Asymptotic Randomization of Multidimensional Finite-type Subshifts by Linear Cellular Automata

Marcus Pivato & Reem Yassawi

(Trent University, Canada)

Cellular Automata

- Spatially distributed dynamical systems;
- *Local interactions*;
- *Spatially homogeneous* rules.

CA are the 'discrete' analog of partial differential equations:

- **Space** is a lattice $\mathbb{M}$ (eg. $\mathbb{Z}^D$ or $\mathbb{N}^D$).
- The **local state** at each point in the lattice is an element of a finite alphabet, $\mathcal{A}$.
- **Global state:** an $\mathbb{M}$-indexed configuration of elements in $\mathcal{A}$. The space of such configurations is $\mathcal{A}^{\mathbb{M}}$.
- **Evolution:** a map $\Phi : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$, computed by applying a '**local rule**' at every point in $\mathbb{M}$.

Preliminaries

$\mathcal{A}$: a finite set, with the discrete topology.

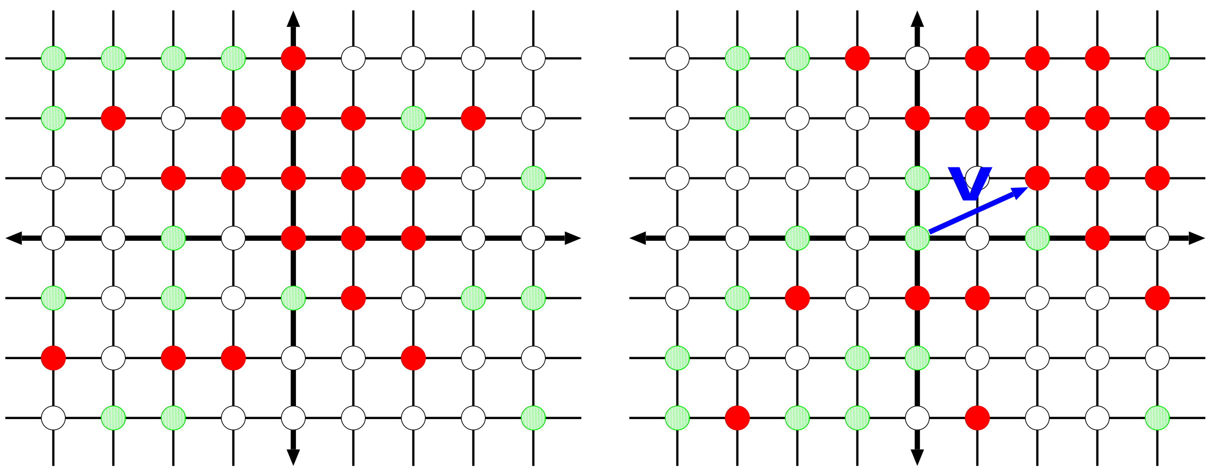
$\mathbb{M}$: a **lattice** (for example, $\mathbb{M} = \mathbb{N}, \quad \mathbb{Z}, \quad \mathbb{N}^3 \times \mathbb{Z}^5$, etc.).

$\mathcal{A}^{\mathbb{M}}$: a compact space under the Tychonoff topology.

An element of $\mathcal{A}^{\mathbb{M}}$ will be written as $\mathbf{a} = [a_m]_{m\in\mathbb{M}}$.

Shift action of $\mathbb{M}$ on $\mathcal{A}^{\mathbb{M}}$: for all $v \in \mathbb{M}$, and $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, define

$$\boldsymbol{\sigma}^v[\mathbf{a}] \;=\; [b_m|_{m\in\mathbb{M}}] \quad \text{where, } \forall m, \quad b_m = a_{(v+m)}.$$



Cellular Automata

Neighbourhood:

$\mathbb{U} \subset \mathbb{M}$ (finite set)

