}.$$

If F and G are two such polynomials, and $\Phi = F(\sigma)$ while $\Gamma = G(\sigma)$, then $\Phi \circ \Gamma = (F \cdot G)(\sigma)$, where $F \cdot G$ is the product of F and G in the polynomial ring $\mathcal{R}[x_1^{\pm 1}, \ldots, x_D^{\pm 1}; y_1, \ldots, y_E]$. In particular, this means that $\Phi^t = F^t(\sigma)$ for all $t \in \mathbb{N}$. Thus, iterating an $\mathcal{R}$-LCA is equivalent to computing the powers of a polynomial. If $\mathcal{R}$ is commutative, we can do this with the binomial theorem, and if $\mathcal{R}$ has characteristic p, then we can compute the binomial coefficients modulo p. In particular, if p is prime, and Φ has polynomial representation (4), then for any $k \in \mathbb{N}$,

$$\Phi^{p^k} = \sum_{\mathsf{h} \in \mathbb{H}} \varphi_{\mathsf{h}}^{p^k}\, \sigma^{p^k \mathsf{h}}. \tag{5}$$

LEMMA 6. *Let $\mathcal{R}$ be a finite ring generated by a set $r_1, \ldots, r_H$, at least one of which is a unit. Let $\mathcal{A}$ be an $\mathcal{R}$-module and let $\mathbf{S} \subseteq \mathcal{A}^{\mathbb{M}}$ be a subshift containing $\mathbf{0}$. The following are equivalent.*

(a) $\mathbf{S}$ *is an $\mathcal{R}$-submodule shift.*
(b) *For any finite $\mathbb{B} \subset \mathbb{M}$, $\mathbf{S}_{\mathbb{B}}$ is an $\mathcal{R}$-submodule of $\mathcal{A}^{\mathbb{B}}$.*
(c) *For any finite $\mathbb{B} \subset \mathbb{M}$ and any $\mathbf{s}_1, \ldots, \mathbf{s}_H \in \mathbf{S}_{\mathbb{B}}$, we have $\sum_{h=1}^{H} r_h \mathbf{s}_h \in \mathbf{S}_{\mathbb{B}}$.*

Proof. Clearly **(a)** $\Leftrightarrow$ **(b)** $\Rightarrow$ **(c)**. To see that **(c)** $\Rightarrow$ **(b)**, let $\widetilde{\mathcal{R}}$ be the set of $\mathbb{N}$-linear combinations of products of $\{r_h\}_{h=1}^{H}$. Then **(c)** implies that $\widetilde{\mathcal{R}}\mathbf{S}_{\mathbb{B}} \subseteq \mathbf{S}_{\mathbb{B}}$ (because $\mathbf{0} \in \mathbf{S}$). Thus it suffices to show that $\widetilde{\mathcal{R}} = \mathcal{R}$.

Every element of $\mathcal{R}$ is a $\mathbb{Z}$-linear combination of products of $\{r_h\}_{h=1}^{H}$; hence we need only show that $-1_{\mathcal{R}} \in \widetilde{\mathcal{R}}$. Some r_h is a unit, and $\mathcal{R}$ is finite, so there exists $n \in \mathbb{N}$ with $1_{\mathcal{R}} = r_h^n \in \widetilde{\mathcal{R}}$. But $\mathcal{R}$ has characteristic $c < \infty$, so $-1_{\mathcal{R}} = (c-1)1_{\mathcal{R}} \in \widetilde{\mathcal{R}}$. □

Proof of Theorem 3(a). Let $\mathbf{C} \subset \mathcal{A}^{\mathbb{M}}$ be a topologically $(p, \mathbb{H})$-mixing, Φ-invariant subshift. Let $\mathbf{S} := \mathbf{C} - \mathbf{C}$; then according to (3) it suffices to show that $\mathbf{S}$ is an $\mathcal{R}_\Phi$-submodule shift. Now, $\mathbf{S}$ is a subshift, $\mathbf{0} \in \mathbf{S}$, and for all $k \in \mathbb{N}$, some element of $\{\varphi_{\mathsf{h}}^{p^k}\}_{\mathsf{h} \in \mathbb{H}}$ is a unit, so we can use Lemma 6.

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

Let $\mathbb{B} \subset \mathbb{M}$ be finite. Now, $\mathbf{S}$ is $(p, \mathbb{H})$-mixing (because $\mathbf{C}$ is), so there exists $N \in \mathbb{N}$ such that, for any $k > N$, and any $\mathbb{H}$-indexed collection $\{\mathbf{b}_\mathsf{h}\}_{\mathsf{h}\in\mathbb{H}} \subseteq \mathbf{S}_\mathbb{B}$, there exists $\mathbf{s} \in \mathbf{S}$ with

$$\mathbf{s}_{\mathbb{B}+p^k\mathsf{h}} = \mathbf{b}_\mathsf{h} \quad \text{for all } \mathsf{h} \in \mathbb{H}. \tag{6}$$

Make k large enough that $\mathcal{R}_\Phi$ is generated by $\{\varphi_\mathsf{h}^{p^k}\}_{\mathsf{h}\in\mathbb{H}}$. Let $\{\mathbf{b}_\mathsf{h}\}_{\mathsf{h}\in\mathbb{H}} \subseteq \mathbf{S}_\mathbb{B}$ be arbitrary, and find $\mathbf{s} \in \mathbf{S}$ satisfying equation (6). Then

$$\Phi^{p^k}(\mathbf{s})_\mathbb{B} \underset{(*)}{=} \sum_{\mathsf{h}\in\mathbb{H}} \varphi_\mathsf{h}^{p^k} \sigma^{p^k\mathsf{h}}(\mathbf{s})_\mathbb{B} = \sum_{\mathsf{h}\in\mathbb{H}} \varphi_\mathsf{h}^{p^k}\, \mathbf{s}_{\mathbb{B}+p^k\mathsf{h}} \underset{(\dagger)}{=} \sum_{\mathsf{h}\in\mathbb{H}} \varphi_\mathsf{h}^{p^k} \mathbf{b}_\mathsf{h}.$$

