Limit measures for affine cellular automata

Journal Item

Limit Measures for Affine Cellular Automata

Marcus Pivato
Department of Mathematics
University of Houston
email: `pivato@math.toronto.edu`
and
Reem Yassawi*
Department of Mathematics,
Trent University,
email: `ryassawi@trentu.ca`

August 6, 2019

Abstract

Let $\mathbb{M}$ be a monoid (e.g. $\mathbb{N}$, $\mathbb{Z}$, or $\mathbb{Z}^D$), and $\mathcal{A}$ an abelian group. $\mathcal{A}^{\mathbb{M}}$ is then 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.

Let μ be a (possibly nonstationary) probability measure on $\mathcal{A}^{\mathbb{M}}$; we develop sufficient conditions on μ and $\mathfrak{F}$ so that the sequence $\{\mathfrak{F}^N \mu\}_{N=1}^{\infty}$ weak*-converges to the Haar measure on $\mathcal{A}^{\mathbb{M}}$, in density (and thus, in Cesàro average as well). As an application, we show: if $\mathcal{A} = \mathbb{Z}_{/p}$ (p prime), $\mathfrak{F}$ is any "nontrivial" LCA on $\mathcal{A}^{(\mathbb{Z}^D)}$, and μ belongs to a broad class of measures (including most Bernoulli measures (for $D \geq 1$) and "fully supported" N-step Markov measures (when $D = 1$), then $\mathfrak{F}^N \mu$ weak*-converges to Haar measure in density.

*This research partially supported by NSERC Canada.

1 Introduction

Let $\mathcal{A}$ be a finite set, and let $\mathbb{M}$ be a monoid (e.g. $\mathbb{M} = \mathbb{Z}^D$, $\mathbb{N}^E$, or $\mathbb{Z}^D \times \mathbb{N}^E$). Let $\mathcal{A}^{\mathbb{M}}$ be the **configuration space** of $\mathbb{M}$-indexed sequences in $\mathcal{A}$. Treat $\mathcal{A}$ as a discrete space; then $\mathcal{A}^{\mathbb{M}}$ is compact and totally disconnected in the Tychonoff product topology. The action of $\mathbb{M}$ on itself by translation induces a natural **shift action** of $\mathbb{M}$ on configuration space: for all $\mathsf{e} \in \mathbb{M}$, and $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, define $\boldsymbol{\sigma}^{\mathsf{e}}[\mathbf{a}] = \left[b_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}\right]$ where, $\forall \mathsf{m}$, $b_{\mathsf{m}} = a_{\mathsf{e.m}}$, where "." is the monoid operator ("+" for $\mathbb{M} = \mathbb{Z}^D \times \mathbb{N}^E$, etc.).

A **cellular automaton** (CA) is a continuous self-map $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ which commutes with all shifts: for any $\mathsf{e} \in \mathbb{M}$, $\mathfrak{F} \circ \boldsymbol{\sigma}^{\mathsf{e}} = \boldsymbol{\sigma}^{\mathsf{e}} \circ \mathfrak{F}$. Hedlund [2] proved that any such map is determined by a **local function** $\mathfrak{f} : \mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$, where $\mathbb{U} \subset \mathbb{M}$ is some finite set (thought of as a "neighbourhood around the identity" in $\mathbb{M}$), so that, for any $\mathbf{a} = \left[a_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}\right] \in \mathcal{A}^{\mathbb{M}}$, with $\mathfrak{F}(\mathbf{a}) = \left[b_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}\right] \in \mathcal{A}^{\mathbb{M}}$, we have:

$$\forall \mathsf{m} \in \mathbb{M}, \quad b_{\mathsf{m}} \;=\; \mathfrak{f}\left(\mathbf{a}_{|(\mathsf{m}.\mathbb{U})}\right).$$

If $\mathcal{A}$ is a finite abelian group with operator "+", then $\mathcal{A}^{\mathbb{M}}$ is a compact abelian group under componentwise addition. A **linear cellular automaton** (LCA) is a CA which is also a group endomorphism from $\mathcal{A}^{\mathbb{M}}$ to itself. This is equivalent to requiring $\mathfrak{f}$ to be a group homomorphism from $\mathcal{A}^{\mathbb{U}}$ into $\mathcal{A}$. An **affine** cellular automaton (ACA) is one having a local map of the form $\mathfrak{f} = \mathfrak{h} + b$, where $\mathfrak{h} : \mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$ is a homomorphism, and $b \in \mathcal{A}$ is some constant.

The term "linear" comes from the special case when $\mathcal{A} = \mathbb{Z}_{/p}$, for some prime p. Since $\mathbb{Z}_{/p}$ is also a finite field, this map is actually a *linear* map from the $(\mathbb{Z}_{/p})$-vector space $(\mathbb{Z}_{/p})^{\mathbb{U}}$ into $\mathbb{Z}_{/p}$; it generally takes the form:

$$\mathfrak{f}\,[\mathbf{a}] \;=\; \sum_{\mathsf{u}\in\mathbb{U}} f_{\mathsf{u}} a_{\mathsf{u}} \tag{1}$$

where $\mathbf{a} = \left[a_{\mathsf{u}}|_{\mathsf{u}\in\mathbb{U}}\right]$ is an element of $\mathcal{A}^{\mathbb{U}}$, and where $\{f_{\mathsf{u}}\ ;\ \mathsf{u} \in \mathbb{U}\}$ is a set of coefficients in $\mathbb{Z}_{/p}$.

The **Haar measure** on $\mathcal{A}^{\mathbb{M}}$ is the measure $\mathcal{H}aar$ assigning mass A^{-N} to any cylinder set on N coordinates, where $A = \mathcal{C}ard\,[\mathcal{A}]$. $\mathcal{H}aar$ is $\mathfrak{F}$-invariant for any LCA $\mathfrak{F}$, raising the question: for what measures μ do the iterates $\mathfrak{F}^N\mu := \mu \circ \mathfrak{F}^{-N}$ converge to $\mathcal{H}aar$ in the weak* topology, as $N \to \infty$?

This was first investigated by D. Lind [5], who studied the LCA on $\left(\mathbb{Z}_{/2}\right)^{\mathbb{Z}}$ with local map $\mathfrak{f}(\mathbf{a}) = a_{(-1)} + a_1$. Using methods from harmonic analysis, Lind showed that, if μ is any nontrivial Bernoulli probability measure on $\left(\mathbb{Z}_{/2}\right)^{\mathbb{Z}}$, then

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathfrak{F}^N \mu \quad = \quad \mathcal{H}aar.$$

Lind also showed that the sequence of measures $\left\{\mathfrak{F}^N\mu\ ;\ N \in \mathbb{N}\right\}$ does not *itself* converge to Haar measure; for all $j \in \{2^n\ ;\ n \in \mathbb{N}\}$ the measure $\mathfrak{F}^j\mu$ is quite far from Haar.

Ferrari *et al.* [10],[9] studied LCA with local maps $\mathfrak{f}(\mathbf{a}) = k_0a_0 + k_1a_1$ acting on $\mathcal{A}^{\mathbb{N}}$, where $\mathcal{A} = \mathbb{Z}_{/q}$, $q = p^n$ for some prime p, and k_0 and k_1 are relatively prime to p, and showed Cesàro convergence to Haar measure in the weak* topology for a broad class of measures satisfying a certain "correlation decay" property, including most Bernoulli and Markov measures. These results are summarized in [1], where the authors also prove that most Markov measures on $\mathcal{A}^{\mathbb{Z}}$ will Cesàro -converge to Haar, when $\mathcal{A} = (\mathbb{Z}_{/2}) \oplus (\mathbb{Z}_{/2})$, and $\mathfrak{f} : \mathcal{A}^2 \longrightarrow \mathcal{A}$ is defined $\mathfrak{f}\left[(x_1, y_1),\ (x_2, y_2)\right] = (y_1,\ x_1 + y_2)$.

These results raise four questions:

1. Is there some broader class of measures whose $\mathfrak{F}$-iterates converge to Haar measure in Cesàro mean?

2. Rather than Cesàro convergence, can we obtain convergence in density? (If μ is stationary, then Cesàro -convergence to $\mathcal{H}^{aar}$ is equivalent to convergence in density. However, when μ is nonstationary, convergence in density is a stronger result.)

3. For what other linear CA can we prove convergence to Haar? What about affine CA?

4. Can these results be generalized to LCA on higher dimensional lattices (e.g. $\mathbb{M} = \mathbb{Z}^D$, $\mathbb{N}^D$) or nonabelian monoids such as free groups?

We address these questions by developing a sufficient condition for the sequence of measures $\left\{\mathfrak{F}^N\mu|_{N\in\mathbb{N}}\right\}$ to converge, *in density*, to Haar measure, where $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ is an LCA, and $\mathbb{M}$ is a finitely generated monoid. We require the measure μ to have a kind of mixing property, called *harmonic mixing* —we demonstrate that, for example, Bernoulli measures (on $\mathcal{A}^{\mathbb{M}}$, where $\mathbb{M}$ is any monoid) and N-step Markov measures (when $\mathbb{M}$ is $\mathbb{Z}$ or $\mathbb{N}$) have this property. We also require the automata $\mathfrak{F}$ to have a kind of "expansiveness" property, called *diffusion*, which we show is true for all "nontrivial" LCA when $\mathcal{A} = \mathbb{Z}_{/p}$.

This paper is organized as follows: in §2, we develop background on harmonic analysis over $\mathcal{A}^{\mathbb{M}}$ (§2.1) and linear cellular automata (§2.2). In §3 we discuss *harmonic mixing* and exhibit some examples of it. In §4 we discuss *diffusion* and its consequences. In §5, we show that, for any prime p and $D \geq 1$, if $\mathcal{A} = \mathbb{Z}_{/p}$, then all "nontrivial" linear cellular automata on $\mathcal{A}^{\left(\mathbb{Z}^D\right)}$ are diffusive; hence, such automata take harmonically mixing measures on $\mathcal{A}^{\left(\mathbb{Z}^D\right)}$ into Haar measure.

Notation: Elements of $\mathcal{A}$ will be written as $a, b, c, \ldots$. We often identify the elements of $\mathcal{A}$ with the set $[0..p) := \{0, 1, \ldots, p-1\}$. Sans-serif letters (e.g. $\mathsf{m}, \mathsf{n}, \mathsf{u}, \ldots$) are elements of $\mathbb{M}$. Boldface letters (e.g. $\mathbf{a}, \mathbf{b}, \ldots$) are elements of $\mathcal{A}^{\mathbb{M}}$, and $\mathbf{a} = \left[a_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}\right]$. Capitalized Gothic letters (eg. $\mathfrak{F}$, $\mathfrak{G}$) denote cellular automata. The corresponding lower-case Gothic letters (eg. $\mathfrak{f}$, $\mathfrak{g}$) denote the corresponding local maps.

2 Preliminaries

2.1 Harmonic Analysis on $\mathcal{A}^{\mathbb{M}}$

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

If $\mathcal{A} = \mathbb{Z}_{/n}$, then $\widehat{\mathcal{A}}$ is canonically isomorphic with $\mathcal{A}$. First define $\boldsymbol{\gamma} \in \widehat{\mathcal{A}}$ by

$$\boldsymbol{\gamma}(a) \quad = \quad \exp\left(\frac{2\pi\mathbf{i}}{n} a\right).$$

(where we identify $\mathcal{A}$ with $[0..n)$ in the obvious way). Then, for each $k \in \mathcal{A}$ and $a \in \mathcal{A}$, define $\boldsymbol{\gamma}^k \in \widehat{\mathcal{A}}$ by: $\boldsymbol{\gamma}^k(a) \ := \ \boldsymbol{\gamma}(k \cdot a) \ = \ \exp\left(\frac{2\pi\mathbf{i}}{n} k \cdot a\right)$, where "$k \cdot a$" refers to multiplication, mod n. Then $\widehat{\mathcal{A}} = \left\{\boldsymbol{\gamma}^k \ ; \ k \in \mathcal{A}\right\}$, and the map $\mathcal{A} \ni k \mapsto \boldsymbol{\gamma}^k \in \widehat{\mathcal{A}}$ is an isomorphism.