A **local rule** $\phi: \mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$

induces **cellular automaton**

$$\Phi: \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$$

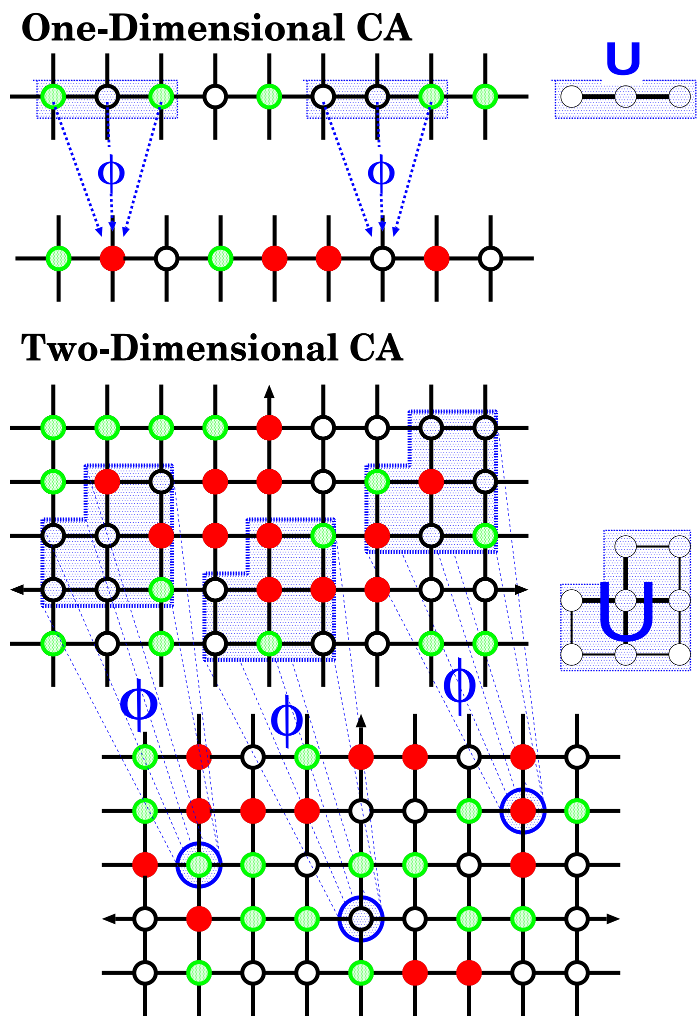
as follows:

For any $\mathbf{a} = [a_m|_{m\in\mathbb{M}}]$ in $\mathcal{A}^{\mathbb{M}}$,

$$\Phi(\mathbf{a}) = [b_m|_{m\in\mathbb{M}}],$$

where, for all $m \in \mathbb{M}$,

$$b_m = \phi\left[a_{(u+m)}|_{u\in\mathbb{U}}\right].$$



Equivalently, a CA is a continuous transformation $\Phi : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ that commutes with all shifts:

$$\forall\ m \in \mathbb{M}, \qquad \Phi \circ \boldsymbol{\sigma}^m = \boldsymbol{\sigma}^m \circ \Phi.$$