($(*)$ is by equation (5) and $(\dagger)$ is by equation (6).) But $[\Phi^{p^k}(\mathbf{s})]_\mathbb{B} \in \mathbf{S}_\mathbb{B}$, because $\Phi(\mathbf{S}) \subseteq \mathbf{S}$, because $\Phi(\mathbf{C}) \subseteq \mathbf{C}$. This verifies (c) in Lemma 6, for any finite $\mathbb{B} \subset \mathbb{M}$ and $\{\mathbf{b}_\mathsf{h}\}_{\mathsf{h}\in\mathbb{H}} \subseteq \mathbf{S}_\mathbb{B}$. □

LEMMA 7. *Let $\mathcal{R}$, $\mathcal{A}$, Φ, and $\mathcal{F}_\Phi$ be as in Theorem 3, and let $\mathbf{S} \subset \mathcal{A}^\mathbb{M}$ be a submodule shift. If $\mathbf{C}$ is any $(p, \mathbb{H})$-mixing, Φ-invariant coset shift of $\mathbf{S}$, then $\overline{\varphi}\,\mathbf{C} \subseteq \mathbf{S}$ for all $\overline{\varphi} \in \mathcal{F}_\Phi$.*

Proof. Let $\overline{\varphi} \in \mathcal{F}_\Phi$ and let $\mathbf{a} \in \mathbf{C}$. To show that $\overline{\varphi}\,\mathbf{a} \in \mathbf{S}$, it suffices to show, for any finite $\mathbb{B} \subset \mathbb{M}$, that $\overline{\varphi}\,\mathbf{a}_\mathbb{B} \in \mathbf{S}_\mathbb{B}$.

There exist arbitrarily large $k \in \mathbb{N}$ with $\overline{\varphi}_k = \overline{\varphi}$. But if k is large enough, then there exists $\mathbf{c} \in \mathbf{C}$ with $\mathbf{c}_{p^k\mathsf{h}+\mathbb{B}} = \mathbf{a}_\mathbb{B}$ for all $\mathsf{h} \in \mathbb{H}$ (because $\mathbf{C}$ is $(p, \mathbb{H})$-mixing). Thus, $\Phi^{p^k}(\mathbf{c})_\mathbb{B} = (\sum_{\mathsf{h}\in\mathbb{H}} \varphi_\mathsf{h}^{p^k})\,\mathbf{a}_\mathbb{B}$, by equation (5). Thus, $\overline{\varphi}_k\,\mathbf{a}_\mathbb{B} = \Phi^{p^k}(\mathbf{c})_\mathbb{B} - \mathbf{c}_\mathbb{B}$. But $\Phi^{p^k}(\mathbf{c})_\mathbb{B} - \mathbf{c}_\mathbb{B} = (\Phi^{p^k}(\mathbf{c}) - \mathbf{c})_\mathbb{B} \in \mathbf{S}_\mathbb{B}$ because $\Phi^{p^k}(\mathbf{c}) - \mathbf{c} \underset{(*)}{\in} \mathbf{C} - \mathbf{C} \underset{(\dagger)}{=} \mathbf{S}$, where $(*)$ is because $\Phi^{p^k}(\mathbf{C}) \subseteq \mathbf{C}$, and $(\dagger)$ is by (3). □

Proof of Theorem 3(b). We argue by contradiction. If $\mathcal{A}^\mathbb{B}/\mathbf{S}_\mathbb{B}$ is $\overline{\varphi}$-torsion-free, then $\mathcal{A}^{\mathbb{B}'}/\mathbf{S}_{\mathbb{B}'}$ is also $\overline{\varphi}$-torsion-free, for any $\mathbb{B}' \supseteq \mathbb{B}$. If $\mathbf{C} \neq \mathbf{S}$, and $\mathbb{B}$ is large enough, then $\mathbf{C}_\mathbb{B}$ is a non-trivial coset of the submodule $\mathbf{S}_\mathbb{B}$ in $\mathcal{A}^\mathbb{B}$; thus, $\mathbf{C}_\mathbb{B}$ is non-trivial as an element of the quotient module $\mathcal{A}^\mathbb{B}/\mathbf{S}_\mathbb{B}$. But Lemma 7 implies that $\overline{\varphi}\mathbf{C}_\mathbb{B} \subseteq \mathbf{S}_\mathbb{B}$, so $\overline{\varphi}$ annihilates $\mathbf{C}_\mathbb{B}$ in $\mathcal{A}^\mathbb{B}/\mathbf{S}_\mathbb{B}$, so $\mathcal{A}^\mathbb{B}/\mathbf{S}_\mathbb{B}$ has non-trivial $\overline{\varphi}$-torsion, which is a contradiction. By contradiction, $\mathbf{C} = \mathbf{S}$. □

Let $\mathbb{T} := \{c \in \mathbb{C}\,;\ |c| = 1\}$ be the unit circle group. If $(\mathbf{G}, +)$ is a compact abelian group (e.g. $\mathbf{G} := \mathcal{A}^\mathbb{M}$ where $(\mathcal{A}, +)$ is a finite abelian group), then a *character* on $\mathbf{G}$ is a continuous group homomorphism $\chi : (\mathbf{G}, +) \longrightarrow (\mathbb{T}, \cdot)$. Let $\widehat{\mathbf{G}}$ denote the group of characters of $\mathbf{G}$. If $\mu \in \mathfrak{M}_{\text{æs}}(\mathbf{G})$, then μ is uniquely identified by its *Fourier coefficients*

$$\widehat{\mu}[\chi] := \int_\mathbf{G} \chi \, d\mu \quad \text{for all } \chi \in \widehat{\mathbf{G}}.$$

For example, if $\eta_\mathbf{G}$ is the Haar measure on $\mathbf{G}$, and $\mathbf{1} \in \widehat{\mathbf{G}}$ is the trivial character, then it is easy to verify the following lemma.