Let $\widehat{\mathcal{A}^{\mathbb{M}}}$ be the group of characters of $\mathcal{A}^{\mathbb{M}}$. If $\mathcal{A}$ is any abelian group, then $\widehat{\mathcal{A}^{\mathbb{M}}}$ is in bijective correspondence with the set

$$\left\{ [\chi_{\mathsf{m}}|_{\mathsf{m} \in \mathbb{M}}] \ \in \ \left(\widehat{\mathcal{A}}\right)^{\mathbb{M}} \ ; \ \chi_{\mathsf{m}} = 1\!\!1 \ \text{ for all but finitely many } \mathsf{m} \in \mathbb{M} \right\}.$$

If $\left[\chi_{\mathsf{m}}|_{\mathsf{m} \in \mathbb{M}}\right]$ is such a sequence, then define

$$\boldsymbol{\chi} \ = \ \bigotimes_{\mathsf{m} \in \mathbb{M}} \chi_{\mathsf{m}} \ \in \ \widehat{\mathcal{A}^{\mathbb{M}}}.$$

That is: if $\mathbf{a} \ = \ \left[a_{\mathsf{m}}|_{\mathsf{m} \in \mathbb{M}}\right]$ is an element of $\mathcal{A}^{\mathbb{M}}$, then $\boldsymbol{\chi}(\mathbf{a}) \ = \ \prod_{\mathsf{m} \in \mathbb{M}} \chi_{\mathsf{m}}(a_{\mathsf{m}})$, (where all but finitely many terms in this product are equal to 1.) The sequence $\left[\chi_{\mathsf{m}}|_{\mathsf{m} \in \mathbb{M}}\right]$ is called the **coefficient system** of $\boldsymbol{\chi}$. The **rank** of the character $\boldsymbol{\chi}$ is the number of nontrivial entries in $\left[\chi_{\mathsf{m}}|_{\mathsf{m} \in \mathbb{M}}\right]$.

For example, if $\mathcal{A} = \mathbb{Z}_{/n}$, then $\widehat{\mathcal{A}^{\mathbb{M}}}$ is naturally isomorphic to the group

$$\left\{ [\chi_{\mathsf{m}}|_{\mathsf{m} \in \mathbb{M}}] \ \in \ \mathcal{A}^{\mathbb{M}} \ ; \ \chi_{\mathsf{m}} = 0 \ \text{ for all but finitely many } \mathsf{m} \in \mathbb{M} \right\}.$$

If $\left[\chi_{\mathsf{m}}|_{\mathsf{m} \in \mathbb{M}}\right]$ is such a sequence, then let $\boldsymbol{\chi} = \bigotimes_{\mathsf{m} \in \mathbb{M}} \boldsymbol{\gamma}^{\chi_{\mathsf{m}}} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathbb{T}^1$. Thus, if $\mathbf{a} \ = \ \left[a_{\mathsf{m}}|_{\mathsf{m} \in \mathbb{M}}\right]$ is an element of $\mathcal{A}^{\mathbb{M}}$, then $\boldsymbol{\chi}(\mathbf{a}) \ = \ \prod_{\mathsf{m} \in \mathbb{M}} \exp\left(\frac{2\pi\mathbf{i}}{p} \chi_{\mathsf{m}} \cdot a_{\mathsf{m}}\right)$.

Let $\mathcal{M}_{\mathcal{EAS}}\left[\mathcal{A}^{\mathbb{M}}\right]$ be the space of (possibly nonstationary) probability measures on $\mathcal{A}^{\mathbb{M}}$. If $\mu \in \mathcal{M}_{\mathcal{EAS}}\left[\mathcal{A}^{\mathbb{M}}\right]$, then the **Fourier coefficients** of μ are defined:

$$\widehat{\mu}[\chi] \ = \ \langle \mu, \chi \rangle \ = \ \int_{\mathcal{A}^{\mathbb{M}}} \chi \, d\mu,$$

for all $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$. These coefficients completely identify μ. We will use the following basic result from harmonic analysis:

Theorem 1: *If* $\mu_1, \mu_2, \mu_3, \ldots, \mu_\infty \in \mathcal{M}_{\mathcal{EAS}}\left[\mathcal{A}^{\mathbb{M}}\right]$, *then*

$$\left(\widehat{\mu_n}[\boldsymbol{\chi}] \xrightarrow[n\to\infty]{} \widehat{\mu_\infty}[\boldsymbol{\chi}] \text{ for all } \boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}} \right) \iff \left(\mu_n \xrightarrow[n\to\infty]{} \mu_\infty \text{ in the weak*-topology} \right).$$

2.2 Linear Cellular Automata

If $\mathcal{A} = \mathbb{Z}_{/n}$, and $\mathfrak{f} : \mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$ is a homomorphism, then there is a unique collection of constant **coefficients** $\left[f_{\mathsf{u}}|_{\mathsf{u}\in\mathbb{U}}\right] \in \mathcal{A}^{\mathbb{U}}$ so that, for any $\mathbf{a} = \left[a_{\mathsf{u}}|_{\mathsf{u}\in\mathbb{U}}\right] \in \mathcal{A}^{\mathbb{U}}$, we have: $\mathfrak{f}(\mathbf{a}) = \sum_{\mathsf{u}\in\mathbb{U}} f_{\mathsf{u}} a_{\mathsf{u}}$. Thus, if $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ is the corresponding LCA, then, $\forall\ \mathbf{a} = \left[a_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}\right] \in \mathcal{A}^{\mathbb{M}}$, $\mathfrak{F}(\mathbf{a}) = \sum_{\mathsf{u}\in\mathbb{U}} f_{\mathsf{u}} \cdot \boldsymbol{\sigma}^{\mathsf{u}}(\mathbf{a})$. In other words, we can formally write $\mathfrak{F}$ as a "polynomial of shift maps":

$$\mathfrak{F} = \sum_{\mathsf{u}\in\mathbb{U}} f_{\mathsf{u}} \cdot \boldsymbol{\sigma}^{\mathsf{u}}.$$

This defines an isomorphism of between the ring of LCA over $\mathcal{A}^{\mathbb{M}}$ and the ring of formal polynomials with coefficients in $\mathcal{A}$ and "powers" in $\mathbb{M}$. Composition of cellular automata corresponds to multiplication of these polynomials.

Proposition 2:

$$\textit{If } \mathfrak{F} = \sum_{\mathsf{u}\in\mathbb{U}} f_{\mathsf{u}} \boldsymbol{\sigma}^{\mathsf{u}}, \textit{ and } \mathfrak{G} = \sum_{\mathsf{v}\in\mathbb{V}} g_{\mathsf{v}} \boldsymbol{\sigma}^{\mathsf{v}}, \quad \textit{then } \mathfrak{F}\circ\mathfrak{G} = \sum_{\mathsf{k}\in\mathbb{M}} \left(\sum_{\substack{\mathsf{u}\in\mathbb{U},\ \mathsf{v}\in\mathbb{V} \\ \mathsf{u}.\mathsf{v}=\mathsf{k}}} f_{\mathsf{u}} g_{\mathsf{v}} \right) \boldsymbol{\sigma}^{\mathsf{k}}.$$

□

If $\mathfrak{F}$ is a linear cellular automata with coefficient system $\mathbf{f} = \left[f_{\mathsf{u}}|_{\mathsf{u}\in\mathbb{U}}\right]$, and χ is a character with coefficient system $\boldsymbol{\chi} = \left[\chi_{\mathsf{m}}|_{\mathsf{m}\in\mathbb{M}}\right]$, then define $\boldsymbol{\chi} * \mathbf{f} = \left[\xi_{\mathsf{k}}|_{\mathsf{k}\in\mathbb{M}}\right]$, where, for all $k \in \mathbb{M}$, $\xi_k \in \mathcal{A}$ is defined:

$$\xi_k = \sum_{\substack{\mathsf{u}\in\mathbb{U},\ \mathsf{m}\in\mathbb{M} \\ \mathsf{m}.\mathsf{u}=\mathsf{k}}} (\chi_{\mathsf{m}} \cdot f_{\mathsf{u}})$$

(almost all terms in this sum are equal to 0). Then it is not hard to show:

Proposition 3: *If* $\chi \in \widehat{\mathcal{A}^{\mathbb{M}}}$ *and* $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ *are determined by coefficient systems* $\boldsymbol{\chi}$ *and* $\mathbf{f}$ *respectively, then* $\chi \circ \mathfrak{F}$ *is also a character, and is determined by coefficient system* $\boldsymbol{\chi} * \mathbf{f}$. □

3 Harmonic Mixing

A measure μ on $\mathcal{A}^{\mathbb{M}}$ is called **harmonically mixing** if, for all $\epsilon > 0$, there is some $R > 0$ so that, for all $\chi \in \widehat{\mathcal{A}^{\mathbb{M}}}$, $\Big(\mathsf{rank}\,[\chi] > R \Big) \implies \Big(|\widehat{\mu}[\chi]| < \epsilon \Big)$. (Notice that this definition does not require μ to be stationary.)

For example, $\mathcal{H}^{aar}$ is harmonically mixing; indeed, for all χ except the trivial character $\mathbb{1}$, we have: $\langle \chi,\ \mathcal{H}^{aar} \rangle \ = \ 0$.

Let $\mathcal{M}eas\left[\mathcal{A}^{\mathbb{M}};\mathbb{C}\right]$ be the Banach algebra of complex-valued measures (with convolution operator "$*$" and the total variation norm "$\|\bullet\|_{var}$"), and let $\mathcal{H} \subset \mathcal{M}eas\left[\mathcal{A}^{\mathbb{M}};\mathbb{C}\right]$ be the set of harmonically mixing measures.

Proposition 4: *$\mathcal{H}$ is an ideal of $\mathcal{M}eas\left[\mathcal{A}^{\mathbb{M}};\mathbb{C}\right]$, closed under $\|\bullet\|_{var}$.*

Proof: $\mathcal{H}$ is clearly closed under linear operations. To show that $\mathcal{H}$ is a convolution ideal, use the fact that $\widehat{\mu * \nu} = \widehat{\mu} \cdot \widehat{\nu}$ and that $\widehat{\nu}$ is bounded by $\|\nu\|_{var}$. Thus, if μ is harmonically mixing, then so are $\mu * \nu$ and $\nu * \mu$.

To show closure in $\|\bullet\|_{var}$, use the fact that, for any measures μ and ν, $\|\mu - \nu\|_{var} \ = \ \sup\left\{|\langle \phi, \mu\rangle - \langle \phi, \nu\rangle| \ ; \ \phi \in \mathbf{C}\left(\mathcal{A}^{\mathbb{M}};\mathbb{C}\right), \ \ \|\phi\|_{\infty} = 1\right\}$. □

Not all measures on $\mathcal{A}^{\mathbb{M}}$ are harmonically mixing. For example, $\mathsf{m} \in \mathbb{M}$, we say $\mu \in \mathcal{M}eas\left[\mathcal{A}^{\mathbb{M}}\right]$ is m**-quasiperiodic** if there is an orthonormal basis $\{\boldsymbol{\xi}_n|_{n\in\mathbb{N}}\}$ of $\mathbf{L}^2\left(\mathcal{A}^{\mathbb{M}};\ \mu\right)$, consisting entirely of eigenfunctions of the shift map $\boldsymbol{\sigma}^{\mathsf{m}}$. It is not difficult to show that, if μ is m-quasiperiodic for any $\mathsf{m} \neq \mathbf{Id}_{\mathbb{M}}$, then μ is not harmonically mixing.

Also, if $\boldsymbol{\chi} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathbb{T}^1$ is a nontrivial character, then the **Markov subgroup** ([12], [6], [4]) induced by $\boldsymbol{\chi}$ is defined:

$$\mathcal{A}^{\mathbb{M}}_{\boldsymbol{\chi}} \ := \ \left\{\mathbf{a} \in \mathcal{A}^{\mathbb{M}} \ ; \ \boldsymbol{\chi} \circ \boldsymbol{\sigma}^{\mathsf{m}}(\mathbf{a}) \ = \ 1, \ \forall \mathsf{m} \in \mathbb{M}\right\}.$$

If $\mathcal{A}^{\mathbb{M}}_{\boldsymbol{\chi}}$ is nontrivial, it is a subshift of finite type. If μ is a stationary probability measure on $\mathcal{A}^{\mathbb{M}}_{\chi}$, then μ cannot be harmonically mixing: if $\mathsf{m}_1, \ldots, \mathsf{m}_K \in \mathbb{M}$ are spaced widely enough apart, and $\boldsymbol{\xi} \ := \ \prod_{k=1}^{K} \boldsymbol{\chi} \circ \boldsymbol{\sigma}^{\mathsf{m}_k}$, then $\langle \mu,\ \boldsymbol{\xi}\rangle \ = \ 1$, no matter how large K becomes.

