Ergod. Th. & Dynam. Sys. (2006), **26**, 1203–1224
doi:10.1017/S0143385706000216
© *2006 Cambridge University Press*
Printed in the United Kingdom

Asymptotic randomization of subgroup shifts by linear cellular automata

ALEJANDRO MAASS†, SERVET MARTÍNEZ†, MARCUS PIVATO‡
and REEM YASSAWI‡

† *Departamento de Ingeniería Matemática and Centro de Modelamiento Matemático, Universidad de Chile, Casilla 170 Correo 3, Santiago, Chile*
(e-mail: {amaass, smartine}@dim.uchile.cl)

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

(*Received* 6 *September* 2004 *and accepted* 28 *March* 2006)

Abstract. Let $\mathbb{M} = \mathbb{N}^D$ be the positive orthant of a D-dimensional lattice and let $(\mathcal{G}, +)$ be a finite abelian group. Let $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ be a subgroup shift, and let μ be a Markov random field whose support is $\mathfrak{G}$. Let $\Phi : \mathfrak{G} \longrightarrow \mathfrak{G}$ be a linear cellular automaton. Under broad conditions on $\mathcal{G}$, we show that the Cesaro average $N^{-1} \sum_{n=0}^{N-1} \Phi^n(\mu)$ converges to a measure of maximal entropy for the shift action on $\mathfrak{G}$.

1. *Introduction and main results*

Let $(\mathcal{G}, +)$ be a finite abelian group and let $\mathbb{M} = \mathbb{N}^D$ be the positive orthant of a D-dimensional lattice. Let $\mathcal{G}^{\mathbb{M}}$ be the set of all $\mathbb{M}$-indexed configurations of values in $\mathcal{G}$, which is a compact abelian topological group under componentwise addition. Let $\mathfrak{G}$ be a subgroup shift of $\mathcal{G}^{\mathbb{M}}$. A *cellular automaton* (CA) on $\mathfrak{G}$ is a continuous function $\Phi : \mathfrak{G} \longrightarrow \mathfrak{G}$ which commutes with all $\mathbb{M}$-shifts, $\boldsymbol{\sigma}^m : \mathcal{G}^{\mathbb{M}} \longrightarrow \mathcal{G}^{\mathbb{M}}$, $m \in \mathbb{M}$. We call Φ a *linear cellular automaton* (LCA) on $\mathfrak{G}$ if

$$\Phi(\mathbf{g}) = \sum_{i \in \mathbb{I}} \varphi_i \cdot \boldsymbol{\sigma}^i(\mathbf{g}) \quad \text{for all } \mathbf{g} = (g_m : m \in \mathbb{M}) \in \mathfrak{G}, \tag{1}$$

where $\mathbb{I} \subseteq \mathbb{M}$ is a finite subset and $\varphi_i \in \mathbb{Z}$ for all $i \in \mathbb{I}$. We say Φ is *proper* if at least two different coefficients φ_j, φ_k are relatively prime to $|\mathcal{G}|$, the cardinality of $\mathcal{G}$.

The *Haar measure* on $\mathfrak{G}$ is the unique Borel probability measure which is invariant under translation by any element of $\mathfrak{G}$. Under certain conditions (e.g. $\mathbb{M} = \mathbb{N}$), the measure of maximal entropy of $\mathfrak{G}$ for the shift action is unique and equal to the Haar measure on $\mathfrak{G}$. In general, however, it is known that the measure of maximal entropy is not unique (see the end of §2).

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

If μ is some probability measure on $\mathfrak{G}$ and Φ is a CA on $\mathfrak{G}$, then Φ *asymptotically randomizes* μ if

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \Phi^n(\mu) = \nu, \tag{2}$$

where ν is some measure of maximal entropy on $\mathfrak{G}$ and convergence is in the weak* topology.

This paper concerns the description of classes of measures that are randomized by LCA on subgroup shifts. More specifically this study is done for subgroup shifts whose follower cosets satisfy a special property called the *follower lifting property* (FLP).

We point out that this study has been done in previous work for the full shift $\mathcal{G}^{\mathbb{M}}$. In that case, the Haar measure corresponds to the uniform Bernoulli measure and it is the unique measure of maximal entropy. A broad class of probability measures are asymptotically randomized under the action of an LCA; these include any fully supported Markov measure when $\mathbb{M} = \mathbb{N}$ or any fully supported Markov random field, when $\mathbb{M} = \mathbb{N}^D$, $D \geq 2$ (see [**Lin84, MM98, FMMN00, PY02, Piv03, MHM03, PY04, Piv05, PY06**]).

Based on these results our strategy is the following: from the FLP property we can reduce the action of an LCA on a subgroup shift to the action of an LCA on a full shift, and then apply known results to establish asymptotic randomization.

In §2 we provide relevant background on LCA and subgroup shifts, and in §3 we study the action of one-dimensional LCA on subgroup Markov shifts of $\mathcal{G}^{\mathbb{N}}$ (simply called *Markov subgroups*). We conclude this introduction by listing our main results.

THEOREM 1. *Let $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}}$ be a transitive Markov subgroup with the FLP. If μ is any M-step Markov measure on $\mathfrak{G}$ with full support, and $\Phi : \mathfrak{G} \longrightarrow \mathfrak{G}$ is any proper LCA, then Φ asymptotically randomizes μ to the Haar measure on $\mathfrak{G}$.*

If p is a prime number, an abelian *p-group* is a product of p-power cyclic groups (e.g. if $p = 3$, then $\mathcal{G} = \mathbb{Z}_{/3} \oplus (\mathbb{Z}_{/27})^2 \oplus \mathbb{Z}_{/81}$ is a p-group). If $\mathcal{G}$ is a p-group, then any Markov subgroup of $\mathcal{G}^{\mathbb{N}}$ has the FLP (Theorem 20), so we get the following result.

COROLLARY 2. *Let $p \in \mathbb{N}$ be prime and let $\mathcal{G}$ be an abelian p-group. If $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}}$ is any transitive Markov subgroup, and μ is any M-step Markov measure on $\mathfrak{G}$ with full support, then any proper LCA acting on $\mathfrak{G}$ asymptotically randomizes μ to the Haar measure on $\mathfrak{G}$.*

Any finite abelian group $\mathcal{G}$ is a product of p-groups, and an LCA on $\mathcal{G}^{\mathbb{N}}$ (respectively subgroup shift) is a product of LCA on the separate p-group (respectively subgroup shift) factors (Lemmas 7 and 9). Thus, Corollary 2 implies the following.

COROLLARY 3. *Let $\mathcal{G}$ be any finite abelian group. Let $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}}$ be a transitive Markov subgroup, and let μ be a measure on $\mathfrak{G}$ with full support. Suppose that $\mathcal{G} = \mathcal{G}_1 \oplus \cdots \oplus \mathcal{G}_N$ and $\mu = \mu_1 \otimes \cdots \otimes \mu_N$, where $\mathcal{G}_n$ is a p_n-group and μ_n is an M_n-step Markov measure on $\mathcal{G}_n^{\mathbb{N}}$ for $n \in \{1, \ldots, N\}$. Then any proper LCA acting on $\mathfrak{G}$ asymptotically randomizes μ to the Haar measure on $\mathfrak{G}$.*

In §4, we turn to D-dimensional LCA acting on a subgroup shift $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}^D}$ with $\mathcal{G}$ a finite abelian p-group and $D \geq 2$. To extend the FLP method to higher dimensions,

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

we interpret $\mathfrak{G}$ as a Markov subgroup of $\mathcal{G}^{\mathbb{N}^{D-1}}$. To formalize this interpretation, we introduce the ring $\mathcal{R}\mathbb{L}$ and associated modules, and develop some basic homological algebra. We generalize the FLP to a property called the 'strong' FLP, and show the following.

THEOREM 4. *Let $p \in \mathbb{N}$ be prime and let $\mathcal{G}$ be an abelian p-group. If $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ is a subgroup shift with the strong FLP and μ is a Markov random field on $\mathfrak{G}$ with full support, then any proper LCA acting on $\mathfrak{G}$ asymptotically randomizes μ to a measure of maximal entropy on $\mathfrak{G}$.*

As before, using the decomposition results Lemmas 7 and 9, we obtain the following corollary.

COROLLARY 5. *Let $\mathcal{G}$ be any finite abelian group. Let $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ be a subgroup shift with the strong FLP, and let μ be a measure on $\mathfrak{G}$ with full support. Suppose that $\mathcal{G} = \mathcal{G}_1 \oplus \cdots \oplus \mathcal{G}_N$ and $\mu = \mu_1 \otimes \cdots \otimes \mu_N$, where $\mathcal{G}_n$ is a p_n-group and μ_n is a Markov random field on $\mathcal{G}_n^{\mathbb{M}}$ for $n \in \{1, \ldots, N\}$. Then any proper LCA acting on $\mathfrak{G}$ asymptotically randomizes μ to a measure of maximal entropy on $\mathfrak{G}$.*

2. *Preliminaries*

In this section, we fix a finite abelian group $(\mathcal{G}, +)$ and we put $\mathbb{M} = \mathbb{N}^D$, $D \geq 2$. For integers $R_1 \leq R_2$, let $[R_1, R_2) := \{R_1, \ldots, R_2 - 1\}$ and $[R_1, R_2] := \{R_1, \ldots, R_2\}$. If $\mathbb{I} \subseteq \mathbb{M}$ is finite, then elements of $\mathcal{G}^{\mathbb{I}}$ are called *blocks*. For $\mathbf{g} \in \mathcal{G}^{\mathbb{M}}$ we set $\mathbf{g}|_{\mathbb{I}} := (g_i : i \in \mathbb{I})$ to be its projection to $\mathcal{G}^{\mathbb{I}}$. Given a subset $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ a block $\mathbf{h} \in \mathcal{G}^{\mathbb{I}}$ is $\mathfrak{G}$-*admissible* if for some $\mathbf{g} \in \mathfrak{G}$, $\mathbf{g}|_{\mathbb{I}} = \mathbf{h}$. Denote $\mathfrak{G}_{\mathbb{I}}$ the set of $\mathfrak{G}$-admissible blocks in $\mathcal{G}^{\mathbb{I}}$. The *cylinder set* associated to a block $\mathbf{h} \in \mathfrak{G}_{\mathbb{I}}$ is $[\mathbf{h}] := \{\mathbf{g} \in \mathfrak{G} : \mathbf{g}|_{\mathbb{I}} = \mathbf{h}\}$.

2.1. *Topological dynamical systems.*

A *topological dynamical system* is a pair (X, T), where X is a compact metric space and $T : X \longrightarrow X$ is a continuous map.

Let $\mathcal{M}(X)$ be the space of all Borel probability measures on X. We equip $\mathcal{M}(X)$ with the *weak* topology*: a sequence $(\mu_n : n \in \mathbb{N})$ in $\mathcal{M}(X)$ converges in this topology to $\mu \in \mathcal{M}(X)$ if and only if $\mu_n(f) \xrightarrow[n\to\infty]{} \mu(f)$ for every continuous function $f : X \longrightarrow \mathbb{R}$. A measure in $\mathcal{M}(X)$ has *full support* if it gives positive measure to any non-empty open set.

A topological dynamical system (Y, S) is a *factor* of (X, T) if there is a continuous onto map $\pi : X \longrightarrow Y$ (called a *factor map*) such that $\pi \circ T = S \circ \pi$. If the factor map is also one-to-one we say the systems are (topologically) *conjugate*. If $\mu \in \mathcal{M}(X)$, then the measure $\pi(\mu) \in \mathcal{M}(Y)$ is defined by $\pi(\mu)(B) = \mu(\pi^{-1}(B))$ for all Borel sets $B \subseteq Y$. If $T(\mu) = \mu$ (where $T(\mu)$ is defined analogously as $\pi(\mu)$) we say μ is T-*invariant*. Given invariant measures $\mu \in \mathcal{M}(X)$ and $\nu \in \mathcal{M}(Y)$, the factor map π defines a *measure-theoretical* factor if $\pi(\mu) = \nu$.

2.2. *Prime decomposition of abelian groups.*

Let $p \in \mathbb{N}$ be a prime number. An abelian group is said to be a p-*group* if every element of it has order p^k for some $k \in \mathbb{N}$.

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

Suppose that $\mathcal{A}$ is an abelian group, and there are distinct primes $p_1 < p_2 < \cdots < p_N$ such that

$$\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_N \quad \text{where } \mathcal{A}_n \text{ is a } p_n\text{-group, for all } n \in [1, N]. \tag{3}$$

We call this a *prime decomposition* of $\mathcal{A}$, and if $\mathcal{A}$ has prime decomposition $\mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_N$, then $\mathcal{A}^{\mathbb{M}}$ has prime decomposition $\mathcal{A}_1^{\mathbb{M}} \oplus \cdots \oplus \mathcal{A}_N^{\mathbb{M}}$. Any finite abelian group $\mathcal{G}$ has a (unique) prime decomposition [**DF91**, Theorem 5, §5.2], and it is a p-group if and only if

$$\mathcal{G} = \mathbb{Z}_{/p^{s_1}} \oplus \mathbb{Z}_{/p^{s_2}} \oplus \cdots \oplus \mathbb{Z}_{/p^{s_J}}, \quad \text{for some } J > 0 \text{ and } s_1, s_2, \ldots, s_J \geq 0. \tag{4}$$

Suppose that $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_N$ and $\mathcal{B} = \mathcal{B}_1 \oplus \cdots \oplus \mathcal{B}_N$ are the prime decompositions of two abelian groups. If $\Phi_n : \mathcal{A}_n \longrightarrow \mathcal{B}_n$ are group homomorphisms for all $n \in [1, N]$, then $\Phi = \Phi_1 \oplus \cdots \oplus \Phi_n : \mathcal{A} \longrightarrow \mathcal{B}$ is the homomorphism such that, for any $\mathbf{a} = (a_1, \ldots, a_N) \in \mathcal{A}$, $\Phi(\mathbf{a}) = (\Phi_1(a_1), \ldots, \Phi_n(a_n))$. The following lemma is straightforward.

LEMMA 6. *Suppose that $\mathcal{A}$ is an abelian group with prime decomposition (3). Let $\mathcal{Z}$ be a subgroup of $\mathcal{A}$.*

(a) *$\mathcal{Z} = \mathcal{Z}_1 \oplus \cdots \oplus \mathcal{Z}_N$, where $\mathcal{Z}_n = \{a_n \in \mathcal{A}_n : \exists z = (z_1, \ldots, z_N) \in \mathcal{Z},\ z_n = a_n\}$ for $n \in [1, N]$.*

(b) *If $\mathcal{Q} = \mathcal{A}/\mathcal{Z}$, then $\mathcal{Q}$ has prime decomposition $\mathcal{Q}_1 \oplus \cdots \oplus \mathcal{Q}_N$, where $\mathcal{Q}_n = \mathcal{A}_n/\mathcal{Z}_n$ for $n \in [1, N]$.*

(c) *If $\mathcal{B}$ is another abelian group, with prime decomposition $\mathcal{B} = \mathcal{B}_1 \oplus \cdots \oplus \mathcal{B}_N$ (in particular, if $\mathcal{B} = \mathcal{Q}$), and $\Phi : \mathcal{A} \longrightarrow \mathcal{B}$ is any homomorphism, then there are unique homomorphisms $\Phi_n : \mathcal{A}_n \longrightarrow \mathcal{B}_n$, $n \in [1, N]$, such that $\Phi = \Phi_1 \oplus \cdots \oplus \Phi_N$.*

2.3. *Subgroup shifts.* For any $m \in \mathbb{M}$, let $\boldsymbol{\sigma}^m : \mathcal{G}^{\mathbb{M}} \longrightarrow \mathcal{G}^{\mathbb{M}}$ be the *shift map*, defined as $(\boldsymbol{\sigma}^m(\mathbf{g}))_j = g_{j+m}$, for $\mathbf{g} \in \mathcal{G}^{\mathbb{M}}$ and $j \in \mathbb{M}$. In particular, if $D = 1$, $\boldsymbol{\sigma} = \boldsymbol{\sigma}^1$ is the left-shift on $\mathcal{G}^{\mathbb{N}}$.

A subgroup $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ is said to be a *subgroup shift* if it is invariant under all $\mathbb{M}$-shifts†. A result of Kitchens and Schmidt (see [**KS89**, Corollary 3.8]) asserts that any subgroup shift is a subshift of finite type. Hence, by replacing $\mathcal{G}$ with some power if necessary, we can recode (by using a topological conjugacy) $\mathfrak{G}$ as a nearest-neighbor subshift of finite type. That is, if $\mathbb{B} = \{0, 1\}^D \subseteq \mathbb{M}$ is the D-dimensional unit cube, there is a subgroup $T_{\mathfrak{G}} \subseteq \mathcal{G}^{\mathbb{B}}$ such that

$$\mathfrak{G} = \{\mathbf{g} \in \mathcal{G}^{\mathbb{M}} : \mathbf{g}|_{\mathbb{B}+m} \in T_{\mathfrak{G}}, \forall m \in \mathbb{M}\}. \tag{5}$$

In particular, if $D = 1$ and $\mathbb{M} = \mathbb{N}$, then $\mathbb{B} = \{0, 1\}$. Thus, $T_{\mathfrak{G}} \subseteq \mathcal{G}^{\{0,1\}}$ is the set (subgroup) of *admissible transitions*, and $\mathfrak{G}$ is a *Markov subgroup*:

$$\mathfrak{G} = \{\mathbf{g} \in \mathcal{G}^{\mathbb{N}} : (g_n, g_{n+1}) \in T_{\mathfrak{G}}, \forall n \in \mathbb{N}\}. \tag{6}$$

If $g \in \mathcal{G}$, then a *follower* of g is any $h \in \mathcal{G}$ so that $(g, h) \in T_{\mathfrak{G}}$. Likewise, a *predecessor* of g is any $h \in \mathcal{G}$ such that $(h, g) \in T_{\mathfrak{G}}$. A Markov subgroup $\mathfrak{G}$ is *proper* if every $g \in \mathcal{G}$ has

† Subgroup shifts are often defined as shift-invariant subgroups of $\mathcal{G}^{\mathbb{Z}^D}$. However, any subshift of $\mathcal{G}^{\mathbb{Z}^D}$ can be projected to a subshift of $\mathcal{G}^{\mathbb{N}^D}$ and, conversely, any subshift of $\mathcal{G}^{\mathbb{N}^D}$ can be extended to a subshift of $\mathcal{G}^{\mathbb{Z}^D}$ in a unique fashion. Thus, there is no loss of generality in restricting to $\mathcal{G}^{\mathbb{N}^D}$, and for our purposes it yields certain technical advantages.