LEMMA 8. *$\eta_\mathbf{G}$ is the unique Borel measure on $\mathbf{G}$ such that $\widehat{\eta}_\mathbf{G}[\mathbf{1}] = 1$ and $\widehat{\eta}_\mathbf{G}[\chi] = 0$ for all other $\chi \in \widehat{\mathbf{G}}$.* □

More generally, we have the following result.

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

LEMMA 9. *Let* $(\mathbf{G}, +)$ *be a compact abelian group, and let* $\mu \in \mathfrak{M}_{\mathrm{acs}}(\mathbf{G})$. *Then*

$(\mu = \eta_{\mathbf{S}}$ *for some closed subgroup* $\mathbf{S} \subseteq \mathbf{G}) \iff (\forall\ \chi \in \widehat{\mathbf{G}}$, *either* $\widehat{\mu}[\chi] = 0$ *or* $\widehat{\mu}[\chi] = 1)$.

Proof. '$\Longrightarrow$': Suppose that $\mu = \eta_{\mathbf{S}}$. If $\chi \in \widehat{\mathbf{G}}$, then $\chi_{|\mathbf{S}} \in \widehat{\mathbf{S}}$. Thus, Lemma 8 implies that

$$\widehat{\mu}[\chi] = \widehat{\mu}[\chi_{|\mathbf{S}}] = \begin{cases} 1 & \text{if } \chi_{|\mathbf{S}} \equiv \mathbf{1}_{\mathbf{S}}, \\ 0 & \text{otherwise.} \end{cases}$$

'$\Longleftarrow$': If $\gamma \in \widehat{\mathbf{G}}$ and $\widehat{\mu}[\gamma] = 1$, then $\mathsf{supp}(\mu) \subseteq \ker(\gamma)$. If $\mathbf{S} := \bigcap\{\ker(\gamma);\ \gamma \in \widehat{\mathbf{G}},\ \widehat{\mu}[\gamma] = 1\}$, then $\mathbf{S}$ is a closed subgroup of $\mathbf{G}$, and $\mathsf{supp}(\mu) \subseteq \mathbf{S}$. We claim $\mu = \eta_{\mathbf{S}}$. If $\chi \in \widehat{\mathbf{S}}$, then $\chi = \gamma_{|\mathbf{S}}$ for some $\gamma \in \widehat{\mathbf{G}}$ (this follows from the Pontryagin duality theorem; [**Wal82**, see, for example, fact (6), §0.7, p. 13]). If $\chi \neq \mathbf{1}_{\mathbf{S}}$, then $\mathbf{S} \not\subset \ker(\gamma)$, so $\widehat{\mu}[\gamma] \neq 1$, so $\widehat{\mu}[\gamma] = 0$ (by hypothesis), so $\widehat{\mu}[\chi] = 0$. Thus, Lemma 8 implies that $\mu = \eta_{\mathbf{S}}$. □

Let $(\mathcal{A}, +)$ be a finite abelian group, so that $(\mathcal{A}^{\mathbb{M}}, +)$ is compact abelian. For any $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$, there is a unique finite subset $\mathbb{B} \subset \mathbb{M}$ and unique non-trivial $\chi_{\mathsf{b}} \in \widehat{\mathcal{A}}$ for all $\mathsf{b} \in \mathbb{B}$ such that

$$\boldsymbol{\chi}(\mathbf{a}) = \prod_{\mathsf{b} \in \mathbb{B}} \chi_{\mathsf{k}}(a_{\mathsf{b}}) \quad \text{for all } \mathbf{a} \in \mathcal{A}^{\mathbb{M}}. \tag{7}$$

We say that $\boldsymbol{\chi}$ is *based* on $\mathbb{B}$. If $\{\boldsymbol{\chi}^{\mathsf{h}}\}_{\mathsf{h} \in \mathbb{H}} \subset \widehat{\mathcal{A}^{\mathbb{M}}}$ is an $\mathbb{H}$-indexed collection of characters based on $\mathbb{B}$, and μ is $(p, \mathbb{H})$-mixing, then equations (2) and (7) together imply that

$$\lim_{k \to \infty} \widehat{\mu}\left[\prod_{\mathsf{h} \in \mathbb{H}} \boldsymbol{\chi}^{\mathsf{h}} \circ \sigma^{-p^k \mathsf{h}} \right] = \prod_{\mathsf{h} \in \mathbb{H}} \widehat{\mu}[\boldsymbol{\chi}^{\mathsf{h}}]. \tag{8}$$

Proof of Theorem 3(c). If $\mathbf{C} = \mathsf{supp}(\mu)$, then Theorem 3(a) says that $\mathbf{C}$ is an $\mathcal{R}_\Phi$-coset shift—that is, $\mathbf{C} = \mathbf{c} + \mathbf{S}$, where $\mathbf{S}$ is an $\mathcal{R}_\Phi$-submodule shift. Let $\nu := \tau^{-\mathbf{c}}(\mu)$; then $\mathsf{supp}(\nu) = \mathbf{S}$. To show that $\mu = \eta_{\mathbf{C}}$, we must show that $\nu = \eta_{\mathbf{S}}$; we will do this with Lemma 9. For any $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$, note that

$$|\widehat{\mu}[\boldsymbol{\chi}]| \underset{(*)}{=} |\boldsymbol{\chi}(\mathbf{c}) \cdot \widehat{\nu}[\boldsymbol{\chi}]| = |\boldsymbol{\chi}(\mathbf{c})| \cdot |\widehat{\nu}[\boldsymbol{\chi}]| \underset{(\dagger)}{=} |\widehat{\nu}[\boldsymbol{\chi}]|. \tag{9}$$

(Here, $(*)$ is because $\mu = \tau^{\mathbf{c}}(\nu)$ and $\boldsymbol{\chi}$ is a homomorphism, while $(\dagger)$ is because $\boldsymbol{\chi}[\mathbf{c}] \in \mathbb{T}$.) Now, let $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$, and suppose that $\widehat{\nu}[\boldsymbol{\chi}] \neq 1$; we must show that $\widehat{\nu}[\boldsymbol{\chi}] = 0$. Let k be large enough that $\mathcal{R}_\Phi$ is generated by $\{\varphi_{\mathsf{h}}^{p^k}\}_{\mathsf{h} \in \mathbb{H}}$. Let Γ be the multiplicative group generated by $\{\varphi_{\mathsf{h}}^{p^k}\}_{\mathsf{h} \in \mathbb{H}}$ (which are units, by hypothesis).