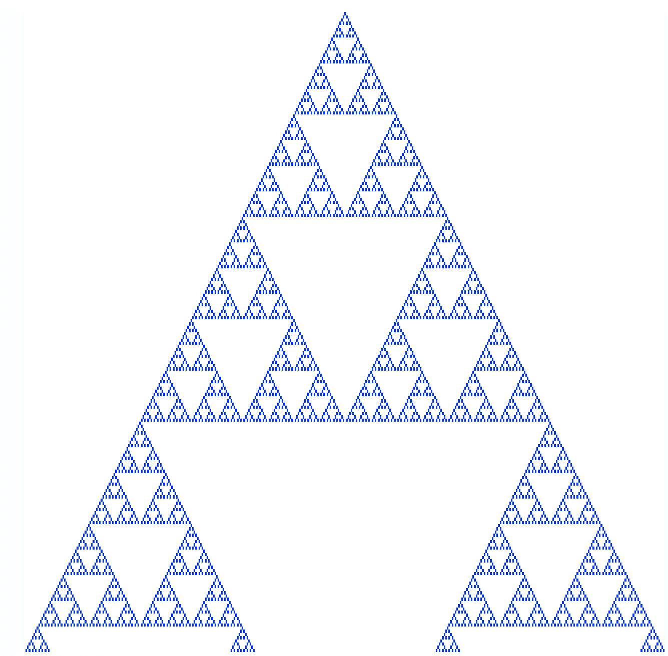
Example: *Nearest-neighbour XOR*

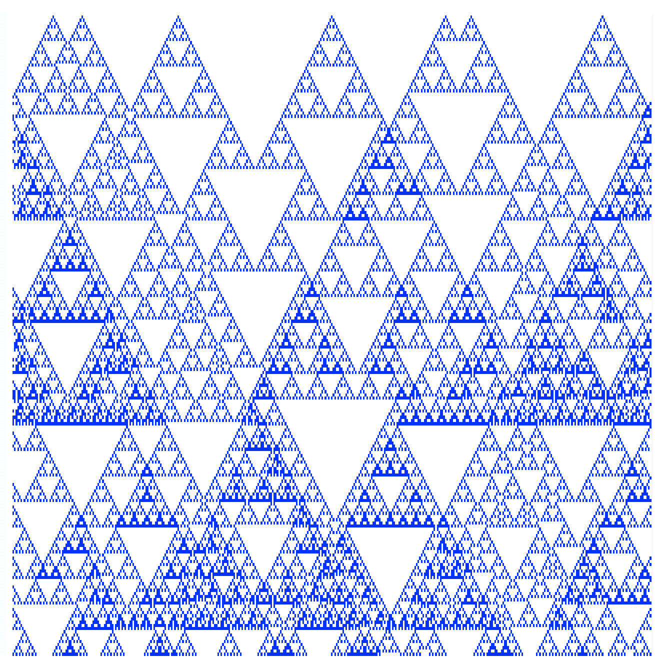
$$\mathbb{M} = \mathbb{Z}, \quad \mathbb{U} = \{-1, +1\}, \quad \mathcal{A} = \{0, 1\}, \quad \phi(\mathbf{a}) \;=\; a_{-1} + a_1 \quad (\text{mod } 2).$$

⟵ Space ⟶

$\mathbb{U}$:					$*$		$*$					...
...						1						...
...					1		1					...
...				1				1				...
...			1		1		1		1			...
...		1								1		...
...	1		1						1		1	...
...1				1				1				1...

Time ↓





Linear Cellular Automata

$\mathcal{A}$: **finite abelian group** (eg, $\mathcal{A} = \mathbb{Z}_{/p}$, p prime).

$\mathcal{A}^{\mathbb{M}}$: **compact abelian group** (Tychonoff topology & pointwise addition)

Linear CA: A CA that is also a group endomorphism.

Equivalently: $\phi : \mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$ is a homomorphism from the product group $\mathcal{A}^{\mathbb{U}}$ into $\mathcal{A}$.

Fact: $\mathcal{A} = \mathbb{Z}_{/p}$ is a field under multiplication.

Any LCA is a 'polynomial of shift maps':

$$\Phi \;=\; \sum_{u \in \mathbb{U}} \varphi_u \cdot \boldsymbol{\sigma}^u, \qquad \text{(where } \{\varphi_u\}_{u \in \mathbb{U}} \text{ are in } \mathbb{Z}_{/p}\text{)}$$

That is, for any $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$: $\quad \Phi(\mathbf{a}) \;=\; \sum_{u \in \mathbb{U}} \varphi_u \cdot \boldsymbol{\sigma}^u(\mathbf{a})$.

Example: (*Nearest-Neighbour XOR*) $\quad \Phi = \boldsymbol{\sigma}^{-1} + \boldsymbol{\sigma}^1$.