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

at least one follower and at least one predecessor. We can assume without loss of generality that all Markov subgroups are proper (if not we replace $\mathfrak{G}$ by $\widetilde{\mathfrak{G}} = \bigcap_{n\in\mathbb{N}} \boldsymbol{\sigma}^n(\mathfrak{G})$).

A sequence $(g_0, g_1, \ldots, g_N) \in \mathcal{G}^{[0,N]}$ is $\mathfrak{G}$-*admissible* if $(g_n, g_{n+1}) \in T_{\mathfrak{G}}$ for all $n \in [0, N-1]$. A Markov subgroup $\mathfrak{G}$ is *transitive* if every element $h \in \mathcal{G}$ is *reachable* from any element $g \in \mathcal{G}$, meaning that there is some $\mathfrak{G}$-admissible sequence $(g, g_1, \ldots, g_{N-1}, h)$ for some $N > 0$.

Subgroup shifts succumb to a p-group decomposition as follows.

LEMMA 7. *Suppose that $\mathcal{G}$ has prime decomposition $\mathcal{G}_1 \oplus \cdots \oplus \mathcal{G}_N$. If $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ is a subgroup shift, then $\mathfrak{G} = \mathfrak{G}_1 \oplus \cdots \oplus \mathfrak{G}_N$, where $\mathfrak{G}_n \subseteq \mathcal{G}_n^{\mathbb{M}}$ is a subgroup shift for all $n \in [1, N]$.*

2.4. *Linear cellular automata.* Recall from the introduction the definition of a proper linear cellular automaton (PLCA).

LEMMA 8. *$\mathfrak{G}$ is invariant under the action of LCA acting on $\mathcal{G}^{\mathbb{M}}$.*

Proof. If $\Phi\colon \mathcal{G}^{\mathbb{M}} \to \mathcal{G}^{\mathbb{M}}$ is the LCA (1) and $\mathbf{g} \in \mathfrak{G}$, then $\varphi_i \cdot \boldsymbol{\sigma}^i(\mathbf{g}) \in \mathfrak{G}$ for all $i \in \mathbb{I}$. Thus, $\Phi(\mathbf{g}) \in \mathfrak{G}$. □

More generally, suppose that $\mathcal{R}$ is a commutative ring and $\mathcal{G}$ is an $\mathcal{R}$-module. An $\mathcal{R}$-*LCA* is one of the form (1), where $\varphi_i \in \mathcal{R}$ for all $i \in \mathbb{I}$.

LCA have a p-group decomposition analogous to Lemma 6(c) as follows.

LEMMA 9. *Suppose that $\mathcal{G}$ has prime decomposition $\mathcal{G}_1 \oplus \cdots \oplus \mathcal{G}_N$ and $\mathfrak{G} = \mathfrak{G}_1 \oplus \cdots \oplus \mathfrak{G}_N$ as in Lemma 7. If $\Phi : \mathfrak{G} \longrightarrow \mathfrak{G}$ is a (proper) LCA, then there are (proper) LCA $\Phi_n : \mathfrak{G}_n \longrightarrow \mathfrak{G}_n$, for $n \in [1, N]$, such that $\Phi = \Phi_1 \oplus \cdots \oplus \Phi_N$.*

Lemmas 7 and 9 allow us to reduce the study of asymptotic randomization by LCA acting on subgroup shifts to the case of $\mathcal{G}^{\mathbb{M}}$, where $\mathcal{G}$ is a p-group for some prime $p \in \mathbb{N}$.

2.5. *The Haar measure.* Let $\mathfrak{G}$ be a subgroup shift of $\mathcal{G}^{\mathbb{M}}$, and $\eta \in \mathcal{M}(\mathfrak{G})$ the Haar measure. Lemma 17(a) in §3 characterizes η when $\mathfrak{G}$ is a Markov subgroup of $\mathcal{G}^{\mathbb{N}}$. The Haar measure is uniformly distributed on $\mathfrak{G}$ in the following sense.

LEMMA 10. *If $\mathbb{I} \subseteq \mathbb{M}$ is finite and $\eta_{\mathbb{I}}$ is the projection of η to $\mathfrak{G}_{\mathbb{I}}$, then $\eta_{\mathbb{I}}$ is the uniform measure on $\mathfrak{G}_{\mathbb{I}}$.*

Proof. $\mathfrak{G}_{\mathbb{I}}$ is a finite group, and $\eta_{\mathbb{I}}$ is the Haar measure on $\mathfrak{G}_{\mathbb{I}}$, so $\eta_{\mathbb{I}}$ is uniform. □

Let $(\mathbb{I}_R : R > 0)$ be an increasing sequence of finite subsets of $\mathbb{M}$ verifying that for any $R' > 0$ there is some $R > 0$ such that $[0, R']^D \subseteq \mathbb{I}_R$, and let $\mathfrak{G}_R := \mathfrak{G}_{\mathbb{I}_R}$. The *topological entropy* of $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ (with respect to $\boldsymbol{\sigma}$) is defined by

$$h_{\mathrm{top}}(\mathfrak{G}) = \lim_{R\to\infty} \frac{1}{|\mathbb{I}_R|} \log |\mathfrak{G}_R|.$$

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

If μ is a shift invariant measure on $\mathfrak{G}$, then the *measurable entropy* of μ (with respect to $\boldsymbol{\sigma}$) is defined by

$$h_\mu(\mathfrak{G}) = -\lim_{R\to\infty} \frac{1}{|\mathbb{I}_R|} \sum_{\mathbf{g}\in\mathfrak{G}_R} \mu([\mathbf{g}]) \cdot \log \mu([\mathbf{g}]).$$

Note that neither notion of entropy depends on the sequence $(\mathbb{I}_R : R > 0)$.

A *measure of maximal entropy* on $\mathfrak{G}$ is a shift invariant measure $\mu \in \mathcal{M}(\mathfrak{G})$ such that $h_\mu(\mathfrak{G}) = h_{\text{top}}(\mathfrak{G})$. The next result summarizes prior results about maximal-entropy measures for subgroup shifts.

PROPOSITION 11. *The Haar measure η is a measure of maximal entropy on $\mathfrak{G}$* [**Sch95**, Proposition 13.5, p. 111].

If $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}}$ is a transitive Markov subgroup, then η is the unique measure of maximal entropy [**Ber69**].

If $D \geq 2$, then η is the unique measure of maximal entropy if and only if $\mathfrak{G}$ has no zero-entropy, nontrivial measurable factors for η [**Sch95**, Theorem 20.15, p. 171].

3. *Asymptotic randomization of Markov subgroups*

Throughout this section $D = 1$, $\mathbb{M} = \mathbb{N}$ and $(\mathcal{G}, +)$ is a finite abelian group. Let $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}}$ be a Markov subgroup, as in (6). For any $g \in \mathcal{G}$, the *follower set* of g is the set

$$\mathcal{F}_{\mathfrak{G}}(g) = \{h \in \mathcal{G} : (g, h) \in T_{\mathfrak{G}}\}.$$

Put $\mathcal{Z}_{\mathfrak{G}} = \mathcal{F}_{\mathfrak{G}}(0)$ (mnemonic: '$\mathcal{Z}$' is for 'zero').

LEMMA 12. *Let $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}}$ be a Markov subgroup. Then:*

(a) *$\mathcal{Z}_{\mathfrak{G}}$ is a normal subgroup of $\mathcal{G}$;*

(b) *for any $g \in \mathcal{G}$, $\mathcal{F}_{\mathfrak{G}}(g)$ is a coset of $\mathcal{Z}_{\mathfrak{G}}$;*

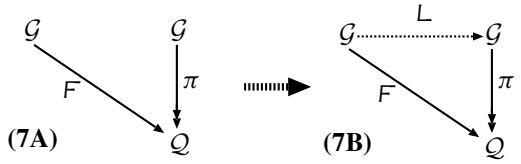
(c) *let $\mathcal{Q}_{\mathfrak{G}} = \mathcal{G}/\mathcal{Z}_{\mathfrak{G}}$ be the quotient group, and define $\mathsf{F}_{\mathfrak{G}} : \mathcal{G} \longrightarrow \mathcal{Q}_{\mathfrak{G}}$ by $\mathsf{F}_{\mathfrak{G}}(g) = \mathcal{F}_{\mathfrak{G}}(g)$; then $\mathsf{F}_{\mathfrak{G}}$ is a group homomorphism;*

(d) *let $\pi_{\mathfrak{G}} : \mathcal{G} \longrightarrow \mathcal{Q}_{\mathfrak{G}}$ be the quotient epimorphism (i.e. $\pi_{\mathfrak{G}}(g) = g + \mathcal{Z}_{\mathfrak{G}}$); then $\mathfrak{G} = \{\mathbf{g} \in \mathcal{G}^{\mathbb{N}} : \mathsf{F}_{\mathfrak{G}}(g_n) = \pi_{\mathfrak{G}}(g_{n+1}), \forall n \in \mathbb{N}\}$.*

Proof. Parts (a) and (b) are parts (ii) and (iii) of Proposition 3 in [**Kit87**], while (c) is discussed at the beginning of [**Kit87**, §4]. Part (d) then follows by definition. □

Throughout this section, let $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}}$ be a Markov subgroup and $\mathcal{Z} = \mathcal{Z}_{\mathfrak{G}}$. Let $\mathcal{Q} = \mathcal{Q}_{\mathfrak{G}}$ be the quotient group and let $\mathsf{F} = \mathsf{F}_{\mathfrak{G}}$ and $\pi = \pi_{\mathfrak{G}}$ be the morphisms associated to $\mathfrak{G}$ as in Lemma 12.

3.1. *The follower lifting property.* We say $\mathfrak{G}$ has the FLP if the map F lifts to a homomorphism $\mathsf{L} : \mathcal{G} \longrightarrow \mathcal{G}$ such that $\pi \circ \mathsf{L} = \mathsf{F}$. In other words, we can transform diagram (7A) into commuting diagram (7B):



(7)

It follows that, for any $g \in \mathcal{G}$, $\mathsf{F}(g) = \mathsf{L}(g) + \mathcal{Z}$.

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

The FLP allows us to project $\mathfrak{G}$ into the full shift $\mathcal{Z}^{\mathbb{N}}$, so that the dynamics of shifts and LCA on $\mathfrak{G}$ are reduced to shifts and LCA on $\mathcal{Z}^{\mathbb{N}}$. We recall that $T_{\mathfrak{G}} \subseteq \mathcal{G}^{\{0,1\}}$ is defined from (6).

LEMMA 13. *Assume that $\mathfrak{G}$ has the FLP.*

(a) *For $(g,h) \in T_{\mathfrak{G}}$, define $\delta(g,h) = h - \mathsf{L}(g)$. Let $\Delta; \mathfrak{G} \longrightarrow \mathcal{Z}^{\mathbb{N}}$ be the corresponding block map, $\Delta(\mathbf{g})_n = \delta(g_n, g_{n+1})$ for $\mathbf{g} \in \mathfrak{G}$ and $n \in \mathbb{N}$. Then Δ is a group homomorphism.*

(b) *Define $\Psi; \mathfrak{G} \longrightarrow \mathcal{G} \times \mathcal{Z}^{\mathbb{N}}$ by $\Psi(\mathbf{g}) = (g_0; \Delta(\mathbf{g}))$ for $\mathbf{g} \in \mathfrak{G}$. Then Ψ is a group isomorphism.*

(c) *Ψ is a conjugacy between $(\mathfrak{G}, \boldsymbol{\sigma})$ and $(\mathcal{G} \times \mathcal{Z}^{\mathbb{N}}, \widetilde{\boldsymbol{\sigma}})$, where $\widetilde{\boldsymbol{\sigma}}; \mathcal{G} \times \mathcal{Z}^{\mathbb{N}} \longrightarrow \mathcal{G} \times \mathcal{Z}^{\mathbb{N}}$ is defined by $\widetilde{\boldsymbol{\sigma}}(g; \mathbf{z}) = (\varsigma(g; \mathbf{z}); \boldsymbol{\sigma}(\mathbf{z}))$, with $\varsigma(g; \mathbf{z}) = \mathsf{L}(g) + z_0$, for $g \in \mathcal{G}$ and $\mathbf{z} \in \mathcal{Z}^{\mathbb{N}}$.*

(d) *For $g \in \mathcal{G}$ and $\mathbf{z} \in \mathcal{Z}^{\mathbb{N}}$, let $\varsigma^{(1)}(g; \mathbf{z}) = \varsigma(g; \mathbf{z})$, and for $m > 1$, let $\varsigma^{(m)}(g; \mathbf{z}) = \varsigma(\varsigma^{(m-1)}(g; \mathbf{z}); \boldsymbol{\sigma}^{m-1}(\mathbf{z}))$. Then for any $m \geq 1$, $\widetilde{\boldsymbol{\sigma}}^m(g; \mathbf{z}) = (\varsigma^{(m)}(g; \mathbf{z}); \boldsymbol{\sigma}^m(\mathbf{z}))$.*

Proof. (a) L is a homomorphism, so δ and Δ are homomorphisms.

(b) Ψ is a homomorphism because Δ is a homomorphism. To show Ψ is invertible, let $g \in \mathcal{G}$ and $\mathbf{z} = (z_n : n \in \mathbb{N}) \in \mathcal{Z}^{\mathbb{N}}$. Define $\mathbf{g} \in \mathcal{G}^{\mathbb{N}}$ as follows: $g_0 = g$ and $g_{n+1} = \mathsf{L}(g_n) + z_n$ for $n \geq 0$. Then $\mathbf{g} \in \mathfrak{G}$, $\Psi(\mathbf{g}) = (g; \mathbf{z})$ and $\mathbf{g}$ is the unique element with this property.