CLAIM 1. $\Gamma \subset \mathcal{R}_\Phi$.

Proof. By definition, $\mathcal{R}_\Phi$ contains all products of positive powers of $\{\varphi_{\mathsf{h}}^{p^k}\}_{\mathsf{h} \in \mathbb{H}}$; we must show that it contains the negative powers as well. For all $\mathsf{h} \in \mathbb{H}$, the unit $\varphi_{\mathsf{h}}^{p^k}$ has finite multiplicative order, because $\mathcal{R}_\Phi$ is finite; thus, there is some $n \in \mathbb{N}$ such that $(\varphi_{\mathsf{h}}^{p^k})^{-1} = (\varphi_{\mathsf{h}}^{p^k})^n \in \mathcal{R}_\Phi$. Thus, $\mathcal{R}_\Phi$ contains all products of integer powers (positive or negative) of $\{\varphi_{\mathsf{h}}^{p^k}\}_{\mathsf{h} \in \mathbb{H}}$; hence, $\Gamma \subset \mathcal{R}_\Phi$. ◇ [Claim 1]

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

If $\gamma \in \Gamma$, then $\boldsymbol{\chi} \circ \gamma \in \widehat{\mathcal{A}^{\mathbb{M}}}$ (it is a composition of two homomorphisms). Define

$$M := \max_{\gamma \in \Gamma} |\widehat{\nu}[\boldsymbol{\chi} \circ \gamma]|. \tag{10}$$

Thus, $|\widehat{\nu}[\boldsymbol{\chi}]| \leq M$. We will show that $M = 0$.

CLAIM 2. $M < 1$.

Proof. The proof is by contradiction. Γ is finite, so if $M = 1$, then there is some $\gamma \in \Gamma$ such that $|\widehat{\nu}[\boldsymbol{\chi} \circ \gamma]| = 1$. Let $t := \widehat{\nu}[\boldsymbol{\chi} \circ \gamma]$; then $t \in \mathbb{T}$, and $\mathsf{supp}(\nu) \subseteq (\boldsymbol{\chi} \circ \gamma)^{-1}\{t\}$. But $\mathbf{0} \in \mathsf{supp}(\nu)$ (because $\mathsf{supp}(\nu) = \mathbf{S}$ is a submodule), so $t = 1$; hence $\widehat{\nu}[\boldsymbol{\chi} \circ \gamma] = 1$. Thus, $\nu[\ker(\boldsymbol{\chi} \circ \gamma)] = 1$, hence $\mathbf{S} \subseteq \ker(\boldsymbol{\chi} \circ \gamma)$, hence $\gamma(\mathbf{S}) \subseteq \ker(\boldsymbol{\chi})$.

Now $\gamma^{-1} \in \Gamma \subset \mathcal{R}_\Phi$ (by Claim 1), and $\mathbf{S}$ is an $\mathcal{R}_\Phi$-module (by Theorem 3(a)), so $\gamma^{-1}(\mathbf{S}) \subseteq \mathbf{S}$, so $\mathbf{S} \subseteq \gamma(\mathbf{S}) \underset{(*)}{\subseteq} \ker(\boldsymbol{\chi})$, where $(*)$ is by the previous paragraph. But then $\widehat{\nu}[\boldsymbol{\chi}] = 1$, which contradicts the definition of $\boldsymbol{\chi}$.

By contradiction, we must have $M < 1$. ◇ [Claim 2]

By replacing $\boldsymbol{\chi}$ with $\boldsymbol{\chi} \circ \gamma$ for some $\gamma \in \Gamma$ if necessary, we can assume without loss of generality that $|\widehat{\nu}[\boldsymbol{\chi}]| = M$. Then $|\widehat{\mu}[\boldsymbol{\chi}]| = M$ also, by equation (9). Thus it suffices to evaluate $\widehat{\mu}[\boldsymbol{\chi}]$. But if Φ has polynomial representation (4), then, for any $k \in \mathbb{N}$,

$$\begin{aligned}
\widehat{\mu}[\boldsymbol{\chi}] &:= \int_{\mathcal{A}^{\mathbb{M}}} \boldsymbol{\chi} \; d\mu \underset{(a)}{=} \int_{\mathcal{A}^{\mathbb{M}}} \boldsymbol{\chi} \; d(\Phi^{(p^k)}\mu) \underset{(b)}{=} \int_{\mathcal{A}^{\mathbb{M}}} \boldsymbol{\chi} \circ \Phi^{(p^k)} \; d\mu \\
&\underset{(c)}{=} \int_{\mathcal{A}^{\mathbb{M}}} \boldsymbol{\chi} \circ \left(\sum_{\mathsf{h} \in \mathbb{H}} \varphi_{\mathsf{h}}^{(p^k \mathsf{h})} \sigma^{(p^k \mathsf{h})} \right) d\mu \underset{(h)}{=} \int_{\mathcal{A}^{\mathbb{M}}} \prod_{\mathsf{h} \in \mathbb{H}} (\boldsymbol{\chi} \circ \varphi_{\mathsf{h}}^{(p^k \mathsf{h})} \circ \sigma^{(p^k \mathsf{h})}) \; d\mu \\
&= \widehat{\mu}\left[\prod_{\mathsf{h} \in \mathbb{H}} \boldsymbol{\chi} \circ \varphi_{\mathsf{h}}^{(p^k \mathsf{h})} \circ \sigma^{(p^k \mathsf{h})} \right].
\end{aligned} \tag{11}$$