However, μ may still be harmonically mixing relative to the elements of $\widehat{\mathcal{A}^{\mathbb{M}}_{\boldsymbol{\chi}}}$; see Corollary 13.

3.1 Harmonic Mixing of Bernoulli Measures

Proposition 5: *Let $\mathcal{A} = \mathbb{Z}_{/p}$, where p is prime. Let β be any measure on $\mathcal{A}$ which is* not *entirely concentrated on one point. Let $\beta^{\otimes\mathbb{M}} \ = \ \bigotimes_{\mathsf{m}\in\mathbb{M}} \beta$ be the corresponding Bernoulli measure on $\mathcal{A}^{\mathbb{M}}$. Then $\beta^{\otimes\mathbb{M}}$ is harmonically mixing.*

Proof: $\forall k \in \mathcal{A}$, let $c_k := \langle \boldsymbol{\gamma}^k, \beta \rangle$, where $\boldsymbol{\gamma}^k \in \widehat{\mathcal{A}}$ is as in §2.1. Since p is prime, $|c_k| < 1$, unless $k = 0$, while $c_0 = 1$. Thus, $c := \max_{0<k<p} |c_k| < 1$. Thus, if $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$ and $\mathsf{rank}[\boldsymbol{\chi}] = R$, then $\left|\langle \boldsymbol{\chi}, \beta^{\otimes \mathbb{M}} \rangle\right| = \left| \left\langle \bigotimes_{\mathsf{m} \in \mathbb{M}} \chi_{\mathsf{m}}, \bigotimes_{\mathsf{m} \in \mathbb{M}} \beta \right\rangle \right| = \left| \prod_{\mathsf{m} \in \mathbb{M}} \langle \chi_{\mathsf{m}}, \beta \rangle \right| < c^R$ becomes arbitrarily small as R gets large. □

A similar argument shows:

Proposition 6: *Let $\mathcal{A}$ be an arbitrary finite abelian group, and β a measure on $\mathcal{A}$. Suppose that, for any subgroup $\mathcal{G} \subset \mathcal{A}$, the support of μ extends over* more than one *coset of $\mathcal{G}$. Then $\beta^{\otimes \mathbb{M}}$ is harmonically mixing.* □

Corollary 7: *$\mathcal{H}$ is weak* dense in $\mathcal{M}_{\mathcal{EAS}}\left[\mathcal{A}^{\mathbb{M}}\right]$.*

Proof: Let $\mu \in \mathcal{M}_{\mathcal{EAS}}\left[\mathcal{A}^{\mathbb{M}}\right]$ be arbitrary. For any $\epsilon \in [0,1]$, let $\nu_\epsilon = \beta_\epsilon^{\otimes \mathbb{M}} \in \mathcal{M}_{\mathcal{EAS}}\left[\mathcal{A}^{\mathbb{M}}\right]$ be the Bernoulli measure with one-dimensional marginal β_ϵ, where $\beta_\epsilon[0] = 1 - \epsilon$, and, for all $a \in \mathcal{A} \setminus \{0\}$, $\beta_\epsilon[a] = \epsilon/(A-1)$ (where $A = \mathcal{C}\!\mathit{ard}\,[\mathcal{A}]$). $\nu_\epsilon \in \mathcal{H}$ by Proposition 3.1 so $\nu_\epsilon * \mu \in \mathcal{H}$ also, by Proposition 4.

We want to show that $\mathbf{wk}^*\text{-}\lim_{\epsilon \to 0} \nu_\epsilon * \mu = \mu$; it is equivalent to show that $\lim_{\epsilon \to 0} \widehat{\nu_\epsilon * \mu} = \widehat{\mu}$, pointwise. Clearly, $\mathbf{wk}^*\text{-}\lim_{\epsilon \to 0} \nu_\epsilon = \delta_0$, where δ_0 is the point mass on the constant zero configuration $0 \in \mathcal{A}^{\mathbb{M}}$. Thus, for any $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$, $\widehat{\nu_\epsilon * \mu}(\boldsymbol{\chi}) = \widehat{\nu_\epsilon}(\boldsymbol{\chi}) \cdot \widehat{\mu}(\boldsymbol{\chi}) \xrightarrow[\epsilon \to 0]{} \widehat{\delta_0}(\boldsymbol{\chi}) \cdot \widehat{\mu}(\boldsymbol{\chi}) = \boldsymbol{\chi}(0) \cdot \widehat{\mu}(\boldsymbol{\chi}) = \widehat{\mu}(\boldsymbol{\chi})$. □

3.2 Harmonic Mixing of Markov Measures

Now let $\mathbb{M} = \mathbb{Z}$, and suppose that μ is a **Markov measure** on $\mathcal{A}^{\mathbb{Z}}$, is determined by the transition probability matrix $\underline{\overline{\mathbf{Q}}} = \left[q_b^a|_{a,b \in \mathcal{A}}\right]$, with stationary probability vector $\boldsymbol{\nu} = \left[\nu_a|_{a \in \mathcal{A}}\right]$, so that $\underline{\overline{\mathbf{Q}}} \cdot \boldsymbol{\nu} = \boldsymbol{\nu}$. Thus, if $\mathbf{c} \in \mathcal{A}^{\mathbb{Z}}$ is a μ-random configuration, then $\boldsymbol{\nu}_a = \mathbf{P}_{\mathit{rob}}[c_0 = a]$, and $q_b^a := \mathbf{P}_{\mathit{rob}}[c_1 = b \mid c_0 = a]$.

Proposition 8: *Let $\mathcal{A}$ be any finite abelian group. If all entries of $\underline{\overline{\mathbf{Q}}}$ are nonzero, then μ is harmonically mixing.*

Proof: Let $\mathbb{C}^{\mathcal{A}}$ be the set of all functions $\xi : \mathcal{A} \longrightarrow \mathbb{C}$.

Define the operator $\mathcal{Q} : \mathbb{C}^{\mathcal{A}} \longrightarrow \mathbb{C}^{\mathcal{A}}$ as follows: for any $\xi \in \mathbb{C}^{\mathcal{A}}$ and any $a \in \mathcal{A}$,

$$\mathcal{Q}[\xi](a) = \sum_{b \in \mathcal{A}} q_b^a \xi(b).$$

In other words, $\mathcal{Q}[\xi](a) = \langle \xi, \mathbf{q}^a \rangle$, where $\mathbf{q}^a$ is the "ath" column of the matrix $\underline{\overline{\mathbf{Q}}}$, and we treat ξ as an $\mathcal{A}$-indexed vector.

Next, for any $\chi \in \widehat{\mathcal{A}}$, define the multiplication-by-χ operator: $\mathcal{M}_\chi : \mathbb{C}^{\mathcal{A}} \longrightarrow \mathbb{C}^{\mathcal{A}}$ so that, for any $\xi \in \mathbb{C}^{\mathcal{A}}$ and any $a \in \mathcal{A}$, $\mathcal{M}_\chi[\xi](a) = \chi(a) \cdot \xi(a)$.

Now, suppose $\boldsymbol{\chi} = \chi_0 \otimes \chi_1 \otimes \ldots \otimes \chi_N$ is a character on $\mathcal{A}^{\mathbb{M}}$ (in other words, $\boldsymbol{\chi} = \bigotimes_{n \in \mathbb{Z}} \chi_{\mathsf{n}}$, but $\chi_{\mathsf{n}} = \mathbb{1}$ for all $n > N$ and $n < 0$).

Claim 1:

(a) If $N \geq 1$, then $\langle \boldsymbol{\chi}, \mu \rangle = \left\langle \mathcal{M}_{\chi_0} \circ \mathcal{Q} \circ \mathcal{M}_{\chi_1} \circ \mathcal{Q} \circ \ldots \circ \mathcal{M}_{\chi_{N-1}} \circ \mathcal{Q}[\chi_N], \ \boldsymbol{\nu} \right\rangle$.

(b) For any $\phi \in \mathbb{C}^{\mathcal{A}}$ and any $\boldsymbol{\chi} \in \widehat{\mathcal{A}}$, $\|\mathcal{M}_\chi[\phi]\|_\infty = \|\phi\|_\infty$.

(c) For any non*constant $\phi \in \mathbb{C}^{\mathcal{A}}$,* $\|\mathcal{Q}[\phi]\|_\infty < \|\phi\|_\infty$.

Proof: (a) is just linear algebra. (b) is because, $\forall a \in \mathcal{A}$, $|\chi(a)| = 1$. To see (c), note that, $\forall a \in \mathcal{A}$, $|\mathcal{Q}[\phi](a)| = \left| \sum_{b \in \mathcal{A}} q_b^a \phi(b) \right| \leq \sum_{b \in \mathcal{A}} q_b^a \, |\phi(b)| \leq \sup_{b \in \mathcal{A}} |\phi(b)| = \|\phi\|_\infty$. The first (triangle) inequality is an equality if and only if all the elements of $\{\phi(b) \ ; \ b \in \mathcal{A}\}$ have the same phase angle. The second inequality is an equality if and only if they all have the same magnitude. Hence, $|\mathcal{Q}[\phi](a)| \leq \|\phi\|_\infty$, with equality if and only if ϕ is constant. .... □ `[Claim 1]`

Now, for any $\xi, \zeta \in \widehat{\mathcal{A}}$, with $\zeta \neq \mathbb{1}$, define $\mathcal{P}_{\xi,\zeta} := \mathcal{M}_\xi \circ \mathcal{Q} \circ \mathcal{M}_\zeta \circ \mathcal{Q}$. Then $\mathcal{P}_{\xi,\zeta} : \mathbb{C}^{\mathcal{A}} \longrightarrow \mathbb{C}^{\mathcal{A}}$ is a linear operator. If $\mathbb{C}^{\mathcal{A}}$ is endowed with the $\|\bullet\|_\infty$ norm, then let $\|\mathcal{P}_{\xi,\zeta}\|_\infty$ be the operator norm of $\mathcal{P}_{\xi,\zeta}$.

Claim 2: $\|\mathcal{P}_{\xi,\zeta}\|_\infty < 1$.

Proof: Let $\phi \in \mathbb{C}^{\mathcal{A}}$, with $\|\phi\|_\infty = 1$. If ϕ is *not* constant, then by **Claim** 1c, $\|\mathcal{Q}[\phi]\|_\infty < 1$; thus, by **Claim** 1b and **Claim** 1c, $\|\mathcal{M}_\xi \circ \mathcal{Q} \circ \mathcal{M}_\zeta \circ \mathcal{Q}[\phi]\|_\infty \leq \|\mathcal{Q}[\phi]\|_\infty < 1$. If ϕ *is* constant, then $\mathcal{M}_\zeta \circ \mathcal{Q}[\phi]$ is *not* constant; thus, by **Claim** 1c, $\|\mathcal{M}_\xi \circ \mathcal{Q} \circ \mathcal{M}_\zeta \circ \mathcal{Q}[\phi]\|_\infty < \|\mathcal{M}_\zeta \circ \mathcal{Q}[\phi]\|_\infty \leq \|\phi\|_\infty = 1$.
$\mathbb{C}^{\mathcal{A}}$ is finite-dimensional, so the unit ball $\mathbb{B}$ relative to the supremum norm $\|\bullet\|_\infty$ is compact; hence $\|\mathcal{P}_{\xi,\zeta}\|_\infty = \sup_{\phi \in \mathbb{B}} \|\mathcal{P}_{\xi,\zeta}[\phi]\|_\infty < 1$. □ `[Claim 2]`

Thus, for all $\xi, \zeta \in \widehat{\mathcal{A}}$, with $\zeta \neq \mathbb{1}$, let $c_{\xi,\zeta} := \|\mathcal{P}_{\xi,\zeta}\|_\infty$, and let

$$C := \max \left\{ c_{\xi,\zeta} \ ; \ \xi, \zeta \in \widehat{\mathcal{A}} \text{ and } \zeta \neq \mathbb{1} \right\}$$

Thus, since $c_{\xi,\zeta} < 1$ for all ξ, ζ, and since $\widehat{\mathcal{A}}$ is finite, we conclude that $C < 1$ also. So, given any $\epsilon > 0$, if K is large enough, then $C^K < \epsilon$.