(c) Let $\mathbf{g} = (g_n : n \in \mathbb{N}) \in \mathfrak{G}$ and $\Psi(\mathbf{g}) = (g_0; \mathbf{z})$, so $\mathbf{z} = \Delta(\mathbf{g})$. By the definitions above, we get

$$\begin{aligned}\Psi(\boldsymbol{\sigma}(\mathbf{g})) &= (g_1; \Delta \circ \boldsymbol{\sigma}(\mathbf{g})) = (g_1; \boldsymbol{\sigma} \circ \Delta(\mathbf{g})) \\ &= (\mathsf{L}(g_0) + \delta(g_0, g_1); \boldsymbol{\sigma}(\mathbf{z})) = (\mathsf{L}(g_0) + z_0; \boldsymbol{\sigma}(\mathbf{z})) = \widetilde{\boldsymbol{\sigma}}(g_0; \mathbf{z}).\end{aligned}$$

(d) This follows inductively from (c). □

LEMMA 14. *Assume $\mathfrak{G}$ has the FLP. Let Φ be a (proper) LCA on $\mathfrak{G}$ as in (1). Define $\widetilde{\Phi} : \mathcal{G} \times \mathcal{Z}^{\mathbb{N}} \longrightarrow \mathcal{G} \times \mathcal{Z}^{\mathbb{N}}$ by $\widetilde{\Phi}(g; \mathbf{z}) = \sum_{i \in \mathbb{I}} \varphi_i \cdot \widetilde{\boldsymbol{\sigma}}^i(g; \mathbf{z})$, for $g \in \mathcal{G}$ and $\mathbf{z} \in \mathcal{Z}^{\mathbb{N}}$. Then:*

(a) *Ψ is a conjugacy between $(\mathfrak{G}, \Phi)$ and $(\mathcal{G} \times \mathcal{Z}^{\mathbb{N}}, \widetilde{\Phi})$;*

(b) *for $g \in \mathcal{G}$ and $\mathbf{z} \in \mathcal{Z}^{\mathbb{N}}$, $\widetilde{\Phi}(g; \mathbf{z}) = (\widetilde{\Phi}_{\mathcal{G}}(g; \mathbf{z}); \widetilde{\Phi}_{\mathcal{Z}}(\mathbf{z}))$, where $\widetilde{\Phi}_{\mathcal{G}}(g; \mathbf{z}) = \sum_{i \in \mathbb{I}} \varphi_i \cdot \varsigma^{(i)}(g; \mathbf{z})$ and $\widetilde{\Phi}_{\mathcal{Z}}(\mathbf{z}) = \sum_{i \in \mathbb{I}} \varphi_i \cdot \boldsymbol{\sigma}^i(\mathbf{z})$; thus, $\widetilde{\Phi}_{\mathcal{Z}}$ is itself a (proper) LCA on $\mathcal{Z}^{\mathbb{N}}$.*

Proof. (a) Ψ is a homomorphism, so Lemma 13(d) implies that

$$\Psi(\Phi(\mathbf{g})) = \Psi\left(\sum_{i \in \mathbb{I}} \varphi_i \cdot \boldsymbol{\sigma}^i(\mathbf{g})\right) = \sum_{i \in \mathbb{I}} \varphi_i \cdot (\Psi \circ \boldsymbol{\sigma}^i)(\mathbf{g}) = \sum_{i \in \mathbb{I}} \varphi_i \cdot (\widetilde{\boldsymbol{\sigma}}^i \circ \Psi)(\mathbf{g}) = \widetilde{\Phi}(\Psi(\mathbf{g})),$$

for any $\mathbf{g} \in \mathfrak{G}$. Then (b) follows from Lemma 13(e). □

Example 15. Let us revisit the example introduced in [**Kit87**] and check the FLP. Let $\mathcal{G} = \mathbb{Z}_{/4} \oplus \mathbb{Z}_{/2}$. Write an element of $\mathcal{G}$ as $\binom{x}{y}$, where $x \in \mathbb{Z}_{/4}$ and $y \in \mathbb{Z}_{/2}$, and an element of

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

$\mathcal{G}^{\mathbb{N}}$ as $\binom{\mathbf{x}}{\mathbf{y}}$, where $\mathbf{x} \in {\mathbb{Z}_{/4}}^{\mathbb{N}}$ and $\mathbf{y} \in {\mathbb{Z}_{/2}}^{\mathbb{N}}$. Let

$$\mathfrak{G} = \left\{ \binom{\mathbf{x}}{\mathbf{y}} \in \mathcal{G}^{\mathbb{N}} : x_n + y_n + y_{n+1} = 0 \bmod 2, \forall n \in \mathbb{N} \right\}.$$

Then

$$\mathcal{Z} = \mathcal{F}\left(\binom{0}{0}\right) = \left\{ \binom{x_1}{0} : x_1 \in \mathbb{Z}_{/4} \right\} = \mathbb{Z}_{/4} \oplus \{0\},$$

and $\mathcal{Q} = \mathcal{G}/\mathcal{Z} \cong \mathbb{Z}_{/2}$. For any $\binom{x_0}{y_0} \in \mathcal{G}$,

$$F\left(\binom{x_0}{y_0}\right) = \left\{ \binom{x_1}{y_1} : x_1 \in \mathbb{Z}_{/4} \text{ and } y_1 = x_0 + y_0 \mod 2 \right\} = \binom{0}{(x_0 + y_0) \bmod 2} + \mathcal{Z}.$$

Thus,

$$\pi\left(\binom{x}{y}\right) = \binom{x}{y} + \mathcal{Z} = \binom{0}{y} + \mathcal{Z}.$$

Hence, if

$$L\left(\binom{x_0}{y_0}\right) = \binom{0}{(x_0 + y_0) \bmod 2},$$

then $\pi \circ L = F$, which proves that $\mathfrak{G}$ has the FLP.

Now, $\delta : T_{\mathfrak{G}} \longrightarrow \mathcal{Z}$ is defined by

$$\delta\left(\binom{x_0}{y_0}, \binom{x_1}{y_1}\right) = \binom{x_1}{(y_1 - (x_0 + y_0)) \bmod 2} = \binom{x_1}{0}.$$

For any $\binom{x_0}{y_0} \in \mathcal{G}$ and $\binom{\mathbf{z}}{0} \in \mathcal{Z}^{\mathbb{N}}$, we have

$$\widetilde{\boldsymbol{\sigma}}\left(\binom{x_0}{y_0}; \binom{\mathbf{z}}{0}\right) = \left(\binom{z_0}{(x_0 + y_0) \bmod 2}; \binom{\boldsymbol{\sigma}(\mathbf{z})}{0}\right).$$

LEMMA 16. *Assume $\mathfrak{G}$ has the FLP. Let $\mu \in \mathcal{M}(\mathfrak{G})$ be a $\boldsymbol{\sigma}$-invariant N-step Markov measure with full support on $\mathfrak{G}$. Then $\Delta(\mu) \in \mathcal{M}(\mathcal{Z}^{\mathbb{N}})$ is a $\boldsymbol{\sigma}$-invariant $(N+1)$-step Markov measure with full support on $\mathcal{Z}^{\mathbb{N}}$.*

Proof. $\Delta(\mu)$ is $\boldsymbol{\sigma}$-invariant and Markov because Δ is a block map whose local map δ looks at only two consecutive symbols. $\Delta(\mu)$ has full support because Δ is surjective by Lemma 13(b). □

LEMMA 17. *Let η be the Haar measure on $\mathfrak{G}$. Then:*

(a) *for any $\mathfrak{G}$-admissible sequence $(g_0, \ldots, g_N)$,*

$$\eta([g_0, \ldots, g_N]) = \frac{1}{|\mathcal{G}|} \cdot \frac{1}{|\mathcal{Z}|^N};$$

(b) $h_\eta(\mathfrak{G}) = h_{\text{top}}(\mathfrak{G}) = \log |\mathcal{Z}|$.

Proof. For any $g \in \mathcal{G}$, $|\mathcal{F}_{\mathfrak{G}}(g)| = |\mathcal{Z}|$. Thus, there are exactly $|\mathcal{G}| \cdot |\mathcal{Z}|^N$ $\mathfrak{G}$-admissible words of length $(N+1)$. Part (a) follows because η must give all $|\mathcal{G}| \cdot |\mathcal{Z}|^N$ words equal mass (Lemma 10). Part (b) follows from the definitions of measurable and topological entropy. □

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

PROPOSITION 18. *Assume that $\mathfrak{G}$ is transitive and has the FLP. Let $\rho \in \mathcal{M}(\mathfrak{G})$ be $\boldsymbol{\sigma}$-invariant. Then ρ is the Haar measure on $\mathfrak{G}$ if and only if $\Delta(\rho)$ is the Haar measure on $\mathcal{Z}^{\mathbb{N}}$.*

Proof. '$\Longrightarrow$': Lemma 13(a), (b) says that Δ is a group epimorphism from $\mathfrak{G}$ to $\mathcal{Z}^{\mathbb{N}}$.

'$\Longleftarrow$': suppose that $\Delta(\rho)$ is the Haar measure on $\mathcal{Z}^{\mathbb{N}}$ (i.e. the uniform Bernoulli measure). Since $(\mathcal{Z}^{\mathbb{N}}, \Delta(\rho), \boldsymbol{\sigma})$ is a measure-theoretical factor of $(\mathfrak{G}, \rho, \boldsymbol{\sigma})$, then Lemma 17(b) implies

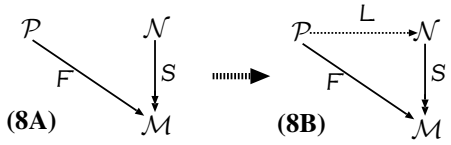
$$\log|\mathcal{Z}| = h_{\Delta(\rho)}(\mathcal{Z}^{\mathbb{N}}) \le h_{\rho}(\mathfrak{G}) \le h_{\eta}(\mathfrak{G}) = \log|\mathcal{Z}|.$$

Thus, $h_{\rho}(\mathfrak{G}) = \log|\mathcal{Z}|$. However, η is the unique maximal-entropy measure on $\mathfrak{G}$ by Proposition 11; hence, $\rho = \eta$. □

COROLLARY 19. *Assume $\mathfrak{G}$ is transitive and has the FLP. Let Φ be an LCA acting on $\mathfrak{G}$ as in (1) and $\mu \in \mathcal{M}(\mathfrak{G})$. Then Φ asymptotically randomizes μ if and only if $\widetilde{\Phi}_{\mathcal{Z}}$ asymptotically randomizes $\Delta(\mu)$.*

Proof of Theorem 1. Let μ be an N-step Markov measure on $\mathfrak{G}$ with full support. From Lemma 16 we get that $\Delta(\mu)$ is an $(N+1)$-step Markov measure with full support on $\mathcal{Z}^{\mathbb{N}}$. Thus, Corollary 10 and Theorem 12 of [**PY02**] and Theorem 9 of [**PY04**] together imply that $\widetilde{\Phi}_{\mathcal{Z}}$ (which is proper) asymptotically randomizes $\Delta(\mu)$. Now apply Corollary 19. □

3.2. *Sufficient conditions for the FLP.* Suppose that $\mathcal{G}$ is a p-group as in (4). Let p^s be the largest power of p in the decomposition (4), and let $\mathcal{R} = \mathbb{Z}_{/p^s}$, treated as a ring. Then $\mathcal{G}$ is an $\mathcal{R}$-module. An $\mathcal{R}$-module $\mathcal{P}$ is *projective* if, given any commuting diagram (8A) below (where $S : \mathcal{N} \longrightarrow \mathcal{M}$ is an $\mathcal{R}$-module epimorphism), there exists an $\mathcal{R}$-module homomorphism $L : \mathcal{P} \longrightarrow \mathcal{N}$ such that we get the commuting diagram (8B):



(8)

A *free* $\mathcal{R}$-module is one of the form $\mathcal{R} \oplus \cdots \oplus \mathcal{R}$. Any free $\mathcal{R}$-module is projective.

PROPOSITION 20. *Let p be prime, and let $\mathcal{G}$ be an abelian p-group. Then any Markov subgroup $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}}$ has the FLP.*

Proof. Let $\mathcal{G} = \mathbb{Z}_{/p^{s_1}} \oplus \mathbb{Z}_{/p^{s_2}} \oplus \cdots \oplus \mathbb{Z}_{/p^{s_J}}$. Put $s = \max\{s_1, \ldots, s_J\}$ and $\mathcal{R} = \mathbb{Z}_{/p^s}$. Then $\mathcal{G}$ is an $\mathcal{R}$-module. Let $\mathcal{P} = \mathcal{R}^J = \mathcal{R} \oplus \cdots \oplus \mathcal{R}$ (J times), then $\mathcal{P}$ is a free (thus projective) $\mathcal{R}$-module.

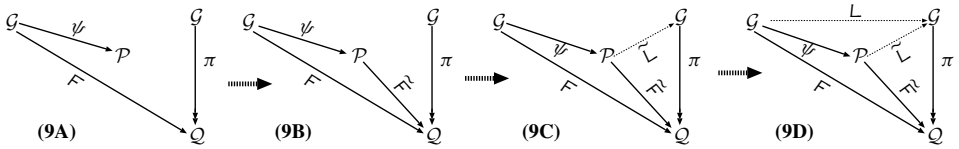
CLAIM 1. *$\mathcal{G}$ is isomorphic to a submodule of $\mathcal{P}$.*

Proof. Let $r_j = s - s_j$ for all $j \in [1, J]$. Then define $\psi : \mathcal{G} \longrightarrow \mathcal{P}$ by

$$\psi((z_1, \ldots, z_J)) = (p^{r_1} z_1, \ldots, p^{r_J} z_J) \quad \text{for any } (z_1, \ldots, z_J) \in \mathcal{G}.$$

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

If $\widetilde{G} = \psi(\mathcal{G}) \subseteq \mathcal{P}$, then $\psi : \mathcal{G} \longrightarrow \widetilde{G}$ is an $\mathcal{R}$-module isomorphism. ◇



(9)

At this point we have diagram (9A).

CLAIM 2. *There is a map $\widetilde{F} : \mathcal{P} \longrightarrow \mathcal{Q}$ such that $\widetilde{F} \circ \psi = F$, as in diagram (9B).*

Proof. Since $\mathcal{Q}$ is a quotient of $\mathcal{G}$, we know that $\mathcal{Q}$ is also a p-group, and $\mathcal{Q} = \mathbb{Z}_{/p^{q_1}} \oplus \mathbb{Z}_{/p^{q_2}} \oplus \cdots \oplus \mathbb{Z}_{/p^{q_K}}$, where $q_k \leq s$ for all $k \in [1, K]$. Thus, $\mathcal{Q}$ is also an $\mathcal{R}$-module. We can embed $\mathcal{Q}$ into $\mathcal{R}^K$ by repeating the argument of Claim 1. We will thus assume that $\mathcal{Q} \subseteq \mathcal{R}^K$. The homomorphism $F : \mathcal{G} \longrightarrow \mathcal{Q}$ can then be written as

$$F(g) = (F_0(g), F_1(g), \ldots, F_K(g)) \quad \text{for any } g \in \mathcal{G},$$

where for each $k \in [0, K]$, $F_k : \mathcal{G} \longrightarrow \mathcal{R}$ is a homomorphism of the form:

$$F_k((z_1, z_2, \ldots, z_J)) = \sum_{j=1}^{J} F_{j,k}(z_j) \quad \text{for any } (z_1, z_2, \ldots, z_J) \in \mathcal{G},$$

for some homomorphisms $F_{j,k} : \mathbb{Z}_{/p^{s_j}} \longrightarrow \mathcal{R}$. Now, $\mathcal{R} = \mathbb{Z}_{/p^s}$ and $s = r_j + s_j$, so there is some $f_{j,k} \in \mathbb{Z}_{/p^{s_j}}$ such that $F_{j,k}(z) = p^{r_j} \cdot f_{j,k} \cdot z$, for any $z \in \mathbb{Z}_{/p^{s_j}}$. Define $\widetilde{F}_{j,k} : \mathcal{R} \longrightarrow \mathcal{R}$ by $\widetilde{F}_{j,k}(r) = f_{j,k} \cdot r$, for any $r \in \mathcal{R}$. Then define $\widetilde{F}_k : \mathcal{P} \longrightarrow \mathcal{R}$ by

$$\widetilde{F}_k((r_1, r_2, \ldots, r_J)) = \sum_{j=1}^{J} \widetilde{F}_{j,k}(r_j) \quad \text{for any } (r_1, r_2, \ldots, r_J) \in \mathcal{R}^J = \mathcal{P}.$$

It follows that $\widetilde{F}_k \circ \psi = F_k$. Finally, define $\widetilde{F} : \mathcal{P} \longrightarrow \mathcal{R}^K$ by

$$\widetilde{F}(p) = (\widetilde{F}_1(p), \widetilde{F}_2(p), \ldots, \widetilde{F}_K(p)) \quad \text{for any } p \in \mathcal{P}.$$

We conclude that $\widetilde{F} \circ \psi = F$. ◇

Now $\mathcal{P}$ is projective, so we can find a morphism $\widetilde{L} : \mathcal{P} \longrightarrow \mathcal{G}$ yielding diagram (9C). Define $L = \widetilde{L} \circ \Psi$ to get commuting diagram (9D). Then $\pi \circ L = F$, as desired. □

Proof of Corollary 2. Proposition 20 says $\mathfrak{G}$ has the FLP. Now apply Theorem 1. □

4. *Randomization of multidimensional subgroup shifts*

We will generalize the results of §3 by treating a $(D+1)$-dimensional subgroup shift as a one-dimensional Markov group, whose alphabet is itself a D-dimensional subgroup shift.

We first fix some notation for this section. Let $\mathbb{L} = \mathbb{N}^D$ and $\mathbb{M} = \mathbb{N}^{D+1} = \mathbb{L} \times \mathbb{N}$. Let $p \in \mathbb{N}$ be prime, and let $\mathcal{G}$ be the abelian p-group:

$$\mathcal{G} = (\mathbb{Z}_{/p})^{s_1} \oplus (\mathbb{Z}_{/p^2})^{s_2} \oplus \cdots \oplus (\mathbb{Z}_{/p^J})^{s_M} \quad \text{for some } J > 0 \text{ and } s_1, s_2, \ldots, s_J \geq 0. \tag{10}$$

Let $\mathcal{R} = \mathbb{Z}_{/p^J}$ (as a ring). Then $\mathcal{G}$ is an $\mathcal{R}$-module.

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

Set $\mathfrak{U} = \mathcal{G}^{\mathbb{L}}$. Any element of $\mathcal{G}^{\mathbb{M}}$ can be seen as an $\mathbb{N}$-indexed sequence of elements in $\mathfrak{U}$. In other words, $\mathcal{G}^{\mathbb{M}}$ is naturally isomorphic to the full shift $\mathfrak{U}^{\mathbb{N}}$. Likewise, if $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ is a nearest-neighbor group shift, then we can interpret $\mathfrak{G}$ as a Markov subgroup of $\mathfrak{U}^{\mathbb{N}}$. Then elements of $\mathfrak{G}$ can be written as $\mathbf{g} = (\mathbf{g}_n : n \in \mathbb{N}) \in \mathfrak{U}^{\mathbb{N}}$. Define $\mathfrak{U}_{\mathfrak{G}} = \{\mathbf{u} \in \mathfrak{U} : \mathbf{u} = \mathbf{g}_0 \text{ for some } \mathbf{g} \in \mathfrak{G}\}$. Then $\mathfrak{U}_{\mathfrak{G}}$ is a subgroup shift of $\mathfrak{U}$ (and possibly $\mathfrak{U} \neq \mathfrak{U}_{\mathfrak{G}}$).

Now we introduce some machinery to make these statements precise.