(Here, (a) is because μ is Φ-invariant; (b) is a change of variables; (c) is by equation (5); and (h) is because $\boldsymbol{\chi}$ is a homomorphism.) Thus,

$$\widehat{\mu}[\boldsymbol{\chi}] \underset{(11)}{=} \lim_{k \to \infty} \widehat{\mu}\left[\prod_{\mathsf{h} \in \mathbb{H}} \boldsymbol{\chi} \circ \varphi_{\mathsf{h}}^{(p^k \mathsf{h})} \circ \sigma^{(p^k \mathsf{h})} \right] \underset{(*)}{\leq} \limsup_{k \to \infty} \prod_{\mathsf{h} \in \mathbb{H}} \widehat{\mu}[\boldsymbol{\chi} \circ \varphi_{\mathsf{h}}^{(p^k \mathsf{h})}], \tag{12}$$

where $(*)$ is by equation (8), because μ is $(p, \mathbb{H})$-mixing and Γ is finite. Thus,

$$M = |\widehat{\mu}[\boldsymbol{\chi}]| \underset{(12)}{\leq} \limsup_{k \to \infty} \prod_{\mathsf{h} \in \mathbb{H}} |\widehat{\mu}[\boldsymbol{\chi} \circ \varphi_{\mathsf{h}}^{(p^k \mathsf{h})}]| \underset{(*)}{\leq} \lim_{k \to \infty} \prod_{\mathsf{h} \in \mathbb{H}} M = M^H.$$

(Here, $(*)$ is by equations (9) and (10).) But $H \geq 2$, and Claim 2 says $M < 1$. Thus, $M = 0$. Thus, $|\widehat{\nu}[\boldsymbol{\chi}]| = 0$.

This holds for any $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$ with $\widehat{\nu}[\boldsymbol{\chi}] \neq 1$, so Lemma 9 says $\nu = \eta_{\mathbf{S}}$; hence $\mu = \eta_{\mathbf{C}}$. □

4. *Constructing coset shifts*

To enumerate all $(p, \mathbb{H})$-mixing, Φ-invariant measures, Theorem 3(c) says it suffices to enumerate all $(p, \mathbb{H})$-mixing, Φ-invariant coset shifts. But if $\mathbf{S} \subset \mathcal{A}^{\mathbb{M}}$ is a submodule shift, not every coset of $\mathbf{S}$ is a coset *shift*. Indeed, let $\mathbf{c} \in \mathcal{A}^{\mathbb{M}}$, and for all $\mathsf{m} \in \mathbb{M}$, let $\mathbf{b}^{\mathsf{m}} := \sigma^{\mathsf{m}}(\mathbf{c}) - \mathbf{c}$. Then it is easy to check that

$$(\text{the coset } \mathbf{c} + \mathbf{S} \text{ is a subshift}) \Longleftrightarrow (\mathbf{b}^{\mathsf{m}} \in \mathbf{S} \text{ for all } \mathsf{m} \in \mathbb{M}). \tag{13}$$

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

We call $\mathbf{B} := \{\mathbf{b}^{\mathsf{m}}\}_{\mathsf{m}\in\mathbb{M}}$ the *coboundary* of $\mathbf{c}$. More generally, an $\mathcal{A}^{\mathbb{M}}$-valued *cocycle* is any $\mathbb{M}$-indexed collection $\{\mathbf{b}^{\mathsf{m}}\}_{\mathsf{m}\in\mathbb{M}} \subseteq \mathcal{A}^{\mathbb{M}}$ such that $\mathbf{b}^{\mathsf{m}+\mathsf{n}} = \sigma^{\mathsf{n}}(\mathbf{b}^{\mathsf{m}}) + \mathbf{b}^{\mathsf{n}}$, for all $\mathsf{n}, \mathsf{m} \in \mathbb{M}$.

LEMMA 10.

(a) *If* $\mathbf{c} \in \mathcal{A}^{\mathbb{M}}$, *then its coboundary* $\mathbf{B}$ *is a cocycle.*

(b) $\mathbf{c}$ *is entirely determined by* c_0 *and* $\mathbf{B}$, *because* $c_{\mathsf{m}} = c_0 + b_0^{\mathsf{m}}$, *for all* $\mathsf{m} \in \mathbb{M}$.

(c) *Let* $\mathbf{B} := \{\mathbf{b}^{\mathsf{m}}\}_{\mathsf{m}\in\mathbb{M}} \subset \mathbf{S}$ *be any cocycle, and let* $c_0 \in \mathcal{A}$ *be arbitrary. Define* $\mathbf{c} := [c_{\mathsf{m}}]_{\mathsf{m}\in\mathbb{M}}$ *according to part* (b). *Then* $\mathbf{B}$ *is the coboundary of* $\mathbf{c}$,

Proof. **(a)** is straightforward. **(b)** is because $c_{\mathsf{m}} = (\sigma^{\mathsf{m}}(\mathbf{c}))_0 = (\mathbf{c} + \mathbf{b}^{\mathsf{m}})_0 = c_0 + b_0^{\mathsf{m}}$. For **(c)**, let $\mathsf{m}, \mathsf{n} \in \mathbb{M}$. Then $[\sigma^{\mathsf{m}}(\mathbf{c}) - \mathbf{c}]_{\mathsf{n}} = c_{\mathsf{m}+\mathsf{n}} - c_{\mathsf{n}} := (c_0 + b_0^{\mathsf{m}+\mathsf{n}}) - (c_0 + b_0^{\mathsf{n}}) = b_0^{\mathsf{m}+\mathsf{n}} - b_0^{\mathsf{n}} = (\mathbf{b}^{\mathsf{m}+\mathsf{n}} - \mathbf{b}^{\mathsf{n}})_0 \underset{(*)}{=} \sigma^{\mathsf{n}}(\mathbf{b}^{\mathsf{m}})_0 = b_{\mathsf{n}}^{\mathsf{m}}$, where $(*)$ is the cocycle property. This holds for all $\mathsf{n} \in \mathbb{M}$, so $\sigma^{\mathsf{m}}(\mathbf{c}) - \mathbf{c} = \mathbf{b}^{\mathsf{m}}$. This holds for all $\mathsf{m} \in \mathbb{M}$, so $\mathbf{B}$ is the coboundary of $\mathbf{c}$. □

