Ergod. Th. & Dynam. Sys. (2004), **24**, 1961–1980
DOI: 10.1017/S0143385704000288
© *2004 Cambridge University Press*
Printed in the United Kingdom

Limit measures for affine cellular automata II

MARCUS PIVATO and REEM YASSAWI

Department of Mathematics, Trent University, Peter Gzowski College, Peterborough, Ontario, K9L 1Z6 Canada
(e-mail: pivato@xaravve.trentu.ca, ryassawi@trentu.ca)

(*Received* 28 *April* 2003 *and accepted in revised form* 4 *March* 2004)

Abstract. If $\mathbb{M}$ is a monoid and $\mathcal{A}$ is an Abelian group, then $\mathcal{A}^{\mathbb{M}}$ is a compact Abelian group; a *linear cellular automaton* (LCA) is a continuous endomorphism $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ that commutes with all shift maps. If $\mathfrak{F}$ is *diffusive*, and μ is a *harmonically mixing* (HM) probability measure on $\mathcal{A}^{\mathbb{M}}$, then the sequence $\{\mathfrak{F}^N\mu\}_{N=1}^{\infty}$ weak* converges to the Haar measure on $\mathcal{A}^{\mathbb{M}}$ in density. Fully supported Markov measures on $\mathcal{A}^{\mathbb{Z}}$ are HM and non-trivial LCA on $\mathcal{A}^{(\mathbb{Z}^D)}$ are diffusive when $\mathcal{A} = \mathbb{Z}_{/p}$ is a prime cyclic group.

In the present work, we provide sufficient conditions for diffusion of LCA on $\mathcal{A}^{(\mathbb{Z}^D)}$ when $\mathcal{A} = \mathbb{Z}_{/n}$ is any cyclic group or when $\mathcal{A} = (\mathbb{Z}_{/p^r})^J$ (p prime). We also show that any fully supported Markov random field on $\mathcal{A}^{(\mathbb{Z}^D)}$ is HM (where $\mathcal{A}$ is any Abelian group).

1. *Introduction*

Let $\mathcal{A}$ be a finite Abelian group, with the discrete topology. If $\mathbb{M}$ is any set, then $\mathcal{A}^{\mathbb{M}}$ is a compact Abelian group when endowed with the Tychonoff product topology and componentwise addition. If $(\mathbb{M}, +)$ is an Abelian monoid (for example, a lattice: $\mathbb{Z}^D \times \mathbb{N}^E$), then the action of $\mathbb{M}$ on itself by translation induces a natural *shift action* of $\mathbb{M}$ on the configuration space: for all $\mathsf{e} \in \mathbb{M}$ and $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, define $\boldsymbol{\sigma}^{\mathsf{e}}[\mathbf{a}] = [b_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}]$ where for all $\mathsf{m} \in \mathbb{M}$, $b_{\mathsf{m}} = a_{\mathsf{e}+\mathsf{m}}$.

A *linear cellular automaton* (LCA) is a continuous endomorphism $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \hookleftarrow$ which commutes with all shift maps. If μ is a measure on $\mathcal{A}^{\mathbb{M}}$, it is natural to consider the sequence of measures $\{\mathfrak{F}^n\mu|_{n\in\mathbb{N}}\}$ and ask whether this sequence converges in the weak* topology on the space $\mathcal{M}[\mathcal{A}^{\mathbb{M}}]$ of Borel probability measures on $\mathcal{A}^{\mathbb{M}}$. If $\{\mathfrak{F}^n\mu|_{n\in\mathbb{N}}\}$ does not itself converge, we might hope at least for convergence in density (i.e. convergence of a subsequence $\{\mathfrak{F}^j\mu|_{j\in\mathbb{J}}\}$, where $\mathbb{J} \subset \mathbb{N}$ is a subset of Cesàro density 1) or convergence of the Cesàro average $(1/N)\sum_{n=1}^{N}\mathfrak{F}^n\mu$.

Let η denote the Haar measure on $\mathcal{A}^{\mathbb{M}}$. Since η is invariant under the algebraic operations of $\mathcal{A}^{\mathbb{M}}$, it seems like a natural limit point for $\{\mathfrak{F}^n\mu|_{n\in\mathbb{N}}\}$. Indeed, Lind has

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

shown [**5**] that, if $\mathcal{A} = \mathbb{Z}_{/2}$, $\mathfrak{F}$ is the automaton defined by $\mathfrak{F}(\mathbf{a})_0 = a_{(-1)} + a_1$ and μ is any Bernoulli measure, then

$$\mathbf{wk}^* - \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathfrak{F}^n \mu = \eta.$$

Lind also showed that $\{\mathfrak{F}^n \mu|_{n\in\mathbb{N}}\}$ does *not* converge to η: convergence fails along the subsequence $\{\mathfrak{F}^{(2^n)} \mu|_{n\in\mathbb{N}}\}$.

Later, Ferrari, Maass, Martinez and Ney showed similar Cesàro convergence results in a variety of special cases [**7, 1**]. Recently, Pivato and Yassawi [**6**] have developed broad sufficient conditions for convergence. The concepts of *harmonic mixing* for measures and *diffusion* for LCA were introduced: if μ is a harmonically mixing probability measure and $\mathfrak{F}$ a diffusive LCA, then $\{\mathfrak{F}^n \mu|_{n\in\mathbb{N}}\}$ weak* converges to η in density and, thus, also in the Cesàro mean.

This paper is a continuation of [**6**]. First we will extend the results on the diffusion of LCA to a broader class of Abelian groups: in §3, to the case when $\mathcal{A} = \mathbb{Z}_{/n}$, for any $n \in \mathbb{N}$, and then in §4, to the case when $\mathcal{A} = (\mathbb{Z}_{/p^r})^J$ (p prime, $J, r \in \mathbb{N}$). Next, in §5, we demonstrate harmonic mixing for any Markov random field on $\mathcal{A}^{(\mathbb{Z}^D)}$ with full support.

2. *Preliminaries*

We recommend that the reader consult [**6**] before reading the present work as we will depend heavily upon results introduced there. We will now briefly review the relevant concepts: all theorems in this section are proved in [**6**].

2.1. *Characters and harmonic mixing.*

Let $\mathbb{T}^1$ be the unit circle group. A *character* of $\mathcal{A}^{\mathbb{M}}$ is a continuous group homomorphism $\phi : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathbb{T}^1$. The set of all characters of $\mathcal{A}^{\mathbb{M}}$ forms a group, denoted $\widehat{\mathcal{A}^{\mathbb{M}}}$.

If $[\chi_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}]$ is a sequence of characters of $\mathcal{A}$, with all but finitely many elements equal to the constant 1-function (denoted '$\mathbb{1}$'), then define $\boldsymbol{\chi} := \bigotimes_{\mathsf{m}\in\mathbb{M}} \chi_{\mathsf{m}} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathbb{T}^1$; thus, if $\mathbf{a} = [a_{\mathsf{m}}|_{\mathsf{m}} \in \mathbb{M}]$ is an element of $\mathcal{A}^{\mathbb{M}}$, then $\boldsymbol{\chi}(\mathbf{a}) = \prod_{\mathsf{m}\in\mathbb{M}} \chi_{\mathsf{m}}(a_{\mathsf{m}})$. All elements of $\widehat{\mathcal{A}^{\mathbb{M}}}$ arise in this manner. The *rank* of the character $\boldsymbol{\chi}$ is the number of non-trivial entries in the *coefficient system* $[\chi_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}]$.

When $\mathcal{A} = \mathbb{Z}_{/n}$, elements of $\widehat{\mathcal{A}}$ are maps of the form $\chi(a) = \exp((2\pi\mathbf{i}/n)c \cdot a)$, where $c \in \mathbb{Z}_{/n}$ is some constant. Elements of $\widehat{\mathcal{A}^{\mathbb{M}}}$ are then products of the form $\boldsymbol{\chi}(\mathbf{a}) = \prod_{\mathsf{m}\in\mathbb{M}} \chi_{\mathsf{m}}(a_{\mathsf{m}})$, where, for all $\mathsf{m} \in \mathbb{M}$,

$$\chi_{\mathsf{m}} : a \mapsto \exp\left(\frac{2\pi\mathbf{i}}{n} c_{\mathsf{m}} \cdot a\right) \quad \text{for some } c_{\mathsf{m}} \in \mathcal{A},$$

with all but finitely many c_{m} are equal to 0. In this case, we will also use the term *coefficient system* to describe the sequence $[c_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}]$.

If μ is a measure on $\mathcal{A}^{\mathbb{M}}$, then the *Fourier coefficients* of μ are defined: $\widehat{\mu}[\boldsymbol{\chi}] = \langle \boldsymbol{\chi}, \mu \rangle = \int_{\mathcal{A}^{\mathbb{M}}} \boldsymbol{\chi}\, d\mu$, for every $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$. The measure μ is called *harmonically mixing* if, for all $\epsilon > 0$, there is some $R > 0$ so that, for all $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$, $(\mathsf{rank}[\boldsymbol{\chi}] \geq R) \Longrightarrow (|\widehat{\mu}[\boldsymbol{\chi}]| < \epsilon)$.

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

Let $\mathcal{M}[\mathcal{A}^{\mathbb{M}}; \mathbb{C}]$ be the space of complex-valued Borel measures on $\mathcal{A}^{\mathbb{M}}$, treated as a Banach algebra under the total variation norm, with operations of addition and convolution. Let $\mathcal{HM} \subset \mathcal{M}[\mathcal{A}^{\mathbb{M}}; \mathbb{C}]$ be the set of harmonically mixing measures.

PROPOSITION 1. [**6**, Propositions 4–10] *Let $\mathcal{A}$ be any finite Abelian group.*

(1) *$\mathcal{HM}$ is an ideal of $\mathcal{M}[\mathcal{A}^{\mathbb{M}}; \mathbb{C}]$.*
(2) *$\mathcal{HM}$ is closed under the total variation norm and dense in the weak* topology.*
(3) *$\mathcal{HM}$ contains all Bernoulli measures $\beta^{\otimes\mathbb{M}}$, where β is a measure on $\mathcal{A}$ such that, for any subgroup $\mathcal{G} \subset \mathcal{A}$, the support of μ extends over more than one coset of $\mathcal{G}$.*
(4) *If $\mathbb{M} = \mathbb{Z}$, then, for any $N > 0$, $\mathcal{HM}$ contains all N-step Markov measures on $\mathcal{A}^{\mathbb{Z}}$ giving non-zero probability to all elements of $\mathcal{A}^{[0..N]}$.*
(5) *$\mathcal{HM}$ contains any measure absolutely continuous with respect to the aforementioned Bernoulli or Markov measures.*

2.2. *Linear cellular automata.* A *cellular automaton* (CA) is a continuous map $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ that commutes with all shift maps. The Curtis–Hedlund–Lyndon theorem [**4**] states that any CA is determined by a *local map* $\mathfrak{f} : \mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$, where $\mathbb{U} \subset \mathbb{M}$ is some finite subset (a 'neighbourhood of the identity'). $\mathfrak{F}$ is a linear cellular automaton (LCA) if and only if $\mathfrak{f}$ is a homomorphism from the product group $\mathcal{A}^{\mathbb{U}}$ into $\mathcal{A}$.

The set $\mathbf{End}(\mathcal{A})$ of group endomorphisms from $\mathcal{A}$ to itself is a ring under composition and pointwise addition: if $\mathfrak{f}, \mathfrak{g}$ are in $\mathbf{End}(\mathcal{A})$, then so are $\mathfrak{f} \circ \mathfrak{g}$ and $\mathfrak{f} + \mathfrak{g}$. If $\mathbf{Hom}(\mathcal{A}^{\mathbb{U}}; \mathcal{A})$ is the set of group homomorphisms from $\mathcal{A}^{\mathbb{U}}$ into $\mathcal{A}$, then there is a natural bijection between $(\mathbf{End}(\mathcal{A}))^{\mathbb{U}}$ and $\mathbf{Hom}(\mathcal{A}^{\mathbb{U}}; \mathcal{A})$, as follows: For each $\mathsf{u} \in \mathbb{U}$, suppose that $\mathfrak{f}_{\mathsf{u}} \in \mathbf{End}(\mathcal{A})$. Define $\mathfrak{f} : \mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$ by $\mathfrak{f}[a_{\mathsf{u}}|_{\mathsf{u}\in\mathbb{U}}] = \sum_{\mathsf{u}\in\mathbb{U}} \mathfrak{f}_{\mathsf{u}}(a_{\mathsf{u}})$. Then $\mathfrak{f}$ is a group homomorphism and every element of $\mathbf{Hom}(\mathcal{A}^{\mathbb{U}}; \mathcal{A})$ arises in this manner.

Thus, if $\mathfrak{F}$ is an LCA, then there is some set of *coefficients* $\{\mathfrak{f}_{\mathsf{u}}; \mathsf{u} \in \mathbb{U}\}$ so that, for any $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, $\mathfrak{F}(\mathbf{a}) = \mathbf{b}$, where, for all $\mathsf{m} \in \mathbb{M}$,

$$b_{\mathsf{m}} = \sum_{\mathsf{u}\in\mathbb{U}} \mathfrak{f}_{\mathsf{u}}(a_{(\mathsf{m}+\mathsf{u})}) = \sum_{\mathsf{u}\in\mathbb{U}} \mathfrak{f}_{\mathsf{u}}(\boldsymbol{\sigma}^{\mathsf{u}}(\mathbf{a})_{\mathsf{m}}).$$

For any $\mathsf{u} \in \mathbb{U}$, treat $\mathfrak{f}_{\mathsf{u}}$ as an endomorphism on $\mathcal{A}^{\mathbb{M}}$ by letting it act componentwise on elements of $\mathcal{A}^{\mathbb{M}}$. Then, for all $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, $\mathfrak{F}(\mathbf{a}) = \sum_{\mathsf{u}\in\mathbb{U}} \mathfrak{f}_{\mathsf{u}} \circ \boldsymbol{\sigma}^{\mathsf{u}}(\mathbf{a})$. Thus, $\mathfrak{F}$ can be written as a formal 'polynomial of shift maps':

$$\mathfrak{F} = \sum_{\mathsf{u}\in\mathbb{U}} \mathfrak{f}_{\mathsf{u}} \circ \boldsymbol{\sigma}^{\mathsf{u}}.$$

If $\mathcal{A} = \mathbb{Z}_{/n}$ ($n \in \mathbb{N}$), then the elements of $\mathbf{End}(\mathcal{A})$ are all maps of the form $\mathfrak{f}([a]_n) = [f \cdot a]_n$, where '$[\bullet]_n$' refers to a mod-$n$ congruence class, and $f \in \mathbb{Z}_{/n}$ is a constant, with multiplication via the natural ring structure on $\mathbb{Z}_{/n}$. In this case, we can write $\mathfrak{F} = \sum_{\mathsf{u}\in\mathbb{U}} f_{\mathsf{u}} \cdot \boldsymbol{\sigma}^{\mathsf{u}}$, a polynomial with coefficients in $\mathbb{Z}_{/n}$. For example, if $\mathbb{M} = \mathbb{Z}$ and $\mathfrak{F} = \boldsymbol{\sigma}^{-1} + 3 \circ \boldsymbol{\sigma}^{1} + 5\boldsymbol{\sigma}^{2}$, then this means that $\mathfrak{F}(\mathbf{a})_k = [a_{(k-1)} + 3 \cdot a_{(k+1)} + 5 \cdot a_{(k+2)}]_n$.