4.1. *The ring $\mathcal{R}\mathbb{L}$ and its modules.* An $\mathcal{R}$-LCA is a map $\Phi : \mathfrak{U} \longrightarrow \mathfrak{U}$ defined by

$$\Phi = \sum_{i \in \mathbb{I}} \varphi_i \cdot \boldsymbol{\sigma}^i \quad \text{where } \mathbb{I} \subseteq \mathbb{L} \text{ is a finite subset and } \varphi_i \in \mathcal{R} \text{ for all } i \in \mathbb{I}.$$

If $\mathcal{R}\mathbb{L}$ is the set of all $\mathcal{R}$-LCA on $\mathfrak{U}$, then $\mathcal{R}\mathbb{L}$ is a ring under addition and function composition. Indeed, $\mathcal{R}\mathbb{L}$ is isomorphic to the ring $\mathcal{R}[\sigma_1, \ldots, \sigma_D]$ of formal polynomials in D indeterminants $\sigma_1, \ldots, \sigma_D$, with coefficients in the ring $\mathcal{R}$. Here, each σ_i corresponds to the shift along the ith axis of $\mathbb{L}$.

An $\mathcal{R}\mathbb{L}$-*module* is a compact, metrizable abelian topological group together with a continuous $\mathcal{R}\mathbb{L}$-action. For example, $\mathcal{G}^{\mathbb{L}}$ is an $\mathcal{R}\mathbb{L}$-module, where $\sigma_1, \ldots, \sigma_D$, act as shifts along the D axes, and other elements of $\mathcal{R}\mathbb{L}$ act as LCA in the obvious way. If $\mathcal{M}$ is an $\mathcal{R}\mathbb{L}$-module, then a *submodule* is a closed subgroup $\mathcal{N} \subseteq \mathcal{M}$ which is invariant under $\mathcal{R}$-multiplication and under all $\mathbb{L}$-shifts; we then write $\mathcal{N} \prec \mathcal{M}$. For example, if $\mathfrak{V} \subseteq \mathcal{G}^{\mathbb{L}}$ is a subgroup shift, then Lemma 8 says that $\mathfrak{V}$ is an $\mathcal{R}\mathbb{L}$-submodule of $\mathcal{G}^{\mathbb{L}}$.

The most obvious examples of $\mathcal{R}\mathbb{L}$-modules are subgroup shifts of $\mathcal{G}^{\mathbb{L}}$, but some $\mathcal{R}\mathbb{L}$-modules (in particular, *quotient modules*) do not admit a natural subgroup shift representation. If $\mathcal{N} \prec \mathcal{M}$, then the *quotient module* is the quotient group $\mathcal{Q} = \mathcal{M}/\mathcal{N}$ with the quotient topology, the natural action of $\mathcal{R}$ and with $\mathbb{L}$ acting on $\mathcal{Q}$ as follows: fix $m \in \mathcal{M}$ and let $(m + \mathcal{N})$ be the corresponding coset; then for any $\ell \in \mathbb{L}$, $\boldsymbol{\sigma}^{\ell}(m + \mathcal{N}) = \boldsymbol{\sigma}^{\ell}(m) + \mathcal{N}$ is another coset (because $\mathcal{N}$ is $\mathbb{L}$-shift-invariant). To show that $\mathcal{Q}$ is an $\mathcal{R}\mathbb{L}$-module, it remains to show the following.

LEMMA 21. *$\mathcal{Q}$ is compact and metrizable, and $\mathbb{L}$ acts continuously on $\mathcal{Q}$.*

Proof. $\mathcal{Q}$ is the continuous image of the compact space $\mathcal{M}$, hence $\mathcal{Q}$ is compact. A topological group is metrizable if and only if it is first-countable [**Wil70**, 38C, p. 259], hence $\mathcal{M}$ is first-countable. The continuous open image of a first-countable space is first-countable [**Wil70**, 16A(#3), p. 113], therefore $\mathcal{Q}$ is also first-countable and finally metrizable.

To see that $\mathbb{L}$ acts continuously, observe that any neighborhood of the coset $(m + \mathcal{N})$ has the form $(\mathcal{B} + \mathcal{N})$, where $\mathcal{B} \subseteq \mathcal{M}$ is a neighborhood of $m \in \mathcal{M}$. However, then $\boldsymbol{\sigma}^{-\ell}(\mathcal{B} + \mathcal{N}) = \boldsymbol{\sigma}^{-\ell}(\mathcal{B}) + \mathcal{N}$ is a neighborhood of $\boldsymbol{\sigma}^{-\ell}(m + \mathcal{N}) = \boldsymbol{\sigma}^{-\ell}(m) + \mathcal{N}$. □

If $\mathcal{M}$ and $\mathcal{N}$ are $\mathcal{R}\mathbb{L}$-modules, then a *morphism* is a continuous group homomorphism $\Phi : \mathcal{M} \longrightarrow \mathcal{N}$ which commutes with the $\mathcal{R}\mathbb{L}$-action. For example:

- any LCA $\Phi : \mathcal{G}^{\mathbb{L}} \longrightarrow \mathcal{G}^{\mathbb{L}}$ is an $\mathcal{R}\mathbb{L}$-module endomorphism of $\mathcal{G}^{\mathbb{L}}$;

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

- if $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{L}}$ and $\mathfrak{H} \subseteq \mathcal{H}^{\mathbb{L}}$ are subgroup shifts (regarded as $\mathcal{R}\mathbb{L}$-modules), then an $\mathcal{R}\mathbb{L}$-morphism from $\mathfrak{G}$ to $\mathfrak{H}$ is just a block map $\Phi : \mathfrak{G} \longrightarrow \mathfrak{H}$ which is also a group homomorphism;
- if $\mathcal{N} \prec \mathcal{M}$ are $\mathcal{R}\mathbb{L}$-modules, and $\mathcal{Q} = \mathcal{M}/\mathcal{N}$ is the quotient module, then the quotient map $\pi : \mathcal{M} \longrightarrow \mathcal{Q}$ is an $\mathcal{R}\mathbb{L}$-epimorphism.

4.2. *Direct sums.* If $\mathcal{M}$ and $\mathcal{N}$ are two $\mathcal{R}\mathbb{L}$-modules, then their *direct sum* $\mathcal{M} \oplus \mathcal{N}$ is the product group $\mathcal{M} \times \mathcal{N}$ endowed with the product topology, with $\mathcal{R}$ and $\mathbb{L}$ acting componentwise. Now suppose that $(\mathcal{M}_n : n \in \mathbb{N})$ is a countable family of $\mathcal{R}\mathbb{L}$-modules. The direct sum $\bigoplus_{n\in\mathbb{N}} \mathcal{M}_n$ is the Cartesian product $\prod_{n\in\mathbb{N}} \mathcal{M}_n$, endowed with the Tychonoff product topology and componentwise addition, with $\mathcal{R}$ and $\mathbb{L}$ acting componentwise†. For the $\mathcal{R}\mathbb{L}$-module $\mathcal{M}$ we define $\mathcal{M}^{\mathbb{N}} = \bigoplus_{n\in\mathbb{N}} \mathcal{M}_n$, where $\mathcal{M}_n \cong \mathcal{M}$ for all $n \in \mathbb{N}$.

LEMMA 22. *Let $\mathcal{M}$ be an $\mathcal{R}\mathbb{L}$-module. Then:*
(a) *$\mathcal{M}^{\mathbb{N}}$ is an $\mathcal{R}\mathbb{M}$-module;*
(b) *if $\mathcal{M} = \mathfrak{U}$, then $\mathcal{M}^{\mathbb{N}} = \mathfrak{U}^{\mathbb{N}} \cong \mathcal{G}^{\mathbb{M}}$ as $\mathcal{R}\mathbb{M}$-modules.*

For the rest of the section, let $\mathfrak{U} = \mathcal{G}^{\mathbb{L}}$ and $\mathfrak{U}^{\mathbb{N}} \cong \mathcal{G}^{\mathbb{M}}$, as in Lemma 22. To avoid confusion, we will use $\boldsymbol{\sigma}_{\mathbb{L}}$ to indicate the action of $\mathbb{L}$ on $\mathfrak{U}$, which we apply componentwise to sequences in $\mathfrak{U}^{\mathbb{N}}$. We will use $\boldsymbol{\sigma}_{\mathbb{N}}$ to indicate the shift on elements of $\mathfrak{U}^{\mathbb{N}}$, which are treated as $\mathbb{N}$-indexed sequences. Finally, $\boldsymbol{\sigma}_{\mathbb{M}}$ indicates the action of $\mathbb{M} = \mathbb{L} \times \mathbb{N}$ obtained by combining $\boldsymbol{\sigma}_{\mathbb{L}}$ and $\boldsymbol{\sigma}_{\mathbb{M}}$. If $\mathbf{g} \in \mathcal{G}^{\mathbb{M}}$, then we write $\mathbf{g} = (\mathbf{g}_0, \mathbf{g}_1, \mathbf{g}_2, \dots) \in \mathfrak{U}^{\mathbb{N}}$, where, for all $n \in \mathbb{N}$, $\mathbf{g}_n = \mathbf{g}|_{\mathbb{L}\times\{n\}}$ is an element of $\mathfrak{U}$.

4.3. *Markov $\mathcal{R}\mathbb{L}$-modules.* Consider the direct sum $\mathfrak{U}^{\mathbb{N}}$ as an $\mathcal{R}\mathbb{L}$-module under $\boldsymbol{\sigma}_{\mathbb{L}}$ and the natural action of $\mathcal{R}$. An *$\mathcal{R}\mathbb{L}$-submodule shift* of $\mathfrak{U}^{\mathbb{N}}$ is a closed $\mathcal{R}\mathbb{L}$-submodule $\mathfrak{V} \subseteq \mathfrak{U}^{\mathbb{N}}$ which is also $\boldsymbol{\sigma}_{\mathbb{N}}$-invariant. A *Markov $\mathcal{R}\mathbb{L}$-submodule* is an $\mathcal{R}\mathbb{L}$-submodule shift $\mathfrak{V}$ which is determined by some set of admissible transitions $T_{\mathfrak{V}} \subseteq \mathfrak{U}^{\{0,1\}}$ such that

$$\mathfrak{V} = \{\mathbf{u} \in \mathfrak{U}^{\mathbb{N}} : (\mathbf{u}_n, \mathbf{u}_{n+1}) \in T_{\mathfrak{V}}, \forall n \in \mathbb{N}\}. \tag{11}$$

For any $\mathbf{u} \in \mathfrak{U}$, let $\mathcal{F}_{\mathfrak{V}}(\mathbf{u}) = \{\mathbf{v} \in \mathfrak{U} : (\mathbf{u}, \mathbf{v}) \in T_{\mathfrak{V}}\}$ be the followers of $\mathbf{u}$. Note that $\mathcal{F}_{\mathfrak{V}}(\mathbf{u})$ could be empty.

PROPOSITION 23. *Let $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ be a nearest-neighbor subgroup shift as in* (5)*. Then:*
(a) *$\mathfrak{G}$ is a Markov $\mathcal{R}\mathbb{L}$-submodule of $\mathfrak{U}^{\mathbb{N}}$.*

Let $\mathfrak{Z} = \mathcal{F}_{\mathfrak{G}}(0) \subseteq \mathfrak{U}$ be the follower set of the zero configuration in $\mathfrak{U}$ (mnemonic: '$\mathfrak{Z}$' is for 'zero'). Then:
(b) *$\mathfrak{Z}$ is an $\mathcal{R}\mathbb{L}$-submodule of $\mathfrak{U}$;*
(c) *for any $\mathbf{u} \in \mathfrak{U}_{\mathfrak{G}}$, $\mathcal{F}_{\mathfrak{G}}(\mathbf{u})$ is a coset of $\mathfrak{Z}$;*
(d) *let $\mathcal{Q} = \mathfrak{U}_{\mathfrak{G}}/\mathfrak{Z}$ be the quotient $\mathcal{R}\mathbb{L}$-module, and define $F : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathcal{Q}$ by $F(\mathbf{u}) = \mathcal{F}_{\mathfrak{G}}(\mathbf{u})$, then F is an $\mathcal{R}\mathbb{L}$-module morphism;*

† Note that this differs from the *algebraic* direct sum of modules, where only *finitely many* coordinates can be non-zero.

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

(e) *let* $\pi : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathfrak{Z}$ *be the quotient map (i.e.* $\pi(\mathbf{u}) = \mathbf{u} + \mathfrak{Z}$*), then* $\mathfrak{G} = \{\mathbf{u} \in \mathfrak{U}_{\mathfrak{G}}^{\mathbb{N}} : F(\mathbf{u}_n) = \pi(\mathbf{u}_{n+1}), \forall n \in \mathbb{N}\}$.

Proof. (a) let $\mathbb{B}$ and $T_{\mathfrak{G}}$ be as in (5), and define

$$S_{\mathfrak{G}} = \{\mathbf{g} \in \mathcal{G}^{\mathbb{L}\times\{0,1\}} : \mathbf{g}|_{\mathbb{B}+(\ell,0)} \in T_{\mathfrak{G}}, \forall \ell \in \mathbb{L}\}. \tag{12}$$

If $\mathbf{u}, \mathbf{v} \in \mathfrak{U} = \mathcal{G}^{\mathbb{L}}$, let $[\mathbf{u}, \mathbf{v}]$ be the corresponding element of $\mathcal{G}^{\mathbb{L}\times\{0,1\}}$. Then for any $\mathbf{u} \in \mathfrak{U}^{\mathbb{N}}$, $\mathbf{u} \in \mathfrak{G}$ if and only if $[\mathbf{u}_n, \mathbf{u}_{n+1}] \in S_{\mathfrak{G}}$, for all $n \in \mathbb{N}$. In other words, (11) is true. Also, $\mathfrak{G}$ is a group and is $\boldsymbol{\sigma}_{\mathbb{N}}$-invariant. It follows that $\mathfrak{G}$ is a Markov $\mathcal{R}\mathbb{L}$-submodule.
(b) We must show that $\mathfrak{Z}$ is a closed, $\boldsymbol{\sigma}_{\mathbb{L}}$-invariant subgroup of $\mathfrak{U}_{\mathfrak{G}}$. We will use the following claim.

CLAIM 1. *If* $S_{\mathfrak{G}}$ *is as in* (12)*, then* $S_{\mathfrak{G}}$ *is a subgroup shift in* $(\mathcal{G}^{\{0,1\}})^{\mathbb{L}}$.

$\mathfrak{Z}$ *is* $\boldsymbol{\sigma}_{\mathbb{L}}$*–invariant.* Let $\mathbf{u} \in \mathfrak{U}$, and let $\ell \in \mathbb{L}$. Then, from definitions of $\mathfrak{Z}$ and $S_{\mathfrak{G}}$, and the claim, we get

$$\begin{aligned}(\mathbf{u} \in \mathfrak{Z}) &\iff ([0, \mathbf{u}] \in S_{\mathfrak{G}}) \iff ([\boldsymbol{\sigma}^{\ell}(0), \boldsymbol{\sigma}^{\ell}(\mathbf{u})] \in S_{\mathfrak{G}}) \iff ([0, \boldsymbol{\sigma}^{\ell}(\mathbf{u})] \in S_{\mathfrak{G}}) \\ &\iff (\boldsymbol{\sigma}^{\ell}(\mathbf{u}) \in \mathfrak{Z}).\end{aligned}$$

$\mathfrak{Z}$ *is closed.* Let $\{\mathbf{z}_n\}_{n\in\mathbb{N}} \subseteq \mathfrak{Z}$ be a sequence with limit $\mathbf{z} \in \mathfrak{U}$. We must show $\mathbf{z} \in \mathfrak{Z}$ also. For all $n \in \mathbb{N}$, treat $[0, \mathbf{z}_n]$ as an element of $\mathcal{G}^{\mathbb{L}\times\{0,1\}}$. By hypothesis, $[0, \mathbf{z}_n] \in S_{\mathfrak{G}}$ for all $n \in \mathbb{N}$. However, $S_{\mathfrak{G}}$ is closed (Claim 1). Hence, $\lim_{n\to\infty} [0, \mathbf{z}_n] = [0, \mathbf{z}]$ is also in $S_{\mathfrak{G}}$. We conclude that $\mathbf{z} \in \mathfrak{Z}$.

$\mathfrak{Z}$ *is a group.* This follows from the fact that $S_{\mathfrak{G}}$ is a group (Claim 1).
(c) Let $\mathbf{u} \in \mathfrak{U}_{\mathfrak{G}}$ and let $\mathbf{v}, \mathbf{w} \in \mathcal{F}_{\mathfrak{G}}(\mathbf{u})$. We want to show that $(\mathbf{v} - \mathbf{w}) \in \mathfrak{Z}$. Observe that $[\mathbf{u}, \mathbf{v}] \in S_{\mathfrak{G}}$ and $[\mathbf{u}, \mathbf{w}] \in S_{\mathfrak{G}}$. Since $S_{\mathfrak{G}}$ is a group (Claim 1), $[\mathbf{u}, \mathbf{v}] - [\mathbf{u}, \mathbf{w}] = [0, (\mathbf{v} - \mathbf{w})]$ is also in $\mathfrak{Z}$, which means $(\mathbf{v} - \mathbf{w}) \in \mathfrak{Z}$.