Lemma 10 and (13) imply that, to construct a coset shift of $\mathbf{S}$, it suffices to construct an $\mathbf{S}$-valued cocycle. In particular, if $a \in \mathcal{A}$ such that $a^{\mathbb{M}} \in \mathbf{S}$, then we can get one $\mathbf{S}$-valued cocycle by defining $\mathbf{b}^{\mathsf{m}} := (m_1 + \cdots + m_D)a^{\mathbb{M}}$, for all $\mathsf{m} = (m_1, \ldots, m_D) \in \mathbb{M}$; in Lemma 10(c) in this case, $c_{\mathsf{m}} = c_0 + (m_1 + \cdots + m_D)a$ for all $\mathsf{m} \in \mathbb{M}$. For example, if $\mathbf{S}$ is as in Example 4, then $1^{\mathbb{M}} \in \mathbf{S}$. In this case, $\mathbf{b}^{(m,n)} = 0^{\mathbb{M}}$ if $m + n$ is even, and $\mathbf{b}^{(m,n)} = 1^{\mathbb{M}}$ if $m + n$ is odd. If $c_0 := 0$, and we define $\mathbf{c}$ as in Lemma 10(b), then we get precisely the 'checkerboard' configuration of Example 4; thus $\mathbf{C} = \mathbf{c} + \mathbf{S}$ is a non-trivial coset shift, as previously claimed.

5. *Extension to rings of squarefree characteristic*

We say $m \in \mathbb{N}$ is *squarefree* if m has prime factorization $m = p_1 p_2 \cdots p_J$, where $p_1, \ldots, p_J$ are distinct primes. If $\mathcal{R}$ has *non-prime* characteristic, then equation (5) is no longer true. However, the next result allows us to reduce squarefree-characteristic LCA to the previous case of prime-characteristic LCA.

PROPOSITION 11. *Let* $\mathcal{R}$ *be a commutative ring with characteristic* $m = p_1^{s_1} p_2^{s_2} \cdots p_J^{s_J}$, *where* $p_1, \ldots, p_J$ *are distinct primes. For all* $j \in [1 \ldots J]$, *let* $q_j := m/p_j^{s_j}$, *and let* $\mathcal{I}_j := \{r \in \mathcal{R} \,;\, q_j r = 0\}$.

(a) $\mathcal{I}_j$ *is an ideal of* $\mathcal{R}$, *and the quotient ring* $\mathcal{R}_j := \mathcal{R}/\mathcal{I}_j$ *has characteristic* $p_j^{s_j}$.

(b) $\mathcal{R}$ *is isomorphic to the direct product* $\widetilde{\mathcal{R}} := \mathcal{R}_1 \oplus \mathcal{R}_2 \oplus \cdots \oplus \mathcal{R}_J$, *via the map* $\mathcal{R} \ni r \mapsto (r^1, r^2, \ldots, r^J) \in \widetilde{\mathcal{R}}$, *where for all* $j \in [1 \ldots J]$, *we define* $r^j := (r + \mathcal{I}_j) \in \mathcal{R}_j$.

(c) *Let* $\mathcal{A}$ *be any* $\mathcal{R}$*-module. For all* $j \in [1 \ldots J]$, *let*

$$\mathcal{B}_j := \mathcal{I}_j\mathcal{A} := \{ia \,;\, i \in \mathcal{I}_j \text{ and } a \in \mathcal{A}\}$$

(a submodule), and let $\mathcal{A}_j := \mathcal{A}/\mathcal{B}_j$ *be the quotient module. Then* $\mathcal{A} \cong \widetilde{\mathcal{A}} := \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_J$, *via the map* $\mathcal{A} \ni a \mapsto (a^1, \ldots, a^J) \in \widetilde{\mathcal{A}}$, *where for all* $j \in [1 \ldots J]$, *we define* $a^j := (a + \mathcal{B}_j) \in \mathcal{A}_j$. *Furthermore,* $\widetilde{\mathcal{R}}$ *acts on* $\widetilde{\mathcal{A}}$ *componentwise; that is, for any* $\widetilde{r} = (r^1, \ldots, r^J) \in \widetilde{\mathcal{R}}$ *and* $\widetilde{a} = (a^1, \ldots, a^J) \in \widetilde{\mathcal{A}}$, *we have* $\widetilde{r} \cdot \widetilde{a} = (r^1 a^1, \ldots, r^J a^J)$.

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

Proof. (a) is straightforward. (b) follows from the Chinese remainder theorem for rings [**DF91**, Theorem 17, p. 268, §10.3] and the following claim. □

CLAIM 1. (i) $\mathcal{I}_1 \cap \mathcal{I}_2 \cap \cdots \cap \mathcal{I}_J = \{0\}$. (ii) *For any* $j \neq k$, $\mathcal{I}_j + \mathcal{I}_k = \mathcal{R}$.

Proof. (i) If $r \in \bigcap_{j=1}^{J} \mathcal{I}_j$ then $q_j r = 0$ for all $j \in [1 \ldots J]$. But $\gcd(q_1, \ldots, q_J) = 1$, so Bezout's identity yields $z_1, \ldots, z_J \in \mathbb{Z}$ such that $\sum_{j=1}^{J} z_j q_j = 1$. But then $r = 1 \cdot r = \sum_{j=1}^{J} z_j q_j r = \sum_{j=1}^{J} z_j 0 = 0$.