2.3. *Diffusion.* If $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \hookleftarrow$ is an LCA and $\boldsymbol{\chi}$ is a character of $\widehat{\mathcal{A}^{\mathbb{M}}}$, then $\boldsymbol{\chi} \circ \mathfrak{F}$ is also a character. $\mathfrak{F}$ is called *diffusive*† if, for every non-trivial $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$, there is some

† In [**6**], this was called *diffusion in density*. Since diffusion in density is the only kind we will encounter in this paper, we have opted for more concise terminology.

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

subset $\mathbb{J}_\chi \subset \mathbb{N}$ of density 1 so that

$$\lim_{\substack{j\to\infty \\ j\in\mathbb{J}_\chi}} \mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{F}^j] = \infty.$$

We will abbreviate this to

$$\text{`}\mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{F}^N] \xrightarrow[N\to\infty]{\text{dense}} \infty\text{'}.$$

THEOREM 2. [**6**, Theorem 15] *Let p be a prime number, and $\mathcal{A} = \mathbb{Z}_{/p}$. Let $D \geq 1$. Then any non-trivial LCA on $\mathcal{A}^{(\mathbb{Z}^D)}$ is diffusive.*

(Here, by *non-trivial* we mean that $\mathfrak{F}$, as a polynomial of shift maps, has more than one non-trivial coefficient.) The significance of diffusion and harmonic mixing is given in the following theorem.

THEOREM 3. [**6**, Theorem 12] *Let $\mathcal{A}$ be a finite Abelian group, and $\mathbb{M}$ a countable monoid. Suppose that $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \hookleftarrow$ is an LCA and that μ is a harmonically mixing measure on $\mathcal{A}^{\mathbb{M}}$.*

If $\mathfrak{F}$ is diffusive, then there is a set $\mathbb{J} \subset \mathbb{N}$ of Cesàro density 1 so that

$$\mathbf{wk}^* \lim_{\substack{j\to\infty \\ j\in\mathbb{J}_\chi}} \mathfrak{F}^j \mu = \eta.$$

Thus,

$$\mathbf{wk}^* \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathfrak{F}^n \mu = \eta.$$

For example, $\mathfrak{F}^n\mu$ weak* converges to Haar measure in density whenever μ is one of the aforementioned Bernoulli or N-step Markov measures.

3. *Diffusion on other cyclic groups*

Suppose $n = p_1^{r_1} \dots p_J^{r_J}$, where $p_1, \dots, p_J$ are distinct primes and $r_1, \dots, r_J \in \mathbb{N}$. Let $\mathcal{A} = \mathbb{Z}_{/n}$ and $\mathcal{A}_j = \mathbb{Z}_{/q_j}$, with $q_j = p_j^{r_j}$, for $j \in [1 \dots J]$. Then $\mathcal{A} \cong \bigoplus_{j=1}^J \mathcal{A}_j$ and, thus, $\widehat{\mathcal{A}} \cong \bigoplus_{j=1}^J \widehat{\mathcal{A}_j}$. There is then a canonical identification $\mathcal{A}^{\mathbb{M}} \cong \bigoplus_{j=1}^J \mathcal{A}_j^{\mathbb{M}}$ and, thus, $\widehat{\mathcal{A}^{\mathbb{M}}} \cong \bigoplus_{j=1}^J \widehat{\mathcal{A}_j^{\mathbb{M}}}$. Concretely, if $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$ has coefficient sequence $[c_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}]$, then $\boldsymbol{\chi} \cong \bigoplus_{j=1}^J \boldsymbol{\chi}^{[j]}$, where for each $j \in [1 \dots J]$, $\boldsymbol{\chi}^{[j]} \in \widehat{\mathcal{A}_j^{\mathbb{M}}}$ has coefficient sequence $[c^{[j]}_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}]$, with $c^{[j]}_{\mathsf{m}} = [c_{\mathsf{m}}]_{q_j}$ for all $\mathsf{m} \in \mathbb{M}$ (recall that $[a]_b$ is the congruence class of a, modulo b). Also,

$$\mathbf{End}(\mathcal{A}) \cong \bigoplus_{i,j=1}^{J} \mathbf{Hom}(\mathcal{A}_i, \mathcal{A}_j) \underset{(*)}{=} \bigoplus_{j=1}^{J} \mathbf{End}(\mathcal{A}_j) \cong \bigoplus_{j=1}^{J} \mathbb{Z}_{/q_j}.$$

($(*)$ is because cross-terms are trivial.) Concretely, if $f \in \mathbb{N}$, and $\mathfrak{f} : \mathcal{A} \hookleftarrow$ is the map $[a]_n \mapsto [f \cdot a]_n$, then $\mathfrak{f} = \mathfrak{f}^{[1]} \oplus \dots \oplus \mathfrak{f}^{[J]}$, where, for each j, $\mathfrak{f}^{[j]} : \mathcal{A}_j \hookleftarrow$ is the map

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

$[a]_{q_j} \mapsto [f_j \cdot a]_{q_j}$ and where $f \equiv f_j \pmod{p}$. In particular, if q_j divides f, then $\mathfrak{f}^{[j]}$ is trivial.

Thus, if $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \hookleftarrow$ is the LCA $\sum_{\mathsf{u}\in\mathbb{U}} \mathfrak{f}_{\mathsf{u}} \circ \boldsymbol{\sigma}^{\mathsf{u}}$, with $\mathfrak{f}_{\mathsf{u}} \in \mathbf{End}(\mathcal{A})$, then, for all $\mathsf{u} \in \mathbb{U}$, we can write $\mathfrak{f}_{\mathsf{u}} = \mathfrak{f}_{\mathsf{u}}^{[1]} \oplus \cdots \oplus \mathfrak{f}_{\mathsf{u}}^{[J]}$, with $\mathfrak{f}_{\mathsf{u}}^{[j]} \in \mathbf{End}(\mathcal{A}_j)$ a scalar-multiplication map determined by some $f_{\mathsf{u}}^{[j]} \in \mathbb{Z}_{/q_j}$, and then write $\mathfrak{F} = \bigoplus_{j=1}^{J} \mathfrak{F}^{[j]}$, where, for all $j \in [1 \ldots J]$, $\mathfrak{F}^{[j]} : \mathcal{A}_j^{\mathbb{M}} \hookleftarrow$ is the LCA given by $\sum_{\mathsf{u}\in\mathbb{U}} f_{\mathsf{u}}^{[j]} \circ \boldsymbol{\sigma}^{\mathsf{u}}$. Note also that, if $\boldsymbol{\chi} = \bigoplus_{j=1}^{J} \boldsymbol{\chi}_j \in \widehat{\mathcal{A}^{\mathbb{M}}}$, then

$$\boldsymbol{\chi} \circ \mathfrak{F} = \bigoplus_{j=1}^{J} (\boldsymbol{\chi}_j \circ \mathfrak{F}^{[j]}).$$

LEMMA 4. *If $\mathfrak{F} = \bigoplus_{j=1}^{J} \mathfrak{F}^{[j]}$ is an LCA on $\bigoplus_{j=1}^{J} \mathcal{A}_j^{\mathbb{M}}$, then*

$$(\mathfrak{F} \textit{ is diffusive}) \iff (\forall j \in [1 \ldots J], \mathfrak{F}^{[j]} \textit{ is diffusive}).$$

Proof. Proof of '$\Longleftarrow$': Let $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$ be non-trivial. Thus, $\boldsymbol{\chi} = \boldsymbol{\chi}^{[1]} \oplus \cdots \oplus \boldsymbol{\chi}^{[J]}$, where at least one of $\boldsymbol{\chi}^{[j]} \in \widehat{\mathcal{A}_j^{\mathbb{M}}}$, is non-trivial: suppose it is $\boldsymbol{\chi}^{[j_0]}$. Since $\mathfrak{F}^{[j_0]}$ is diffusive, we conclude that

$$\mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{F}^N] \geq \mathsf{rank}[\boldsymbol{\chi}^{[j_0]} \circ (\mathfrak{F}^{j_0})^N] \xrightarrow[n\to\infty]{\text{dense}} \infty.$$

Proof of '$\Longrightarrow$': Suppose that $\mathfrak{F}_{j_0}$ is not diffusive. Let $\boldsymbol{\chi}_{j_0}$ be some character on $\mathcal{A}_{j_0}^{\mathbb{M}}$ so that $\mathsf{rank}[\boldsymbol{\chi}_{j_0} \circ \mathfrak{F}_{j_0}] \xrightarrow[n\not\to\infty]{\text{dense}} \infty$, and let $\boldsymbol{\chi} = \bigoplus_{j=1}^{J} \chi_j$, where $\chi_j = \mathbb{1}$ for all $j \neq j_0$. Then $\mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{F}] = \mathsf{rank}[\boldsymbol{\chi}_{j_0} \circ \mathfrak{F}_{j_0}] \xrightarrow[n\not\to\infty]{\text{dense}} \infty$, so $\mathfrak{F}$ is not diffusive. □

Hence, we have reduced the proof of diffusion to the prime power case.

Suppose $\mathcal{A} = \mathbb{Z}_{/8}$, and let $\mathfrak{F} = \mathbf{Id} + 2\boldsymbol{\sigma}^1$ act on $\mathcal{A}^{\mathbb{Z}}$. Then $\mathfrak{F}^{4\cdot N} = \mathbf{Id}$ for all $N \in \mathbb{N}$, so $\mathfrak{F}$ cannot be diffusive. This motivates the conditions of the following lemma.

LEMMA 5. *Let $\mathbb{M} = \mathbb{Z}^D$. Let $\mathcal{A} = \mathbb{Z}_{/q}$, where $q = p^r$, p is prime and $r \in \mathbb{N}$. Let $\mathfrak{F} = \sum_{\mathsf{u}\in\mathbb{U}} f_{\mathsf{u}} \circ \boldsymbol{\sigma}^{\mathsf{u}}$.*

If $f_{\mathsf{u}} \in [0 \ldots q)$ are relatively prime to p for at least two $\mathsf{u} \in \mathbb{U}$, then $\mathfrak{F}$ is diffusive.

Proof. Let $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$ have coefficient sequence $[c_{\mathsf{v}}|_{\mathsf{v}\in\mathbb{V}}]$, where $c_{\mathsf{v}} \in \mathbb{Z}_{/q}$, for all $\mathsf{v} \in \mathbb{V}$, with $\mathbb{V} \subset \mathbb{M}$ some finite subset. Thus, $\boldsymbol{\chi}^{[N]} = \boldsymbol{\chi} \circ \mathfrak{F}^N$ has coefficient sequence $[c_{\mathsf{m}}^{[N]}|_{\mathsf{m}\in\mathbb{M}}]$, where, for all $m \in \mathbb{M}$,

$$c_{\mathsf{m}}^{[N]} = \sum_{\mathsf{v}\in\mathbb{V}} \sum_{\substack{\mathsf{u}_1,\ldots,\mathsf{u}_N\in\mathbb{U} \\ \mathsf{v}+\mathsf{u}_1+\cdots+\mathsf{u}_N=\mathsf{m}}} c_{\mathsf{v}} \cdot f_{\mathsf{u}_1} \ldots f_{\mathsf{u}_N}. \tag{1}$$

Thus, $\mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{F}^N]$ is the number of these coefficients that are non-zero, mod q.

Case 1. One of the coefficients $\{c_{\mathsf{v}}|_{\mathsf{v}\in\mathbb{V}}\}$ is non-zero, mod p. Consider the character $\boldsymbol{\chi}_{/p}$ and the (non-trivial) LCA $\mathfrak{F}_{/p}$ on $\mathbb{Z}_{/p}{}^{\mathbb{M}}$ induced by the coefficients $[c_{\mathsf{v}}|_{\mathsf{v}\in\mathbb{V}}]$ and $[f_{\mathsf{u}}|_{\mathsf{u}\in\mathbb{U}}]$ respectively, and, for all $N \in \mathbb{N}$, the character $\boldsymbol{\chi}_{/p}^{[N]}$ induced by $[c_{\mathsf{m}}^{[N]}|_{\mathsf{m}\in\mathbb{M}}]$.

First, note that for all $N \in \mathbb{N}$, $\boldsymbol{\chi}_{/p}^{[N]} = \boldsymbol{\chi}_{/p} \circ \mathfrak{F}_{/p}^N$ (simply consider equation (1), only mod p instead). Note that, for any m and N, if the expression in (1) is non-zero mod p, then it

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

must be non-zero mod q. Thus, $\mathsf{rank}[\boldsymbol{\chi}^{[N]}] \geq \mathsf{rank}[\boldsymbol{\chi}_{/p}^{[N]}] = \mathsf{rank}[\boldsymbol{\chi}_{/p} \circ \mathfrak{F}_{/p}^{N}]$. Hence, it suffices to show that $\mathsf{rank}[\boldsymbol{\chi}_{/p} \circ \mathfrak{F}_{/p}^{N}] \xrightarrow[n\to\infty]{\text{dense}} \infty$.

But one of $\{c_{\mathsf{v}}|_{\mathsf{v}\in\mathbb{V}}\}$ is non-zero, mod p, so $\boldsymbol{\chi}_{/p}$ is non-trivial as a character on $\mathbb{Z}_{/p}{}^{\mathbb{M}}$. Thus, by Theorem 2, $\mathsf{rank}[\boldsymbol{\chi}_{/p} \circ \mathfrak{F}_{/p}^{N}] \xrightarrow[n\to\infty]{\text{dense}} \infty$.

Case 2. All the coefficients $\{c_{\mathsf{v}}|_{\mathsf{v}\in\mathbb{V}}\}$ *are divisible by* p. Let p^s be the greatest power of p that divides all elements of $\{c_{\mathsf{v}}|_{\mathsf{v}\in\mathbb{V}}\}$: clearly $s < r$. Let $\widetilde{r} = r - s$ and $\widetilde{q} = p^{\widetilde{r}}$ and let $\widetilde{\mathcal{A}} = \mathbb{Z}_{/\widetilde{q}}$. We will reduce the problem to consideration of an LCA on $\mathbb{Z}_{/\widetilde{q}}$ and then apply Case 1.