(d) F *is a group homomorphism.* Let $\mathbf{u}_1, \mathbf{u}_2 \in \mathfrak{U}_{\mathfrak{G}}$ and suppose that $F(\mathbf{u}_1) = \mathbf{v}_1 + \mathfrak{Z}$ and $F(\mathbf{u}_2) = \mathbf{v}_2 + \mathfrak{Z}$. We want to show that $F(\mathbf{u}_1 + \mathbf{u}_2) = (\mathbf{v}_1 + \mathbf{v}_2) + \mathfrak{Z}$. Observe that $[\mathbf{u}_1, \mathbf{v}_1] \in S_{\mathfrak{G}}$ and $[\mathbf{u}_1, \mathbf{v}_2] \in S_{\mathfrak{G}}$. However, $S_{\mathfrak{G}}$ is a group, so $[\mathbf{u}_1, \mathbf{v}_1] + [\mathbf{u}_2, \mathbf{v}_2] = [\mathbf{u}_1 + \mathbf{u}_2, \mathbf{v}_1 + \mathbf{v}_2]$ is in $S_{\mathfrak{G}}$; thus, $F(\mathbf{u}_1 + \mathbf{u}_2) = (\mathbf{v}_1 + \mathbf{v}_2) + \mathfrak{Z}$.

F *commutes with* $\boldsymbol{\sigma}_{\mathbb{L}}$. Let $\mathbf{u} \in \mathfrak{U}_{\mathfrak{G}}$ and $m \in \mathbb{L}$. Suppose $F(\mathbf{u}) = \mathbf{v} + \mathfrak{Z}$. Thus, $[\mathbf{u}, \mathbf{v}] \in S_{\mathfrak{G}}$ and $[\boldsymbol{\sigma}^m(\mathbf{u}), \boldsymbol{\sigma}^m(\mathbf{v})] \in S_{\mathfrak{G}}$ (Claim 1 says $S_{\mathfrak{G}}$ is $\boldsymbol{\sigma}_{\mathbb{L}}$-invariant). Hence, $F(\boldsymbol{\sigma}^m(\mathbf{u})) = \boldsymbol{\sigma}^m(\mathbf{v}) + \mathfrak{Z} = \boldsymbol{\sigma}^m(\mathbf{v} + \mathfrak{Z}) = \boldsymbol{\sigma}^m(F(\mathbf{u}))$.

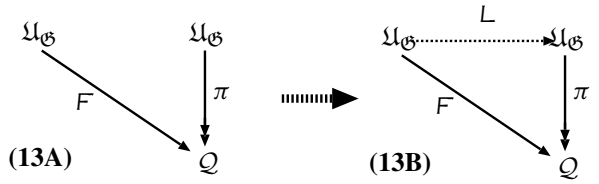
F *is continuous.* Let $\{\mathbf{u}_n\}_{n\in\mathbb{N}} \subseteq \mathfrak{U}_{\mathfrak{G}}$ be a sequence converging to $\mathbf{u} \in \mathfrak{U}$, and let $F(\mathbf{u}_n) = \mathbf{v}_n + \mathfrak{Z}$. We want to show that the sequence $\{\mathbf{v}_n + \mathfrak{Z}\}_{n\in\mathbb{N}} \subseteq \mathcal{Q}$ converges to $F(\mathbf{u}) = \mathbf{v} + \mathfrak{Z}$.

Let $\mathbf{u}'_n = \mathbf{u}_n - \mathbf{u}$ and let $\mathbf{v}'_n = \mathbf{v}_n - \mathbf{v}$. Hence, $\lim_{n\to\infty} \mathbf{u}'_n = 0$, and it suffices to show that the sequence $\{\mathbf{v}'_n + \mathfrak{Z}\}_{n\in\mathbb{N}} \subseteq \mathcal{Q}$ converges to $F(0) = \mathfrak{Z}$. Recall that the element $\mathbf{v}'_n$ can be any representative of its coset; it suffices to show that we can pick elements such that $\lim_{n\to\infty} \mathbf{v}'_n = 0$, in which case $\lim_{n\to\infty} \mathbf{v}'_n + \mathfrak{Z} = 0 + \mathfrak{Z} = \mathfrak{Z}$.

Let $R > 0$. Since $\lim_{n\to\infty} \mathbf{u}'_n = 0$, we know that there is some $N > 0$ such that, for all $n > N$, $\mathbf{u}'_n|_{[0,R]^D} = 0|_{[0,R]^D}$ (i.e. $\mathbf{u}'_n$ is constantly zero inside of $[0, R]^D$). Thus, we can pick $\mathbf{v}$ such that $\mathbf{v}'_n|_{[0,R-2]^D} = 0|_{[0,R-2]^D}$. We conclude $\lim_{n\to\infty} \mathbf{v}'_n = 0$ as required.
(e) Follows from the definition of F and π. □

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

4.4. *The FLP.* Let $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ be a nearest-neighbor subgroup shift as in (5). Then $\mathfrak{G}$ is a Markov $\mathcal{RL}$-submodule of $\mathfrak{U}^{\mathbb{N}}$ by Proposition 23. Let $\mathfrak{Z}$ and $\mathcal{Q}$ be as in Proposition 23, with morphisms $F : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathcal{Q}$ and $\pi : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathcal{Q}$. We say that $\mathfrak{G}$ has the FLP if the map F lifts to an $\mathcal{RL}$-morphism $L : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathfrak{U}_{\mathfrak{G}}$ such that $\pi \circ L = F$. In other words, we can transform diagram (13A) into commuting diagram (13B):



(13)

It follows that for any $\mathbf{u} \in \mathfrak{U}_{\mathfrak{G}}$, $\mathcal{F}_{\mathfrak{G}}(\mathbf{u}) = L(\mathbf{u}) + \mathfrak{Z}$. The FLP allows us to project $\mathfrak{G}$ into a full shift on $\mathfrak{Z}^{\mathbb{N}}$, so that the dynamics of LCA on $\mathfrak{G}$ are reduced to the dynamics of LCA on $\mathfrak{Z}^{\mathbb{N}}$. In what follows $L : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathfrak{U}_{\mathfrak{G}}$ will always be the lifting map of a nearest-neighbor subgroup shift $\mathfrak{G}$ with the FLP.

LEMMA 24. *Suppose that $\mathfrak{G}$ has the FLP.*

(a) *Let $S_{\mathfrak{G}}$ be as in (12). For any $(\mathbf{v}, \mathbf{w}) \in S_{\mathfrak{G}}$, let $\delta(\mathbf{v}, \mathbf{w}) = \mathbf{w} - L(\mathbf{v})$ and let $\Delta : \mathfrak{G} \longrightarrow \mathfrak{Z}^{\mathbb{N}}$ be the block map $\Delta(\mathbf{g})_n = \delta(\mathbf{g}_n, \mathbf{g}_{n+1})$ for $\mathbf{g} \in \mathfrak{G}$ and $n \in \mathbb{N}$. Treat $\mathfrak{G}$ and $\mathfrak{Z}^{\mathbb{N}}$ as $\mathcal{RL}$-modules under componentwise $\boldsymbol{\sigma}_{\mathbb{L}}$-action. Then Δ is an $\mathcal{RL}$-module morphism.*

(b) *Define $\Psi : \mathfrak{G} \longrightarrow \mathfrak{U}_{\mathfrak{G}} \times \mathfrak{Z}^{\mathbb{N}}$ by $\Psi(\mathbf{g}) = (\mathbf{g}_0; \Delta(\mathbf{g}))$, $\mathbf{g} \in \mathfrak{G}$. Then Ψ is an $\mathcal{RL}$-module isomorphism.*

(c) *Ψ is a conjugacy between $(\mathfrak{G}, \boldsymbol{\sigma}_{\mathbb{N}})$ and $(\mathfrak{U}_{\mathfrak{G}} \times \mathfrak{Z}^{\mathbb{N}}, \widetilde{\boldsymbol{\sigma}})$, where $\widetilde{\boldsymbol{\sigma}} : \mathfrak{U}_{\mathfrak{G}} \times \mathfrak{Z}^{\mathbb{N}} \longrightarrow \mathfrak{U}_{\mathfrak{G}} \times \mathfrak{Z}^{\mathbb{N}}$ is defined by $\widetilde{\boldsymbol{\sigma}}(\mathbf{u}; \mathbf{v}) = (\varsigma(\mathbf{u}; \mathbf{v}); \boldsymbol{\sigma}_{\mathbb{N}}(\mathbf{v}))$, where $\varsigma(\mathbf{u}; \mathbf{v}) = L(\mathbf{u}) + \mathbf{v}_0$, for all $\mathbf{u} \in \mathfrak{U}_{\mathfrak{G}}$ and $\mathbf{v} \in \mathfrak{Z}^{\mathbb{N}}$.*

(d) *For $\mathbf{u} \in \mathfrak{U}_{\mathfrak{G}}$ and $\mathbf{z} \in \mathfrak{Z}^{\mathbb{N}}$, let $\varsigma^{(1)}(\mathbf{u}; \mathbf{z}) = \varsigma(\mathbf{u}; \mathbf{z})$, and for $n > 1$, let $\varsigma^{(n)}(\mathbf{u}; \mathbf{z}) = \varsigma(\varsigma^{(n-1)}(\mathbf{u}; \mathbf{z}); \boldsymbol{\sigma}_{\mathbb{N}}^{n-1}(\mathbf{z}))$. Then, for any $n \in \mathbb{N}$, $\widetilde{\boldsymbol{\sigma}}^n(\mathbf{u}; \mathbf{z}) = (\varsigma^{(n)}(\mathbf{u}; \mathbf{z}); \boldsymbol{\sigma}_{\mathbb{N}}^n(\mathbf{z}))$.*

Proof. (a) and (b): L is a morphism, so δ and Δ are morphisms. Thus, Ψ is a morphism. The remainder of the proof is exactly as in Lemma 13. □

Example 25. We have the following.

(a) Let $D = 0$. Then $\mathbb{L} = \mathbb{N}^0$ is the trivial group and $\mathbb{M} = \mathbb{N}$. Interpret $\mathcal{R}$ as $\mathcal{R}\mathbb{N}^0$; then $\mathcal{G}$ is an $\mathcal{R}\mathbb{N}^0$-module, and Proposition 23 becomes Lemma 12. Here diagram (13) becomes diagram (7), the FLP for Markov subgroups.

(b) Let $\mathcal{G} = \mathcal{R} = \mathbb{Z}_{/27}$ and let $D = 1$, so that $\mathbb{L} = \mathbb{N}$, $\mathbb{M} = \mathbb{N}^2$ and $\mathfrak{U} = \mathcal{G}^{\mathbb{N}}$. Let $\mathbb{J} = \{(0, 0), (0, 1), (1, 0)\} \subseteq \mathbb{N}^2$, and define

$$\mathfrak{G} = \left\{ \mathbf{g} \in \mathcal{G}^{\mathbb{M}} : \sum_{j \in \mathbb{J}} 3 \cdot g_{m+j} = 0 \bmod 27, \forall m \in \mathbb{N}^2 \right\}.$$

Then $\mathfrak{U}_{\mathfrak{G}} = \mathfrak{U}$,

$$S_{\mathfrak{G}} = \left\{ \mathbf{s} \in \mathcal{G}^{\mathbb{N} \times \{0,1\}} : \sum_{j \in \mathbb{J}} 3 \cdot s_{(\ell,0)+j} = 0 \bmod 27, \forall \ell \in \mathbb{N} \right\} \text{ and}$$

$$\mathfrak{Z} = \{ \mathbf{z} \in \mathcal{G}^{\mathbb{N}} : 3 \cdot z_\ell = 0 \bmod 27, \forall \ell \in \mathbb{N} \} = \mathcal{Z}^{\mathbb{N}},$$

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

where $\mathcal{Z} := \{0, 9, 18\}$ is the cyclic subgroup of $\mathbb{Z}_{/27}$ generated by 9. Thus,

$$\mathcal{Q} = \mathfrak{U}/\mathfrak{Z} = \mathcal{G}^{\mathbb{N}}/\mathcal{Z}^{\mathbb{N}} \cong (\mathcal{G}/\mathcal{Z})^{\mathbb{N}} \cong \mathcal{P}^{\mathbb{N}},$$

where $\mathcal{P} = \mathbb{Z}_{/9}$ and $\cong$ represents $\mathcal{R}\mathbb{N}^1$-module isomorphism. For any $\mathbf{g} \in \mathcal{G}^{\mathbb{N}}$,

$$\mathcal{F}_{\mathfrak{G}}(\mathbf{g}) = \{\mathbf{h} \in \mathcal{G}^{\mathbb{N}} : 3h_\ell = -3g_\ell - 3g_{\ell+1} \bmod 27,\ \forall \ell \in \mathbb{N}\} = \mathbf{f} + \mathfrak{Z},$$

where $\mathbf{f} = -\mathbf{g} - \boldsymbol{\sigma}_{\mathbb{L}}(\mathbf{g}) \in \mathcal{G}^{\mathbb{N}}$.

Put $L(\mathbf{g}) = \mathbf{f}$, then $L : \mathfrak{U} \longrightarrow \mathfrak{U}$ is an $\mathcal{R}\mathbb{L}$-module homomorphism (i.e. an $\mathcal{R}$-LCA) and $\mathcal{F}_{\mathfrak{G}}(\mathbf{g}) = L(\mathbf{g}) + \mathfrak{Z}$. Hence, $\mathfrak{G}$ has the FLP.

For $\mathbf{u}, \mathbf{v} \in \mathfrak{U}$, $\delta(\mathbf{u}, \mathbf{v}) = \mathbf{v} + (\mathbf{u} + \boldsymbol{\sigma}_{\mathbb{L}}(\mathbf{u})) \in \mathfrak{U}$. Thus, for any $\mathbf{g} = (\mathbf{g}_n : n \in \mathbb{N}) \in \mathfrak{G}$, $\Delta(\mathbf{g}) = \mathbf{v} = (\mathbf{v}_n : n \in \mathbb{N}) \in \mathfrak{Z}^{\mathbb{N}}$, where $\mathbf{v}_n = \mathbf{g}_{n+1} + (\mathbf{g}_n + \boldsymbol{\sigma}_{\mathbb{L}}(\mathbf{g}_n))$. Clearly, $\Delta : \mathfrak{G} \longrightarrow \mathfrak{Z}^{\mathbb{N}}$ is an $\mathcal{R}\mathbb{N}$-module homomorphism. Put, $\Psi(\mathbf{g}) = (\mathbf{g}_0; \mathbf{v})$, thus,

$$\begin{aligned}\varsigma(\mathbf{g}_0; \mathbf{v}) &= L(\mathbf{g}) + \mathbf{v}_0 = (-\mathbf{g}_0 - \boldsymbol{\sigma}_{\mathbb{L}}(\mathbf{g}_0)) + \mathbf{v}_0 \\ &= (-\mathbf{g}_0 - \boldsymbol{\sigma}_{\mathbb{L}}(\mathbf{g}_0)) + \mathbf{g}_1 + (\mathbf{g}_0 + \boldsymbol{\sigma}_{\mathbb{L}}(\mathbf{g}_0)) = \mathbf{g}_1,\end{aligned}$$

in accord with Lemma 24(c).

(c) Again let $\mathbb{L} = \mathbb{N}$, $\mathbb{M} = \mathbb{N}^2$ and $\mathfrak{U} = \mathcal{G}^{\mathbb{N}}$. Now, however, let $\mathcal{G} = \mathcal{R} = \mathbb{Z}_{/2}$ and let $\mathbb{K} = \{(0, 0), (0, 1), (1, 1)\} \subseteq \mathbb{N}^2$. Define

$$\mathfrak{G} = \left\{\mathbf{g} \in \mathcal{G}^{\mathbb{M}} : \sum_{k \in \mathbb{K}} g_{m+k} = 0 \bmod 2, \forall m \in \mathbb{N}^2\right\}.$$

Then $\mathfrak{U}_{\mathfrak{G}} = \mathfrak{U}$ and $\mathfrak{Z} = \{\mathbf{z} \in \mathcal{G}^{\mathbb{N}} : z_\ell + z_{\ell+1} = 0 \bmod 2, \forall \ell \in \mathbb{N}\} = \{\mathbf{0}, \mathbf{1}\} \cong \mathbb{Z}_{/2}$, where $\mathbf{0} = (0\,0\,0\ldots)$ and $\mathbf{1} = (1\,1\,1\ldots)$. Define $\overline{0} = 1$ and $\overline{1} = 0$, and for any $\mathbf{g} = (g_\ell : \ell \in \mathbb{N}) \in \mathcal{G}^{\mathbb{N}}$, let $\overline{\mathbf{g}} = \mathbf{1} + \mathbf{g} = (\overline{g}_\ell : \ell \in \mathbb{N})$. Then $\mathbf{g} + \mathfrak{Z} = \{\mathbf{g}, \overline{\mathbf{g}}\}$, and

$$\mathcal{Q} = \mathfrak{U}/\mathfrak{Z} = \{\{\mathbf{g}, \overline{\mathbf{g}}\} : \mathbf{g} \in \mathcal{G}^{\mathbb{N}}\}.$$

For any $\mathbf{g} \in \mathcal{G}^{\mathbb{N}}$, $\mathcal{F}_{\mathfrak{G}}(\mathbf{g}) = \{\mathbf{h} \in \mathcal{G}^{\mathbb{N}} : h_\ell + h_{\ell+1} = g_\ell \bmod 2, \forall \ell \in \mathbb{N}\}$.