$\mathbf{a}$:		0	1	0	1	1	1	0	1	1	0	1	
$\boldsymbol{\sigma}(\mathbf{a})$:	0	1	0	1	1	1	0	1	1	0	1	$\Longleftarrow$	
$\boldsymbol{\sigma}^{-1}(\mathbf{a})$:		$\Longrightarrow$	0	1	0	1	1	1	0	1	1	0	1
$\Phi(\mathbf{a})$:			0	0	1	0	1	0	1	1	0		

The Haar Measure

Let $\mathbb{L} \subset \mathbb{M}$ be a finite set. Let $\mathbf{b} \in \mathcal{A}^{\mathbb{L}}$.

$$[\mathbf{b}] \;=\; \left\{\mathbf{a} \in \mathcal{A}^{\mathbb{M}} \;;\; \text{for all } \ell \in \mathbb{L},\; a_\ell = b_\ell\right\};$$

This is a **cylinder set** of **size** $L = \mathrm{card}\,[\mathbb{L}]$.

If $A = \mathrm{card}\,[\mathcal{A}]$, then there are A^L cylinder sets of size L.

Haar measure: Probability measure $\mathcal{H}$ on $\mathcal{A}^{\mathbb{M}}$ assigning mass A^{-L} to all cylinder sets of size L.

- $\mathcal{H}$ is the 'most random' measure on $\mathcal{A}^{\mathbb{M}}$. (maximal entropy)
- $\mathcal{H}$ is Φ-invariant for any surjective CA Φ.

Asymptotic Randomization

Let μ be a probability measure on $\mathcal{A}^{\mathbb{M}}$.

Φ **asymptotically randomizes** μ if

$$\mathbf{wk}^*\!-\!\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} \Phi^n \mu \quad = \quad \mathcal{H}.$$

CA 'Second Law of Thermodynamics'.

Asymptotic Randomization; One-dimensional CA

Theorem (Lind, 1984)

$$\left(\begin{array}{l} \bullet\ \mathcal{A} = \mathbb{Z}_{/2} \text{ and } \mathbb{M} = \mathbb{Z}. \\ \bullet\ \Phi = \boldsymbol{\sigma}^{-1} + \boldsymbol{\sigma}^{1}. \\ \bullet\ \mu \textit{ is a } \textbf{Bernoulli measure}. \end{array}\right) \Longrightarrow \left(\begin{array}{l} \Phi \textit{ asymptotically} \\ \textit{randomizes } \mu \end{array}\right)$$

However, $\mathbf{wk}^*\text{–}\lim_{n\to\infty} \Phi^N \mu \neq \mathcal{H}$, *because* $\{\Phi^2\mu,\ \Phi^4\mu,\ \Phi^8\mu,\ \Phi^{16}\mu,\ \Phi^{32}\mu,\ \Phi^{64}\mu, \ldots\}$ *does not converge to* $\mathcal{H}$.

Theorem (Ferrari, Ney, Maass & Martínez, 1998)

$$\left(\begin{array}{l} \bullet\ p \textit{ prime;} \quad \mathcal{A} = \mathbb{Z}_{/(p^n)}; \quad \mathbb{M} = \mathbb{N}. \\ \bullet\ \Phi = \varphi_0 \cdot \boldsymbol{\sigma}^0 + \varphi_1 \cdot \boldsymbol{\sigma}^1. \\ \quad \varphi_0 \not\equiv 0 \not\equiv \varphi_1 \pmod{p}. \\ \bullet\ \mu \textit{ is a } \textbf{Markov measure}. \\ \quad \textit{All transition probabilities nonzero.} \end{array}\right) \Longrightarrow \left(\begin{array}{l} \Phi \textit{ asympt.} \\ \textit{randomizes } \mu \end{array}\right)$$

Theorem (Maass & Martínez, 1999)

$$\left(\begin{array}{l} \bullet\ \mathcal{A} = \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}; \quad \mathbb{M} = \mathbb{N}. \\ \bullet\ \textit{Local map } \phi\left[\binom{x_0}{y_0}; \binom{x_1}{y_1}\right] = \binom{y_0}{x_0+y_1} \\ \bullet\ \mu \textit{ a } \textbf{Markov measure}. \\ \quad \textit{All transition probabilities nonzero.} \end{array}\right) \Longrightarrow \left(\begin{array}{l} \Phi \textit{ asympt.} \\ \textit{randomizes } \mu \end{array}\right)$$