For all $\mathsf{v} \in \mathbb{V}$, let $\widetilde{c}_{\mathsf{v}} = c_{\mathsf{v}}/p^s$ and let $\widetilde{\boldsymbol{\chi}} \in \widehat{\widetilde{\mathcal{A}}^{\mathbb{M}}}$ be the corresponding character. Let $\widetilde{\mathfrak{F}}$ be the LCA on $\widetilde{\mathcal{A}}^{\mathbb{M}}$ having the same coefficients as $\mathfrak{F}$; thus, $\widetilde{\boldsymbol{\chi}}^{[N]} = \widetilde{\boldsymbol{\chi}} \circ \widetilde{\mathfrak{F}}^{N}$ has coefficient sequence $[\widetilde{c}_{\mathsf{m}}^{[N]}|_{\mathsf{m}\in\mathbb{M}}]$, where, for all $m \in \mathbb{M}$,

$$\widetilde{c}_{\mathsf{m}}^{[N]} = \sum_{\mathsf{v}\in\mathbb{V}} \sum_{\substack{\mathsf{u}_1,\ldots,\mathsf{u}_N\in\mathbb{U} \\ \mathsf{v}+\mathsf{u}_1+\cdots+\mathsf{u}_N=\mathsf{m}}} \widetilde{c}_{\mathsf{v}} \cdot f_{\mathsf{u}_1} \cdot \cdots \cdot f_{\mathsf{u}_N}.$$

Clearly, for all $N \in \mathbb{N}$ and $\mathsf{m} \in \mathbb{M}$, $c_{\mathsf{m}}^{[N]} = p^s \cdot \widetilde{c}_{\mathsf{m}}^{[N]}$, so if $\widetilde{c}_{\mathsf{m}}^{[N]} \not\equiv 0 \pmod{\widetilde{q}}$, then $c_{\mathsf{m}}^{[N]} \not\equiv 0 \pmod{q}$. Thus, $\mathsf{rank}[\boldsymbol{\chi}^{[N]}] \geq \mathsf{rank}[\widetilde{\boldsymbol{\chi}}^{[N]}]$. But, by construction, at least one coefficient of $\widetilde{\boldsymbol{\chi}}$ is non-zero, mod p. Thus, by Case 1, we have $\mathsf{rank}[\widetilde{\boldsymbol{\chi}} \circ \widetilde{\mathfrak{F}}^{N}] \xrightarrow[n\to\infty]{\text{dense}} \infty$. □

THEOREM 6. *Let* $n \in \mathbb{N}$ *and* $\mathcal{A} = \mathbb{Z}_{/n}$. *Let* $D \geq 1$ *and let* $\mathfrak{F} : \mathcal{A}^{(\mathbb{Z}^D)} \hookleftarrow$ *be an LCA such that, for each prime divisor* p *of* n, *at least two coefficients of* $\mathfrak{F}$ *are relatively prime to* p. *Then* $\mathfrak{F}$ *is diffusive.*

Proof. Write $n = p_1^{r_1} \ldots p_J^{r_J}$, $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_J$, $\mathfrak{F} = \mathfrak{F}_1 \oplus \cdots \oplus \mathfrak{F}_J$ as before. By Lemma 4, it suffices to show that each of $\mathfrak{F}_1, \ldots, \mathfrak{F}_J$ is diffusive. By Lemma 5 and the hypothesis, this is the case. □

4. *Diffusion on finite Abelian groups*

Now suppose $\mathcal{A}$ is an arbitrary finite Abelian group. Then $\mathcal{A}$ has a canonical decomposition:

$$\mathcal{A} = \bigoplus_{k=1}^{K} \bigoplus_{j=1}^{J_k} \mathcal{A}_{(k,j)},$$

with $\mathcal{A}_{(k,j)} = \mathbb{Z}_{/q_{(k,j)}}$; $q_{(k,j)} = p_k^{r_{(k,j)}}$, where $p_1, \ldots, p_K$ are distinct primes with $r_{(k,1)}, r_{(k,2)}, \ldots, r_{(k,J_k)}$ natural numbers for each $k \in [1 \ldots K]$.

We will assume that $\mathcal{A}$ is of the special form where, for all $k \in [1 \ldots K]$, $r_{k,1} = \cdots = r_{k,J_k} = r_k$. In other words,

$$\mathcal{A} = \bigoplus_{k=1}^{K} \mathcal{A}_k, \quad \text{with } \mathcal{A}_k = (\mathbb{Z}_{/q_k})^{J_k},$$

where $p_1, \ldots, p_K$ are distinct primes, with $q_k = p_k^{r_k}$ and $r_k, J_k \in \mathbb{N}$. Thus, as before,

$$\mathbf{End}(\mathcal{A}) = \bigoplus_{j,k=1}^{K} \mathbf{Hom}(\mathcal{A}_j, \mathcal{A}_k) = \bigoplus_{k=1}^{K} \mathbf{End}(\mathcal{A}_k),$$

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

(cross-terms are trivial) and $\mathcal{A}^{\mathbb{M}} \cong \mathcal{A}_1^{\mathbb{M}} \oplus \cdots \oplus \mathcal{A}_K^{\mathbb{M}}$, so we can write any LCA $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \hookleftarrow$ as a direct sum $\mathfrak{F} = \mathfrak{F}_1 \oplus \cdots \oplus \mathfrak{F}_K$, where $\mathfrak{F}_k : \mathcal{A}_k^{\mathbb{M}} \hookleftarrow$.

By Lemma 4, to prove $\mathfrak{F}$ is diffusive, it suffices to show that each of $\mathfrak{F}_1, \ldots, \mathfrak{F}_K$ is diffusive. Hence, we will assume from now on that $\mathcal{A} = (\mathbb{Z}_{/q})^J$, where p is prime, $q = p^r$ and $J \in \mathbb{N}$. Elements of $\mathcal{A}$ are thought of as J-tuples of $\mathbb{Z}_{/q}$-elements. $\mathcal{A}$ is a J-dimensional module over the commutative ring‡ $\mathbb{Z}_{/q}$. The endomorphisms of $\mathcal{A}$ as an Abelian group are just the $\mathbb{Z}_{/q}$-linear endomorphisms of this $\mathbb{Z}_{/q}$-module, and are described by $J \times J$ matrices of elements in $\mathbb{Z}_{/q}$.

LEMMA 7. *Let $\mathcal{A} = (\mathbb{Z}_{/q})^J$, where p is prime and $q = p^r$.*

(1) *Any $\chi \in \widehat{\mathcal{A}}$ is of the form $\chi(\mathbf{a}) = \exp((2\pi\mathbf{i}/q) \cdot \langle \mathbf{c}, \mathbf{a} \rangle)$, where $\mathbf{c} = (c_1, \ldots, c_J) \in (\mathbb{Z}_{/q})^J$, and for any $\mathbf{a} = (a_1, \ldots, a_J) \in (\mathbb{Z}_{/q})^J$, we define $\langle \mathbf{c}, \mathbf{a} \rangle = c_1 a_1 + \cdots + c_J a_J$. Thus, χ is non-trivial if and only if $\mathbf{c} \neq 0$.*

(2) *If $\mathfrak{f} \in \mathbf{End}(\mathcal{A})$ has matrix $\mathbf{F}$ with adjoint ${}^{\dagger}\mathbf{F}$, then $\chi \circ \mathfrak{f}$ is the character $\mathbf{a} \mapsto \exp((2\pi\mathbf{i}/q) \cdot \langle \mathbf{c}', \mathbf{a} \rangle)$, where $\mathbf{c}' = {}^{\dagger}\mathbf{F} \cdot \mathbf{c}$. In particular, $\chi \circ \mathfrak{f}$ is non-trivial if and only if $\mathbf{c}$ is not in $\ker[{}^{\dagger}\mathbf{F}]$.*

(3) *Let $\mathfrak{f} \in \mathbf{Aut}(\mathcal{A})$. If $\chi \in \widehat{\mathcal{A}}$ is non-trivial, then $\chi \circ \mathfrak{f}$ is also non-trivial.*

Let $\mathbb{V} \subset \mathbb{M}$ be a subset not containing 0. If $\mathfrak{G} = \sum_{\mathsf{m} \in \mathbb{M}} \mathfrak{g}_{\mathsf{m}} \boldsymbol{\sigma}^{\mathsf{m}}$ is an LCA on $\mathcal{A}^{\mathbb{M}}$ (where all but finitely many $\mathfrak{g}_{\mathsf{m}}$ are zero), then a subset $\mathbb{W} \subset \mathbb{M}$ is called $\mathbb{V}$-*separating* for $\mathfrak{G}$ if, for every $\mathsf{w} \in \mathbb{W}$, $\mathfrak{g}_{\mathsf{w}} \in \mathbf{Aut}(\mathcal{A})$, but for all $\mathsf{v} \in \mathbb{V}$, $\mathfrak{g}_{(\mathsf{w}-\mathsf{v})} = 0$. Intuitively, $\mathbb{W}$ indexes a set of non-trivial (indeed, automorphic) coefficients of $\mathfrak{G}$, separated from one another by $\mathbb{V}$-shaped 'gaps'. If $\mathbb{K} = \mathbb{V} \sqcup \{0\}$ and $\boldsymbol{\chi} = \bigotimes_{\mathsf{k} \in \mathbb{K}} \chi_{\mathsf{k}}$ is a character, then we will show that these gaps ensure that $(\boldsymbol{\chi} \circ \mathfrak{G})_{\mathsf{w}}$ is non-trivial for all $\mathsf{w} \in \mathbb{W}$. We will then construct $\mathbb{V}$-separating sets for $\mathfrak{G} = \mathfrak{F}^N$. This argument has already been used implicitly to prove Theorem 15 in [**6**].

PROPOSITION 8. *Let $\mathbb{M} = \mathbb{Z}^D$. An LCA $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \hookleftarrow$ is diffusive if, for every finite subset $\mathbb{V} \subset \mathbb{M}$ not containing zero and every $R \in \mathbb{N}$, there is a set $\mathbb{J}_{(\mathbb{V};R)} \subset \mathbb{N}$ of density 1 so that, for all $j \in \mathbb{J}_{(\mathbb{V};R)}$, there is a $\mathbb{V}$-separating set $\mathbb{W}_j \subset \mathbb{M}$ for $\mathfrak{F}^j$ with $\mathsf{card}[\mathbb{W}_j] > R$.*

Proof. Suppose $\mathfrak{F}$ is not diffusive; thus, there is some character $\boldsymbol{\chi} = \bigotimes_{\mathsf{k} \in \mathbb{K}} \chi_{\mathsf{k}}$ so that $\mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{F}^N] \xrightarrow[n \not\to \infty]{\text{dense}} \infty$. Hence, there is some subset $\mathbb{B} \subset \mathbb{N}$ of non-zero upper density and some bound R so that $\mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{F}^N] < R$ for all $N \in \mathbb{B}$.

Fix $\mathsf{k}_0 \in \mathbb{K}$ and let $\mathbb{V} = \{\mathsf{k} - \mathsf{k}_0; \mathsf{k} \in \mathbb{K} \setminus \{\mathsf{k}_0\}\}$ and let $\mathbb{J}_{(\mathbb{V};R)}$ be the set described by the hypothesis. The set $\mathbb{B} \subset \mathbb{N}$ has non-zero upper density, so $\mathbb{B} \cap \mathbb{J}_{(\mathbb{V};R)} \neq \emptyset$. Let $j \in \mathbb{B} \cap \mathbb{J}_{(\mathbb{V};R)}$ and let $\mathbb{W}_j \subset \mathbb{M}$ be the $\mathbb{V}$-separating set for $\mathfrak{F}^j$.

Write $\mathfrak{F}^j = \sum_{\mathsf{m} \in \mathbb{M}} \mathfrak{f}_{\mathsf{m}}^{[j]} \boldsymbol{\sigma}^{\mathsf{m}}$, and then write

$$\chi \circ \mathfrak{F}^j = \bigotimes_{\mathsf{m} \in \mathbb{M}} \chi_{\mathsf{m}}^{[j]}, \quad \text{where } \chi_{\mathsf{m}}^{[j]} = \prod_{\mathsf{k} \in \mathbb{K}} (\chi_{\mathsf{k}} \circ \mathfrak{f}_{\mathsf{m}-\mathsf{k}}^{[j]}).$$

‡ If $r = 1$ then $q = p$ is prime, $\mathbb{Z}_{/q}$ is a field and $\mathcal{A}$ is a $\mathbb{Z}_{/q}$-vector space. It may be helpful to keep this case in mind in what follows.

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

Then, for all $\mathsf{w} \in \mathbb{W}_j$,

$$\chi^{[j]}_{(\mathsf{w}+\mathsf{k}_0)} = \prod_{\mathsf{k}\in\mathbb{K}} (\chi_{\mathsf{k}} \circ \mathfrak{f}^{[j]}_{(\mathsf{w}+\mathsf{k}_0-\mathsf{k})}) = (\chi_{\mathsf{k}_0} \circ \mathfrak{f}^{[j]}_{\mathsf{w}}) \prod_{\mathsf{v}\in\mathbb{V}} (\chi_{(\mathsf{v}+\mathsf{k}_0)} \circ \mathfrak{f}^{[j]}_{(\mathsf{w}-\mathsf{v})})$$
$$= (\chi_{\mathsf{k}_0} \circ \mathfrak{f}^{[j]}_{\mathsf{w}}) \Big(\prod_{\mathsf{v}\in\mathbb{V}} \mathbb{1} \Big) = (\chi_{\mathsf{k}_0} \circ \mathfrak{f}^{[j]}_{\mathsf{w}}),$$

which is non-trivial by Lemma 7, because $\mathfrak{f}^{[j]}_{\mathsf{w}}$ is an automorphism. Thus, $\chi^{[j]}_{\mathsf{w}} \neq \mathbb{1}$ for all $\mathsf{w} \in \mathbb{W} + \mathsf{k}_0$, a set of cardinality greater than R, contradicting the hypothesis that $\mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{F}^j] < R$. □

Applying Proposition 8 often involves tracking binomial coefficients, mod p, via Lucas' theorem [**6**]. For a fixed prime p and any $n \in \mathbb{N}$, let $\mathbb{P}(n) \in [0 \ldots p)^{\mathbb{N}}$ be the *p-ary expansion* of n (conventionally written with digits in reversed order). Thus, for example, if $p = 3$, then $\mathbb{P}(34) = \ldots 000\,000\,1021$.

If $n, N \in \mathbb{N}$, with $\mathbb{P}(n) = [n^{[i]}|_{i=0}^{\infty}]$ and $\mathbb{P}(N) = [N^{[i]}|_{i=0}^{\infty}]$, then we write '$n \ll N$' if $n^{[i]} \leq N^{[i]}$ for all $i \in \mathbb{N}$. Lucas' theorem then implies that

$$\left(\begin{bmatrix} N \\ n \end{bmatrix}_p \neq 0 \right) \iff (n \ll N).$$

A *commuting automorphism linear cellular automaton* is an LCA of the form $\mathfrak{F} = \sum_{\mathsf{u}\in\mathbb{U}} \mathfrak{f}_{\mathsf{u}} \circ \boldsymbol{\sigma}^{\mathsf{u}}$, where $\{\mathfrak{f}_{\mathsf{u}}|_{\mathsf{u}\in\mathbb{U}}\} \subset \mathbf{Aut}(\mathcal{A})$ is a commuting collection of automorphisms of $\mathcal{A}$. The following are examples.

- $\{\mathfrak{f}_{\mathsf{u}}|_{\mathsf{u}\in\mathbb{U}}\}$ are simultaneously diagonalizable automorphisms. In other words, there is some $\mathbb{Z}_{/q}$-basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_J\}$ for $\mathcal{A}$, so that the elements of $\mathcal{B}$ are eigenvectors for every element of $\{\mathfrak{f}_{\mathsf{u}}|_{\mathsf{u}\in\mathbb{U}}\}$, and all eigenvalues are relatively prime to p.
- There is some $\mathfrak{f} \in \mathbf{Aut}(\mathcal{A})$ so that for all $\mathsf{u} \in \mathbb{U}$, $\mathfrak{f}_{\mathsf{u}} = \mathfrak{f}^{n_{\mathsf{u}}}$ for some $n_{\mathsf{u}} \in \mathbb{Z}$.