In this example $\mathfrak{G}$ does not have the FLP. To see this, let $\mathbf{d}_n = (\overbrace{0\ \ldots\ 0}^{n}\ 1\,0\,0\,0\ldots)$. Then $\mathcal{F}_{\mathfrak{G}}(\mathbf{d}_n) = \{\mathbf{h}_n, \overline{\mathbf{h}}_n\}$, where

$$\mathbf{h}_n = (\underbrace{0\ \ldots\ 0}_{n}\ 0\,1\,1\,1\ldots) \quad \text{and} \quad \overline{\mathbf{h}}_n = (\underbrace{1\ \ldots\ 1}_{n}\ 1\,0\,0\,0\ldots).$$

So, if $L : \mathfrak{U} \longrightarrow \mathfrak{U}$ satisfies diagram (13), then either $L(\mathbf{d}_n) = \mathbf{h}_n$ or $L(\mathbf{d}_n) = \overline{\mathbf{h}}_n$. Suppose that $L(\mathbf{d}_n) = \mathbf{h}_n$. Since L is an $\mathcal{R}\mathbb{N}$-module homomorphism, L commutes with $\boldsymbol{\sigma}_{\mathbb{L}}$. Thus, $\mathbf{1} = \boldsymbol{\sigma}_{\mathbb{L}}^{n+1}(\mathbf{h}_n) = \boldsymbol{\sigma}_{\mathbb{L}}^{n+1}(L(\mathbf{d}_n)) = L(\boldsymbol{\sigma}_{\mathbb{L}}^{n+1}(\mathbf{d}_n)) = L(\mathbf{0}) = \mathbf{0}$, a contradiction. Hence, we must have $L(\mathbf{d}_n) = \overline{\mathbf{h}}_n$, for all $n \in \mathbb{N}$. However, L must also be continuous. Hence, $\mathbf{1} = \lim_{n\to\infty} \overline{\mathbf{h}}_n = \lim_{n\to\infty} L(\mathbf{d}_n) = L(\lim_{n\to\infty} \mathbf{d}_n) = L(\mathbf{0}) = \mathbf{0}$, again, a contradiction. □

Let $\mathfrak{V} \subseteq \mathfrak{U}^{\mathbb{N}}$ be a Markov $\mathcal{R}\mathbb{L}$-submodule. An *$\mathcal{R}\mathbb{L}$-LCA* on $\mathfrak{V}$ is a function $\Phi : \mathfrak{V} \longrightarrow \mathfrak{V}$ given by

$$\Phi(\mathbf{u}) = \sum_{i \in \mathbb{I}} \phi_i \circ \boldsymbol{\sigma}_{\mathbb{N}}^i(\mathbf{u}) \quad \text{for all } \mathbf{u} \in \mathfrak{V}, \tag{14}$$

where $\mathbb{I} \subseteq \mathbb{N}$ is some finite subset and $\phi_i \in \mathcal{R}\mathbb{L}$ for all $i \in \mathbb{I}$. Thus, the maps ϕ_i are themselves $\mathcal{R}$-LCA on subgroups of $\mathfrak{U}$. It is easy to verify the following.

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

PROPOSITION 26. *Identify $\mathcal{G}^{\mathbb{M}} \cong \mathfrak{U}^{\mathbb{N}}$ as in Lemma 22. Let $\Phi : \mathfrak{G} \longrightarrow \mathfrak{G}$ be some map. Then Φ is an $\mathcal{R}$-LCA on $\mathfrak{G}$ (as a subgroup of $\mathcal{G}^{\mathbb{M}}$) if and only if Φ is an $\mathcal{RL}$-LCA on $\mathfrak{G}$ (as an $\mathcal{RL}$-submodule of $\mathfrak{U}^{\mathbb{N}}$).*

LEMMA 27. *Assume $\mathfrak{G}$ has the FLP and let $\Phi : \mathfrak{G} \longrightarrow \mathfrak{G}$ be an $\mathcal{RL}$-LCA as in* (14)*. Define $\widetilde{\Phi} : \mathfrak{U}_{\mathfrak{G}} \times \mathfrak{Z}^{\mathbb{N}} \longrightarrow \mathfrak{U}_{\mathfrak{G}} \times \mathfrak{Z}^{\mathbb{N}}$ by $\Phi(\mathbf{u}; \mathbf{z}) = \sum_{i \in \mathbb{I}} \phi_i \circ \widetilde{\boldsymbol{\sigma}}^i(\mathbf{u}; \mathbf{z})$, for any $\mathbf{u} \in \mathfrak{U}_{\mathfrak{G}}$ and $\mathbf{z} \in \mathfrak{Z}^{\mathbb{N}}$. Then:*

(a) *Ψ is a conjugacy between $(\mathfrak{G}, \Phi)$ and $(\mathfrak{U}_{\mathfrak{G}} \times \mathfrak{Z}^{\mathbb{N}}, \widetilde{\Phi})$;*

(b) *for $\mathbf{u} \in \mathfrak{U}_{\mathfrak{G}}$ and $\mathbf{z} \in \mathfrak{Z}^{\mathbb{N}}$, $\widetilde{\Phi}(\mathbf{u}; \mathbf{z}) = (\widetilde{\Phi}_{\mathfrak{U}}(\mathbf{u}; \mathbf{z}), \widetilde{\Phi}_{\mathfrak{Z}}(\mathbf{z}))$, where $\widetilde{\Phi}_{\mathfrak{U}}(\mathbf{u}; \mathbf{z}) = \sum_{i \in \mathbb{I}} \phi_i \circ \varsigma^{(i)}(\mathbf{u}; \mathbf{z})$ and where $\widetilde{\Phi}_{\mathfrak{Z}} = \sum_{i \in \mathbb{I}} \phi_i \circ \boldsymbol{\sigma}_{\mathbb{N}}^i$ is itself an $\mathcal{RL}$-LCA on $\mathfrak{Z}^{\mathbb{N}}$.*

Proof. The proof is analogous to Lemma 14. □

For any $\mathbb{I} \subseteq \mathbb{M}$ and $R > 0$, let $\mathbb{I}(R) = \{j \in \mathbb{M} : |i - j| < R \text{ for some } i \in \mathbb{I}\}$, and let $\partial_R \mathbb{I} = \mathbb{I}(R) \setminus \mathbb{I}$. A measure $\mu \in \mathcal{M}(\mathfrak{G})$ is a *Markov random field* (MRF) of range R if for any finite subsets $\mathbb{I} \subseteq \mathbb{M}$ and $\mathbb{J} \subseteq \mathbb{M} \setminus \mathbb{I}(R)$, and any $\mathfrak{G}$-admissible blocks $\mathbf{u} \in \mathcal{G}^{\mathbb{I}}$, $\mathbf{v} \in \mathcal{G}^{\partial_R \mathbb{I}}$ and $\mathbf{w} \in \mathcal{G}^{\mathbb{J}}$,

$$\frac{\mu([\mathbf{u}] \cap [\mathbf{w}] \cap [\mathbf{v}])}{\mu([\mathbf{v}])} = \frac{\mu([\mathbf{u}] \cap [\mathbf{v}])}{\mu([\mathbf{v}])} \cdot \frac{\mu([\mathbf{w}] \cap [\mathbf{v}])}{\mu([\mathbf{v}])}.$$

In other words, the events $[\mathbf{u}]$ and $[\mathbf{w}]$ are conditionally independent given $[\mathbf{v}]$.

LEMMA 28. *Let $\mu \in \mathcal{M}(\mathfrak{G})$. If μ is a ($\boldsymbol{\sigma}_{\mathbb{N}}$-invariant) MRF with full support on $\mathfrak{G}$, then $\Delta(\mu)$ is a ($\boldsymbol{\sigma}_{\mathbb{N}}$-invariant) MRF with full support on $\mathfrak{Z}^{\mathbb{N}}$.*

Proof. The proof is analogous to Lemma 16. □

PROPOSITION 29. *Assume $\mathfrak{G}$ has the FLP and let $\mu \in \mathcal{M}(\mathfrak{G})$. Then:*

(a) *μ is a measure of maximal entropy on $\mathfrak{G}$ if and only if $\Delta(\mu)$ is of maximal entropy on $\mathfrak{Z}^{\mathbb{N}}$;*

(b) *Φ asymptotically randomizes μ if and only if $\widetilde{\Phi}_{\mathfrak{Z}}$ asymptotically randomizes $\Delta(\mu)$, where Φ and $\widetilde{\Phi}_{\mathfrak{Z}}$ are as in Lemma 27.*

Proof. If $\mathfrak{G}$ has the FLP, then $L : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathfrak{U}_{\mathfrak{G}}$ is an $\mathcal{RL}$-morphism, that is, a CA. Suppose that L has local rule $L_{\text{loc}} : \mathcal{G}^{[0,R]^D} \longrightarrow \mathcal{G}$ for some $R > 0$, such that for any $\ell \in \mathbb{L}$ and $\mathbf{u} \in \mathfrak{U}$, $L(\mathbf{u})_\ell = L_{\text{loc}}(\mathbf{u}|_{\ell + [0,R]^D})$. The local map L_{loc} acts naturally on any block of $\mathfrak{U}$ containing translations of $[0, NR]^D$ for any $N > 0$. □

For $N \geq 0$, let $\underline{\triangle}(N) = \{(\ell, n) \in \mathbb{M} : n \in [0, N] \text{ and } \ell \in [0, (N-n)R]^D\} \subseteq \mathbb{M}$, and let $\triangle(N) = \{(\ell, n) \in \mathbb{M} : n \in [1, N] \text{ and } \ell \in [0, (N-n)R]^D\}$. For example, if $\mathbb{L} = \mathbb{N}$ and $R = 2$ then $\triangle(4) = \{(0,1), \ldots, (6,1), (0,2), \ldots, (4,2), (0,3), (1,3), (2,3), (0,4)\}$ and $\underline{\triangle}(4) = \triangle(4) \cup \{(0,0), \ldots, (8,0)\}$.

For any $N > 0$, let $\mathfrak{G}_{N \times 0} = \{\mathbf{g}|_{[0,NR]^D \times \{0\}} : \mathbf{g} \in \mathfrak{G}\} \subseteq \mathcal{G}^{[0,NR]^D}$.

CLAIM 1. *For any $N > 0$, $|\mathfrak{G}_{\underline{\triangle}(N)}| = |\mathfrak{G}_{N \times 0}| \cdot |(\mathfrak{Z}^{\mathbb{N}})_{\triangle(N)}|$.*

Proof. Suppose that $\mathbf{g} \in \mathfrak{G}_{\underline{\triangle}(N)}$ and write $\mathbf{g} = (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_N)$, where $\mathbf{g}_n \in \mathcal{G}^{[0,(N-n)R]^D}$. Thus, $\mathbf{g}_0 \in \mathfrak{G}_{N \times 0} \subseteq (\mathfrak{U}_{\mathfrak{G}})_{[0,NR]^D}$. Let $\mathbf{f}_1 = L_{\text{loc}}(\mathbf{g}_0) \in (\mathfrak{U}_{\mathfrak{G}})_{[0,(N-1)R]^D}$, and for all $n \in [2, N]$, let $\mathbf{f}_n = L_{\text{loc}}(\mathbf{f}_{n-1}) \in (\mathfrak{U}_{\mathfrak{G}})_{[0,(N-n)R]^D}$. Then $\mathbf{g}_n = \mathbf{f}_n + \mathbf{z}_n$,

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

where $\mathbf{z}_n \in \mathfrak{Z}_{[(N-n)R]^D}$. Then $\mathbf{g}_0$ and $(\mathbf{z}_1, \ldots, \mathbf{z}_N) \in (\mathfrak{Z}^{\mathbb{N}})_{\underline{\triangle}(N)}$ completely determine $\mathbf{g}$. Conversely, any element of $\mathfrak{G}_{\underline{\triangle}(N)}$ can be generated in this fashion by choosing some $\mathbf{g} \in \mathfrak{G}_{N\times 0}$ and some $\mathbf{z} = (\mathbf{z}_1, \ldots, \mathbf{z}_N) \in (\mathfrak{Z}^{\mathbb{N}})_{\underline{\triangle}(N)}$. Thus, $|\mathfrak{G}_{\underline{\triangle}(N)}| = |\mathfrak{G}_{N\times 0}| \cdot |(\mathfrak{Z}^{\mathbb{N}})_{\underline{\triangle}(N)}|$. □

CLAIM 2. *We claim that* $h_{\mathrm{top}}(\mathfrak{G}) = h_{\mathrm{top}}(\mathfrak{Z}^{\mathbb{N}})$.

Proof. It follows from the definition of topological entropy that

$$h_{\mathrm{top}}(\mathfrak{G}) = \lim_{N\to\infty} \frac{\log|\mathfrak{G}_{\underline{\triangle}(N)}|}{|\underline{\triangle}(N)|} = \lim_{N\to\infty} \frac{\log|\mathfrak{G}_{N\times 0}| + \log(|(\mathfrak{Z}^{\mathbb{N}})_{\underline{\triangle}(N)}|)}{|\underline{\triangle}(N)|}$$
$$= \lim_{N\to\infty} \frac{\log|(\mathfrak{Z}^{\mathbb{N}})_{\underline{\triangle}(N)}|}{\underline{\triangle}(n)} + \lim_{N\to\infty} \frac{\log|\mathfrak{G}_{N\times 0}|}{|\underline{\triangle}(N)|} = h_{\mathrm{top}}(\mathfrak{Z}^{\mathbb{N}}). \qquad \square$$

CLAIM 3. *We claim that* $h_\mu(\mathfrak{G}) = h_{\Delta(\mu)}(\mathfrak{Z}^{\mathbb{N}})$.

Proof. As in Claim 2, we have

$$h_\mu(\mathfrak{G}) = -\lim_{N\to\infty} \frac{1}{|\underline{\triangle}(N)|} \sum_{\mathbf{g}\in\mathfrak{G}_{\underline{\triangle}(N)}} \mu([\mathbf{g}]) \cdot \log(\mu([\mathbf{g}])). \tag{15}$$

Let $\zeta := \Delta(\mu)$, and use the bijection $\mathfrak{G}_{\underline{\triangle}(N)} \ni \mathbf{g} \mapsto (\mathbf{g}_0; \mathbf{z}) \in \mathfrak{G}_{N\times 0} \times (\mathfrak{Z}^{\mathbb{N}})_{\underline{\triangle}(N)}$ from Claim 1 to see that

$$\sum_{\mathbf{g}\in\mathfrak{G}_{\underline{\triangle}(N)}} \mu([\mathbf{g}]) \cdot \log\mu([\mathbf{g}])$$
$$= \sum_{\mathbf{g}_0\in\mathfrak{G}_{N\times 0}} \sum_{\mathbf{z}\in(\mathfrak{Z}^{\mathbb{N}})_{\underline{\triangle}(N)}} \mu([\mathbf{g}_0]) \cdot \zeta([\mathbf{z}]) \cdot [\log(\mu([\mathbf{g}_0])) + \log(\zeta([\mathbf{z}]))]$$
$$= \sum_{\mathbf{g}_0\in\mathfrak{G}_{N\times 0}} \mu([\mathbf{g}_0]) \cdot \log\mu([\mathbf{g}_0]) + \sum_{\mathbf{z}\in(\mathfrak{Z}^{\mathbb{N}})_{\underline{\triangle}(N)}} \zeta([\mathbf{z}]) \cdot \log(\zeta([\mathbf{z}])).$$

Substituting the last expression into (15) yields

$$h_\mu(\mathfrak{G}) = -\lim_{N\to\infty} \frac{1}{|\underline{\triangle}(N)|}$$
$$\times \left(\sum_{\mathbf{g}_0\in\mathfrak{G}_{N\times 0}} \mu([\mathbf{g}_0]) \cdot \log\mu([\mathbf{g}_0]) + \sum_{\mathbf{z}\in(\mathfrak{Z}^{\mathbb{N}})_{\underline{\triangle}(N)}} \zeta([\mathbf{z}]) \cdot \log(\zeta([\mathbf{z}])) \right)$$
$$= -\lim_{N\to\infty} \frac{1}{|\triangle(N)|} \sum_{\mathbf{z}\in(\mathfrak{Z}^{\mathbb{N}})_{\underline{\triangle}(N)}} \zeta([\mathbf{z}]) \cdot \log(\zeta([\mathbf{z}])) = h_\zeta(\mathfrak{Z}^{\mathbb{N}}).$$

Finally, Claims 2 and 3 yield (a), and then Lemma 27(a) yields (b). □

Suppose that $D = 1$, so that $\mathbb{L} = \mathbb{N}$ and $\mathbb{M} = \mathbb{N}^2$. If $\mathfrak{G} \subset \mathcal{G}^{\mathbb{M}}$ has the FLP, then Lemma 24(b) yields an isomorphism $\Psi : \mathfrak{G} \longrightarrow \mathfrak{U}_{\mathfrak{G}} \times \mathfrak{Z}^{\mathbb{N}}$, where $\mathfrak{U}_{\mathfrak{G}} \subset \mathcal{G}^{\mathbb{N}}$ and $\mathfrak{Z} \subset \mathcal{G}^{\mathbb{N}}$ are themselves one-dimensional Markov subgroups. We will say that $\mathfrak{G}$ has the *strong* FLP if the group $\mathfrak{Z}$ *also* has the FLP, as described in §3.1.

If $D \geq 2$ (and $\mathbb{M} = \mathbb{N}^{D+1}$), and $\mathfrak{G} \subset \mathcal{G}^{\mathbb{M}}$ has the FLP, then we get an isomorphism $\Psi : \mathfrak{G} \longrightarrow \mathfrak{U}_{\mathfrak{G}} \times \mathfrak{Z}^{\mathbb{N}}$, where $\mathfrak{U}_{\mathfrak{G}} \subset \mathcal{G}^{\mathbb{N}^D}$ and $\mathfrak{Z} \subset \mathcal{G}^{\mathbb{N}^D}$. We inductively define $\mathfrak{G}$ to have the *strong* FLP if the group $\mathfrak{Z}$ has the FLP as a subgroup shift of $\mathcal{G}^{\mathbb{N}^D}$.