Now, if $\mathsf{rank}\,[\boldsymbol{\chi}] > 2K$, then the product: $\boldsymbol{\chi} \;=\; \chi_0 \otimes \chi_1 \otimes \ldots \otimes \chi_N$ can be rewritten:

$$\begin{aligned}\boldsymbol{\chi} \quad = \quad & \Bigg(\underbrace{\mathbb{1} \otimes \ldots \otimes \mathbb{1}}_{n_0}\Bigg) \otimes (\xi_1 \otimes \zeta_1) \otimes \Bigg(\underbrace{\mathbb{1} \otimes \ldots \otimes \mathbb{1}}_{n_1}\Bigg) \otimes (\xi_2 \otimes \zeta_2) \otimes \ldots \\ & \ldots \otimes \Bigg(\underbrace{\mathbb{1} \otimes \ldots \otimes \mathbb{1}}_{n_{R-1}}\Bigg) \otimes (\xi_R \otimes \zeta_R) \otimes \Bigg(\underbrace{\mathbb{1} \otimes \ldots \otimes \mathbb{1}}_{n_R}\Bigg),\end{aligned}$$

where $R > K$, and, for all $r \in [0..R)$, ξ_r, ζ_r are successive elements in the list $\chi_0, \chi_1, \ldots, \chi_{N-1}$, with $\zeta_r \neq \mathbb{1}$, and where $n_0, n_1, \ldots, n_R \geq 0$, so that $n_0 + n_1 + \ldots + n_R + 2R \;=\; N$. Thus, the operator $\mathcal{M}_{\chi_0} \circ \mathcal{Q} \circ \mathcal{M}_{\chi_1} \circ \mathcal{Q} \circ \ldots \circ \mathcal{M}_{\chi_{N-1}} \circ \mathcal{Q}$ can be rewritten as
$(\mathcal{Q}^{n_0} \circ \mathcal{P}_{\xi_1,\zeta_1}) \circ (\mathcal{Q}^{n_1} \circ \mathcal{P}_{\xi_2,\zeta_2}) \circ \ldots \circ (\mathcal{Q}^{n_{R-1}} \circ \mathcal{P}_{\xi_R,\zeta_R}) \circ \mathcal{Q}^{n_R}$. But then

$$\begin{aligned}
\left|\langle \boldsymbol{\chi}, \mu\rangle\right| \quad &=_{(1)} \quad \left|\left\langle \mathcal{M}_{\chi_0} \circ \mathcal{Q} \circ \mathcal{M}_{\chi_1} \circ \mathcal{Q} \circ \ldots \circ \mathcal{M}_{\chi_{N-1}} \circ \mathcal{Q}[\chi_N], \;\; \boldsymbol{\nu}\right\rangle\right| \\
&\leq_{(2)} \quad \left\|\mathcal{M}_{\chi_0} \circ \mathcal{Q} \circ \mathcal{M}_{\chi_1} \circ \mathcal{Q} \circ \ldots \circ \mathcal{M}_{\chi_{N-1}} \circ \mathcal{Q}[\chi_N]\right\|_\infty \\
&\leq_{(3)} \quad \left\|\mathcal{M}_{\chi_0} \circ \mathcal{Q} \circ \mathcal{M}_{\chi_1} \circ \mathcal{Q} \circ \ldots \circ \mathcal{M}_{\chi_{N-1}} \circ \mathcal{Q}\right\|_\infty \\
&= \quad \|(\mathcal{Q}^{n_0} \circ \mathcal{P}_{\xi_1,\zeta_1}) \circ (\mathcal{Q}^{n_1} \circ \mathcal{P}_{\xi_2,\zeta_2}) \circ \ldots \\
&\qquad\qquad \ldots \circ (\mathcal{Q}^{n_{R-1}} \circ \mathcal{P}_{\xi_R,\zeta_R}) \circ \mathcal{Q}^{n_R}\|_\infty \\
&\leq \quad \|\mathcal{P}_{\xi_1,\zeta_1}\|_\infty \cdot \|\mathcal{P}_{\xi_2,\zeta_2}\|_\infty \cdot \ldots \cdot \|\mathcal{P}_{\xi_R,\zeta_R}\|_\infty \\
&\leq \quad C^R \;\; < \;\; C^K \;\; < \;\; \epsilon
\end{aligned}$$

(1) by **Claim** 1a. (2) $\boldsymbol{\nu}$ is a probability measure. (3) $\|\chi_N\|_\infty = 1$.

In summary, if $\mathsf{rank}\,[\boldsymbol{\chi}] > 2R$, then $|\langle \boldsymbol{\chi}, \mu\rangle| < \epsilon$. □

Corollary 9: *Let $\mathcal{A}$ and μ be as in Theorem 8, and suppose ν is a measure on $\mathcal{A}^{\mathbb{Z}}$ absolutely continuous relative to μ. Then ν is also harmonically mixing .*

Proof: Let $\phi = \dfrac{d\nu}{d\mu}$, and suppose first that $\phi = \dfrac{\mathbb{1}_{[\mathbf{a}]}}{\mu[\mathbf{a}]}$ is the (renormalized) characteristic function of some cylinder set $[\mathbf{a}] = \left\{\mathbf{b} \in \mathcal{A}^{\mathbb{Z}} \; ; \; \mathbf{b}_{\mathbb{U}} \;=\; \mathbf{a}\right\}$, where $\mathbb{U} = [-U \ldots U] \subset \mathbb{Z}$ and $\mathbf{a} \in \mathcal{A}^{\mathbb{U}}$. Thus $\nu = \mu_{[\mathbf{a}]}$, the (renormalized) restriction of μ to a probability measure on $[\mathbf{a}]$ (that is: $\nu(B) = \mu\left([\mathbf{a}] \cap B\right)/\mu\left([\mathbf{a}]\right)$ for any measurable $B \subset \mathcal{A}^{\mathbb{Z}}$).

Let $\boldsymbol{\chi} = \displaystyle\bigotimes_{n=-N}^{N} \chi_n$ be a character, and suppose $N > U$. Let $\boldsymbol{\chi}_{(-)} = \displaystyle\bigotimes_{n=-N}^{-U-1} \chi_n$ and $\boldsymbol{\chi}_{(+)} \;=\; \displaystyle\bigotimes_{n=U+1}^{N} \chi_n$. Let $\mu^{(+)}_{[\mathbf{a}]} \in \mathcal{M}_{\mathcal{EAS}}\left[\mathcal{A}^{(U\ldots\infty)}\right]$ be the projection of $\mu_{[\mathbf{a}]}$ onto coordinates $(U...\infty)$ (thus, if $\mathbf{b} \in \mathcal{A}^{(U..N]}$, then $\mu^{(+)}_{[\mathbf{a}]}[\mathbf{b}] \;=\; q^{a_U}_{b_{(U+1)}} \cdot q^{b_{(U+1)}}_{b_{(U+2)}} \cdot$

$\ldots \cdot q_{b_N}^{b_{(N-1)}}$). Similarly, let $\mu_{[\mathbf{a}]}^{(-)}$ be the projection of $\mu_{[\mathbf{a}]}$ onto coordinates $(-\infty \ldots -U)$. Thus, using the Markov property of μ,

$$\langle \boldsymbol{\chi}, \nu \rangle \;=\; \left\langle \boldsymbol{\chi}_{(-)},\ \mu_{[\mathbf{a}]}^{(-)} \right\rangle \cdot \left(\prod_{u=-U}^{U} \chi_u a_u \right) \cdot \left\langle \boldsymbol{\chi}_{(+)},\ \mu_{[\mathbf{a}]}^{(+)} \right\rangle$$

Now, analogous to Claim 1a of Theorem 8, we have:

$$\left\langle \boldsymbol{\chi}_{(-)}, \mu_{[\mathbf{a}]}^{(-)} \right\rangle \;=\; \left\langle \mathcal{M}_{\chi_{(-N)}} \circ \mathcal{Q} \circ \mathcal{M}_{\chi_{(1-N)}} \circ \mathcal{Q} \circ \ldots \circ \mathcal{M}_{\chi_{(-U-1)}} \circ \mathcal{Q}[\chi_U],\quad \mathbf{q}_{a_{(-U)}} \right\rangle,$$

where $\mathbf{q}_{a_{(-U)}}$ is the $a_{(-U)}$th "row" of transition matrix $\underline{\overline{\mathbf{Q}}}$, and, in a manner analagous to the proof of Theorem 8, we can show that

$$\left| \left\langle \boldsymbol{\chi}_{(-)},\ \mu_{[\mathbf{a}]}^{(-)} \right\rangle \right| \to 0 \quad \text{as} \quad \mathsf{rank}\left[\boldsymbol{\chi}_{(-)} \right] \to \infty.$$

By a similar argument (with reversed time), we can show

$$\left| \left\langle \boldsymbol{\chi}_{(+)},\ \mu_{[\mathbf{a}]}^{(+)} \right\rangle \right| \to 0 \quad \text{as} \quad \mathsf{rank}\left[\boldsymbol{\chi}_{(+)} \right] \to \infty.$$

This shows that ν is harmonically mixing.

The case when ϕ is **simple** —ie. a finite linear combination of characteristic functions of cylinder sets —then follows immediately, via Proposition 4. If $\phi \in \mathbf{L}^1(\mu)$ is arbitrary, let $\{\phi_n|_{n\in\mathbb{N}}\}$ be a sequence of simple functions converging to ϕ in the $\mathbf{L}^1$ norm. Let $\{\nu_n|_{n\in\mathbb{N}}\}$ be the corresponding measures (all harmonically mixing); thus, $\{\nu_n|_{n\in\mathbb{N}}\}$ converges to ν in total variation norm, so ν is also harmonically mixing, by Proposition 4. □

Notice that the measure ν need not be stationary (and will not be, unless ϕ is shift-invariant.)

An **N-step Markov process** is analogous to a Markov process, but the probability distribution of each letter is dependent upon the previous N letters, and conditionally independent of what comes before. When $N = 0$, we have a Bernoulli process; when $N = 1$, a standard Markov process. In general, an N-step process is determined by a collection of transition probabilities $\underline{\overline{\mathbf{Q}}} = \left\{ q_b^{\mathbf{a}}\ ;\ \mathbf{a} \in \mathcal{A}^{[0..N)},\ \ b \in \mathcal{A} \right\}$ so that, for each $\mathbf{a} \in \mathcal{A}^{[0..N)}$, $\sum_{b\in\mathcal{A}} q_b^{\mathbf{a}} = 1$. One can then find a (generally unique) stationary distribution $\boldsymbol{\nu}$ on $\mathcal{A}^{[0..N)}$.

Corollary 10: *Let $\mathcal{A}$ be a finite abelian group and let α be an N-step Markov process on $\mathcal{A}$, where all elements of $\underline{\overline{\mathbf{Q}}}$ are nonzero. Then α is harmonically mixing.*

Proof: Let $\mathcal{B} = \mathcal{A}^{[1..N]}$, and consider the standard N-*block coding* map $\phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{B}^{\mathbb{Z}}$, defined:

$$\phi(\ldots, a_1, \ldots, a_N, a_{N+1}, \ldots, a_{2N}, \ldots) \;=\; \left(\ldots, \begin{bmatrix} a_1 \\ \vdots \\ a_N \end{bmatrix}, \begin{bmatrix} a_{N+1} \\ \vdots \\ a_{2N} \end{bmatrix}, \ldots \right)$$

This is an isomorphism of topological groups, and the following diagram commutes:

$$\begin{array}{ccc} \mathcal{A}^{\mathbb{Z}} & \stackrel{\boldsymbol{\sigma}^N}{\longrightarrow} & \mathcal{A}^{\mathbb{Z}} \\ \phi \big\downarrow & & \big\downarrow \phi \\ \mathcal{B}^{\mathbb{Z}} & \stackrel{\boldsymbol{\sigma}}{\longrightarrow} & \mathcal{B}^{\mathbb{Z}} \end{array}$$

Thus, $\beta = \phi^*\alpha$ is a (1-step) Markov measure, with transition matrix $\underline{\overline{\mathbf{P}}} = \left[p_{\mathbf{b}}^{\mathbf{a}}|_{\mathbf{a},\mathbf{b}\in\mathcal{B}}\right]$, where $p_{(b_1,\ldots,b_N)}^{(a_1,\ldots,a_N)} = q_{b_1}^{(a_1,\ldots,a_N)} \cdot q_{b_2}^{(a_2,\ldots,a_N,b_1)} \cdot q_{b_3}^{(a_3,\ldots,a_N,b_1,b_2)} \cdot \ldots \cdot q_{b_N}^{(a_N,b_1,\ldots,b_{(N-1)})}$. Clearly, if all entries of $\underline{\overline{\mathbf{Q}}}$ are nonzero, then, so are all entries of $\underline{\overline{\mathbf{P}}}$, and thus, by Proposition 8, β is harmonically mixing. Hence, it suffices to show:

Claim 1: *If β is harmonically mixing, then so is α.*

Proof: The isomorphism $\phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{B}^{\mathbb{Z}}$ induces isomorphism $\widehat{\phi} : \widehat{\mathcal{B}^{\mathbb{Z}}} \longrightarrow \widehat{\mathcal{A}^{\mathbb{Z}}}$ given: $\widehat{\phi}(\boldsymbol{\chi}) := \boldsymbol{\chi} \circ \phi$. Thus, $\widehat{\phi}^{-1} : \widehat{\mathcal{A}^{\mathbb{Z}}} \longrightarrow \widehat{\mathcal{B}^{\mathbb{Z}}}$ is an isomorphism, and, for any $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{Z}}}$,

1. $\mathsf{rank}\left[\widehat{\phi}^{-1}(\boldsymbol{\chi})\right] \geq \dfrac{1}{N}\mathsf{rank}\left[\boldsymbol{\chi}\right]$.
2. $\left\langle \widehat{\phi}^{-1}(\boldsymbol{\chi}),\ \beta \right\rangle \ = \ \langle \boldsymbol{\chi},\ \alpha \rangle$.