(ii) $\mathcal{I}_j + \mathcal{I}_k$ is an ideal, so it suffices to show that $\mathcal{I}_j + \mathcal{I}_k$ contains $1_{\mathcal{R}}$. Let $\widetilde{\mathbf{Z}}_m$ be the subring of $\mathcal{R}$ generated by $1_{\mathcal{R}}$; then $\widetilde{\mathbf{Z}}_m$ is isomorphic to $\mathbb{Z}_{/m}$. It is easy to check that $\widetilde{\mathbf{Z}}_m \cap \mathcal{I}_j = p_j^{s_j} \widetilde{\mathbf{Z}}_m$ and $\widetilde{\mathbf{Z}}_m \cap \mathcal{I}_k = p_k^{s_k} \widetilde{\mathbf{Z}}_m$. But then $1_{\mathcal{R}} \in p_j^{s_j} \widetilde{\mathbf{Z}}_m + p_k^{s_k} \widetilde{\mathbf{Z}}_m$, because $1 \in p_j^{s_j} \mathbb{Z}_{/m} + p_k^{s_k} \mathbb{Z}_{/m}$ by Bezout's identity, because $\gcd(p_j^{s_j}, p_k^{s_k}) = 1$ (because p_j and p_k are distinct primes). ◇ [Claim 1]

(c) follows from Claim 1 and the Chinese remainder theorem for modules [**DF91**, Ex. 16–17, p. 333, §10.3]. □

Example 12. Suppose $\mathcal{A} = \mathcal{R} := \mathbb{Z}_{/m}$, where $m = p_1 \cdots p_J$. Then for all $j \in [1 \ldots J]$, we have $\mathcal{I}_j = p_j \mathbb{Z}_{/m}$ in Proposition 11(a), so $\mathcal{A}_j = \mathcal{R}_j = \mathbb{Z}_{/m}/(p_j \mathbb{Z}_{/m}) \cong \mathbb{Z}_{/p_j}$ in Proposition 11(b,c) which is the classic Chinese remainder theorem.

Let $\mathcal{A} \cong \bigoplus_{j=1}^{J} \mathcal{A}_j$ as in Proposition 11(c). Define $\Psi : \mathcal{A}^{\mathbb{M}} \longrightarrow \bigoplus_{j=1}^{J} \mathcal{A}_j^{\mathbb{M}}$ by

$$\Psi([a_{\mathsf{m}}]_{\mathsf{m} \in \mathbb{M}}) := ([a_{\mathsf{m}}^1]_{\mathsf{m} \in \mathbb{M}}, [a_{\mathsf{m}}^2]_{\mathsf{m} \in \mathbb{M}}, \ldots, [a_{\mathsf{m}}^J]_{\mathsf{m} \in \mathbb{M}}), \tag{14}$$

where, for any $a \in \mathcal{A}$, we write $a \cong (a^1, \ldots, a^J)$ as in Proposition 11(c). Then Ψ is a σ-commuting, homeomorphic $\mathcal{R}$-module isomorphism. If $\mu \in \mathfrak{M}_{\text{ergs}}(\mathcal{A}^{\mathbb{M}})$, then for all $j \in [1 \ldots J]$, let μ_j be the projection of $\Psi(\mu)$ to $\mathcal{A}_j^{\mathbb{M}}$; we say that μ is a *joining* of $\mu_1, \ldots, \mu_J$. (See [**dlR06**] or [**Rud90**, Ch. 6] for more about joinings.)

PROPOSITION 13. *Let $\mathcal{R}$ be a commutative ring of squarefree characteristic, let $\mathcal{A}$ be an $\mathcal{R}$-module, and write $\mathcal{A} \cong \bigoplus_{j=1}^{J} \mathcal{A}_j$ as in Proposition 11(c). Let $\Phi \in \mathcal{R}\text{-}\mathsf{LCA}(\mathcal{A}^{\mathbb{M}})$ have neighbourhood $\mathbb{H}$ and coefficients $\{\varphi_{\mathsf{h}}\}_{\mathsf{h} \in \mathbb{H}}$, all of which are units. If $\mu \in \mathfrak{M}_{\text{ergs}}(\mathcal{A}^{\mathbb{M}}; \Phi, \sigma)$ is $\mathbb{H}$-mixing, then μ is a joining of measures $\mu_1, \ldots, \mu_J$, where for each $j \in [1 \ldots J]$, μ_j is the Haar measure of some Φ_j-invariant $\mathcal{R}_j$-coset shift of $\mathcal{A}_j^{\mathbb{M}}$.*

Proof. For all $\mathsf{h} \in \mathbb{H}$, write $\varphi_{\mathsf{h}} = (\varphi_{\mathsf{h}}^1, \ldots, \varphi_{\mathsf{h}}^J)$ as in Proposition 11(b). Then φ_{h}^j is a unit in $\mathcal{R}_j$ for each $j \in [1 \ldots J]$. For all $j \in [1 \ldots J]$, let $\Phi_j \in \mathcal{R}_j\text{-}\mathsf{LCA}(\mathcal{A}_j^{\mathbb{M}})$ have local rule $\phi(\mathbf{a}_{\mathbb{H}}^j) = \sum_{\mathsf{h} \in \mathbb{H}} \varphi_{\mathsf{h}}^j a_{\mathsf{h}}^j$, for any $\mathbf{a}_{\mathbb{H}}^j \in \mathcal{A}_j^{\mathbb{H}}$. If Ψ is as in equation (14), then Proposition 11(c) implies that Ψ is a topological conjugacy from $(\mathcal{A}^{\mathbb{M}}, \Phi)$ to the direct product $(\mathcal{A}_1^{\mathbb{M}}, \Phi_1) \times \cdots \times (\mathcal{A}_J^{\mathbb{M}}, \Phi_J)$. For all $j \in [1 \ldots J]$, let μ_j be the projection of $\Psi(\mu)$ to $\mathcal{A}_j^{\mathbb{M}}$; then $\mu_j \in \mathfrak{M}_{\text{ergs}}(\mathcal{A}_j^{\mathbb{M}}; \Phi_j, \sigma)$ and is $\mathbb{H}$-mixing; hence, Theorem 3(c) implies that μ_j is the Haar measure for some $\mathcal{R}_j$-coset shift of $\mathcal{A}_j^{\mathbb{M}}$. □

COROLLARY 14. *Let $\mathcal{A} = \mathbb{Z}_{/m}$, where $m = p_1 \cdots p_J$ is squarefree. Let $\mathbb{M} := \mathbb{Z}^D \times \mathbb{N}^E$, and let $\Phi \in \mathbb{Z}_{/m}\text{-}\mathsf{LCA}(\mathcal{A}^{\mathbb{M}})$ have a neighbourhood of cardinality $H \geq 2$. Let $\mu \in \mathfrak{M}_{\text{ergs}}(\mathcal{A}^{\mathbb{M}}; \Phi, \sigma)$ be (σ, H)-mixing, and suppose that either:*

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

(i) $D + E = 1$; *or* *(ii)* $h(\mu, \sigma) > \log_2(m) - \log_2(\min\{p_1, \ldots, p_J\})$.