THEOREM 9. *If $\mathfrak{G} : \mathcal{A}^{(\mathbb{Z}^D)} \hookleftarrow$ is a commuting automorphism LCA with two or more non-trivial coefficients, then $\mathfrak{G}$ is diffusive.*

Proof. We will use Proposition 8: the argument is basically identical to the proof of Theorem 15 in [**6**], so we will only sketch it here.

Suppose $\mathfrak{G} = \mathfrak{g}_0\boldsymbol{\sigma}^{\mathsf{n}_0} + \mathfrak{g}_1\boldsymbol{\sigma}^{\mathsf{n}_1} + \cdots + \mathfrak{g}_U\boldsymbol{\sigma}^{\mathsf{n}_U}$, where $\mathfrak{g}_0, \mathfrak{g}_1, \ldots, \mathfrak{g}_U \in \mathbf{Aut}(\mathcal{G})$ commute and where $\mathsf{n}_0, \mathsf{n}_1, \ldots, \mathsf{n}_U \in \mathbb{Z}^D$. We can rewrite: $\mathfrak{G} = \mathfrak{g}_0 \circ (\mathfrak{F} \circ \boldsymbol{\sigma}^{\mathsf{n}_0})$, where

$$\mathfrak{F} = \mathbf{Id} + \mathfrak{f}_1\boldsymbol{\sigma}^{\mathsf{m}_1}\big(\mathbf{Id} + \mathfrak{f}_2\boldsymbol{\sigma}^{\mathsf{m}_2}\big[\ldots(\mathbf{Id} + \mathfrak{f}_{U-1}\boldsymbol{\sigma}^{\mathsf{m}_{U-1}}[\mathbf{Id} + \mathfrak{f}_U\boldsymbol{\sigma}^{\mathsf{m}_U}])\ldots\big]\big),$$

and, for all $u \in [1 \ldots U]$, $\mathsf{m}_{\mathsf{u}} = \mathsf{n}_{\mathsf{u}} - \mathsf{n}_{u-1}$ and $\mathfrak{f}_{\mathsf{u}} = \mathfrak{g}_{u-1}^{-1} \circ \mathfrak{g}_{\mathsf{u}}$. We can do this because $\mathfrak{g}_0, \mathfrak{g}_1, \ldots, \mathfrak{g}_U$ are automorphisms and, thus, invertible. It suffices to show that $\mathfrak{F}$ is diffusive.

Let $J \in \mathbb{N}$. The coefficients of $\mathfrak{F}$ commute, so we can employ the Binomial theorem —and, thus, Lucas' theorem —to compute the coefficients of $\mathfrak{F}^J$, mod p. Let

$$\mathcal{L}^U(J) = \{[k_1, k_2, \ldots, k_U] \in \mathbb{N}^U; k_U \ll k_{U-1} \ll \cdots \ll k_2 \ll k_1 \ll J\}.$$

Then

$$\mathfrak{F}^J = \sum_{\mathsf{n}\in\mathbb{Z}^D} \mathfrak{f}^{[J]}_{\mathsf{n}} \circ \boldsymbol{\sigma}^{\mathsf{n}},$$

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

where

$$\mathfrak{f}_{\mathsf{n}}^{[J]} = \sum_{\substack{\mathbf{k}\in\mathcal{L}^U(J)\\(k_1\mathsf{m}_1+\cdots+k_U\mathsf{m}_U)=\mathsf{n}}} \mathfrak{f}_{(\mathbf{k})}^{[J]},$$

and, for any $\mathbf{k} = [k_1, k_2, \ldots, k_U] \in \mathbb{N}^U$, we define

$$\mathfrak{f}_{(\mathbf{k})}^{[J]} := \begin{bmatrix} J \\ k_1 \end{bmatrix}_p \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}_p \cdots \begin{bmatrix} k_{U-1} \\ k_U \end{bmatrix}_p \mathfrak{f}_1^{k_1} \circ \mathfrak{f}_2^{k_2} \circ \cdots \circ \mathfrak{f}_U^{k_U}.$$

(See [**6**] for details.)

Fix a finite subset $\mathbb{V} \subset \mathbb{Z}^D$ not containing 0 and let $R > 0$. We want to build a $\mathbb{V}$-separating set for $\mathfrak{F}^J$ of cardinality R. To do this, note that there is some $\Gamma \in \mathbb{N}$ such that, if $J \in \mathbb{N}$ and $\mathbb{P}(J)$ contains at least R 'gaps' of size at least Γ (i.e. sequences of Γ successive zeros, delimited by non-zero entries), then we can construct a set $\mathbb{W}_J \subset \mathbb{Z}^D$ with $\mathsf{card}[\mathbb{W}_J] \geq R$, so that

(1) for every $\mathsf{w} \in \mathbb{W}_J$, there is a unique $\mathbf{k} \in \mathcal{L}^U(J)$ so that $(k_1\mathsf{m}_1 + \cdots + k_U\mathsf{m}_U) = \mathsf{w}$; thus $\mathfrak{f}_{\mathsf{w}}^{[J]} = \mathfrak{f}_{(\mathbf{k})}^{[J]} \in \mathbf{Aut}(\mathcal{A})$; and

(2) for all $\mathsf{v} \in \mathbb{V}$, there are no $\mathbf{k} \in \mathcal{L}^U(J)$ with $(k_1\mathsf{m}_1 + \cdots + k_U\mathsf{m}_U) = \mathsf{w} - \mathsf{v}$; thus, $\mathfrak{f}_{(\mathsf{w}-\mathsf{v})}^{[J]} = 0$.

Thus, $\mathbb{W}_J$ is $\mathbb{V}$-separating for $\mathfrak{F}^J$. By Birkhoff's ergodic theorem, the set $\mathbb{J}_{(\Gamma;R)}$ of $J \in \mathbb{N}$ with R such Γ-gaps is a set of Cesàro density 1. Thus, we satisfy the conditions of Proposition 8. □

To apply Proposition 8, it is clearly sufficient to construct sets $\mathbb{J}_{(\mathbb{V};R)}$ for some increasing sequence of numbers $R_1, R_2, \ldots \to \infty$, along with a sequence $\mathbb{V}_1, \mathbb{V}_2, \ldots$ so that, for any finite $\mathbb{V} \subset \mathbb{M}$, we have $\mathbb{V} \subset \mathbb{V}_k + \mathsf{m}$ for some $\mathsf{m} \in \mathbb{M}$ and $k \in \mathbb{N}$. Also, it suffices to prove that the LCA $\mathfrak{F}^K$ is diffusive for some power $K > 0$: for any $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$ and any $k \in [0 \ldots K)$, $\boldsymbol{\chi} \circ \mathfrak{F}^k$ is also a character; if $\mathfrak{F}^K$ is diffusive, then $\mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{F}^k \circ \mathfrak{F}^{n\cdot K}] \xrightarrow[n\to\infty]{\text{dense}} \infty$ for every $k \in [0 \ldots K)$ which, in turn, implies that $\mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{F}^n] \xrightarrow[n\to\infty]{\text{dense}} \infty$.

Proposition 8 can be applied even when the coefficients of $\mathfrak{F}$ do not commute.

Example 10. Let $\mathcal{A} = (\mathbb{Z}_{/p})^2$ and let $\mathfrak{F} : \mathcal{A}^{\mathbb{Z}} \hookleftarrow$ have local map $\mathfrak{f} : \mathcal{A}^{\{0,1\}} \longrightarrow \mathcal{A}$ given

$$\mathfrak{f}\left(\begin{bmatrix} x_0 \\ y_0 \end{bmatrix}, \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}\right) = (y_0, x_0 + y_1) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} x_0 \\ y_0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}.$$

This invertible LCA was studied in [**1**], where it was shown to take fully supported Markov measures to Haar measure in the weak* Cesàro limit. Proposition 3.1 of [**1**] can be reformulated as

$$\mathfrak{F}^N = \sum_{m=0}^{N} \mathfrak{f}_m^{[N]} \boldsymbol{\sigma}^m, \quad \text{where } \mathfrak{f}_m^{[N]} = \begin{bmatrix} \varphi_m^{(N-2)} & \varphi_m^{(N-1)} \\ \varphi_m^{(N-1)} & \varphi_m^{(N)} \end{bmatrix},$$

with

$$\varphi_m^{(N)} = \begin{cases} \left[\begin{pmatrix} \frac{N+m}{2} \\ m \end{pmatrix}\right]_p & \text{if } m \equiv N \pmod 2 \\ 0 & \text{if } m \not\equiv N \pmod 2. \end{cases}$$

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

Thus, if $m \equiv (N-1) \pmod 2$, then the matrix $\mathfrak{f}_m^{[N]}$ is antidiagonal and an automorphism if and only if

$$\varphi_m^{(N-1)} = \left[\binom{N-1+m}{m} \right]_p \neq 0,$$

which, by Lucas' theorem, occurs only when $m \ll \frac{1}{2}(N-1+m)$. If $m \equiv N \equiv (N-2) \pmod 2$, then matrix $\mathfrak{f}_m^{[N]}$ is diagonal and an automorphism if and only if $m \ll \frac{1}{2}(N+m)$ and $m \ll \frac{1}{2}(N-2+m)$.

As noted earlier, it suffices to prove that $\mathfrak{F}^2$ is diffusive. So, fix $\mathbb{V} = (0 \dots 2V] \subset \mathbb{Z}$ and $R > 0$: we will find a set $\mathbb{J}_{(\mathbb{V};R)}$ and, for all $j \in \mathbb{J}_{(\mathbb{V};R)}$, some $\mathbb{W}_j \subset \mathbb{Z}$ with $\mathsf{card}[\mathbb{W}_j] > R$, so that $2\mathbb{W}_j$ is $\mathbb{V}$-separating for $\mathfrak{F}^{2j}$. In other words, for all $w \in \mathbb{W}_j$, $\mathfrak{f}_{2w}^{[2j]} \in \mathbf{Aut}(\mathcal{A})$ but for all $v \in \mathbb{V}$, $\mathfrak{f}_{(2w-v)}^{[2j]} = 0$. This is equivalent to saying: for all $w \in \mathbb{W}_j$,

$$\varphi_{2w}^{(2j)} \neq 0 \neq \varphi_{2w}^{(2j-2)},$$

but for all even $v = 2u \in \mathbb{V}$,

$$\varphi_{(2w-v)}^{(2j)} = 0 = \varphi_{(2w-v)}^{(2j-2)},$$

and for all odd $v = 2u+1 \in \mathbb{V}$,

$$\varphi_{(2w-v)}^{(2j-1)} = 0.$$

This, in turn, is equivalent to saying: *for all* $w \in \mathbb{W}_j$,

$$2w \ll j+w \quad \text{and} \quad 2w \ll j+w-1, \tag{2}$$

but for all $u \in (0 \dots V]$,

$$2w-2u \not\ll j+w-u, \quad 2w-2u \not\ll j+w-u-1,$$

and

$$2w-2u-1 \not\ll j+w-u-1. \tag{3}$$

So, let $q = p-1$, $L_V = \lceil \log_p(V) \rceil + 1$ and $L_R = \lceil \log_2(R) \rceil$ and let $\mathbb{J}_{(\mathbb{V};R)}$ be the set of all $j \in \mathbb{N}$ such that $\mathbb{P}(j)$ contains the word '$0q1$' somewhere after the first L_V digits and contains at least L_R separate instances of the word '10' after the '$0q1$'. By Birkhoff's ergodic theorem, $\mathbb{J}_{(\mathbb{V};R)} \subset \mathbb{N}$ has density 1.

Suppose $j \in \mathbb{J}_{(\mathbb{V};R)}$ and suppose that '$0q1$' occurs at position $i_0 > L_v$, while '10' occurs at positions $i_{(L_R)} > \cdots > i_2 > i_1$. Let w to be a number so that $\mathbb{P}(w)$ contains the word '010' at i_0, and contains either '01' or '00' at each of $i_1, i_2, \dots, i_{(L_R)}$, with zeros everywhere else. Clearly, we can construct $2^{L_R} > R$ distinct numbers w of this kind: let $\mathbb{W}_j$ be the set of all such numbers.

For example, if w has '01' at i_1 and '00' at i_2, and $v \in [0 \dots V]$, then the p-ary expansions of the relevant numbers are depicted in Figure 1. By inspection, one can see that equations (2) and (3) are satisfied. Clearly, this will be true for any choice of $w \in \mathbb{W}_j$ and $v \in \mathbb{V}$.

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

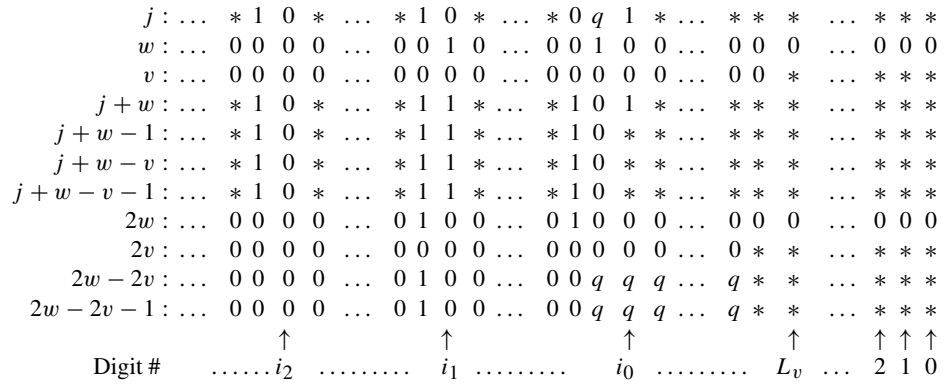


FIGURE 1. The p-ary expansions of j, w, v, etc. Here, '$*$' represents any digit in $[0 \dots q]$.

5. *Harmonic mixing of Markov random fields*

Notation. Suppose $\mathbf{a} = \mathcal{A}^{\mathbb{M}}$, with $\mathbf{a} = [a_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}]$. If $\mathbb{V} \subset \mathbb{M}$, then we define $\mathbf{a}|_{\mathbb{V}} := [a_{\mathsf{v}}|_{\mathsf{v}\in\mathbb{V}}] \in \mathcal{A}^{\mathbb{V}}$. This determines a continuous map $\mathbf{pr}_{\mathbb{V}} : \mathcal{A}^{\mathbb{M}} \ni \mathbf{a} \mapsto \mathbf{a}|_{\mathbb{V}} \in \mathcal{A}^{\mathbb{V}}$; if $\mu \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$, then let $\mathbf{pr}_{\mathbb{V}}{}^*(\mu)$ be the $\mathbb{V}$-marginal projection of μ (so that, for any $\mathcal{U} \subset \mathcal{A}^{\mathbb{V}}$, $\mathbf{pr}_{\mathbb{V}}{}^*(\mu)[\mathcal{U}] = \mu[\mathcal{U} \times \mathcal{A}^{\mathbb{M}\setminus\mathbb{V}}]$).