Thus, if $\mathsf{rank}\left[\boldsymbol{\chi}\right]$ is large, then so is $\mathsf{rank}\left[\widehat{\phi}^{-1}(\boldsymbol{\chi})\right]$; then $\left\langle \widehat{\phi}^{-1}(\boldsymbol{\chi}),\ \beta \right\rangle$ is small, and thus so is $\langle \boldsymbol{\chi},\ \alpha \rangle$. .... □ `[Claim 1]`

□

An N-step Markov measure satisfying the hypothesis of Corollary 10 gives nonzero probability to all cylinder sets of finite length; we might say it has "full support".

The technique of Theorem 8 can be used to prove the corresponding result for stationary Markov random fields on free groups and monoids [13],[14]. Now, instead of *one* transition probability matrix, there are several: one for each generator of the group/monoid. As long as there are finitely many generators, the bound C on the operator norms in the proof of Theorem 8 will still be less than 1, and the same argument can be used to show:

Theorem 11: *Let $\mathcal{A}$ be a finite group. Let $\mathbb{M}$ be a free group or free monoid on finitely many generators, and let μ be a stationary Markov random field on $\mathcal{A}^{\mathbb{M}}$ so that all entries in all transition probability matrices are nonzero. Then μ is harmonically mixing.* □

4 Diffusive Linear Automata

Let $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ be a linear cellular automaton. We say that $\mathfrak{F}$ is **diffusive** if, for every nontrivial $\chi \in \widehat{\mathcal{A}^{\mathbb{M}}}$, $\lim_{n\to\infty} \mathsf{rank}\left[\chi \circ \mathfrak{F}^n\right] = \infty$.

For example, let $\mathcal{A} = \mathbb{Z}_{/p}$ for some prime p. Let $\mathbb{M}$ be the free group or free monoid on $D \geq 2$ generators. Let $\mathbb{U} \subset \mathbb{M}$ be a finite subset with at least two elements, so that each $\mathsf{u} \in \mathbb{U}$ is a product of at least two distinct generators. It is straightforward to show:

If $0 \neq f_{\mathsf{u}} \in \mathbb{Z}_{/p}$, *for all* $\mathsf{u} \in \mathbb{U}$, *then the automaton* $\mathfrak{F} = \sum_{\mathsf{u}\in\mathbb{U}} f_{\mathsf{u}} \boldsymbol{\sigma}^{\mathsf{u}}$ is diffusive.

Unfortunately, linear cellular automata on $\left(\mathbb{Z}_{/p}\right)^{\left(\mathbb{Z}^D\right)}$ are never diffusive: if $\mathfrak{F}$ is such an LCA (e.g. $\mathfrak{F} = f_0 + f_1 \cdot \boldsymbol{\sigma}^{\mathsf{m}_1} + f_2 \cdot \boldsymbol{\sigma}^{\mathsf{m}_2}$), then, for any $n \in \mathbb{N}$ the LCA $\mathfrak{F}^{(p^n)}$ is simply $\mathfrak{F}$, "rescaled" by a factor of p^n (e.g. $\mathfrak{F}^p = f_0 + f_1 \cdot \boldsymbol{\sigma}^{(p\cdot\mathsf{m}_1)} + f_2 \cdot \boldsymbol{\sigma}^{(p\cdot\mathsf{m}_2)}$). This follows from the **Fermat property** for the field $\mathbb{Z}_{/p}$. Thus, the polynomial of $\mathfrak{F}^{(p^n)}$ has the same number of nonzero coefficients as that of $\mathfrak{F}$, so $\mathfrak{F}$ cannot "diffuse" along the subsequence $\{p^n \,;\, n \in \mathbb{N}\}$.

This motivates a slight weakening of the concept of diffusion: we say that $\mathfrak{F}$ is **diffusive in density** if, for every nontrivial $\chi \in \widehat{\mathcal{A}^{\mathbb{M}}}$, there is a subset $\mathbb{J} \subset \mathbb{N}$ of Cesàro density 1 so that $\lim_{\substack{j\to\infty \\ j\in\mathbb{J}}} \mathsf{rank}\left[\chi \circ \mathfrak{F}^j\right] = \infty$.

Theorem 12: *Let $\mathcal{A}$ be a finite abelian group, and $\mathbb{M}$ a countable monoid. Suppose that $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ is a linear cellular automata, and suppose that μ is a measure on $\mathcal{A}^{\mathbb{M}}$ that is harmonically mixing.*

1. *If $\mathfrak{F}$ is diffusive, then* $\mathbf{wk}^*\text{-}\lim_{j\to\infty} \mathfrak{F}^j \mu = \mathcal{H}\!\mathit{aar}$.
2. *If $\mathfrak{F}$ is diffusive* in density, *then there is a set $\mathbb{J} \subset \mathbb{N}$ of Cesàro density 1 so that* $\mathbf{wk}^*\text{-}\lim_{\substack{j\to\infty \\ j\in\mathbb{J}}} \mathfrak{F}^j \mu = \mathcal{H}\!\mathit{aar}$. *Thus* $\mathbf{wk}^*\text{-}\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathfrak{F}^n \mu = \mathcal{H}\!\mathit{aar}$.

Proof: We'll prove convergence in density, from which Cesàro convergence follows immediately. The proof of strict convergence is much the same.

We'll show that the Fourier coefficients of $\mathfrak{F}^n \mu$ all converge to zero in density. Weak* convergence in density then follows by Theorem 1. So, let $\chi \in \widehat{\mathcal{A}^{\mathbb{M}}}$. Then

$$\langle \chi,\ \mathfrak{F}^n \mu \rangle = \int_{\mathcal{A}^{\mathbb{M}}} \chi \; d\left(\mathfrak{F}^n \mu\right) = \int_{\mathcal{A}^{\mathbb{M}}} \chi \circ \mathfrak{F}^n \; d\mu = \langle \left(\chi \circ \mathfrak{F}^n\right), \mu \rangle$$

Now, since $\mathfrak{F}$ is diffusive in density, we can find a subset $\mathbb{J}_\chi \subset \mathbb{N}$ of density 1 so that $\lim_{\substack{j\to\infty \\ j\in\mathbb{J}_\chi}} \mathsf{rank}\left[\chi \circ \mathfrak{F}^j\right] = \infty$. But then, since μ is harmonically mixing, it follows that $\lim_{\substack{j\to\infty \\ j\in\mathbb{J}_\chi}} \left\langle \left(\chi \circ \mathfrak{F}^j\right), \mu \right\rangle = 0$.

Now, $\mathcal{A}$ is finite and $\mathbb{M}$ is countable; thus, $\widehat{\mathcal{A}^{\mathbb{M}}}$ is countable, so we can find a "common tail set" $\mathbb{J} \subset \mathbb{N}$ so that:

- $\mathbb{J}$ has Cesàro density 1.
- For every $\chi \in \widehat{\mathcal{A}^{\mathbb{M}}}$, there is some $N > 0$ so that $\mathbb{J}_\chi \cap [N..\infty) \subset \mathbb{J}$.

(for details, see [11], Remark 6.3, Chapter 2, or [3]). Thus, for all $\chi \in \widehat{\mathcal{A}^{\mathbb{M}}}$, $\lim_{\substack{j\to\infty \\ j\in\mathbb{J}}} \langle (\chi \circ \mathfrak{F}^n), \mu \rangle = 0.$ $\square$

The same reasoning applies stationary measures supported on shift-invariant subgroups of $\mathcal{A}^{\mathbb{M}}$:

Corollary 13: *Let $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ be as in Theorem 12. Suppose that $\mathcal{G} \subset \mathcal{A}^{\mathbb{M}}$ is a closed subgroup, and μ is a measure supported on $\mathcal{G}$. Suppose μ is harmonically mixing relative to the elements of $\widehat{\mathcal{G}}$, and $\mathfrak{F}(\mathcal{G}) \subseteq \mathcal{G}$. If $\mathfrak{F}$ is diffusive (in density), then $\mathbf{wk}^*\text{–}\lim_{j\to\infty} \mathfrak{F}^j \mu = \mathcal{H}^{aar}_{\mathcal{G}}$, where $\mathcal{H}^{aar}_{\mathcal{G}}$ is the Haar measure on the compact group $\mathcal{G}$ (and where convergence is either absolute or in density, as appropriate).* $\square$

To extend these results to *affine* cellular automata, use the following:

Proposition 14: *Let $\mathcal{A}$ be any finite group. Let $\mathfrak{F} : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ be an LCA with local transformation $\mathfrak{f} : \mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$. Let $c \in \mathcal{A}$ be some constant, and let $\mathfrak{G}$ be the ACA with local map $\mathfrak{g} : \mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$ given: $\mathfrak{g}(\mathbf{a}) = \mathfrak{f}(\mathbf{a}) + c$.*

Let μ be a measure on $\mathcal{A}^{\mathbb{M}}$, and let $\mathbb{J} \subset \mathbb{N}$.

$$\text{If } \mathbf{wk}^*\text{–}\lim_{\substack{j\to\infty \\ j\in\mathbb{J}}} \mathfrak{F}^j \mu = \mathcal{H}^{aar} \quad \text{then} \quad \mathbf{wk}^*\text{–}\lim_{\substack{j\to\infty \\ j\in\mathbb{J}}} \mathfrak{G}^j \mu = \mathcal{H}^{aar}.$$

Proof: Let $\mathbf{c}_0 \in \mathcal{A}^{\mathbb{M}}$ be the constant configuration whose entries are all equal to c, and, $\forall n \in \mathbb{N}$, let $\mathbf{c}_n = \mathfrak{F}^n(\mathbf{c}_0)$. Let $\mathbf{h}_n = \mathbf{c}_0 + \mathbf{c}_1 + \ldots + \mathbf{c}_n$, and define $\mathfrak{H}_n : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ by: $\mathfrak{H}_n(\mathbf{a}) = \mathbf{a} + \mathbf{h}_n$. A simple computation establishes:

$$\forall n \in \mathbb{N}, \quad \mathfrak{G}^n = \mathfrak{H}_n \circ \mathfrak{F}^n.$$

If $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$, then for any $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, we have: $\boldsymbol{\chi} \circ \mathfrak{H}_n(\mathbf{a}) = \boldsymbol{\chi}(\mathbf{a} + \mathbf{h}_n) = K_n \cdot \boldsymbol{\chi}(\mathbf{a})$, where $K_n = \boldsymbol{\chi}(\mathbf{h}_n)$ is some element of $\mathbb{T}^1$. Concisely: $\boldsymbol{\chi} \circ \mathfrak{H}_n = K_n \cdot \boldsymbol{\chi}$.

Now, $\mathfrak{F}^n \mu$ converges in density to the Haar measure, in the weak* topology, which is equivalent to saying: for every nontrivial character $\boldsymbol{\chi}$, there is a subset $\mathbb{J} \subset \mathbb{N}$ of density one such that $\lim_{\substack{j\to\infty \\ j\in\mathbb{J}}} \left\langle \boldsymbol{\chi} \circ \mathfrak{F}^j,\ \mu \right\rangle = 0$.