Harmonic Mixing and Asymptotic Randomization

Theorem 1: (Y & P, 2000)

- *Let $\mathcal{A} = \mathbb{Z}_{/p}$ (p prime).*
- *Let $\mathbb{M} = \mathbb{Z}^D \times \mathbb{N}^d$ be any lattice.*
- *Let $\Phi : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ be any linear CA such that*
  Φ has at least two nonzero coefficients (ie. not a shift).
- *Let μ be a* **harmonically mixing** *measure.*

Then Φ asymptotically randomizes μ.

Examples of Harmonic Mixing: Bernoulli measures, Markov chains, or Markov random fields with 'full support'.

Theorem 2: (Y & P, 2001)

- *Let $\mathcal{A} = \mathbb{Z}_{/n}$ (any $n \in \mathbb{N}$).*
- *Let $\mathbb{M} = \mathbb{Z}^D \times \mathbb{N}^d$ be any lattice.*
- *Let $\Phi : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ be any linear CA such that*
  $\forall$ prime p dividing n, at least two coefficients are $\not\equiv 0 \pmod{p}$.
- *Let μ be a* **harmonically mixing** *measure.*

Then Φ asymptotically randomizes μ.

The Characters of $\mathcal{A}^{\mathbb{M}}$

$\mathbb{T}^1$: The unit circle group $\{z \in \mathbb{C} \,;\, |z| = 1\}$.

Character: A continuous homomorphism $\boldsymbol{\chi}: \mathcal{A}^{\mathbb{M}} \longrightarrow \mathbb{T}^1$.

Example: $(\mathcal{A} = \mathbb{Z}_{/2})$ Characters of $\mathcal{A}^{\mathbb{Z}}$:

$$\boldsymbol{\beta}(\mathbf{a}) \;=\; (-1)^{a_0}; \qquad\qquad \boldsymbol{\gamma}(\mathbf{a}) \;=\; (-1)^{(a_0+a_3+a_5)}.$$

Example: $(\mathcal{A} = \mathbb{Z}_{/5})$ $\quad \boldsymbol{\kappa}(\mathbf{a}) \;=\; \exp\left(\frac{2\pi\mathbf{i}}{5}\,(a_0 + 3a_1 + 2a_3 + 4a_7)\right).$

Example: $(\mathcal{A} = \mathbb{Z}_{/p})$ For any $m \in \mathbb{M}$ and $c \in \mathbb{Z}_{/p}$, the map $\boldsymbol{\xi}_m^c(\mathbf{a}) \;=\; \exp\left(\frac{2\pi\mathbf{i}}{p} \cdot c \cdot a_m\right)$ is a character of $\mathcal{A}^{\mathbb{M}}$.

Lemma: *All characters of $\mathcal{A}^{\mathbb{M}}$ are products of the form*

$$\boldsymbol{\chi}(\mathbf{a}) \;=\; \prod_{m \in \mathbb{M}} \exp\left(\frac{2\pi\mathbf{i}}{p} \cdot \chi_m \cdot a_m\right).$$

That is: $$\boldsymbol{\chi} \;=\; \bigotimes_{m \in \mathbb{M}} \boldsymbol{\xi}_m^{\chi_m}.$$

Coefficients: $\chi_m \in \mathbb{Z}_{/p}$; *all but finitely many are zero.*

The **rank** of $\boldsymbol{\chi}$ is the number of nonzero coefficients.

Example: $\mathsf{rank}\,[\boldsymbol{\beta}] \;=\; 1. \qquad \mathsf{rank}\,[\boldsymbol{\gamma}] \;=\; 3. \qquad \mathsf{rank}\,[\boldsymbol{\kappa}] \;=\; 4.$

Fourier Coefficients

If $\boldsymbol{\chi}$ is a character and μ is a measure on $\mathcal{A}^{\mathbb{M}}$, then define

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

These **Fourier Coefficients** completely identify μ.