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

For example, if $\mathcal{G}$ is a p-group, and $\mathfrak{G} \subset \mathcal{G}^{\mathbb{N}^2}$ has the FLP, then $\mathcal{G}$ automatically has the strong FLP, because Proposition 20 implies that $\mathfrak{Z} \subset \mathcal{G}^{\mathbb{N}}$ has the FLP.

PROPOSITION 30. *Let $\mathfrak{G} \subset \mathcal{G}^{\mathbb{N}^{D+1}}$ have the strong FLP.*

(a) *There is a finite abelian group $\mathcal{Z}$, and for each $d \in [1, D]$, there is a subgroup shift $\mathfrak{U}_d \subset \mathcal{G}^{\mathbb{N}^d}$, and a topological group isomorphism $\Gamma\colon \mathfrak{G} \longrightarrow \overline{\mathfrak{G}}$, where $\overline{\mathfrak{G}} := \mathfrak{U}_D \times \mathfrak{U}_{D-1}^{\mathbb{N}} \times \cdots \times \mathfrak{U}_1^{\mathbb{N}^{D-1}} \times \mathcal{G}^{\mathbb{N}^D} \times \mathcal{Z}^{\mathbb{N}^{D+1}}$.*

(b) *If $\Phi\colon \mathfrak{G} \longrightarrow \mathfrak{G}$ is an LCA, then there is an LCA $\overline{\Phi}_{\mathcal{Z}}\colon \mathcal{Z}^{\mathbb{N}^{D+1}} \longrightarrow \mathcal{Z}^{\mathbb{N}^{D+1}}$, there is a homomorphism $\overline{\Phi}_0\colon \mathcal{G}^{\mathbb{N}^D} \times \mathcal{Z}^{\mathbb{N}^{D+1}} \longrightarrow \mathcal{G}^{\mathbb{N}^D}$ and, for every $d \in [1, D]$, there is a homomorphism*

$$\overline{\Phi}_d\colon \mathfrak{U}_d^{\mathbb{N}^{D-d}} \times \cdots \times \mathfrak{U}_1^{\mathbb{N}^{D-1}} \times \mathcal{G}^{\mathbb{N}^D} \times \mathcal{Z}^{\mathbb{N}^{D+1}} \longrightarrow \mathfrak{U}_d^{\mathbb{N}^{D-d}}$$

such that, if we define $\overline{\Phi}\colon \overline{\mathfrak{G}} \longrightarrow \overline{\mathfrak{G}}$ by

$$\overline{\Phi}(\mathbf{u}_D, \ldots, \mathbf{u}_1, \mathbf{g}; \mathbf{z}) := (\overline{\Phi}_D(\mathbf{u}_D, \ldots, \mathbf{u}_1, \mathbf{g}; \mathbf{z}), \ldots, \overline{\Phi}_2(\mathbf{u}_2, \mathbf{u}_1, \mathbf{g}; \mathbf{z}), \overline{\Phi}_1(\mathbf{u}_1, \mathbf{g}; \mathbf{z}); \overline{\Phi}_0(\mathbf{g}; \mathbf{z}); \overline{\Phi}_{\mathcal{Z}}(\mathbf{z})), \tag{16}$$

then Γ is a conjugacy from $(\mathfrak{G}, \Phi)$ to $(\overline{\mathfrak{G}}, \overline{\Phi})$.

Let $\mu \in \mathcal{M}(\mathfrak{G})$, and let $\zeta \in \mathcal{M}(\mathcal{Z}^{\mathbb{N}^{D+1}})$ be the projection of $\Gamma(\mu)$ to $\mathcal{Z}^{\mathbb{N}^{D+1}}$. Then:

(c) *μ is a $\boldsymbol{\sigma}$-invariant MRF with full support on $\mathfrak{G}$ if and only if ζ is a $\boldsymbol{\sigma}$-invariant MRF with full support on $\mathcal{Z}^{\mathbb{N}^{D+1}}$;*

(d) *Φ asymptotically randomizes μ if and only if $\overline{\Phi}_{\mathcal{Z}}$ asymptotically randomizes ζ.*

Proof (By induction on D.) If $D = 0$, then $\overline{\mathfrak{G}} = \mathcal{G} \times \mathcal{Z}^{\mathbb{N}}$. Thus, if we set $\Gamma = \Psi$, then (a) is Lemma 13(b), (b) is just Lemma 14, (c) is Lemma 16 and (d) is Corollary 19.

Suppose that the proposition is true for $D = k - 1$, and let $D = k$. Lemma 24(b) yields an isomorphism $\Psi : \mathfrak{G} \longrightarrow \mathfrak{U}_D \times \mathfrak{Z}^{\mathbb{N}}$, where $\mathfrak{U}_D \subset \mathcal{G}^{\mathbb{N}^D}$ and $\mathfrak{Z} \subset \mathcal{G}^{\mathbb{N}^D}$ are subgroup shifts.

(a) $\mathfrak{Z}$ has the strong FLP, so induction yields an isomorphism

$$\Gamma_{\mathfrak{Z}} : \mathfrak{Z} \longrightarrow \overline{\mathfrak{Z}} \quad := \quad \mathfrak{U}_{D-1} \times \mathfrak{U}_{D-2}^{\mathbb{N}} \times \cdots \times \mathfrak{U}_1^{\mathbb{N}^{D-2}} \times \mathcal{G}^{\mathbb{N}^{D-1}} \times \mathcal{Z}^{\mathbb{N}^D},$$

where $\mathfrak{U}_1, \ldots, \mathfrak{U}_{D-1} \subset \mathcal{G}^{\mathbb{N}^{D-1}}$ and $\mathcal{Z}$ are as described above. We extend this to an isomorphism

$$\Gamma_{\mathfrak{Z}}^{\mathbb{N}} : \mathfrak{Z}^{\mathbb{N}} \longrightarrow \overline{\mathfrak{Z}}^{\mathbb{N}} \cong \mathfrak{U}_{D-1}^{\mathbb{N}} \times \mathfrak{U}_{D-2}^{\mathbb{N}^2} \times \cdots \times \mathfrak{U}_1^{\mathbb{N}^{D-1}} \times \mathcal{G}^{\mathbb{N}^D} \times \mathcal{Z}^{\mathbb{N}^{D+1}}$$

by applying $\Gamma_{\mathfrak{Z}}$ componentwise.

Now, for any $\mathbf{g} \in \mathfrak{G}$, if $\Psi(\mathbf{g}) = (\mathbf{u}_D, \mathfrak{z}) \in \mathfrak{U}_D \times \mathfrak{Z}^{\mathbb{N}}$, then define $\Gamma(\mathbf{g}) := (\mathbf{u}_D, \Gamma_{\mathfrak{Z}}^{\mathbb{N}}(\mathfrak{z})) \in \overline{\mathfrak{G}}$.

(b) Lemma 27(b) yields an LCA $\widetilde{\Phi}_{\mathfrak{Z}} : \mathfrak{Z}^{\mathbb{N}} \longrightarrow \mathfrak{Z}^{\mathbb{N}}$ and a homomorphism $\widetilde{\Phi}_D : \mathfrak{U}_D \times \mathfrak{Z}^{\mathbb{N}} \longrightarrow \mathfrak{U}_D$ so that $\widetilde{\Psi}$ is a conjugacy from $(\mathfrak{G}, \Phi)$ to $(\mathfrak{U}_D \times \mathfrak{Z}^{\mathbb{N}}, \widetilde{\Phi})$, where $\widetilde{\Phi}(\mathbf{u}, \mathfrak{z}) := (\widetilde{\Phi}_D(\mathbf{u}, \mathfrak{z}), \widetilde{\Phi}_{\mathfrak{Z}}(\mathfrak{z}))$.

As in (14), write $\widetilde{\Phi}_{\mathfrak{Z}} = \sum_{i \in \mathbb{I}} \widetilde{\phi}^i \circ \boldsymbol{\sigma}_{\mathbb{N}}^i$, where $\mathbb{I} \subset \mathbb{N}$, and, for each $i \in \mathbb{I}$, $\widetilde{\phi}^i : \mathfrak{Z} \longrightarrow \mathfrak{Z}$ is an LCA. By induction, for each $i \in \mathbb{I}$, we can find $\overline{\phi}_{\mathcal{Z}}^i : \mathcal{Z}^{\mathbb{N}^D} \longrightarrow \mathcal{Z}^{\mathbb{N}^D}$, a homomorphism $\overline{\phi}_0^i : \mathcal{G} \times \mathcal{Z}^{\mathbb{N}^D} \longrightarrow \mathcal{G}$ and, for all $d \in [1, D)$, a homomorphism

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

$\overline{\phi}^i_d : \mathfrak{U}_d^{\mathbb{N}^{D-d-1}} \times \cdots \times \mathfrak{U}_1^{\mathbb{N}^{D-2}} \times \mathcal{G}^{\mathbb{N}^{D-1}} \times \mathcal{Z}^{\mathbb{N}^D} \longrightarrow \mathfrak{U}_d^{\mathbb{N}^{D-d-1}}$ such that, if we define $\overline{\phi}^i : \overline{\mathfrak{Z}} \longrightarrow \overline{\mathfrak{Z}}$ analogously to (16), then $\overline{\phi}^i \circ \Gamma_{\mathfrak{Z}} = \Gamma_{\mathfrak{Z}} \circ \widetilde{\phi}^i$.

Identify $\mathcal{Z}^{\mathbb{N}^{D+1}} \cong (\mathcal{Z}^{\mathbb{N}^D})^{\mathbb{N}}$, and define $\overline{\Phi}_{\mathcal{Z}} : (\mathcal{Z}^{\mathbb{N}^D})^{\mathbb{N}} \longrightarrow (\mathcal{Z}^{\mathbb{N}^D})^{\mathbb{N}}$ by $\overline{\Phi}_{\mathcal{Z}} := \sum_{i \in \mathbb{I}} \overline{\phi}^i_{\mathcal{Z}} \circ \boldsymbol{\sigma}^i_{\mathbb{N}}$. Identify $\mathcal{G}^{\mathbb{N}^D} \cong (\mathcal{G}^{\mathbb{N}^{D-1}})^{\mathbb{N}}$, and define $\overline{\Phi}_0 : (\mathcal{G}^{\mathbb{N}^{D-1}})^{\mathbb{N}} \times (\mathcal{Z}^{\mathbb{N}^D})^{\mathbb{N}} \longrightarrow (\mathcal{G}^{\mathbb{N}^{D-1}})^{\mathbb{N}}$ by $\overline{\Phi}_0 := \sum_{i \in \mathbb{I}} \overline{\phi}^i_0 \circ \boldsymbol{\sigma}^i_{\mathbb{N}}$. For each $d \in [1, D)$, identify $\mathfrak{U}_d^{\mathbb{N}^{D-d}} \cong (\mathfrak{U}_d^{\mathbb{N}^{D-d-1}})^{\mathbb{N}}$, and define $\overline{\Phi}_d : (\mathfrak{U}_d^{\mathbb{N}^{D-d-1}})^{\mathbb{N}} \times \cdots \times (\mathfrak{U}_1^{\mathbb{N}^{D-2}})^{\mathbb{N}} \times (\mathcal{G}^{\mathbb{N}^{D-1}})^{\mathbb{N}} \times (\mathcal{Z}^{\mathbb{N}^D})^{\mathbb{N}} \longrightarrow (\mathfrak{U}_d^{\mathbb{N}^{D-d-1}})^{\mathbb{N}}$ by $\overline{\Phi}_d := \sum_{i \in \mathbb{I}} \overline{\phi}^i_d \circ \boldsymbol{\sigma}^i_{\mathbb{N}}$. If we define $\overline{\Phi}_{\mathfrak{Z}} : \overline{\mathfrak{Z}}^{\mathbb{N}} \longrightarrow \overline{\mathfrak{Z}}^{\mathbb{N}}$ analogously to (16), then it follows that $\overline{\Phi}_{\mathfrak{Z}} \circ \Gamma^{\mathbb{N}}_{\mathfrak{Z}} = \Gamma^{\mathbb{N}}_{\mathfrak{Z}} \circ \widetilde{\Phi}_{\mathfrak{Z}}$. Finally, for any $(\mathbf{u}_D; \mathbf{u}_{D-1}, \ldots, \mathbf{u}_1, \mathbf{g}; \mathbf{z}) \in \overline{\mathfrak{G}} \cong \mathfrak{U}_D \times \overline{\mathfrak{Z}}^{\mathbb{N}}$, let $\overline{\Phi}_D(\mathbf{u}_D; \mathbf{u}_{D-1}, \ldots, \mathbf{u}_1, \mathbf{g}; \mathbf{z}) := \widetilde{\Phi}_D(\mathbf{u}_D, \mathfrak{z})$, where $\mathfrak{z} = (\Gamma^{\mathbb{N}}_{\mathfrak{Z}})^{-1}(\mathbf{u}_{D-1}, \ldots, \mathbf{u}_1, \mathbf{g}; \mathbf{z}) \in \mathfrak{Z}^{\mathbb{N}}$. If we define $\overline{\Phi} : \overline{\mathfrak{G}} \longrightarrow \overline{\mathfrak{G}}$ as in (16), then (b) follows.

Prove (c) by inductively applying Lemma 28. Prove (d) by inductively applying Proposition 29(b). □

Proof of Theorem 4. If μ is an MRF with full support on $\mathfrak{G}$, then Proposition 30(c) says that ζ is an MRF with full support on $\mathcal{Z}^{\mathbb{N}^{D+1}}$. Thus, Theorems 12 and 15 of [**PY02**] and Theorem 6 of [**PY04**] together imply that $\overline{\Phi}_{\mathcal{Z}}$ asymptotically randomizes ζ. Now apply Proposition 30(d). □

4.5. *Sufficient conditions for the FLP.* Let $\mathfrak{V} \subseteq \mathcal{G}^{\mathbb{L}}$ be a subgroup shift. An *endomorphic cellular automaton* (ECA) is a CA $\Phi : \mathfrak{V} \longrightarrow \mathfrak{V}$ that is also an endomorphism of $\mathfrak{V}$ as a topological group. For example, all LCA are ECA, but not *vice versa*. It is not hard to show the following.

LEMMA 31. *Let $\Phi : \mathfrak{V} \longrightarrow \mathfrak{V}$ be a CA. Then Φ is an ECA if and only if Φ is an $\mathcal{R}\mathbb{L}$-endomorphism of $\mathfrak{V}$ as an $\mathcal{R}\mathbb{L}$-module.*

Let $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{M}}$ be a nearest-neighbor subgroup shift. Then $\mathfrak{G}$ is a Markov $\mathcal{R}\mathbb{L}$-submodule of $\mathfrak{U}^{\mathbb{N}}$ by Proposition 23. Let $\mathfrak{Z}$ and $\mathcal{Q}$ be as in Proposition 23, with morphisms $F : \mathfrak{U} \longrightarrow \mathcal{Q}$ and $\pi : \mathfrak{U} \longrightarrow \mathcal{Q}$. Write elements of $\mathfrak{G}$ as $\mathbf{g} = (\mathbf{g}_n : n \in \mathbb{N}) \in \mathfrak{U}^{\mathbb{N}}$.

PROPOSITION 32. *The subgroup shift $\mathfrak{G}$ has the FLP if and only if there exists an ECA $L : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathfrak{U}_{\mathfrak{G}}$ such that $\mathfrak{G} = \{(\mathbf{g}_n : n \in \mathbb{N}) \in \mathfrak{U}^{\mathbb{N}}_{\mathfrak{G}} : \mathbf{g}_{n+1} - L(\mathbf{g}_n) \in \mathfrak{Z}, \forall n \in \mathbb{N}\}$.*

Proof. '$\Longrightarrow$' Suppose that $\mathfrak{G}$ satisfies the FLP. Let $L : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathfrak{U}_{\mathfrak{G}}$ be as in diagram (13). Then $L : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathfrak{U}_{\mathfrak{G}}$ is an $\mathcal{R}\mathbb{L}$-morphism, so Lemma 31 says that L is an ECA.

If $\mathbf{g}, \mathbf{f} \in \mathfrak{U}_{\mathfrak{G}}$ then $\pi(\mathbf{g} - L(\mathbf{f})) = \pi(\mathbf{g}) - \pi(L(\mathbf{f})) = \pi(\mathbf{g}) - F(\mathbf{f})$. Thus, the following are equivalent: (i) $(\mathbf{g} - L(\mathbf{f})) \in \mathfrak{Z}$; (ii) $\pi(\mathbf{g} - L(\mathbf{f})) = 0$; and (iii) $\pi(\mathbf{g}) = F(\mathbf{f})$.