Then μ is a joining of the uniform Bernoulli measures on $\mathcal{A}_1^{\mathbb{M}}, \ldots, \mathcal{A}_J^{\mathbb{M}}$, where $\mathcal{A}_j := \mathbb{Z}_{/p_j}$ for each $j \in [1 \ldots J]$.

Proof. Case (i) follows immediately from Proposition 13 and case (i) of Corollary 5.

Case (ii): For each $i \in [1 \ldots J]$, let μ_i be as in Proposition 13. Then

$$h(\mu_i) \underset{(*)}{\geq} h(\mu) - \sum_{i \neq j = 1}^{J} h(\mu_j) \underset{(\dagger)}{\geq} h(\mu) - \sum_{i \neq j = 1}^{J} \log_2(p_j) \underset{(\ddagger)}{=} h(\mu) - \log_2(m) + \log_2(p_i)$$
$$\underset{(\diamond)}{>} \log_2(m) - \log_2(\min\{p_j\}_{j=1}^{J}) - \log_2(m) + \log_2(p_i) \geq 0.$$

Here, $(*)$ is because $h(\mu) \leq \sum_{j=1}^{J} h(\mu_j)$, while $(\dagger)$ is because for each $j \in [1 \ldots J]$ we have $h(\mu_j) \leq h_{\text{top}}(\mathcal{A}_j^{\mathbb{M}}) = \log_2 |\mathcal{A}_j| = \log_2(p_j)$. Next, $(\ddagger)$ is because $m = p_1 \cdots p_J$, and $(\diamond)$ is by the hypothesis of case (ii).

Thus, case (ii) of Corollary 5 implies that μ_i is the uniform Bernoulli measure on $\mathcal{A}_i^{\mathbb{M}}$. This holds for all $i \in [1 \ldots J]$; the result follows. □

References

[DF91] D. S. Dummit and R. M. Foote. *Abstract Algebra*. Prentice Hall, Englewood Cliffs, NJ, 1991.

[dlR06] T. de la Rue. An introduction to joinings in ergodic theory. *Discrete Contin. Dyn. Syst.* **15**(1) (2006), 121–142.

[Ein05] M. Einsiedler. Isomorphism and measure rigidity for algebraic actions on zero-dimensional groups. *Monatsh. Math.* **144**(1) (2005), 39–69.

[Hed69] G. A. Hedlund. Endormorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory* **3** (1969), 320–375.

[HMM03] B. Host, A. Maass and S. Martıńez. Uniform Bernoulli measure in dynamics of permutative cellular automata with algebraic local rules. *Discrete Contin. Dyn. Syst.* **9**(6) (2003), 1423–1446.

[Kit87] B. P. Kitchens. Expansive dynamics on zero-dimensional groups. *Ergod. Th. & Dynam. Sys.* **7**(2) (1987), 249–261.

[Kit00] B. Kitchens. Dynamics of $\mathbf{Z}^d$ actions on Markov subgroups. *Topics in Symbolic Dynamics and Applications (Temuco, 1997) (London Mathematical Society Lecture Note Seres, 279)*. Cambridge University Press, Cambridge, 2000, pp. 89–122.

[KS89] B. Kitchens and K. Schmidt. Automorphisms of compact groups. *Ergod. Th. & Dynam. Sys.* **9**(4) (1989), 691–735.

[KS92] B. Kitchens and K. Schmidt. Markov subgroups of $(\mathbf{Z}/2\mathbf{Z})^{\mathbf{Z}^2}$. *Symbolic Dynamics and its Applications (New Haven, CT, 1991) (Contemporary Mathematics, 135)*. American Mathematical Society, Providence, RI, 1992, pp. 265–283.

[KS93] B. Kitchens and K. Schmidt. Mixing sets and relative entropies for higher-dimensional Markov shifts. *Ergod. Th. & Dynam. Sys.* **13**(4) (1993), 705–735.

[Led78] F. Ledrappier. Un champ markovien peut être d'entropie nulle et mélangeant. *C. R. Acad. Sci. Paris Sér. A-B* **287**(7) (1978), A561–A563.

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

[Piv05] M. Pivato. Invariant measures for bipermutative cellular automata. *Discrete Contin. Dyn. Syst.* **12**(4) (2005), 723–736.

[Rud90] D. J. Rudolph. *Fundamentals of Measurable Dynamics (Ergodic Theory on Lebesgue Spaces)*. Oxford University Press, New York, 1990.

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press

[Sab07] M. Sablik. Measure rigidity for algebraic bipermutative cellular automata. *Ergodic Th. & Dynam. Sys.* **27**(6) (2007), 1965–1990.

[Sch95a] K. Schmidt. *Dynamical Systems of Algebraic Origin (Progress in Mathematics, 128)*. Birkhäuser, Basel, 1995.

[Sch95b] K. Schmidt. Invariant measures for certain expansive $\mathbf{Z}^2$-actions. *Israel J. Math.* **90**(1–3) (1995), 295–300.

[Wal82] P. Walters. *An Introduction to Ergodic Theory (Graduate Texts in Mathematics, 79)*. Springer, New York, 1982.

https://doi.org/10.1017/S0143385708000096 Published online by Cambridge University Press