Example: If $\mu = \mathcal{H}$, then $\widehat{\mathcal{H}}[\boldsymbol{\chi}] \quad = \quad \begin{cases} 1 & \text{if } \boldsymbol{\chi} = \mathbb{1} \\ 0 & \text{otherwise} \end{cases}.$

Harmonic Mixing

μ is **harmonically mixing** if, for all $\epsilon > 0$, $\exists\, R \in \mathbb{N}$ so that for all characters $\boldsymbol{\chi}$,

$$\left(\mathsf{rank}\,[\boldsymbol{\chi}] \;>\; R \right) \quad \Longrightarrow \quad \left(\left|\widehat{\mu}[\boldsymbol{\chi}]\right| \;<\; \epsilon \right)$$

Examples: $\mathcal{H}$ is obviously harmonically mixing.

A *Bernoulli measure* is HM if all $a \in \mathcal{A}$ have nonzero probability.

A *Markov chain* is HM if all transition probabilities are nonzero.

An N*-step Markov chain* is HM if all $(N+1)$-words get nonzero probability.

A *Markov random field* is HM if all cylinder sets get nonzero probability.

Common theme: *full support* –ie. $\mathsf{supp}\,(\mu) = \mathcal{A}^{\mathbb{M}}$.

Question: What if μ does *not* have full support?

eg. What if $\mathsf{supp}\,(\mu)$ is a subshift of finite type?

tape

Characters and LCA

If $\boldsymbol{\chi}$ is a character on $\mathcal{A}^{\mathbb{M}}$, and Φ is a linear CA, then:

- $\boldsymbol{\chi} \circ \Phi$ is also a character on $\mathcal{A}^{\mathbb{M}}$.
- Get coefficients of $\boldsymbol{\chi} \circ \Phi$ by 'convolving' coefficients of $\boldsymbol{\chi}$ and Φ.

Example: $(\mathcal{A} = \mathbb{Z}_{/2})$ Suppose $\boldsymbol{\chi} = \boldsymbol{\xi}_0 \otimes \boldsymbol{\xi}_1 \otimes \boldsymbol{\xi}_5$
ie. $\boldsymbol{\chi}(\mathbf{a}) \;=\; (-1)^{a_0} \cdot (-1)^{a_1} \cdot (-1)^{a_5}$.

If $\Phi \;=\; 1 + \boldsymbol{\sigma}$, then $\boldsymbol{\chi} \circ \Phi \;=\; \boldsymbol{\xi}_0 \otimes \boldsymbol{\xi}_2 \otimes \boldsymbol{\xi}_5 \otimes \boldsymbol{\xi}_6$.

Definition: Φ is **diffusive** if, for all nontrivial characters $\boldsymbol{\chi}$, there is a set $\mathbb{J} \subset \mathbb{N}$ of Cesàro density 1, so that

$$\lim_{\substack{j\to\infty \\ j\in\mathbb{J}}} \mathsf{rank}\left[\boldsymbol{\chi} \circ \Phi^j\right] \quad = \quad \infty.$$

Proposition A: Let $\mathcal{A}$ be a finite abelian group, $\mathbb{M}$ a lattice.

$$\left(\begin{array}{l} \bullet\ \ \Phi \textit{ is a } \textbf{diffusive} \textit{ LCA on } \mathcal{A}^{\mathbb{M}} \\ \bullet\ \ \mu \textit{ is } \textbf{harmonically mixing} \end{array}\right) \Longrightarrow \left(\begin{array}{l} \Phi \textit{ asymptotically} \\ \textit{randomizes } \mu \end{array}\right)$$

Proposition B:

- *Let $\mathcal{A} = \mathbb{Z}_{/n}$ (any $n \in \mathbb{N}$).*
- *Let $\mathbb{M} = \mathbb{Z}^D \times \mathbb{N}^d$ be any lattice.*
- *Let $\Phi : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathcal{A}^{\mathbb{M}}$ be any linear CA such that*

$\forall$ prime p dividing n, at least two coefficients are $\not\equiv 0 \pmod{p}$.