If $\mathbf{b} \in \mathcal{A}^{\mathbb{V}}$, then $\langle \mathbf{b} \rangle = \{\mathbf{a} \in \mathcal{A}^{\mathbb{M}}; \mathbf{a}|_{\mathbb{V}} = \mathbf{b}\}$ is the associated *cylinder set* and, if $\mu \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$, then $\mu[\mathbf{b}]$ is the measure of this cylinder set. If $\mathbb{W} \subset \mathbb{M}$ is disjoint from $\mathbb{V}$ and $\mathbf{c} \in \mathcal{A}^{\mathbb{W}}$, then $\mathbf{b_c} \in \mathcal{A}^{\mathbb{V}\sqcup\mathbb{W}}$ is defined so that $(\mathbf{b_c})|_{\mathbb{V}} = \mathbf{b}$ and $(\mathbf{b_c})|_{\mathbb{W}} = \mathbf{c}$; thus, $\langle \mathbf{b_c} \rangle = \langle \mathbf{b} \rangle \cap \langle \mathbf{c} \rangle$.

Let $\mathcal{B}(\mathbb{V})$ be the sigma-subalgebra of $\mathcal{A}^{\mathbb{M}}$ generated by coordinates in $\mathbb{V}$: if $\phi \in \mathbf{L}^1(\mathcal{A}^{\mathbb{M}}, \mu)$, let $\mathbf{E}_{\mathbb{V}}[\phi] \in \mathbf{L}^1(\mathcal{A}^{\mathbb{V}}, \mu)$ be the *conditional expectation* of ϕ given $\mathcal{B}(\mathbb{V})$, which we regard as a function on $\mathcal{A}^{\mathbb{V}}$. If $\mathbf{b} \in \mathcal{A}^{\mathbb{V}}$, then the *conditional probability measure* of μ, given $\mathbf{b}$, is the unique measure $\mu_{\mathbf{b}} \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$ such that $\langle \phi, \mu_{\mathbf{b}} \rangle = \mathbf{E}_{\mathbb{V}}[\phi](\mathbf{b})$ for every $\phi \in \mathbf{L}^1(\mathcal{A}^{\mathbb{M}}, \mu)$. The map $\mathcal{A}^{\mathbb{V}} \ni \mathbf{b} \mapsto \mu_{\mathbf{b}} \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$ is measurable and, if $\mu_{\mathbb{V}} = \mathbf{pr}_{\mathbb{V}}{}^*(\mu)$ is the marginal projection of μ onto $\mathcal{A}^{\mathbb{V}}$, then μ has the *disintegration* [**10, 3**]: $\mu = \int_{\mathcal{A}^{\mathbb{V}}} \mu_{\mathbf{b}}\, d\mu_{\mathbb{V}}[\mathbf{b}]$. Note that $\mathbf{pr}_{\mathbb{V}}(\mu_{\mathbf{b}}) = \delta_{\mathbf{b}}$, the point mass at $\mathbf{b}$. If $\mathbb{W} \subset \mathbb{M} \setminus \mathbb{V}$ and $\mathbf{c} \in \mathcal{A}^{\mathbb{W}}$, we will sometimes write $\mu_{\mathbf{b}}[\mathbf{c}]$ as '$\mu[\mathbf{c}/\!\!/\mathbf{b}]$' or, if $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$ is a μ-random configuration, as '$\mu\left[\frac{\mathbf{a}|_{\mathbb{W}}=\mathbf{c}}{\mathbf{a}|_{\mathbb{V}}=\mathbf{b}}\right]$'.

5.1. *Markov processes.*

Let $(\mathbf{X}, \mathcal{X})$ be a measurable space (i.e. $\mathbf{X}$ is a set, $\mathcal{X}$ is a sigma-algebra) and let $\mu \in \mathcal{M}[\mathbf{X}^{\mathbb{Z}}]$ be a probability measure. Let $\mathbb{U} = [0 \dots U) \subset \mathbb{Z}$. If $n \in \mathbb{Z}$ and $\mathbf{x} \in \mathbf{X}^{(\mathbb{U}+n)}$, then $\langle \mathbf{x} \rangle = \{\mathbf{y} \in \mathbf{X}^{\mathbb{Z}}; \mathbf{y}|_{(\mathbb{U}+n)} = \mathbf{x}\}$ and $\mu_{\mathbf{x}}$ is the conditional probability measure of μ, given $\mathbf{x}$.

μ is the *path distribution* of a ($\mathbf{X}$-valued, U-step, non-stationary) *Markov process* if, for any $n \in \mathbb{Z}$ and $\mathbf{x} \in \mathbf{X}^{(\mathbb{U}+n)}$, events occurring after time $n + U$ are independent of those occurring before time n, relative to $\mu_{\mathbf{x}}$: for any $\mathbb{V}_p \subset (-\infty \dots n)$, $\mathbb{V}_f \subset [U + n \dots \infty)$ and $\mathbf{y}_p \in \mathbf{X}^{\mathbb{V}_p}$ and $\mathbf{y}_f \in \mathbf{X}^{\mathbb{V}_f}$, we have $\mu_{\mathbf{x}}[\mathbf{y}_p_\mathbf{y}_f] = \mu_{\mathbf{x}}[\mathbf{y}_p] \cdot \mu_{\mathbf{x}}[\mathbf{y}_f]$.

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

Any U-step Markov process is entirely described by its $(U+1)$-dimensional marginals $\mu_{[n\ldots U+n]} = \mathbf{pr}_{[n\ldots U+n]}{}^*[\mu]$ for all $n \in \mathbb{Z}$, which are called the (U-step) *transition probabilities* of μ. If $\mathbf{X}$ is finite, then $\mathcal{M}[\mathbf{X};\mathbb{R}] \cong \mathbb{R}^{\mathbf{X}}$; if $U = 1$, then the transition probabilities $\{\mu_{\{n,n+1\}}\}_{n\in\mathbb{Z}}$ can be encoded by a sequence of *transition probability matrices* $\{\mathbf{Q}^{(n)} \in \mathbb{R}^{\mathbf{X}\times\mathbf{X}}; n \in \mathbb{Z}\}$ and *state distributions* $\{\zeta_n \in \mathbb{R}^{\mathbf{X}}; n \in \mathbb{Z}\}$ so that, for any $n \in \mathbb{Z}$, $\zeta_{(n+1)} = \mathbf{Q}^{(n)} \cdot \zeta_n$, and, for any $x_n, x_{(n+1)} \in \mathbf{X}$, $\mu_{\{n,n+1\}}[x_n, x_{(n+1)}] = \mathbf{Q}^{(n)}_{(x_{(n+1)};x_n)} \cdot \zeta_n(x_n)$.

If $\mu_{[n\ldots U+n]} = \mu_{[0\ldots U]}$ for all $n \in \mathbb{Z}$, then μ is *stationary*. If $\mathbf{X}$ is finite and $U = 1$, this means there is some $\mathbf{Q} \in \mathbb{R}^{\mathbf{X}\times\mathbf{X}}$ and $\zeta \in \mathcal{M}[\mathbf{X}]$ (with $\mathbf{Q}\cdot\zeta = \zeta$) so that $\mathbf{Q}^{(n)} = \mathbf{Q}$ and $\zeta_n = \zeta$ for all $n \in \mathbb{Z}$. We call ζ the *stationary state distribution*.

If $\mathfrak{M} \subset \mathcal{M}[\mathbf{X}^{[0\ldots n]}]$ is a finite family of transition probabilities, we say μ is $\mathfrak{M}$-*semistationary* if $\mu_{[n\ldots U+n]} \in \mathfrak{M}$ for all $n \in \mathbb{Z}$. When $\mathbf{X}$ is finite and $U = 1$, this means that there are some finite families $\mathfrak{Q}$ and $\mathfrak{H}$ of transition probability matrices and state distributions, respectively, for μ so that, for any $\zeta \in \mathfrak{H}$ and $\mathbf{Q} \in \mathfrak{Q}$, $\mathbf{Q}\cdot\zeta \in \mathfrak{H}$, we say that μ is $\mathfrak{Q}$-*semistationary*.

If μ is $\mathfrak{M}$-semistationary, then μ has *full support* if every element of $\mathfrak{M}$ has full support on $\mathbf{X}^{[0\ldots U]}$; as a consequence, μ assigns non-zero probability to every finite cylinder set. If $\mathbf{X}$ is finite and $U = 1$, this means that every entry of every transition probability matrix in $\mathfrak{Q}$ is non-zero.

If $\mu \in \mathcal{M}[\mathbf{X}^{\mathbb{Z}}]$ is a Markov process, $u, w \in \mathbf{X}$ and $n \in \mathbb{Z}$, then the *sandwich measure* ${}_n\mu_u^w \in \mathcal{M}[\mathbf{X}]$ is defined so that, if $\mathbf{x} = [x_n|_{n\in\mathbb{Z}}]$ is a μ-random sequence, then, for any $\mathcal{V} \subset \mathbf{X}$,

$$ {}_n\mu_u^w(\mathcal{V}) = \mu\left[\frac{x_{n+1} \in \mathcal{V}}{(x_n = u)\&(x_{n+2} = w)}\right]. $$

5.2. *Exponential harmonic mixing.* If $\mathcal{A}$ is a finite Abelian group and $\mu \in \mathcal{M}[\mathcal{A}^{\mathbb{M}};\mathbb{C}]$, we will say μ is *exponentially harmonically mixing* with *decay parameter* $\lambda > 0$ (or 'λ-EHM') if, for all $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$ with $\mathsf{rank}[\boldsymbol{\chi}] \geq R$, we have $|\langle\boldsymbol{\chi},\mu\rangle| < e^{-\lambda\cdot R}$. It is straightforward to verify the following lemma.

LEMMA 11. *Suppose* $(\mathbf{X},\rho)$ *is a probability space and* $\mathbf{X} \ni \mathbf{x} \mapsto \nu_{\mathbf{x}} \in \mathcal{M}[\mathcal{A}^{\mathbb{M}};\mathbb{C}]$ *is a measurable function so that* $\nu_{\mathbf{x}}$ *is* λ*-EHM for all* $\mathbf{x} \in \mathbf{X}$*. If* $\phi : \mathbf{X} \longrightarrow \mathbb{C}$ *is measurable and* $\|\phi\|_\infty = 1$*, then* $\int_{\mathbf{X}} \phi(x)\cdot\nu_{\mathbf{x}}\, d\rho[\mathbf{x}]$ *is also* λ*-EHM.*

If μ is a stationary, fully supported U-step Markov measure on $\mathcal{A}^{\mathbb{Z}}$, then μ is harmonically mixing (Part 4 of Proposition 1 in this paper, or Corollary 10 of [**6**]). The same method easily generalizes to show the following proposition.

PROPOSITION 12. *Suppose* $\mathcal{A}$ *is a finite Abelian group and that* $\mathfrak{M} \subset \mathcal{M}[\mathcal{A}^{[0\ldots n]}]$ *is a finite family of fully supported transition probabilities.*

(1) *There is a constant* $\lambda > 0$ *determined by* $\mathfrak{M}$*, so that, if* μ *is any* $\mathfrak{M}$*-semistationary Markov process on* $\mathcal{A}^{\mathbb{Z}}$*, then* μ *is* λ*-EHM.*

(2) *In particular, if* μ *is a one-step* $\mathfrak{Q}$*-semistationary Markov process with full support, then*

$$ -\lambda = \tfrac{1}{2}\cdot \sup_{\substack{\xi,\chi\in\widehat{\mathcal{A}}\\ \chi\neq\mathbb{1}}} \sup_{\mathbf{Q},\mathbf{P}\in\mathfrak{Q}} \log\|\xi_\bullet\cdot {}^\dagger\mathbf{Q}\cdot\chi_\bullet\cdot {}^\dagger\mathbf{P}\|_\infty, $$

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

where $\xi_\bullet$ is the diagonal matrix with elements of ξ along the diagonal (so that, for any $\phi \in \mathbb{C}^{\mathcal{A}}$, $\xi_\bullet\phi$ is the result of multiplying ξ and ϕ componentwise) and where $\| \bullet \|_\infty$ is the uniform operator norm.

Proof. (Sketch) Proposition 8 in [**6**] showed that a stationary one-step Markov matrix was harmonically mixing; in fact, the proof showed that $|\langle \boldsymbol{\chi}, \mu\rangle| < e^{-\lambda R}$ for all $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{Z}}}$ with $\mathsf{rank}[\boldsymbol{\chi}] = R$, where

$$-\lambda := \tfrac{1}{2} \cdot \sup_{\substack{\xi,\chi\in\widehat{\mathcal{A}} \\ \chi\neq\mathbb{1}}} \log \|\xi_\bullet \cdot {}^{\dagger}\mathbf{Q} \cdot \chi_\bullet \cdot {}^{\dagger}\mathbf{Q}\|_\infty.$$

The same argument works for a semistationary one-step process; this yields Part 2.

The proof of Corollary 10 in [**6**] showed how any fully supported U-step process could be 'recoded' as a fully supported one-step process: harmonic mixing of the latter implied harmonic mixing of the former. Corollary 10 thus followed from Proposition 8. By an identical argument, Part 1 follows from Part 2. □

5.3. *Markov random fields.* Let $\mathbb{U} \subset \mathbb{M}$ be a finite 'neighbourhood of 0' (e.g. $\mathbb{M} = \mathbb{Z}^D$ and $\mathbb{U} = [-1 \dots 1]^D$). For any subset $\mathbb{V} \subset \mathbb{M}$, let $cl(\mathbb{V}) := \mathbb{V}+\mathbb{U}$ and let $\partial(\mathbb{V}) := cl(\mathbb{V})\backslash\mathbb{V}$ (see Figure 2(a)).

$\mu \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$ is a *(non-stationary) Markov random field* [**2, 9**] with *interaction range* $\mathbb{U}$ (or '$\mathbb{U}$-MRF') if, for any $\mathbb{W} \subset \mathbb{M}$ and any $\mathbf{a} \in \mathcal{A}^{\partial(\mathbb{W})}$, events occurring 'inside' $\mathbb{W}$ are independent of those occurring 'outside', relative to the conditional measure $\mu_{\mathbf{a}}$. In other words, for any $\mathbb{V}_{\text{in}} \subset \mathbb{W}$, $\mathbb{V}_{\text{out}} \subset \mathbb{M} \setminus cl(\mathbb{W})$ and $\mathbf{b}_{\text{in}} \in \mathcal{A}^{\mathbb{V}_{\text{in}}}$, $\mathbf{b}_{\text{out}} \in \mathcal{A}^{\mathbb{V}_{\text{out}}}$, we have $\mu_{\mathbf{a}}[\mathbf{b}_{\text{in}}_\mathbf{b}_{\text{out}}] = \mu_{\mathbf{a}}[\mathbf{b}_{\text{in}}] \cdot \mu_{\mathbf{a}}[\mathbf{b}_{\text{out}}]$.

For example, if $\mathbb{M} = \mathbb{Z}$, then the U-step Markov processes on $\mathcal{A}^{\mathbb{M}}$ are exactly the Markov random fields with interaction range $\mathbb{U} = (-U \dots U)$.