Now, for any j, $\left\langle \boldsymbol{\chi} \circ \mathfrak{G}^j,\ \mu \right\rangle = \left\langle \boldsymbol{\chi} \circ \mathfrak{H}_j \circ \mathfrak{F}^j,\ \mu \right\rangle = \left\langle K_j \cdot \boldsymbol{\chi} \circ \mathfrak{F}^j,\ \mu \right\rangle = K_j \cdot \left\langle \boldsymbol{\chi} \circ \mathfrak{F}^j,\ \mu \right\rangle$. But $|K_j| = 1$, and thus,

$$\left| \left\langle \boldsymbol{\chi} \circ \mathfrak{G}^j,\ \mu \right\rangle \right| = \left| \left\langle \boldsymbol{\chi} \circ \mathfrak{F}^j,\ \mu \right\rangle \right| \xrightarrow[j\to\infty]{j\in\mathbb{J}} 0.$$

Since this is true for each character, we conclude that $\mathfrak{G}^n\mu$ also converges in density to the Haar measure. $\square$

5 Diffusion on Lattices

Say that an LCA $\mathfrak{F}$ on $\mathcal{A}^{\mathbb{M}}$ is **nontrivial** if $\mathfrak{F}$ is *not* merely a shift map or the identity map. If we write $\mathfrak{F}$ as a polynomial of shift maps, then $\mathfrak{F}$ is nontrivial if this polynomial contains two or more nonzero coefficients.

Theorem 15: *Let p be a prime number, and $\mathcal{A} = \mathbb{Z}_{/p}$. Let $D \geq 1$. Then any nontrivial linear cellular automaton on $\mathcal{A}^{(\mathbb{Z}^D)}$ is diffusive in density.*

The proof of this theorem will occupy the rest of this section. We will eventually accomplish a reduction to the case when $D = 1$; hence, the reader may initially find it helpful to assume $D = 1$, and to treat all elements of $\mathbb{Z}^D$ (indicated as vectors, eg. "$\vec{m}$") as elements of $\mathbb{Z}$ instead (indicated as scalars, eg. "m"). It will also be helpful to first work through the details of the proof in the special case when $p = 2$; we will make reference to this special case in footnotes.

We will represent LCA using the polynomial notation introduced in §2.2. It will be convenient to write these polynomials in a special recursive fashion. For example, suppose $D = 1$, and suppose that $g_0, g_1, g_2 \in [1..p)$, and $\ell_0, \ell_1, \ell_2 \in \mathbb{Z}$. Let $\mathcal{G}$ be the linear CA on $\mathcal{A}^{\mathbb{Z}}$ defined: $\mathcal{G} = g_0\boldsymbol{\sigma}^{\ell_0} + g_1\boldsymbol{\sigma}^{\ell_1} + g_2\boldsymbol{\sigma}^{\ell_2}$. Then we can rewrite $\mathfrak{G}$ as:

$$\mathfrak{G} \;=\; g_0 \cdot \left(\mathfrak{F} \circ \boldsymbol{\sigma}^{\ell_0}\right), \quad \text{where } \mathfrak{F} \;=\; \mathbf{Id} + f_1\boldsymbol{\sigma}^{m_1}\left(1 + f_2\boldsymbol{\sigma}^{m_2}\right), \tag{2}$$

with $m_1 = \ell_1 - \ell_0$, $m_2 = \ell_2 - \ell_1$, $f_1 = g_0^{-1}g_1$ and $f_2 = g_1^{-1}g_2$ (with inversion in the field $\mathbb{Z}_{/p}$)[1]. More generally, we have the following:

Lemma 16: *Let $g_0, g_1, \ldots, g_J \in [1..p)$, and $\vec{\ell}_0, \vec{\ell}_1, \ldots, \vec{\ell}_J \in \mathbb{Z}^D$, and suppose that $\mathfrak{G}$ is the linear CA on $\mathcal{A}^{(\mathbb{Z}^D)}$ defined:*

$$\mathfrak{G} \;=\; g_0\boldsymbol{\sigma}^{\vec{\ell}_0} + g_1\boldsymbol{\sigma}^{\vec{\ell}_1} + \ldots + g_J\boldsymbol{\sigma}^{\vec{\ell}_J}. \tag{3}$$

Then $\mathfrak{G} \;=\; g_0 \cdot \left(\mathfrak{F} \circ \boldsymbol{\sigma}^{\vec{\ell}_0}\right)$, *where:*

$$\mathfrak{F} \;=\; \mathbf{Id} + f_1\boldsymbol{\sigma}^{\vec{m}_1}\left(\mathbf{Id} + f_2\boldsymbol{\sigma}^{\vec{m}_2}\left[\ldots\left(\mathbf{Id} + f_{J-1}\boldsymbol{\sigma}^{\vec{m}_{J-1}}\left[\mathbf{Id} + f_J\boldsymbol{\sigma}^{\vec{m}_J}\right]\right)\ldots\right]\right) \tag{4}$$

and, for all $j \in [1..J]$, $\vec{m}_j \;=\; \vec{\ell}_j - \vec{\ell}_{j-1}$, *and* $f_j \;=\; g_{j-1}^{-1} \cdot g_j$. $\square$

[1] If $p = 2$, we can assume that $f_1 = f_2 = 1$.

Composing with the shift $\boldsymbol{\sigma}^{\vec{\ell}_0}$ and multiplying by the scalar g_0 does not affect the diffusion property; hence, it is sufficient to prove Theorem for polynomials like (4). On first reading, it may be helpful to assume that $J = 2$, as in (2).

By Proposition 2, the powers $\mathfrak{F}^N$ of the linear cellular automaton $\mathfrak{F}$ correspond to powers of the corresponding polynomial. To prove Theorem 15, we will therefore need to develop some machinery concerning multiplication of polynomials with coefficients in $\mathbb{Z}_{/p}$, by using the classical formula of Lucas [7] for the mod p binomial coefficients, which has become ubiquitous in the theory of LCA.

Definition 17: *p-ary expansion, Index set.*

If $n \in \mathbb{N}$, then the p**-ary expansion** *of n is the sequence $\mathbb{P}(n) = \{n^{[i]}\}_{i=0}^{\infty} \in [0..p)^{\mathbb{N}}$, such that $n = \sum_{i=0}^{\infty} n^{[i]} p^i$.*

The **index set** *$\mathcal{S}(n)$ of n is defined to be:* $\mathcal{S}(n) = \left\{ i \in \mathbb{N} \,;\, n^{[i]} \neq 0 \right\}.$

If $m \in \mathbb{N}$, then let $[m]_p$ be the congruence class of m, mod p.

Lucas' Theorem: *Let $N, n \in \mathbb{N}$, with p-ary expansions as before. Then*

$$\begin{bmatrix} N \\ n \end{bmatrix}_p = \prod_{k=0}^{\infty} \begin{bmatrix} N^{[k]} \\ n^{[k]} \end{bmatrix}_p$$

where we define $\begin{pmatrix} 0 \\ 0 \end{pmatrix} = 1$, *and* $\begin{pmatrix} a \\ b \end{pmatrix} = 0$, *for any $b > a > 0$.* ______□[7]

Write "$n \ll N$" if $n^{[i]} \leq N^{[i]}$ for all $i \in \mathbb{N}$. Thus, Lucas' Theorem implies:

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

If $n \in \mathbb{N}$, then the **Lucas set** of n is the set $\mathcal{L}(n) := \{k \in \mathbb{N} \,;\, k \ll n\}$. The following elementary arithmetic observation will be used later.

Lemma 18: *Let $n_1, n_2, \ldots, n_L \in \mathbb{N}$. If $M > 0$, and for all $\ell \in [1..L]$ and $i \geq M$, $n_l^{[i]} = 0$, then, for all $i \geq M + \lceil \log_p L \rceil$,* $\left(\sum_{l=1}^{L} n_l \right)^{[i]} = 0.$

(Here, $\lceil n \rceil \in \mathbb{N}$ is the smallest integer such that $\lceil n \rceil \geq n$.)

Proof: The "$\log_p$" term comes from the fact that, in summing L distinct p-ary numbers, there is the possibility of up to $\log_p[L]$ digits of carried value spilling forward. □

With Lucas' theorem, one can obtain expressions for powers of linear automata. For example, if $f \in \mathbb{Z}_{/p}$, and $\mathfrak{F}$ is the linear automata on $\mathcal{A}^{\mathbb{Z}}$ defined by $\mathfrak{F}(x) = x + f \cdot \boldsymbol{\sigma}(x)$, then Lucas' Theorem tell us that

$$\mathfrak{F}^N(x) = \sum_{k \in \mathcal{L}(N)} \begin{bmatrix} N \\ k \end{bmatrix}_p f^k \cdot \boldsymbol{\sigma}^k x .$$

Next, if $m_1, m_2 \in \mathbb{Z}$, and $f_1, f_2 \in \mathbb{Z}_{/p}$, and $\mathfrak{F}$ is as in (2), then

$$\begin{aligned}
\mathfrak{F}^N &= \sum_{k_1 \in \mathcal{L}(N)} \begin{bmatrix} N \\ k_1 \end{bmatrix}_p f_1^{k_1} \cdot \boldsymbol{\sigma}^{m_1 k_1} \left(1 + f_2 \cdot \boldsymbol{\sigma}^{m_2}\right)^{k_1} \\
&= \sum_{k_1 \in \mathcal{L}(N)} \begin{bmatrix} N \\ k_1 \end{bmatrix}_p f_1^{k_1} \cdot \boldsymbol{\sigma}^{m_1 k_1} \left(\sum_{k_2 \in \mathcal{L}(k_1)} \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}_p f_2^{k_2} \cdot \boldsymbol{\sigma}^{m_2 k_2} \right) \\
&= \sum_{k_1 \in \mathcal{L}(N)} \sum_{k_2 \in \mathcal{L}(k_1)} \left(\begin{bmatrix} N \\ k_1 \end{bmatrix}_p \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}_p f_1^{k_1} f_2^{k_2} \right) \cdot \boldsymbol{\sigma}^{m_1 k_1 + m_2 k_2}. \\
&= \sum_{k_1 \in \mathcal{L}(N)} \sum_{k_2 \in \mathcal{L}(k_1)} f_{(k_1,k_2)} \cdot \boldsymbol{\sigma}^{m_1 k_1 + m_2 k_2}, \\
&\qquad \text{where we define } \; f_{(k_1,k_2)} \; := \; \begin{bmatrix} N \\ k_1 \end{bmatrix}_p \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}_p f_1^{k_1} f_2^{k_2}.
\end{aligned}$$

A similar argument works in $\mathbb{Z}^D$, and for an arbitrary number of "nested" polynomial terms of this type. This leads to the following

Lemma 19: *If $\vec{m}_1, \vec{m}_2, \ldots, \vec{m}_J \in \mathbb{Z}^D$, and $f_1, \ldots, f_J \in \mathbb{Z}_{/p}$, and $\mathfrak{F}$ is as in (4), then*

$$\mathfrak{F}^N \;=\; \sum_{\mathbf{k} \in \mathcal{L}^J(N)} f_{(\mathbf{k})} \boldsymbol{\sigma}^{\langle \mathbf{k}, \mathbf{m} \rangle}, \tag{5}$$

where:

$$\begin{aligned}
\mathbf{m} &:= [\vec{m}_1, \vec{m}_2, \ldots, \vec{m}_J], \\
\mathcal{L}^J(N) &:= \left\{ [k_1, k_2, \ldots, k_J] \in \mathbb{N}^J \; ; \; k_J \ll k_{J-1} \ll \ldots k_2 \ll k_1 \ll N \right\},
\end{aligned}$$

and, for any such $\mathbf{k} = [k_1, k_2, \ldots, k_J]$, we define

$$\begin{aligned}
\langle \mathbf{k}, \mathbf{m} \rangle &:= k_1 \vec{m}_1 + k_2 \vec{m}_2 + \ldots + k_J \vec{m}_J \\
\text{and} \;\; f_{(\mathbf{k})} &:= \begin{bmatrix} N \\ k_1 \end{bmatrix}_p \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}_p \cdots \begin{bmatrix} k_{J-1} \\ k_J \end{bmatrix}_p f_1^{k_1} f_2^{k_2} \ldots f_J^{k_J}.
\end{aligned}$$

(the dependence on N is suppressed in the notation "$f_{(\mathbf{k})}$".) □

Proof of Theorem 15: It suffices to prove the theorem for polynomials $\mathfrak{F}$ like (4). So, suppose $\mathfrak{F}$ is *not* diffusive in density. Thus, there exists some nontrivial character $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{(\mathbb{Z}^D)}}$, some $R \in \mathbb{N}$, and a subset $\mathbb{B} \subset \mathbb{N}$ (of "bad" numbers), of upper density $\delta > 0$, so that, for all $n \in \mathbb{B}$, $\quad \mathsf{rank}\left[\boldsymbol{\chi} \circ \mathfrak{F}^n\right] \leq R$.