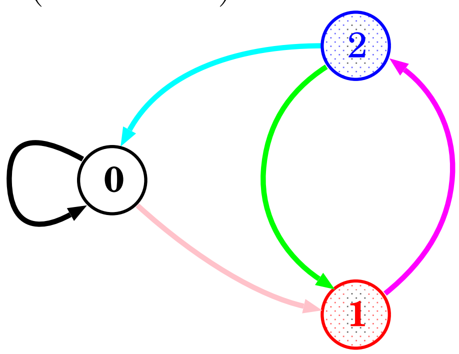
Then Φ is **diffusive**.

Theorems 1 & 2 follow from Propositions A & B.

Subshifts of Finite Type

A **subshift of finite type** (SFT) is a closed, shift-invariant subset $\mathfrak{X} \subset \mathcal{A}^{\mathbb{M}}$ determined by local 'matching rules'

Topological Markov chain: One-dimensional SFT determined by a digraph (or matrix) of 'admissible transitions'.

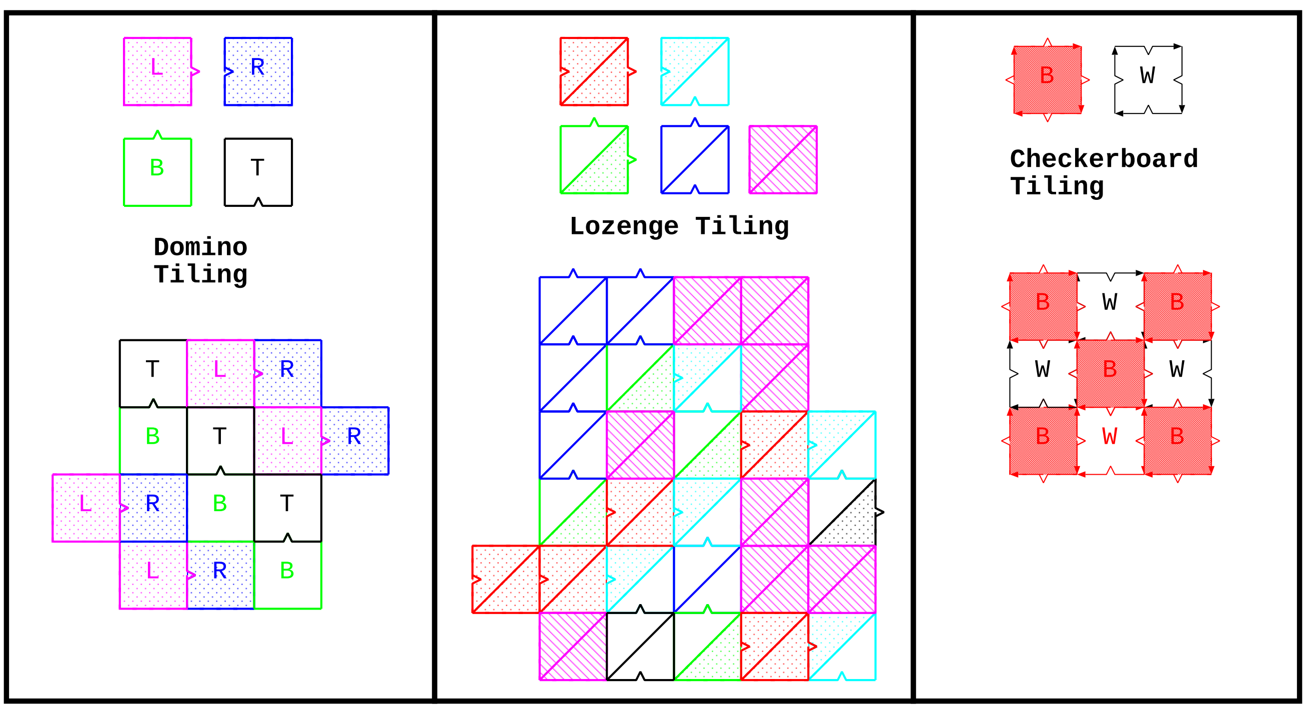


$$\mathbf{A} = \{0,1,2\}$$

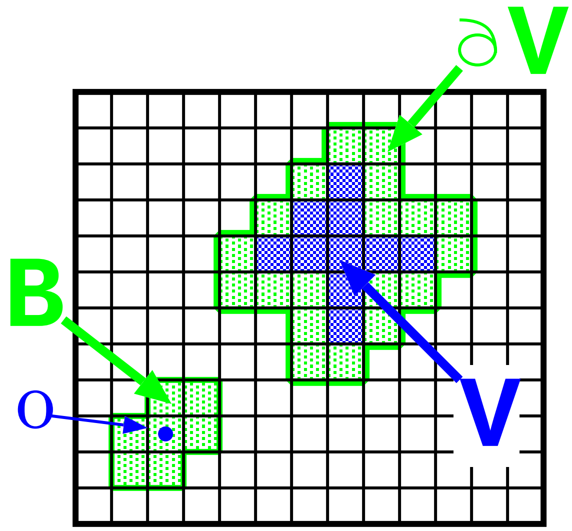
$$\mathbf{T} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\mathbf{a} = [\ldots 0,1,2,1,2,0,0,0,0,1,2,0,0,1,2,1,2,1,2,0,0,\ldots]$$

Tiling: Multi-dimensional SFT determined by notched tiles.



Markov Random Fields



Let $\mathbb{M} = \mathbb{Z}^D$.

Let $\mathbb{B} \subset \mathbb{M}$ be a symmetric, finite 'ball' around 0. e.g. $\mathbb{B} = [-1...1]^D$.

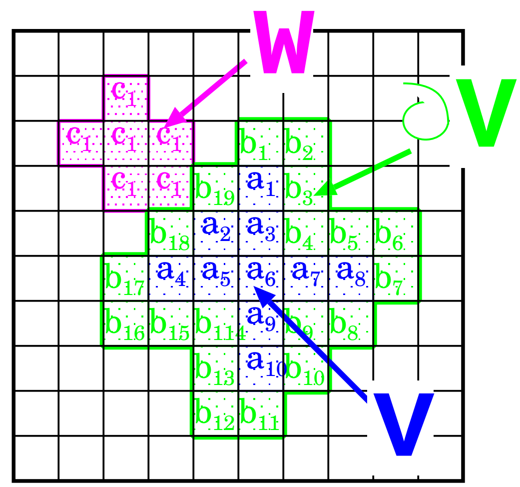