μ is *stationary* if it is invariant under translation by $\mathbb{M}$. In this case, $\mu_{(\mathbb{U}+\mathsf{m})} = \mu_{\mathbb{U}}$ for every $\mathsf{m} \in \mathbb{M}$ and $\mu_{\mathbb{U}} = \mathbf{pr}_{\mathbb{U}}{}^*(\mu)$ is called the *local interaction* for μ.

If $\mathfrak{I} \subset \mathcal{M}[\mathcal{A}^{\mathbb{U}}]$ is finite, then μ is $\mathfrak{I}$-*semistationary* if $\mu_{(\mathbb{U}+\mathsf{m})} \in \mathfrak{I}$ for every $\mathsf{m} \in \mathbb{M}$. $\mathfrak{I}$ is called the set of *local interactions*. We say μ has *full support* if all elements of $\mathfrak{I}$ have full support on $\mathcal{A}^{\mathbb{U}}$.

Lamination processes. Suppose $\widetilde{\mathbb{U}} \subset \widetilde{\mathbb{M}} = \mathbb{M} \times \mathbb{Z}$ and $\mu \in \mathcal{M}[\mathcal{A}^{\widetilde{\mathbb{M}}}]$ is a $\widetilde{\mathbb{U}}$-MRF. By a suitable recoding, we can assume $\widetilde{\mathbb{U}} = \mathbb{U} \times \{-1, 0, 1\}$ for some $\mathbb{U} \subset \mathbb{M}$. We can then realize μ via an $\mathcal{A}^{\mathbb{M}}$-valued, one-step Markov process, called the *lamination process*. Intuitively, we imagine this Markov process as constructing a μ-random configuration in $\mathcal{A}^{\widetilde{\mathbb{M}}}$ by laying down successive random '$\mathbb{M}$-layers', with each $\mathbb{M}$-layer conditional on the previous one.

To see that this is a Markov process on $\mathcal{A}^{\mathbb{M}}$, fix k and let $\widetilde{\mathbb{V}}_k = \mathbb{M} \times (-\infty \dots k)$ (the 'past'). Then $\partial(\widetilde{\mathbb{V}}_k) = \mathbb{M} \times \{k\}$ (the 'present') and $\widetilde{\mathbb{M}} \setminus cl(\widetilde{\mathbb{V}}_k) = \mathbb{M} \times (k \dots \infty)$ (the 'future'): the Markov field condition of μ implies that events in the past are independent of those in the future, given complete information about the present (see Figure 3). The original field measure $\mu \in \mathcal{M}[\mathcal{A}^{\mathbb{M}\times\mathbb{Z}}]$ is also the path distribution (as a measure on $(\mathcal{A}^{\mathbb{M}})^{\mathbb{Z}}$) for the lamination process.

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

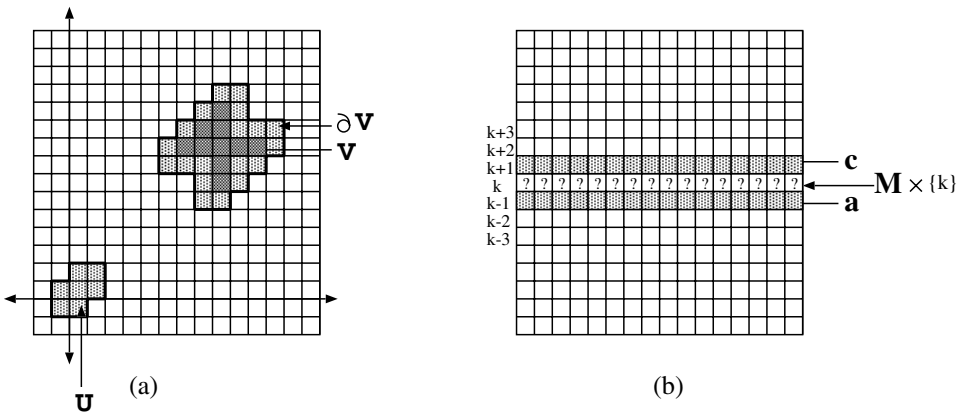


FIGURE 2. (a) $\mathbb{U}$, $\mathbb{V}$, and $\partial\mathbb{V}$. (b) A sandwich measure.

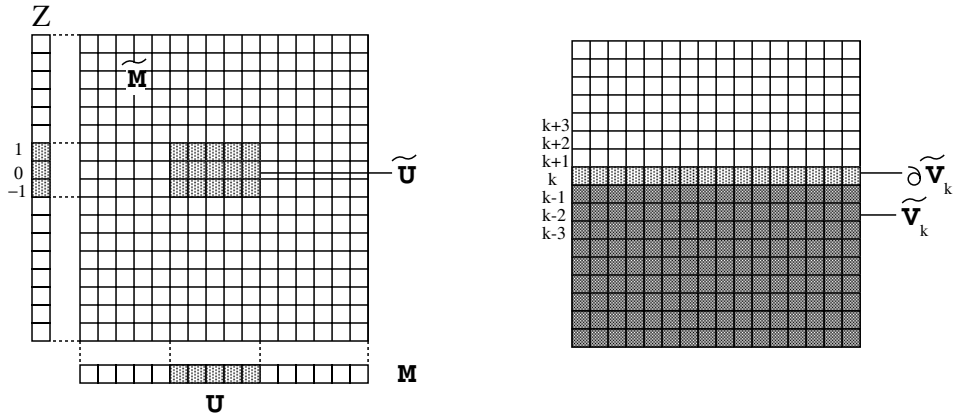


FIGURE 3. $\widetilde{\mathbb{M}} = \mathbb{M} \times \mathbb{Z}$ and $\widetilde{\mathbb{U}} = \mathbb{U} \times \{-1, 0, 1\}$; $\widetilde{\mathbb{V}}_k$ and $\partial\widetilde{\mathbb{V}}_k$.

Sandwich measures. Again assume $\widetilde{\mathbb{M}} = \mathbb{M} \times \mathbb{Z}$ and $\widetilde{\mathbb{U}} = \mathbb{U} \times \{-1, 0, 1\}$. If $\mathbf{a} \in \mathcal{A}^{\mathbb{M}\times\{k-1\}}$ and $\mathbf{c} \in \mathcal{A}^{\mathbb{M}\times\{k+1\}}$ (see Figure 2(b)), then the *sandwich measure* is determined by $\mathbf{a}$ and $\mathbf{c}$ is the sandwich measure ${}_{(k-1)}\mu^{\mathbf{c}}_{\mathbf{a}} \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$ of the lamination process: since k is implicit in the definition of $\mathbf{a}$ and $\mathbf{c}$, we will suppress it and denote the sandwich measure as '$\mu^{\mathbf{c}}_{\mathbf{a}}$'. In other words, $\mu^{\mathbf{c}}_{\mathbf{a}}$ is the conditional measure $\mu_{\mathbf{a}_\mathbf{c}}$, projected onto $\mathcal{A}^{\mathbb{M}\times\{k\}}$. The following lemma is easy to verify.

LEMMA 13.

(1) *$\mu^{\mathbf{c}}_{\mathbf{a}}$ is a Markov random field on $\mathcal{A}^{\mathbb{M}}$, with interaction range $\mathbb{U}$.*

(2) *If $\widetilde{\mathfrak{I}} \subset \mathcal{M}[\mathcal{A}^{\widetilde{\mathbb{U}}}]$ and μ is $\widetilde{\mathfrak{I}}$-semistationary, then there is some finite $\mathfrak{I} \subset \mathcal{M}[\mathcal{A}^{\mathbb{U}}]$ so that all sandwich measures of μ are $\mathfrak{I}$-semistationary.*

(3) *If μ has full support, then so does every sandwich measure of μ.*

The harmonic mixing of a Markov random field (MRF) depends on the harmonic mixing of its sandwich measures.

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

PROPOSITION 14. *If $\mathcal{A}$ is a finite Abelian group, and μ is a semistationary MRF on $\mathcal{A}^{\mathbb{M}\times\mathbb{Z}}$ and all sandwich measures of μ are λ-EHM, then μ is λ'-EHM, where $\lambda' = \lambda/2$.*

Proof. See §5.5. □

From this follows our main result.

THEOREM 15. *Suppose $\mathcal{A}$ is a finite Abelian group, $\mathbb{U} \subset \mathbb{Z}^D$, and let $\widetilde{\mathfrak{I}} \subset \mathcal{M}[\mathcal{A}^{\mathbb{U}}]$ be a finite set of local interactions with full support. Then $\exists\lambda > 0$ so that if μ is any $\widetilde{\mathfrak{I}}$-semistationary MRF on $\mathcal{A}^{\mathbb{Z}^D}$, then μ is λ-EHM.*

Proof. (By induction on D) If $D = 1$, this is just Proposition 12.

Suppose inductively that the claim is true for MRFs on $\mathbb{Z}^{D-1}$ and let $\mu \in \mathcal{A}^{\mathbb{Z}^D}$. By Lemma 13, all sandwich measures of μ are $\mathfrak{I}$-semistationary MRFs on $\mathcal{A}^{\mathbb{Z}^{D-1}}$, where $\mathfrak{I}$ is some finite set of local interactions with full support. Thus, by the induction hypothesis, all these sandwich measures are λ-EHM for some $\lambda > 0$. Thus, by Proposition 14, μ is λ'-EHM, with $\lambda' = -\lambda/2$. □

5.4. *Markov operators.* When $\mathbf{X}$ is finite, a one-step $\mathbf{X}$-valued Markov process can be defined by a series of transition probability matrices $\{\mathbf{Q}^{(n)}\}_{n\in\mathbb{Z}}$. These matrices define linear operators on the space $\mathcal{M}[\mathbf{X};\mathbb{R}] \cong \mathbb{R}^{\mathbf{X}}$, so that, if $\zeta_n \in \mathcal{M}[\mathbf{X}]$ is the state distribution at time n, then $\mathbf{Q}^{(n)} \cdot \zeta_n = \zeta_{n+1}$ is the state distribution at time $n+1$.

When $\mathbf{X}$ is an arbitrary measurable space (with sigma-algebra $\mathcal{X}$), transition probabilities are described by linear operators on the vector space $\mathcal{M}[\mathbf{X};\mathbb{R}]$ (which, for technical reasons, we will treat as linear operators on $\mathcal{M}[\mathbf{X};\mathbb{C}]$).

Idea. Informally speaking, a *Markov operator* is a linear operator $\mathbf{Q} : \mathcal{M}[\mathbf{X};\mathbb{C}] \hookleftarrow$ mapping the set $\mathcal{M}[\mathbf{X}]$ of probability measures into itself. Suppose $(y_0, y_1) \in \mathbf{X}^{\{0,1\}}$ is a random couple and $\mathbf{Q}$ is the transition probability operator from time 0 to time 1. If $x \in \mathbf{X}$, and $\delta_x \in \mathcal{M}[\mathbf{X}]$ is the point mass at x, then the probability measure $\mathbf{q}_x := \mathbf{Q}(\delta_x)$ is the conditional state distribution of y_1 given that $y_0 = x$: for all $\mathcal{U} \subset \mathbf{X}$, $\mathbf{q}_x[\mathcal{U}] = \mathsf{Prob}[(y_1 \in \mathcal{U})/(y_0 = x)]$. When $\mathbf{X}$ is finite, measures on $\mathbf{X}$ are vectors and $\mathbf{Q}$ is a matrix and $\mathbf{q}_x$ is just the xth column of this matrix.

Suppose y_0, y_1 have distributions $\zeta_0, \zeta_1 \in \mathcal{M}[\mathbf{X}]$ respectively, with $\zeta_1 = \mathbf{Q}(\zeta_0)$. If $\phi : \mathbf{X} \longrightarrow \mathbb{C}$ is a measurable function, then the expected value of $\phi(y_1)$ is given by $\langle \phi, \zeta_1\rangle = \langle \phi, \mathbf{Q}(\zeta_0)\rangle = \langle {}^{\dagger}\mathbf{Q}(\phi), \zeta_0\rangle$, where ${}^{\dagger}\mathbf{Q}$ is the *adjoint* of $\mathbf{Q}$.

For any measurable $\mathcal{U} \subset \mathbf{X}$, let ${}^{\dagger}\mathbf{q}_{\mathcal{U}} := {}^{\dagger}\mathbf{Q}(\mathbb{1}_{\mathcal{U}})$. Thus, for any $x \in \mathbf{X}$, ${}^{\dagger}\mathbf{q}_{\mathcal{U}}(x) = {}^{\dagger}\mathbf{Q}(\mathbb{1}_{\mathcal{U}})(x) = \langle {}^{\dagger}\mathbf{Q}(\mathbb{1}_{\mathcal{U}}), \delta_x\rangle = \langle \mathbb{1}_{\mathcal{U}}, \mathbf{Q}(\delta_x)\rangle = \langle \mathbb{1}_{\mathcal{U}}, \mathbf{q}_x\rangle = \mathbf{q}_x[\mathcal{U}]$. When $\mathbf{X}$ is finite and $\mathbf{Q}$ is a matrix and $\mathcal{U} = \{u\}$ is a singleton set, then ${}^{\dagger}\mathbf{q}_{\mathcal{U}}$ is just the uth row of $\mathbf{Q}$ (or the uth column of ${}^{\dagger}\mathbf{Q}$).

We need to develop some technology to make these ideas well defined.

Formalism. If $\Phi : \mathbf{X} \longrightarrow \mathbb{C}$ is measurable, then let $\|\Phi\|_\infty = \sup_{\mathbf{x}\in\mathbf{X}} |\Phi(x)|$, and consider the Banach space $\mathcal{M}_\infty(\mathbf{X}, \mathcal{X}) = \{\Phi : \mathbf{X} \longrightarrow \mathbb{C};\ \Phi \text{ measurable}, \|\Phi\|_\infty < \infty\}$ and its unit ball, $\mathcal{B}_1 = \{\Phi \in \mathcal{M}_\infty;\ \|\Phi\|_\infty \le 1\}$. Now, $\mathcal{M}[\mathbf{X};\mathbb{C}]$ embeds into the dual

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

space $\mathcal{M}_\infty^*$ in a natural way: endow it with the appropriate weak* topology. The following results are straightforward.

LEMMA 16. *The* simple functions *of the form* $\Phi = \sum_n \phi_n \mathbb{1}_{\mathcal{U}_n}$ *are dense in* $\mathcal{M}_\infty$ *(where* $\phi_n \in \mathbb{C}$ *and* $\mathcal{U}_n \subset \mathbf{X}$ *are measurable).*

The weak topology on* $\mathcal{M}[\mathbf{X}; \mathbb{C}]$ *is determined by convergence on measurable sets. Thus, a sequence* $\{\mu_n\}_{n=1}^\infty$ *converges to* $\mu \in \mathcal{M}[\mathbf{X}; \mathbb{C}]$ *if and only if* $\mu_n[\mathcal{U}] \xrightarrow[n\to\infty]{} \mu[\mathcal{U}]$ *for all measurable* $\mathcal{U} \subset \mathbf{X}$.