Now, for each $\vec{n} \in \mathbb{Z}^D$, let $\mathbf{pr}_{\vec{n}} : \mathcal{A}^{(\mathbb{Z}^D)} \longrightarrow \mathcal{A}$ be projection onto the $\vec{n}$th coordinate: $\mathbf{pr}_{\vec{n}}(\mathbf{a}) = a_{\vec{n}}$. Let $\boldsymbol{\gamma} : \mathcal{A} \longrightarrow \mathbb{T}^1$ be the character introduced in §2.1: $\boldsymbol{\gamma}(a) = \exp\left(\frac{2\pi\mathbf{i}}{p} \cdot a\right)$. Thus, there is a finite subset $\mathcal{Q} \subset \mathbb{Z}^D$, and a collection of coefficients $\{\chi_{\vec{q}} \in [1..p)\ ;\ \vec{q} \in \mathcal{Q}\}$ so that $\boldsymbol{\chi}$ is defined[2]:

$$\boldsymbol{\chi}(\mathbf{a}) = \prod_{\vec{q} \in \mathcal{Q}} \boldsymbol{\gamma}\left(\chi_{\vec{q}} \cdot \mathbf{pr}_{\vec{q}}(\mathbf{a})\right) \tag{6}$$

Thus, if $\mathfrak{F}^N$ is as in (5) of Lemma 19, and $\boldsymbol{\chi}$ is as in (6), then, by Proposition 3, the character $\boldsymbol{\chi} \circ \mathfrak{F}^N$ has the following expansion[3]:

$$\boldsymbol{\chi} \circ \mathfrak{F}^N \quad = \quad \prod_{\vec{q} \in \mathcal{Q}} \prod_{\mathbf{k} \in \mathcal{L}^J(N)} \boldsymbol{\gamma}\left(\chi_{\vec{q}} \cdot f_{(\mathbf{k})} \cdot \mathbf{pr}_{(\langle \mathbf{k}, \mathbf{m} \rangle + \vec{q})}\right). \tag{7}$$

Note that, for every $\vec{q} \in \mathcal{Q}$ and $\mathbf{k} \in \mathcal{L}^J(N)$, the factor $\boldsymbol{\gamma}\left(\chi_{\vec{q}} \cdot f_{(\mathbf{k})} \cdot \mathbf{pr}_{(\langle \mathbf{k}, \mathbf{m} \rangle + \vec{q})}\right)$ is nontrivial: $f_{(\mathbf{k})}$ is never a multiple of p, and thus, if $\chi_{\vec{q}}$ is nontrivial, then $\boldsymbol{\gamma}\left(\chi_{\vec{q}} \cdot f_{(\mathbf{k})} \cdot \mathbf{pr}_{(\langle \mathbf{k}, \mathbf{m} \rangle + \vec{q})}\right)$ is also nontrivial. Thus, the *only* way the coefficients of the character defined by (7) can be trivial is if two terms of the form $\boldsymbol{\gamma}\left(\chi^*_{\vec{q}} \cdot f_{(\mathbf{k}^*)} \cdot \mathbf{pr}_{(\langle \mathbf{k}^*, \mathbf{m} \rangle + \vec{q}^*)}\right)$ and $\boldsymbol{\gamma}\left(\chi_{\vec{q}} \cdot f_{(\mathbf{k})} \cdot \mathbf{pr}_{(\langle \mathbf{k}, \mathbf{m} \rangle + \vec{q})}\right)$ cancel out, which can only occur when

$$\langle \mathbf{k}^*, \mathbf{m} \rangle + \vec{q}^* \quad = \quad \langle \mathbf{k}, \mathbf{m} \rangle + \vec{q}. \tag{8}$$

This is an equation of D-tuples of integers, and hence, is only true if, for all $d \in [1...D]$,

$$\langle \mathbf{k}^*, \mathbf{m} \rangle_{(d)} + q^*_{(d)} \quad = \quad \langle \mathbf{k}, \mathbf{m} \rangle_{(d)} + q_{(d)} \tag{9}$$

where the subscript "(d)" refers to the dth component of the D-tuple.

The idea of the proof is thus as follows: In order for the rank of the character $\boldsymbol{\chi} \circ \mathfrak{F}^N$ (for $N \in \mathbb{B}$) to be less than R, most of the terms in the expression (7) must cancel out; this requires a specific kind of "destructive interference" between the the index sets $\mathcal{S}(N)$ and various translations of $\mathcal{S}(N)$ so that virtually all elements $(\mathbf{k}, \vec{q}) \in \mathcal{L}^J(N) \times \mathcal{Q}$ must be paired up as in equation (8), so as to cancel with each other.

---

[2]In the case when $p = 2$, we can write this: $\boldsymbol{\chi}(\mathbf{a}) = \prod_{\vec{q} \in \mathcal{Q}} (-1)^{a_{\vec{q}}}$.

[3]When $J = 2 = p$, and $D = 1$ the expansion is:

$$\boldsymbol{\chi} \circ \mathfrak{F}^n(\mathbf{x}) \quad = \quad \prod_{q \in \mathcal{Q}} \prod_{k_1 \in \mathcal{L}(n)} \prod_{k_2 \in \mathcal{L}(k_1)} (-1)^{(k_1 m_1 + k_2 m_2 + q)}$$

.

Our goal, then, is to show that the equation (8) is hard to achieve, so that, after the dust settles, more than R nontrivial coefficients remain. We will show that, the set $\mathbb{B}$ (indeed, *any* set of nonzero density) must contain numbers for which sufficient cancellation fails to occur.

Reduction to Case $D = 1$: In order for cancellation of terms (ie. equation (8)) to occur in $\mathbb{Z}^D$, equation (9) must be true for *every* $d \in [1..D]$ simultaneously. Hence, it is enough to disrupt the equation in one dimension. Hence, at this point, we can reduce the argument to the case when $D = 1$. We will treat $m_1, \ldots, m_J$ as elements of $\mathbb{Z}$, and $\mathbf{m} = [m_1, \ldots, m_J]$ as a J-tuple of integers; thus, for any other J-tuple $\mathbf{k} = [k_1, \ldots, k_J]$, we have $\langle \mathbf{k}, \mathbf{m} \rangle = k_1 m_1 + \ldots k_J m_J$. Likewise, $\mathcal{Q}$ will be some finite subset of $\mathbb{Z}$.

Gaps in the Index set: We will use an ergodic argument to show that any subset of $\mathbb{N}$ of nonzero density must contain numbers N possessing large "gaps" in their index sets: i.e. $\mathbb{P}[N]$ has long blocks of 0's terminated by 1's. We can then find elements $k_1^* \in \mathcal{L}(N)$ also exhibiting these long gaps. The gap in such a k_1^* is long enough that it is impossible to find some other element $(\mathbf{k}, q) \in \mathcal{L}^J(N) \times \mathcal{Q}$ so that the terms in the expression $\langle \mathbf{k}, \mathbf{m} \rangle + \vec{q}$ sum together to "cancel" the terminating 1 in the gap of $\mathcal{S}(k_1^*)$.

Since there are many of these gaps, there are many such elements k_1^*, and thus, there will be at least $(R+1)$ distinct 1's that remain uncancelled, and thus at least $(R+1)$ nontrivial terms in expression (7), contradicting the hypothesis that $\mathsf{rank}\left[\boldsymbol{\chi} \circ \mathfrak{F}^N\right] \leq R$ for all $N \in \mathbb{B}$.

We can assume that, when we transformed expression (3) into expression (4), we had $\ell_0 < \ell_1 < \ldots < \ell_J$; hence, we can assume that $m_1, \ldots, m_J > 0$. Thus, they have well-defined Lucas sets, $\mathcal{S}(m_1), \ldots, \mathcal{S}(m_J)$. So, to begin, define:

$$\Gamma \;:=\; \max\left[\bigcup_{j=1}^{J} \mathcal{S}(m_j)\right] \;+\; \left\lceil \log_p\left(\sum_{j=1}^{J} \mathcal{C}\!ard\left[\mathcal{S}(m_j)\right]\right) + \log_p(J)\right\rceil + 2$$

Γ stands for "gap", and is the size of the gaps we will require.

Let q_1 be the smallest element of $\mathcal{Q}$, and define

$$\mathcal{Q}_1 \;:=\; \left\{q - q_1 \;;\; q \in \mathcal{Q}\right\}, \quad \text{and} \quad \mathcal{U} \;:=\; \bigcup_{q \in \mathcal{Q}_1} \mathcal{S}(q).$$

Next, let $\mathbf{w}$ be the element of $[0..p)^{\Gamma+1}$ defined: $\mathbf{w} := (\underbrace{0, \ldots, 0}_{\Gamma}, 1)$. We will be concerned with the frequency of occurrence of $\mathbf{w}$ in the p-ary expansions of integers.

Notation: If $\mathbf{s} = s_0 s_1 \dots s_n$ is a string in $[0..p)^n$, then we define the **frequency** of the word $\mathbf{w}$ in $\mathbf{s}$, denoted by $fr[\mathbf{w}, \mathbf{s}]$, as

$$fr[\mathbf{w}, \mathbf{s}] := \frac{\mathcal{C}ard\left[\{i \in [0, n-1] : s_i s_{(i+1)} \dots s_{(i+\Gamma)} = \mathbf{w}\}\right]}{n}$$

If $s_i s_{(i+1)} \dots s_{(i+\Gamma)} = \mathbf{w}$, we'll say that $\mathbf{w}$ **occurs** at s_i. **Claim 1:** *For any $\epsilon > 0$, there exists M^* such that, for any $M > M^*$, there is a set $\mathcal{G}_{\mathbf{w}}^M(\epsilon) \subset [1...p)^M$ so that:*

$$\mathcal{C}ard\left[\mathcal{G}_{\mathbf{w}}^M(\epsilon)\right] > (1-\epsilon)p^M, \quad \textit{and}, \quad \forall \mathbf{g} \in \mathcal{G}_{\mathbf{w}}^M(\epsilon), \quad fr[\mathbf{w}, \mathbf{g}] > \frac{(1-\epsilon)}{p^{(\Gamma+1)}}.$$

Proof: Consider the ergodic dynamical system $\left([0..p)^{\mathbb{N}}, \ \mathcal{H}aar, \ \boldsymbol{\sigma}\right)$, where $\mathcal{H}aar$ is the Haar measure and $\boldsymbol{\sigma} : [0..p)^{\mathbb{N}} \to [0..p)^{\mathbb{N}}$ is the shift action. The set $\left\{\mathbf{a} \in [0..p)^{\mathbb{Z}} \ ; \ \mathbf{a}_{[0...\Gamma]} = \mathbf{w}\right\}$ has measure $p^{-\Gamma-1}$. The result now follows from Birkhoff's Ergodic Theorem. .... □ `[Claim 1]`

In particular, let $\epsilon := \frac{\delta}{2p}$. Also, let $\epsilon^* := \frac{1-\epsilon}{2}\mathcal{H}aar(\mathbf{w}) = \frac{1-\epsilon}{2}p^{-1-\Gamma}$.

Claim 2: *There exist M and N such that the following conditions are satisfied:*

1. $M\epsilon^* > R + 2$,
2. $\mathcal{U} \subset [0, M\epsilon^*]$,
3. $N \in \mathbb{B} \cap [0, p^M)$,
4. $fr[\mathbf{w}, \vec{N}] > (1-\epsilon)\, p^{-1-\Gamma}$.