Hence,

$$\begin{aligned}\mathfrak{G} &= \{(\mathbf{g}_n : n \in \mathbb{N}) \in \mathfrak{U}^{\mathbb{N}}_{\mathfrak{G}} : \pi(\mathbf{g}_{n+1}) = F(\mathbf{g}_n), \forall n \in \mathbb{N}\} && \text{(by Proposition 23(e))}\\ &= \{(\mathbf{g}_n : n \in \mathbb{N}) \in \mathfrak{U}^{\mathbb{N}}_{\mathfrak{G}} : (\mathbf{g}_{n+1} - L(\mathbf{g}_n)) \in \mathfrak{Z}, \forall n \in \mathbb{N}\} && \text{as desired.}\end{aligned}$$

'$\Longleftarrow$' Suppose that $\mathfrak{G} = \{(\mathbf{g}_n : n \in \mathbb{N}) \in \mathfrak{U}^{\mathbb{N}}_{\mathfrak{G}} : \mathbf{g}_{n+1} - L(\mathbf{g}_n) \in \mathfrak{Z}, \forall n \in \mathbb{N}\}$ with $L : \mathfrak{U}_{\mathfrak{G}} \longrightarrow \mathfrak{U}_{\mathfrak{G}}$ an ECA. Clearly, $\mathcal{F}_{\mathfrak{G}}(0) = \mathfrak{Z}$ and for any $\mathbf{b} \in \mathfrak{U}_{\mathfrak{G}}$, $\mathcal{F}_{\mathfrak{G}}(\mathbf{b}) = L(\mathbf{b}) + \mathfrak{Z}$.

It follows that $\pi \circ L = F$, in accord with diagram (13). □

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

Example 33. In Example (25b) $D = 1$, so $\mathbb{L} = \mathbb{N}$ and $\mathbb{M} = \mathbb{N}^2$. Also, $\mathcal{G} = \mathbb{Z}_{/27}$, and $\mathfrak{U}_{\mathfrak{G}} = \mathfrak{U} = \mathcal{G}^{\mathbb{N}}$, and $\mathfrak{Z} = \mathcal{Z}^{\mathbb{N}}$, where $\mathcal{Z} = \{0, 9, 18\}$. Finally, $\llcorner : \mathcal{G}^{\mathbb{N}} \longrightarrow \mathcal{G}^{\mathbb{N}}$ is the LCA $\llcorner(\mathbf{g}) = -\mathbf{g} - \boldsymbol{\sigma}_{\mathbb{L}}(\mathbf{g})$.

4.6. *Natural extension to* $\mathbb{Z}^D$. Let $\mathbf{pr}_{\mathbb{N}} : \mathcal{G}^{\mathbb{Z}^D} \longrightarrow \mathcal{G}^{\mathbb{N}^D}$ be the projection map. Any subshift $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}^D}$ has a *natural extension* to a unique subshift $\overline{\mathfrak{G}} \subseteq \mathcal{G}^{\mathbb{Z}^D}$ such that $\mathfrak{G} = \mathbf{pr}_{\mathbb{N}}(\overline{\mathfrak{G}})$. If $\alpha \in \mathbb{GL}(\mathbb{Z}^D)$ is a linear transformation, then α induces a continuous group automorphism $\alpha_* : \mathcal{G}^{\mathbb{Z}^D} \longrightarrow \mathcal{G}^{\mathbb{Z}^D}$ such that, if $\mathbf{g} = (g_z : z \in \mathbb{Z}^D) \in \mathcal{G}^{\mathbb{Z}^D}$, then $\alpha_*(\mathbf{g}) = (g'_z : z \in \mathbb{Z}^D)$ where $g'_z = g_{\alpha(z)}$ for all $z \in \mathbb{Z}^D$. If $\overline{\mathfrak{G}}, \overline{\mathfrak{H}} \subseteq \mathcal{G}^{\mathbb{Z}^D}$ are two subshifts of $\mathcal{G}^{\mathbb{Z}^D}$, we say that $\overline{\mathfrak{G}}$ is α-*equivalent* to $\overline{\mathfrak{H}}$ if $\alpha_*(\overline{\mathfrak{G}}) = \overline{\mathfrak{H}}$. If $\mathfrak{G}, \mathfrak{H} \subseteq \mathcal{G}^{\mathbb{N}^D}$ are two subshifts of $\mathcal{G}^{\mathbb{N}^D}$, with natural extensions $\overline{\mathfrak{G}}$ and $\overline{\mathfrak{H}}$, respectively, then we say $\mathfrak{G}$ is α-*equivalent* to $\mathfrak{H}$ if $\overline{\mathfrak{G}}$ and $\overline{\mathfrak{H}}$ are α-equivalent.

Any shift invariant measure $\mu \in \mathcal{M}(\mathcal{G}^{\mathbb{N}^D})$ extends to a unique shift invariant measure $\overline{\mu} \in \mathcal{M}(\mathcal{G}^{\mathbb{Z}^D})$ such that $\mathbf{pr}_{\mathbb{N}}(\overline{\mu}) = \mu$, and any cellular automaton $\Phi : \mathcal{G}^{\mathbb{N}^D} \longrightarrow \mathcal{G}^{\mathbb{N}^D}$ extends to a unique CA $\overline{\Phi} : \mathcal{G}^{\mathbb{Z}^D} \longrightarrow \mathcal{G}^{\mathbb{Z}^D}$ such that $\mathbf{pr}_{\mathbb{N}} \circ \overline{\Phi} = \Phi \circ \mathbf{pr}_{\mathbb{N}}$. We say the triple $(\overline{\mathfrak{G}}, \overline{\mu}, \overline{\Phi})$ is the *natural extension* of $(\mathfrak{G}, \mu, \Phi)$.

If $\alpha \in \mathbb{GL}(\mathbb{Z}^D)$ and $z \in \mathbb{Z}$, then $\boldsymbol{\sigma}^z \circ \alpha_* = \alpha_* \circ \boldsymbol{\sigma}^{\alpha(z)}$. Thus, if $\overline{\Phi} : \mathcal{G}^{\mathbb{Z}^D} \longrightarrow \mathcal{G}^{\mathbb{Z}^D}$ is a (linear) CA, and we define $\overline{\Psi} = \alpha_* \circ \overline{\Phi} \circ \alpha_*^{-1}$, then $\overline{\Psi}$ is also a (linear) CA, and $\alpha_* \circ \overline{\Phi} = \overline{\Psi} \circ \alpha_*$. If $\overline{\mathfrak{G}}, \overline{\mathfrak{H}} \subseteq \mathcal{G}^{\mathbb{Z}^D}$ are subshifts, and $\overline{\mu} \in \mathcal{M}(\overline{\mathfrak{G}})$ and $\overline{\nu} \in \mathcal{M}(\overline{\mathfrak{H}})$ are shift invariant measures, $\overline{\Phi}, \overline{\Psi} : \mathcal{G}^{\mathbb{Z}^D} \longrightarrow \mathcal{G}^{\mathbb{Z}^D}$ are CA, then $(\overline{\mathfrak{G}}, \overline{\mu}, \overline{\Phi})$ is α-*equivalent* to $(\overline{\mathfrak{H}}, \overline{\nu}, \overline{\Psi})$ if $\alpha_*(\overline{\mathfrak{G}}) = \overline{\mathfrak{H}}$, $\alpha_*(\overline{\mu}) = \overline{\nu}$ and $\overline{\Psi} = \alpha_* \circ \overline{\Phi} \circ \alpha_*^{-1} \circ \boldsymbol{\sigma}^z$ for some $z \in \mathbb{Z}^D$.

If $\mathfrak{G}, \mathfrak{H} \subseteq \mathcal{G}^{\mathbb{N}^D}$ are two subshifts of $\mathcal{G}^{\mathbb{N}^D}$ and $\mu, \nu \in \mathcal{M}(\mathcal{G}^{\mathbb{N}^D})$ are two shift invariant measures, and $\Phi, \Psi : \mathcal{G}^{\mathbb{N}^D} \longrightarrow \mathcal{G}^{\mathbb{N}^D}$ are two CA, then we say that the triple $(\mathfrak{G}, \mu, \Phi)$ is *affine equivalent* to $(\mathfrak{H}, \nu, \Psi)$ if $(\mathfrak{G}, \mu, \Phi)$ has natural extension $(\overline{\mathfrak{G}}, \overline{\mu}, \overline{\Phi})$ and $(\mathfrak{H}, \nu, \Psi)$ has natural extension $(\overline{\mathfrak{H}}, \overline{\nu}, \overline{\Psi})$, and $(\overline{\mathfrak{G}}, \overline{\mu}, \overline{\Phi})$ is α-equivalent to $(\overline{\mathfrak{H}}, \overline{\nu}, \overline{\Psi})$, for some $\alpha \in \mathbb{GL}(\mathbb{Z}^D)$.

LEMMA 34. *Suppose* $(\mathfrak{G}, \mu, \Phi)$ *is affine equivalent to* $(\mathfrak{H}, \nu, \Psi)$. *Then* Φ *asymptotically randomizes* μ *on* $\mathfrak{G}$ *if and only if* Ψ *asymptotically randomizes* ν *on* $\mathfrak{H}$.

Proof. Let $(\overline{\mathfrak{G}}, \overline{\mu}, \overline{\Phi})$ and $(\overline{\mathfrak{H}}, \overline{\nu}, \overline{\Psi})$ be the natural extensions as above. Let $\widehat{\Phi} = \alpha_* \circ \overline{\Phi} \circ \alpha_*^{-1}$ and suppose $\overline{\Psi} = \widehat{\Phi} \circ \boldsymbol{\sigma}^z$ for some $z \in \mathbb{Z}^D$. However, μ and ν are shift invariant, and $\widehat{\Phi}^n(\overline{\nu}) = \alpha_* \circ \overline{\Phi}^n \circ \alpha_*^{-1} \circ \alpha_*(\overline{\mu}) = \alpha_* \circ \overline{\Phi}^n(\overline{\mu})$. Thus, the following are equivalent: (i) Φ randomizes μ on $\mathfrak{G}$; (ii) $\overline{\Phi}$ randomizes $\overline{\mu}$ on $\overline{\mathfrak{G}}$; (iii) $\widehat{\Phi}$ randomizes $\overline{\nu}$ on $\overline{\mathfrak{H}}$; (iv) $\overline{\Psi}$ randomizes $\overline{\nu}$ on $\overline{\mathfrak{H}}$; (v) Ψ randomizes ν on $\mathfrak{H}$. □

PROPOSITION 35. *Suppose that* $\mathfrak{G} \subseteq \mathcal{G}^{\mathbb{N}^D}$ *is a subgroup shift which is affine-equivalent to a subgroup shift* $\mathfrak{H} \subseteq \mathcal{G}^{\mathbb{N}^D}$ *having the strong FLP. If* μ *is a Markov random field with full support on* $\mathfrak{G}$, *then any PLCA acting on* $\mathfrak{G}$ *asymptotically randomizes* μ *to a measure of maximal entropy on* $\mathfrak{G}$.

Proof. Suppose $\alpha \in \mathbb{GL}(\mathbb{Z}^D)$ defines an affine equivalence of $\mathfrak{G}$ and $\mathfrak{H}$. If $\mu \in \mathcal{M}(\mathcal{G}^{\mathbb{N}^D})$, let $\overline{\mu} \in \mathcal{M}(\mathcal{G}^{\mathbb{Z}^D})$ be its extension, $\overline{\nu} = \alpha_*(\overline{\mu})$ and $\nu = \mathbf{pr}_{\mathbb{N}}(\overline{\mu})$. If μ is an MRF with full support on $\mathfrak{G}$, then ν is an MRF with full support on $\mathfrak{H}$.

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

Let $\Phi : \mathcal{G}^{\mathbb{N}^D} \longrightarrow \mathcal{G}^{\mathbb{N}^D}$ be a PLCA as in (1), and let $\overline{\Phi} : \mathcal{G}^{\mathbb{Z}^D} \longrightarrow \mathcal{G}^{\mathbb{Z}^D}$ be its natural extension. Put $\widehat{\Phi} = \alpha_* \circ \overline{\Phi} \circ \alpha_*^{-1}$. Then $\widehat{\Phi} = \sum_{i \in \widehat{\mathbb{I}}} \widehat{\varphi}_i \cdot \boldsymbol{\sigma}^i$, where $\widehat{\mathbb{I}} = \alpha^{-1}(\mathbb{I})$ and for each $i \in \widehat{\mathbb{I}}$, $\widehat{\varphi}_i = \varphi_{\alpha(i)}$.

We want to project $\widehat{\Phi}$ to an LCA on $\mathcal{G}^{\mathbb{N}^D}$, but $\widehat{\mathbb{I}} \not\subseteq \mathbb{N}^D$, because some of the elements of $\widehat{\mathbb{I}}$ may have negative coordinates. Let $\mathbf{z} = (z_1, \ldots, z_D)$, where for each $d \in [1, D]$, $z_d = -\min\{i_d : i = (i_1, \ldots, i_D) \in \widehat{\mathbb{I}}\}$. Now let $\overline{\Psi} = \widehat{\Phi} \circ \boldsymbol{\sigma}^{\mathbf{z}} = \sum_{j \in \mathbb{J}} \psi_j \cdot \boldsymbol{\sigma}^j$, where $\mathbb{J} = \widehat{\mathbb{I}} + \mathbf{z} \subseteq \mathbb{N}^D$, and where for each $j \in \mathbb{J}$, $\psi_j = \widehat{\varphi}_{j-\mathbf{z}}$. Then $\overline{\Psi}$ projects to an LCA $\Psi : \mathcal{G}^{\mathbb{N}^D} \longrightarrow \mathcal{G}^{\mathbb{N}^D}$ and $(\mathfrak{G}, \mu, \Phi)$ is affine equivalent to $(\mathfrak{H}, \nu, \Psi)$. Theorem 4 says that Ψ asymptotically randomizes ν; hence Lemma 34 implies that Φ also randomizes μ. □

Example 36. If $\mathfrak{G}$ is from Example 25(c), then $\overline{\mathfrak{G}} = \{\mathbf{g} \in \mathcal{G}^{\mathbb{Z}^2}; \sum_{k \in \mathbb{K}} g_{z+k} = 0 \bmod 2, \forall z \in \mathbb{Z}^2\}$. Now, define $\alpha : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$ by $\alpha(x, y) = (x, -y)$. Then $\alpha(\mathbb{K}) = \mathbb{J}$, where $\mathbb{J}$ is as in Example (25b). Thus, $\alpha_*(\overline{\mathfrak{G}}) = \{\mathbf{h} \in \mathcal{G}^{\mathbb{Z}^2}; \sum_{j \in \mathbb{J}} \mathbf{h}_{z+j} = 0, \forall z \in \mathbb{Z}^2\} =: \overline{\mathfrak{H}}$. Finally, let $\mathfrak{H} = \mathbf{pr}_{\mathbb{N}}(\overline{\mathfrak{H}}) = \{\mathbf{h} \in \mathcal{G}^{\mathbb{N}^2} : \sum_{j \in \mathbb{J}} \mathbf{h}_{n+j} = 0, \forall n \in \mathbb{N}^2\}$. Then $\mathfrak{G}$ is α-equivalent to $\mathfrak{H}$.

$\mathfrak{G}$ does not have the FLP, but $\mathfrak{G}$ is affine equivalent to $\mathfrak{H}$, and $\mathfrak{H}$ satisfies the conditions of Proposition 32 (similarly to Example 33). Thus, $\mathfrak{H}$ has the FLP. Hence, Proposition 35 says that any PLCA asymptotically randomizes any MRF with full support on $\mathfrak{G}$ to a measure of maximal entropy on $\mathfrak{G}$.

Acknowledgements. A.M. and S.M. were supported by Nucleus Millennium P01-005 and P04-069-F. M.P. and R.Y. were supported by NSERC Canada.

References

[Ber69] K. R. Berg. Convolution of invariant measures, maximal entropy. *Math. Sys. Th.* **3**, (1969), 146–150.

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

[FMMN00] P. A. Ferrari, A. Maass, S. Martínez, and P. Ney. Cesàro mean distribution of group automata starting from measures with summable decay. *Ergod. Th. & Dynam. Sys.* **20**(6) (2000), 1657–1670.

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

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

[Lin84] D. Lind. Applications of ergodic theory and sofic systems to cellular automata. *Physica* D **10** (1984), 36–44.

[MHM03] A. Maass, B. Host and S. Martínez. Uniform Bernoulli measure in dynamics of permutative cellular automata with algebraic local rules. *Discrete Continuous Dyn. Sys.* **9**(6) (2003), 1423–1446.

[MM98] A. Maass and S. Martínez. On Cesàro limit distribution of a class of permutative cellular automata. *J. Stat. Phys.* **90**(1–2) (1998), 435–452.

[Piv03] M. Pivato. Multiplicative cellular automata on nilpotent groups: structure, entropy, and asymptotics. *J. Stat. Phys.* **110**(1–2) (2003), 247–267.

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

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press

[PY02] M. Pivato and R. Yassawi. Limit measures for affine cellular automata. *Ergod. Th. & Dynam. Sys.* **22**(4) (2002), 1269–1287.

[PY04] M. Pivato and R. Yassawi. Limit measures for affine cellular automata. II. *Ergod. Th. & Dynam. Sys.* **24**(6) (2004), 1961–1980.

[PY06] M. Pivato and R. Yassawi. Asymptotic randomization of sofic shifts by linear cellular automata. *Ergod. Th. & Dynam. Sys.* **26** (2006), to appear.

[Sch95] K. Schmidt. *Dynamical Systems of Algebraic Origin (Progress in Mathematics, 128)*. Birkhäuser, Boston, MA, 1995.

[Wil70] S. Willard. *General Topology*. Addison-Wesley, Don Mills, ON, 1970.

https://doi.org/10.1017/S0143385706000216 Published online by Cambridge University Press