If a function $\mathbf{X} \ni x \mapsto \mu_x \in \mathcal{M}[\mathbf{X}; \mathbb{C}]$ is measurable relative to the weak* Borel algebra of $\mathcal{M}[\mathbf{X}; \mathbb{C}]$ and ν is some other measure on $\mathbf{X}$, then $\mu = \int_{\mathbf{X}} \mu_x \, d\nu[x]$ is the measure so that, for all $\mathcal{U} \subset \mathbf{X}$, $\mu[\mathcal{U}] = \int_{\mathbf{X}} \mu_x[\mathcal{U}] \, d\nu[x]$; by Lemma 16, this well defines the action of μ on $\mathcal{M}_\infty$.

If $\mathbf{Q} : \mathcal{M}[\mathbf{X}; \mathbb{C}] \hookleftarrow$, then define $\|\mathbf{Q}\| := \sup_{x\in\mathbf{X}} \|\mathbf{q}_x\|_{\text{var}}$ (note: this is *not* the operator norm of $\mathbf{Q}$). Say that $\mathbf{Q}$ is *smooth* if $\mathbf{Q}$ is linear, measurable relative to the weak* Borel sigma-algebra, and $\|\mathbf{Q}\| < \infty$.

LEMMA 17.

(a) *If* $\mathbf{Q}$ *is smooth, then its adjoint* ${}^\dagger\mathbf{Q} : \mathcal{M}_\infty \hookleftarrow$ *is a well-defined, bounded linear operator and* $\| {}^\dagger\mathbf{Q}\|_\infty \leq \|\mathbf{Q}\|$.

(b) *If* $\mathbf{X} \ni x \mapsto \mathbf{q}_x \in \mathcal{M}[\mathbf{X}; \mathbb{C}]$ *is a measurable function and* $M = \sup_{x\in\mathbf{X}} \|\mathbf{q}_x\|_{\text{var}} < \infty$*, then the function* $\mathbf{Q} : \mathcal{M}[\mathbf{X}; \mathbb{C}] \hookleftarrow$ *defined:* $\mathbf{Q}(\mu) = \int_{\mathbf{X}} \mathbf{q}_x \, d\mu[x]$ *is smooth and continuous and* $\|\mathbf{Q}\| = M$.

Proof of (a). For any $\phi \in \mathcal{M}_\infty$ and any $x \in \mathbf{X}$, define $({}^\dagger\mathbf{Q}\phi)(x) = \langle \phi, \mathbf{q}_x \rangle$. Then ${}^\dagger\mathbf{Q}(\phi)$ is measurable (the function $\mathbf{X} \ni x \mapsto \delta_x \in \mathcal{M}[\mathbf{X}; \mathbb{C}]$ is measurable; hence, so is the function $(x \mapsto \mathbf{q}_x)$; thus, so is ${}^\dagger\mathbf{Q}(\phi)$). Also, $\| {}^\dagger\mathbf{Q}(\phi)\|_\infty \leq \|\phi\|_\infty \cdot \sup_{x\in\mathbf{X}} \|\mathbf{q}_x\|_{var}$.

Proof of (b). Clearly, $\mathbf{Q}$ is well defined and linear and $\|\mathbf{Q}\| = M$. To see that $\mathbf{Q}$ is continuous, let $\mathcal{U} \subset \mathbf{X}$, then $\mathbf{Q}(\mu)[\mathcal{U}] = \int_{\mathbf{X}} \mathbf{q}_x[\mathcal{U}] \, d\mu[x]$. The function $\mathbf{X} \ni x \mapsto \mathbf{q}_x[\mathcal{U}] \in \mathbb{C}$ is measurable; thus, if $\mu_n \xrightarrow[n\to\infty]{} \mu$ in the weak* topology, then $\mathbf{Q}(\mu_n)[\mathcal{U}] = \int_{\mathbf{X}} \mathbf{q}_x[\mathcal{U}] \, d\mu_n[x] \xrightarrow[n\to\infty]{} \int_{\mathbf{X}} \mathbf{q}_x[\mathcal{U}] \, d\mu[x] = \mathbf{Q}(\mu)[\mathcal{U}]$. □

We define a *Markov operator* to be a smooth linear operator on $\mathcal{M}[\mathbf{X}; \mathbb{C}]$ that maps $\mathcal{M}[\mathbf{X}]$ into itself. By Lemma 17, it suffices to define a measurable collection $(x \mapsto \mathbf{q}_x)$ of transition probability measures. We will be concerned with the following case.

Example 18. Suppose $\widetilde{\mathbb{M}} = \mathbb{M} \times \mathbb{Z}$ and $\mu \in \mathcal{M}[\mathcal{A}^{\widetilde{\mathbb{M}}}]$ is an MRF and consider the lamination process: we claim the transition probabilities are determined by a sequence $\{\mathbf{Q}^{(n)}\}_{n\in\mathbb{Z}}$ of Markov operators.

Let $\mathbb{M}_k := \mathbb{M} \times \{k\}$ for $k = n$ or $n+1$. If $\mathbf{c} \in \mathcal{A}^{\widetilde{\mathbb{M}}}$ is a μ-random configuration, then for each $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, $\mathbf{q}_{\mathbf{a}}^{(n)}$ is the conditional distribution of $\mathbf{c}|_{\mathbb{M}_{(n+1)}}$ given that $\mathbf{c}|_{\mathbb{M}_n} = \mathbf{a}$. Formally, if $\mu_{\mathbf{a}} \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$ is the conditional distribution given $\mathbf{a}$, then $\mathbf{q}_{\mathbf{a}}^{(n)} = \mathbf{pr}_{\mathbb{M}_{(n+1)}}{}^*(\mu_{\mathbf{a}})$. The map $\mathcal{A}^{\mathbb{M}} \ni \mathbf{a} \mapsto \mathbf{q}_{\mathbf{a}}^{(n)} \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$ is measurable because the map $\mathcal{A}^{\mathbb{M}_n} \ni \mathbf{a} \mapsto \mu_{\mathbf{a}} \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$ is measurable [**10**], while $\mathbf{pr}_{\mathbb{M}_{(n+1)}} : \mathcal{M}[\mathcal{A}^{\mathbb{M}}] \longrightarrow \mathcal{M}[\mathcal{A}^{\mathbb{M}_{(n+1)}}]$ is continuous. ◇

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

If $\boldsymbol{\chi} \in \mathcal{M}_\infty$, then let $\boldsymbol{\chi}_\bullet : \mathcal{M}_\infty \hookleftarrow$ be the bounded linear operator induced by multiplication with $\boldsymbol{\chi}$: for any $\phi \in \mathcal{M}_\infty$ and $x \in \mathbf{X}$, $(\boldsymbol{\chi}_\bullet\phi)(x) = \boldsymbol{\chi}(x) \cdot \phi(x)$. To establish that Markov processes on $\mathcal{A}^{\mathbb{Z}}$ were EHM (Proposition 12), we bounded the norm of operators of the form $\boldsymbol{\xi}_\bullet \circ \mathbf{Q} \circ \boldsymbol{\chi}_\bullet \circ \mathbf{P}$, where $\boldsymbol{\xi}, \boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$. We will employ a similar strategy to show that MRFs are EHM: this will require the following result.

LEMMA 19. *Let $\mathbf{Q}, \mathbf{P} : \mathcal{M}[\mathbf{X}] \hookleftarrow$ be Markov operators. For any $\phi \in \mathcal{M}_\infty$, define $\mu_x^\phi \in \mathcal{M}[\mathbf{X}; \mathbb{C}]$ by $d\mu_x^\phi = {}^\dagger\mathbf{P}(\phi) \cdot d\mathbf{q}_x$.*

(a) *For any $\boldsymbol{\chi} \in \mathcal{M}_\infty$,*

$$\| {}^\dagger\mathbf{Q} \circ \boldsymbol{\chi}_\bullet \circ {}^\dagger\mathbf{P}\|_\infty = \sup_{\phi\in\mathcal{B}_1} \sup_{x\in\mathbf{X}} |\langle \boldsymbol{\chi}, \mu_x^\phi\rangle|.$$

(b) *Suppose that $\mu \in \mathcal{M}[\mathbf{X}^{\mathbb{Z}}]$ is a Markov process and $\mathbf{Q}$ and $\mathbf{P}$ are the transition probability operators at time 0 and 1, respectively. For any $u, w \in \mathbf{X}$, let $\mu_u = \mathbf{P} \circ \mathbf{Q}(\delta_u)$ be the conditional probability measure on $\mathbf{X}$ at time 2 induced by state $u \in \mathbf{X}$ at time 0, and let μ_u^w be the sandwich measure on $\mathbf{X}$ induced by $u \in \mathbf{X}$ at time 0 and $w \in \mathbf{X}$ at time 2. Then, for any $\Phi \in \mathcal{M}_\infty$,*

$$\mu_u^\Phi = \int_{\mathbf{X}} \Phi(w) \cdot \mu_u^w \, d\mu_u[w].$$

Proof of (a). For any $\phi \in \mathcal{B}_1$ and $x \in \mathbf{X}$,

$$\begin{aligned} {}^\dagger\mathbf{Q} \circ \boldsymbol{\chi}_\bullet \circ {}^\dagger\mathbf{P}(\phi)(x) &= \langle {}^\dagger\mathbf{Q} \circ \boldsymbol{\chi}_\bullet \circ {}^\dagger\mathbf{P}(\phi), \delta_x\rangle = \langle \boldsymbol{\chi}_\bullet \circ {}^\dagger\mathbf{P}(\phi), \mathbf{Q}(\delta_x)\rangle \\ &= \langle \boldsymbol{\chi} \cdot {}^\dagger\mathbf{P}(\phi), \mathbf{q}_x\rangle = \langle \boldsymbol{\chi}, \mu_x^\phi\rangle. \end{aligned}$$

Thus,

$$\begin{aligned} \| {}^\dagger\mathbf{Q} \circ \boldsymbol{\chi}_\bullet \circ {}^\dagger\mathbf{P}\|_\infty &= \sup_{\phi\in\mathcal{B}_1} \| {}^\dagger\mathbf{Q} \circ \boldsymbol{\chi}_\bullet \circ {}^\dagger\mathbf{P}(\phi)\|_\infty \\ &= \sup_{\phi\in\mathcal{B}_1} \sup_{x\in\mathbf{X}} | {}^\dagger\mathbf{Q} \circ \boldsymbol{\chi}_\bullet \circ {}^\dagger\mathbf{P}(\phi)(x)| \\ &= \sup_{\phi\in\mathcal{B}_1} \sup_{x\in\mathbf{X}} |\langle \boldsymbol{\chi}, \mu_x^\phi\rangle|. \end{aligned}$$

Proof of (b). We want to show that, for any $\mathbf{V} \subset \mathbf{X}$,

$$\mu_u^\Phi(\mathbf{V}) = \int_{\mathbf{X}} \Phi(w) \cdot \mu_u^w(\mathbf{V}) \, d\mu_u[w].$$

First, suppose that $\mathbf{W} \subset \mathbf{X}$ and $\Phi = \mathbb{1}_{\mathbf{W}}$. Let $\mu_x^{\mathbf{W}} := \mu_x^{\mathbb{1}_{\mathbf{W}}}$; thus, $d\mu_x^{\mathbf{W}} = {}^\dagger\mathbf{p}_{\mathbf{W}} \, d\mathbf{q}_x$. Then,

$$\begin{aligned} \mu_u^{\mathbf{W}}(\mathbf{V}) &= \int_{\mathbf{V}} d\mu_u^{\mathbf{W}}[v] = \int_{\mathbf{V}} {}^\dagger\mathbf{p}_{\mathbf{W}}(v) \, d\mathbf{q}_u[v] = \int_{\mathbf{V}} \mathbf{p}_v[\mathbf{W}] \, d\mathbf{q}_u[v] \\ &= \int_{\mathbf{V}} \mu\left[\frac{x_2 \in \mathbf{W}}{x_1 = v}\right] d\mathbf{q}_u[v] \underset{\text{(a)}}{=} \int_{\mathbf{V}} \mu\left[\frac{x_2 \in \mathbf{W}}{(x_1 = v)\&(x_0 = u)}\right] d\mathbf{q}_u[v] \\ &\underset{\text{(b)}}{=} \int_{\mathbf{W}} \mu_u^w(\mathbf{V}) \, d\mu_u[w] = \int_{\mathbf{X}} \mathbb{1}_{\mathbf{W}}(w) \cdot \mu_u^w(\mathbf{V}) \, d\mu_u[w]. \end{aligned}$$

(a) follows from the Markov property. To see (b), let $\mathcal{X}_k$ be the sigma-subalgebra of $\mathbf{X}^{\mathbb{Z}}$ generated by coordinate x_k and let $\mathbf{E}_k[\bullet]$ (respectively $\mathbf{E}_{k,j}[\bullet]$) be the conditional

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

expectation with respect to $\mathcal{X}_k$ (respectively $\mathcal{X}_k \vee \mathcal{X}_j$). Let $\mathbf{W}_2 = \{\mathbf{x} \in \mathbf{X}^{\mathbb{Z}}; x_2 \in \mathbf{W}\}$ and $\mathbf{V}_1 = \{\mathbf{x} \in \mathbf{X}^{\mathbb{Z}}; x_1 \in \mathbf{V}\}$. Then,

$$\begin{aligned}
\int_{\mathbf{V}} \mu\left[\frac{x_2 \in \mathbf{W}}{(x_1 = v)\&(x_0 = u)}\right] d\mathbf{q}_u[v] &= \int_{\mathbf{V}} \mathbf{E}_{0,1}[\mathbb{1}_{\mathbf{W}_2}](u, v)\, d\mathbf{q}_u[v] \\
&= \int_{\mathbf{X}} \mathbb{1}_{\mathbf{V}} \cdot \mathbf{E}_{0,1}[\mathbb{1}_{\mathbf{W}_2}](u, v)\, d\mathbf{q}_u[v] = \mathbf{E}_0\big[\mathbb{1}_{\mathbf{V}_1} \cdot \mathbf{E}_{0,1}[\mathbb{1}_{\mathbf{W}_2}]\big](u) \\
&= \mathbf{E}_0\big[\mathbf{E}_{0,1}[\mathbb{1}_{\mathbf{V}_1} \cdot \mathbb{1}_{\mathbf{W}_2}]\big](u) = \mathbf{E}_0[\mathbb{1}_{\mathbf{V}_1} \cdot \mathbb{1}_{\mathbf{W}_2}](u) \\
&= \mathbf{E}_0\big[\mathbf{E}_{0,2}[\mathbb{1}_{\mathbf{V}_1} \cdot \mathbb{1}_{\mathbf{W}_2}]\big](u) = \mathbf{E}_0\big[\mathbb{1}_{\mathbf{W}_2} \cdot \mathbf{E}_{0,2}[\mathbb{1}_{\mathbf{V}_1}]\big](u) \\
&= \int_{\mathbf{W}} \mu\left[\frac{x_1 \in \mathbf{V}}{(x_2 = w)\&(x_0 = u)}\right] d\mu_u[w] = \int_{\mathbf{W}} \mu_u^w(\mathbf{V})\, d\mu_u[w].
\end{aligned}$$