Proof: $\mathbb{B}$ has upper density δ, so there is some sequence $\{n_k\}_{k=0}^{\infty}$ such that,

$$\frac{\mathcal{C}ard\left[\mathbb{B} \cap [0, n_k]\right]}{n_k} \xrightarrow[k\to\infty]{} \delta.$$

Find K so that, for $k > K$, $\frac{\mathcal{C}ard\left[\mathbb{B} \cap [0..n_k]\right]}{n_k} > \frac{\delta}{2}$. Then choose M large enough to satisfy [1] and [2], and such that $p^{M-1} \le n_k \le p^M$. Thus,

$$\begin{aligned} \mathcal{C}ard\left[\mathbb{B} \cap \left[0, p^M\right]\right] &\ge \mathcal{C}ard\left[\mathbb{B} \cap [0, n_k]\right] \ge \frac{\delta n_k}{2} \ge \frac{\delta p^{M-1}}{2} \\ &\ge \frac{\delta p^M}{2p}. \end{aligned} \tag{10}$$

Also, by Claim 1, let M be large enough so that there is a subset $\mathcal{G}_{\mathbf{w}}^M(\epsilon) \subset [0..p)^M$ so that

$$\mathcal{C}ard\left[\mathcal{G}_{\mathbf{w}}^M(\epsilon)\right] > (1-\epsilon)p^M = \left(1 - \frac{\delta}{2p}\right)p^M, \tag{11}$$

$$\text{and} \quad fr[\mathbf{w}, \mathbf{a}] > (1-\epsilon)\, p^{-1-\Gamma}, \quad \text{for all } \mathbf{a} \in \mathcal{G}_{\mathbf{w}}^M(\epsilon).$$

Now, if $\mathbb{G} := \{n \in [1..p^M] ; \mathbb{P}(n) \in \mathcal{G}_{\mathbf{w}}^M(\epsilon)\}$, then $\mathcal{C}ard[\mathbb{G}] = \mathcal{C}ard[\mathcal{G}_{\mathbf{w}}^M(\epsilon)]$. Thus, combining (10) and (11), we see that $\mathcal{C}ard[\mathbb{B} \cap [0, p^M]] + \mathcal{C}ard[\mathbb{G}] > p^M$; hence, the two sets must intersect nontrivially. Let $N \in \mathbb{B} \cap [0, p^M] \cap \mathbb{G}$; then N satisfies [3] and [4]. .... $\square$ `[Claim 2]`

Claim 3: *Let $Q = \lceil M\epsilon^* \rceil$. Then $\mathbf{w}$ occurs more than R times in the string: $(N^{[Q+1]}\, N^{[Q+2]}\, N^{[Q+3]} \ldots N^{[M]})$.*

Proof: N satisfies condition [4] of Claim 2, and of course $\mathbf{w}$ occurs at most Q times in the string $(N^0\, N^{[1]} \ldots N^{[Q]})$. Thus, beyond position Q, $\mathbf{w}$ must occurs at least

$$\begin{aligned}\big((1-\epsilon)p^{-1-\Gamma}M\big) - Q &\geq \big((1-\epsilon)p^{-1-\Gamma}M\big) - M\epsilon^* - 1 \\ &= (1-\epsilon)p^{-1-\Gamma}M - \left(M\frac{1-\epsilon}{2}p^{-1-\Gamma}\right) - 1 \\ &= M\frac{1-\epsilon}{2}p^{-1-\Gamma} - 1 \;=\; M\epsilon^* - 1\end{aligned}$$

times and so, by condition [1] of Claim 1, at least $R+1$ times. $\square$ `[Claim 3]`

Say $\mathbf{w}$ occurs at some positions $N^{[j_1]}, N^{[j_2]}, \ldots, N^{[j_{R+1}]}$ beyond Q. Thus, for each $r \in [1...R+1]$, we have: $N^{[j_r+k]} = 0$ for $0 \leq k < \Gamma$ and $N^{[j_r+\Gamma]} = 1$. In particular,

$$\forall r \in [1...R+1], \quad p^{j_r+\Gamma} \in \mathcal{L}(N). \tag{12}$$

Now, $N \in \mathbb{B}$, so $\mathsf{rank}\left[\boldsymbol{\chi} \circ \mathfrak{F}^N\right] \leq R$. This means that in the expression (7), all but at most R of the terms are cancelled by a like term. In other words, for all but R of the elements: $(\mathbf{k}^*, q^*) \in \mathcal{L}^J(N) \times \mathcal{Q}$, there exists some $(\mathbf{k}, q) \in \mathcal{L}^J(N) \times \mathcal{Q}$ so that

$$\langle \mathbf{k}^*, \mathbf{m} \rangle + q^* = \langle \mathbf{k}, \mathbf{m} \rangle + q. \tag{13}$$

—we say that $(\mathbf{k}^*, q^*)$ is *annihilated* by $(\mathbf{k}, q)$.

However, there are $R+1$ elements in the set $\{j_r\}_{r=1}^{R+1}$, and thus, there are $R+1$ pairs of the form $(\mathbf{k}_r^*, q_1)$, where $\mathbf{k}_r^* = \big(p^{(j_r+\Gamma)}, 0, \ldots, 0\big)$. Hence there exists some r such that the pair $(\mathbf{k}_r^*, q_1)$ is annihilated by some other pair $(\mathbf{k}, q)$. Define $n := j_r + \Gamma$; then $\langle \mathbf{k}_r^*, \mathbf{m} \rangle = m_1 p^n$, so we can rewrite (13) as:

$$m_1 p^n = \langle \mathbf{k}, \mathbf{m} \rangle + (q - q_1), \tag{14}$$

where $\mathbf{k} = [k_1, \ldots, k_J]$ is some other element in $\mathcal{L}^J(N)$.

Claim 4: *For all $j \in [1..J]$, and all $i \geq n - \Gamma$, we have: ${k_j}^{[i]} = 0$.*

Proof: First we'll show $k_1^{[i]} = 0$ for $i \geq n$. The RHS and LHS of (14) must come from different terms of the expansion (7), which means that either $q \neq q_1$ or $k_j \neq 0$ for some $j > 1$; either way, one of the *other* terms on the RHS is positive besides "$m_1 k_1$", and therefore, $m_1 k_1 < m_1 p^n$. Thus, $k_1 < p^n$, and thus, $k_1^{[i]} = 0$ for all $i \geq n$.

Next we'll show $k_1^{[i]}$ for $n - \Gamma \leq i < n$. Recall that $k_1 \in \mathcal{L}(N)$, and by hypothesis, $N^{[i]} = 0$ for all $i \in [j_r ... (j_r + \Gamma))$, where $n = j_r + \Gamma$ and $n - \Gamma = j_r$. Thus, ${k_1}^{[i]} = 0$ for $n - \Gamma \leq i < n$.

Since $k_J \lll k_{J-1} \lll \ldots \lll k_2 \lll k_1$, the same holds for $k_2, \ldots, k_J$. □ `[Claim 4]`

Claim 5: *For all $j \in [1..J]$, and all $i \geq n - 2 - \log_p(J)$, we have: $(m_j k_j)^{[i]} = 0$.*

Proof: Fix $j \in [1..J]$. For any $s \in \mathcal{S}(m_j)$, it follows from Claim 4 that

$$\left(m_j^{[s]} p^s k_j\right)^{[i]} = 0, \quad \text{for all } i \geq n - \Gamma + s.$$

Hence, by Lemma 18,

$$\begin{aligned} (m_j k_j)^{[i]} &= \left(\sum_{s \in \mathcal{S}(m_j)} m_j^{[s]} p^s k_j\right)^{[i]} \\ &= 0, \quad \forall i \geq n - \Gamma + \max\left[\mathcal{S}(m_j)\right] + \log_p\left(\mathcal{C}\text{ard}\left[\mathcal{S}(m_j)\right]\right). \end{aligned}$$

The claim now follows from the definition of Γ. .... □ `[Claim 5]`

Claim 6: *For all $i \geq n - 3$, $(q - q_1)^{[i]} = 0$.*

Proof: By definition, $n - 3 > n - \Gamma = j_r > Q \geq M\epsilon^*$. Recall that condition [2] defining M was: $\mathcal{U} \subset [0, M\epsilon^*]$. Thus, $(q - q_1)^{[i]} = 0$ for $i \geq M\epsilon^*$. .... □ `[Claim 6]`

Claim 7: *For all $i \geq n - 1$, $(\langle \mathbf{k}, \mathbf{m} \rangle + (q - q_1))^{[i]} = 0$.*

Proof: Recall that $\langle \mathbf{k}, \mathbf{m} \rangle = (k_1 m_1) + \ldots + (k_J m_J)$; thus, it follows from Claim 5 and Lemma 18 that $\langle \mathbf{k}, \mathbf{m} \rangle^{[i]} = 0, \forall i \geq n - 2$.

Thus, the claim follows from Claim 6 and Lemma 18. ... □ `[Claim 7]`

Now, by hypothesis, $\langle \mathbf{k}, \mathbf{m} \rangle + (q - q_1) = m_1 p^n$. Hence, $(\langle \mathbf{k}, \mathbf{m} \rangle + (q - q_1))^{[i]} = (m_1 p^n)^{[i]}$ for all $i \in \mathbb{N}$. In particular, if $I := \min\left[\mathcal{S}(m_1)\right] \geq 0$, then

$$(\langle \mathbf{k}, \mathbf{m} \rangle + (q - q_1))^{[I+n]} = (m_1 p^n)^{[I+n]} = m_1^{[I]} \neq 0.$$

But $I + n \geq n$, so this is a contradiction of Claim 7. ________________ □

Conclusion

We have shown that harmonically mixing measures on $\mathcal{A}^{\mathbb{M}}$, when acted upon by diffusive linear cellular automata (possibly with an affine part), will weak*-converge, in Cesàro mean, to the Haar measure. This sufficient condition is broadly applicable: in particular, if $\mathcal{A} = \mathbb{Z}_{/p}$, then any nontrivial linear cellular automata acting upon a "fully supported" N-step Markov measure (in $\mathbb{Z}$, a regular tree, or a free group) or a nontrivial Bernoulli measure (in $\mathbb{Z}^D$) will converge to Haar in Cesàro mean.

In a forthcoming paper [8], we generalize the results on diffusion to the case when $\mathcal{A} = \mathbb{Z}_{/n}$ ($n \in \mathbb{N}$ arbitrary) and $\mathcal{A} = \left(\mathbb{Z}_{/(p^r)}\right)^J$ (p prime, $r, J \in \mathbb{N}$), and we demonstrate harmonic mixing for Markov random fields on $\mathcal{A}^{\left(\mathbb{Z}^D\right)}$, for $D \geq 2$. However, many questions remain unanswered. What other classes of measures on $\mathbb{Z}$ or $\mathbb{Z}^D$ are harmonically mixing? Measures on $\mathcal{A}^{\mathbb{M}}$ exhibiting quasiperiodicity cannot be harmonically mixing; what is the Cesàro limit of such a measure, if anything? Also, what LCA are diffusive, when $\mathbb{M}$ is neither a lattice nor a free group?

Acknowledgments: We would like to thank David Poole of Trent University for introducing us to Lucas' Theorem, and Dan Rudolph of the University of Maryland for reminding us that, for stationary μ, Cesàro convergence to $\mathcal{H}aar$ is equivalent to convergence in density.

References

[1] Alejandro Maass and Servet Martínez. Time averages for some classes of expansive one-dimensional cellular automata. In Eric Goles and Servet Martinez, editors, *Cellular Automata and Complex Systems*, pages 37–54. Kluwer Academic Publishers, Dordrecht, 1999.

[2] G. Hedlund. Endomorphisms and automorphisms of the shift dynamical systems. *Mathematical System Theory*, 3:320–375, 1969.

[3] Lee Kenneth Jones. A mean ergodic theorem for weakly mixing operators. *Advances in Mathematics*, 7:211–216, 1971.

[4] Bruce Kitchens and K. Schmidt. Markov subgroups of $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{Z}^2}$. In Peter Walters, editor, *Symbolic Dynamics and its Applications*, volume 135 of *Contemporary Mathematics*, pages 265–283, Providence, 1992.

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

[6] Douglas Lind and Brian Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, New York, first edition, 1995.

[7] E. Lucas. Sur les congruences des nombres Eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier. *Bulletin de la Société Mathématique de France*, 6:49–54, 1878.

[8] Marcus Pivato and Reem Yassawi. Limit measures for affine cellular automata II. Submitted to *Ergodic Theory and Dynamical Systems;* preprint available at: `http://xxx.lanl.gov`, 2001.

[9] Servet Martínez Pablo Ferrari, Alejandro Maass. Cesàro mean distribution of group automata starting from Markov measures. *(preprint)*, 1998.

[10] Servet Martínez Pablo Ferrari, Alejandro Maass and Peter Ney. Cesàro mean distribution of group automata starting from measures with summable decay. *Ergodic Theory and Dynamical Systems*, 20(6):1657–1670, 2000.

[11] Karl Petersen. *Ergodic Theory.* Cambridge University Press, New York, 1989.

[12] Klaus Schmidt. *Dynamical Systems of Algebraic Origin.* Birkhäuser Verlag, Boston, Massachusetts, 1995.

[13] F. Spitzer. Markov random fields on an infinite tree. *Annals of Probability*, 3:387–398, 1975.

[14] S. Zachary. Countable state space Markov random fields and Markov chains on trees. *Annals of Probability*, 11:894–903, 1983.