Next, if $\Phi = \sum_n \phi_n \mathbb{1}_{\mathbf{W}_n}$ is a simple function, then ${}^{\dagger}\mathbf{P}(\Phi) = \sum_n \phi_n\, {}^{\dagger}\mathbf{p}_{\mathbf{W}_n}$, so that

$$d\mu_x^{\Phi} = {}^{\dagger}\mathbf{P}(\Phi) \cdot d\mathbf{q}_x = \sum_n \phi_n\, {}^{\dagger}\mathbf{p}_{\mathbf{W}_n}\, d\mathbf{q}_x = \sum_n \phi_n\, d\mu_x^{\mathbf{W}_n}.$$

Thus,

$$\begin{aligned}
\mu_x^{\Phi}(\mathbf{V}) = \int_{\mathbf{V}} d\mu_x^{\Phi} &= \sum_n \phi_n \cdot \int_{\mathbf{V}} d\mu_x^{\mathbf{W}_n} = \sum_n \phi_n \cdot \mu_x^{\mathbf{W}_n}[\mathbf{V}] \\
&= \sum_n \phi_n \cdot \int_{\mathbf{X}} \mathbb{1}_{\mathbf{W}_n}(w) \mu_u^w(\mathbf{V})\, d\mu_u[w] \\
&= \int_{\mathbf{X}} \left(\sum_n \phi_n \mathbb{1}_{\mathbf{W}_n}(w)\right) \cdot \mu_u^w(\mathbf{V})\, d\mu_u[w] \\
&= \int_{\mathbf{X}} \Phi(w) \cdot \mu_u^w(\mathbf{V})\, d\mu_u[w],
\end{aligned}$$

as desired. Finally, if $\{\Phi_n\}_{n=1}^{\infty}$ is a bounded sequence of simple functions so that $\Phi_n \xrightarrow[n\to\infty]{} \Phi$ in $\mathcal{M}_\infty$, then ${}^{\dagger}\mathbf{P}(\Phi_n) \xrightarrow[n\to\infty]{} {}^{\dagger}\mathbf{P}(\Phi)$ in $\mathcal{M}_\infty$, so that $\mu_x^{\Phi_n} \xrightarrow[n\to\infty]{} \mu_x^{\Phi}$ in the weak* topology on $\mathcal{M}[\mathbf{X}]$. But, by dominated convergence, we also know that

$$\mu_x^{\Phi_n}(\mathbf{V}) = \int_{\mathbf{X}} \Phi_n(w) \cdot \mu_u^w(\mathbf{V})\, d\mu_u[w] \xrightarrow[n\to\infty]{} \int_{\mathbf{X}} \Phi(w) \cdot \mu_u^w(\mathbf{V})\, d\mu_u[w];$$

hence, $\mu_x^{\Phi}(\mathbf{V}) = \int_{\mathbf{X}} \Phi(w) \cdot \mu_u^w(\mathbf{V})\, d\mu_u[w]$, for all $\mathbf{V} \subset \mathbf{X}$, as desired. □

5.5. *Uniform harmonic mixing.* Now, let $\mathbf{X} = \mathcal{A}^{\mathbb{M}}$ and consider a one-step Markov process on $\mathcal{A}^{\mathbb{M}}$ determined by a sequence of Markov operators $\{\mathbf{Q}^{(n)}; n \in \mathbb{Z}\}$. For every $n \in \mathbb{Z}$, $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$ and $\phi \in \mathcal{M}_\infty$, define ${}_n\mu_{\mathbf{a}}^{\phi} \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}; \mathbb{C}]$ so that $d\,{}_n\mu_{\mathbf{a}}^{\phi} = {}^{\dagger}\mathbf{Q}^{(n+1)}(\phi)\, d\mathbf{q}_{\mathbf{a}}^{(n)}$ as in Lemma 19.

If $\lambda > 0$, then the sequence $\{\mathbf{Q}^{(n)}; n \in \mathbb{Z}\}$ is *uniformly harmonically mixing* with *decay parameter* λ (or 'λ-UHM') if, for every $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$ and measurable $\phi \in \mathcal{B}_1$, and every $n \in \mathbb{Z}$, the measure ${}_n\mu_{\mathbf{a}}^{\phi}$ is λ-EHM. Thus, applying Lemma 19(a), we have

$$\| {}^{\dagger}\mathbf{Q}^{(n+1)} \circ \boldsymbol{\chi}_\bullet \circ {}^{\dagger}\mathbf{Q}^{(n)} \|_\infty \leq e^{-\lambda \cdot R}$$

for any $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$ with $\mathsf{rank}[\boldsymbol{\chi}] \geq R$.

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

PROPOSITION 20. *Let* $\widetilde{\mathbb{U}} = \mathbb{U} \times \{-1, 0, 1\}$ *and* $\mu \in \mathcal{M}[\mathcal{A}^{\mathbb{M}\times\mathbb{Z}}]$ *be a* $\widetilde{\mathbb{U}}$*-MRF such that for all* $n \in \mathbb{Z}$, $\mathbf{a} \in \mathcal{A}^{\mathbb{M}\times\{n\}}$ *and* $\mathbf{c} \in \mathcal{A}^{\mathbb{M}\times\{n+2\}}$, *the sandwich measure* $\mu_{\mathbf{a}}^{\mathbf{c}}$ *is* λ*-EHM. Then* $\{\mathbf{Q}^{(n)}; n \in \mathbb{Z}\}$ *is* λ*-UHM.*

Proof. Let $\phi \in \mathcal{B}_1$. By Lemma 19(b),

$$ {}_n\mu_{\mathbf{a}}^{\phi} = \int_{\mathcal{A}^{\mathbb{M}}} \phi(\mathbf{c}) \cdot \mu_{\mathbf{a}}^{\mathbf{c}} \, d\mu_{\mathbf{a}}[\mathbf{c}], $$

where $\mu_{\mathbf{a}} = \mathbf{Q}^{(n+1)} \circ \mathbf{Q}^{(n)}(\delta_{\mathbf{a}})$. By hypothesis, $\mu_{\mathbf{a}}^{\mathbf{c}}$ is λ-EHM for all $\mathbf{c} \in \mathcal{A}^{\mathbb{M}}$; apply Lemma 11 to conclude that ${}_n\mu_{\mathbf{a}}^{\phi}$ is also λ-EHM. □

PROPOSITION 21. *Let* $\mu \in \mathcal{M}[\mathcal{A}^{\mathbb{M}\times\mathbb{Z}}]$ *be the path distribution of a Markov process determined by Markov operators* $\{\mathbf{Q}^{(n)}; n \in \mathbb{Z}\}$.

If $\{\mathbf{Q}^{(n)}; n \in \mathbb{Z}\}$ *is* λ*-UHM, then* μ *is* λ'*-HM, where* $\lambda' = \lambda/2$.

Proof. Let $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}\times\mathbb{Z}}}$ with $\mathsf{rank}[\boldsymbol{\chi}] = 2R$, and suppose that $\boldsymbol{\chi} = \bigotimes_{k=0}^{2K} \boldsymbol{\chi}^{(k)}$, where, for all $k \in [0 \ldots 2K]$, $\boldsymbol{\chi}^{(k)}$ is a character on $\mathcal{A}^{\mathbb{M}\times\{n_k\}}$, with $\mathsf{rank}[\boldsymbol{\chi}^{(k)}] = R_k$, for some $n_0 < n_1 < \cdots < n_{2K}$. For any $k \in [1 \ldots 2K]$, define ${}^{\dagger}\mathbf{Q}_k = {}^{\dagger}\mathbf{Q}^{(n_k)} \circ {}^{\dagger}\mathbf{Q}^{(n_k-1)} \circ \cdots \circ {}^{\dagger}\mathbf{Q}^{(n_{(k-1)}+2)} \circ {}^{\dagger}\mathbf{Q}^{(n_{(k-1)}+1)}$.

If $\{\zeta_n; n \in \mathbb{Z}\} \subset \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$ are the state distributions of the process, then it is not hard to show that

$$ \langle \boldsymbol{\chi}, \mu \rangle = \langle {}^{\dagger}\mathbf{Q}^{(n_{(2K)}+1)} \circ \boldsymbol{\chi}_{\bullet}^{(2K)} \circ {}^{\dagger}\mathbf{Q}_{2K} \circ \boldsymbol{\chi}_{\bullet}^{(2K-1)} \circ {}^{\dagger}\mathbf{Q}_{(2K-1)} \circ \cdots \cdots \circ {}^{\dagger}\mathbf{Q}_2 \circ \boldsymbol{\chi}_{\bullet}^{(1)} \circ {}^{\dagger}\mathbf{Q}_1(\boldsymbol{\chi}^{(0)}), \zeta_{(n_{(2K)}+1)} \rangle, $$

(see, e.g., Claim 1 of Proposition 8 in [**6**]). Thus,

$$ \begin{aligned} |\langle \boldsymbol{\chi}, \mu \rangle| &\underset{(1)}{\leq} \| {}^{\dagger}\mathbf{Q}^{(n_{(2K)}+1)} \circ \boldsymbol{\chi}_{\bullet}^{(2K)} \circ {}^{\dagger}\mathbf{Q}_{2K} \circ \boldsymbol{\chi}_{\bullet}^{(2K-1)} \circ \cdots \circ {}^{\dagger}\mathbf{Q}_2 \circ \boldsymbol{\chi}_{\bullet}^{(1)} \circ {}^{\dagger}\mathbf{Q}_1(\boldsymbol{\chi}^{(0)}) \|_{\infty} \\ &\underset{(2)}{\leq} \| {}^{\dagger}\mathbf{Q}^{(n_{(2K)}+1)} \circ \boldsymbol{\chi}_{\bullet}^{(2K)} \circ {}^{\dagger}\mathbf{Q}_{2K} \circ \boldsymbol{\chi}_{\bullet}^{(2K-1)} \circ \cdots \circ {}^{\dagger}\mathbf{Q}_2 \circ \boldsymbol{\chi}_{\bullet}^{(1)} \circ {}^{\dagger}\mathbf{Q}_1 \|_{\infty} \\ &\underset{(3)}{\leq} \| {}^{\dagger}\mathbf{Q}^{(n_{(2K)}+1)} \circ \boldsymbol{\chi}_{\bullet}^{(2K)} \circ {}^{\dagger}\mathbf{Q}_{2K} \|_{\infty} \\ &\quad \times \prod_{k=1}^{K-1} \| {}^{\dagger}\mathbf{Q}_{(2k+1)} \circ \boldsymbol{\chi}_{\bullet}^{(2k)} \circ {}^{\dagger}\mathbf{Q}_{2k} \|_{\infty} \cdot \prod_{k=0}^{K-1} \| \boldsymbol{\chi}_{\bullet}^{(2k+1)} \|_{\infty} \\ &\underset{(4)}{\leq} \prod_{k=1}^{K} \| {}^{\dagger}\mathbf{Q}^{(n_{(2k)}+1)} \circ \boldsymbol{\chi}_{\bullet}^{(2k)} \circ {}^{\dagger}\mathbf{Q}^{(n_{(2k)})} \|_{\infty} \\ &\underset{(5)}{\leq} \prod_{k=1}^{K} \exp[-\lambda \cdot R_{2k}] = \exp\left[\sum_{k=1}^{K} -\lambda \cdot R_{2k} \right] = \exp\left[-\lambda \cdot \sum_{k=1}^{K} R_{2k} \right]. \end{aligned} $$

(1) Because $\zeta_{(n_{(2K)}+1)}$ is a probability measure.

(2) Because $\| \boldsymbol{\chi}^{(0)} \|_{\infty} = 1$.

(3) Separating out $\boldsymbol{\chi}_{\bullet}^{(k)}$ for all odd k.

(4) Dropping $\boldsymbol{\chi}_{\bullet}^{(k)}$ for all odd k, and ${}^{\dagger}\mathbf{Q}^{(n_{(2k)}-1)}$, ${}^{\dagger}\mathbf{Q}^{(n_{(2k)}-2)}, \ldots,$ ${}^{\dagger}\mathbf{Q}^{(n_{(2k-1)}+2)}$ for every k (because $\| {}^{\dagger}\mathbf{Q}^{(n)} \| \leq 1$ for every $n \in \mathbb{Z}$).

(5) By the UHM hypothesis and Lemma 19(a). By the same logic,

$$ |\langle \boldsymbol{\chi}, \mu \rangle| \leq \exp\left[-\lambda \cdot \sum_{k=1}^{K} R_{(2k-1)} \right]. $$

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press

Now, clearly, one of $\left(\sum_{k=1}^{K} R_{2k}\right)$ and $\left(\sum_{k=1}^{K} R_{(2k-1)}\right)$ must equal or exceed R, since together, they sum to $\mathsf{rank}[\boldsymbol{\chi}] = 2R$. Thus either

$$-\lambda \cdot \sum_{k=1}^{K} R_{2k} \leq -\lambda \cdot R \quad \text{or} \quad -\lambda \cdot \sum_{k=1}^{K} R_{(2k-1)} \leq -\lambda \cdot R.$$

Hence,

$$|\langle \boldsymbol{\chi}, \mu \rangle| \leq -\lambda \cdot R. \qquad \square$$

Proof of Proposition 14. If μ is an MRF and all sandwich measures of μ are λ-EHM, then, by Proposition 20, the sequence $\{\mathbf{Q}^{(n)}; n \in \mathbb{Z}\}$ is λ-UHM. Then, by Proposition 21, μ is λ'-HM, where $\lambda' = \lambda/2$. $\square$

6. *Conclusion*

We have demonstrated that a broad class of probability measures on $\mathcal{A}^{\mathbb{M}}$ weak* converge to Haar measure in density, when acted on by a wide class of LCA. Many interesting questions remain. For example, can we establish harmonic mixing for Markov random fields *without* full support, such as those supported on subshifts of finite type? What about measures on sofic shifts? How can we characterize either diffusion or harmonic mixing when $\mathbb{M}$ is not a lattice but instead, a non-Abelian group or monoid? Finally, what happens when $\mathcal{A}$ is a non-Abelian group? The natural analogy of LCA for non-Abelian $\mathcal{A}$ are 'multiplicative' cellular automata [**8**], where the local map is computed by (non-commutatively) multiplying the values of neighbouring coordinates. What is the asymptotic behaviour of measures under such automata?

Acknowledgement. This research is partially supported by NSERC Canada.

References

[1] A. Maass and S. Martínez. Time averages for some classes of expansive one-dimensional cellular automata. *Cellular Automata and Complex Systems*. Eds. E. Goles and S. Martínez. Kluwer, Dordrecht, 1999, pp. 37–54.

[2] P. Brémaud. *Markov Chains: Gibbs Fields, Monte Carlo Simulation, and Queues*. Springer, Berlin, 1999.

[3] H. Furstenberg. *Ergodic Theory and Combinatorial Number Theory*. Princeton University Press, Princeton, NJ, 1981.

[4] G. Hedlund. Endomorphisms and automorphisms of the shift dynamical systems. *Math. Sys. Theory* **3** (1969), 320–375.

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

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

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

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

[9] R. Kindermann and J. L. Snell. *Markov Random Fields and their Applications*. American Mathematical Society, Providence, RI, 1980.

[10] L. Schwartz. *Lectures on Disintegration of Measures*. Tata Institute of Fundamental Research, Bombay, 1975.

https://doi.org/10.1017/S0143385704000288 Published online by Cambridge University Press