If $\mathbb{V} \subset \mathbb{M}$ is any subset, define:

- 'Closure': $cl(\mathbb{V}) = \mathbb{V} + \mathbb{B}$
- 'Boundary': $\partial(\mathbb{V}) = cl(\mathbb{V}) \setminus \mathbb{V}$.

μ is a **Markov random field** (MRF) if, for $\forall\ \mathbb{V} \subset \mathbb{M}$, and $\forall\ \mathbf{b} \in \mathcal{A}^{\partial(\mathbb{V})}$, events 'inside' $\mathbb{V}$ are independent of events 'outside', relative to conditional measure $\mu^{(\mathbf{b})}$.

That is: if $\mathbb{W} \subset \mathbb{M} \setminus cl(\mathbb{V})$, $\mathbf{c} \in \mathcal{A}^{\mathbb{W}}$, and $\mathbf{a} \in \mathcal{A}^{\mathbb{V}}$, then:

$$\mu^{(\mathbf{b})}\left[\mathbf{a} \smile \mathbf{c}\right] \;=\; \mu^{(\mathbf{b})}\left[\mathbf{a}\right] \cdot \mu^{(\mathbf{b})}\left[\mathbf{c}\right].$$



If μ is an MRF, then $\mathsf{supp}\,(\mu)$ is a SFT.

Example: If $\mathbb{M} = \mathbb{Z}$ and $\mathbb{B} = \{-1, 0, 1\}$, then an MRF is a **Markov Chain**. If $\mathbb{V} = \{1, 2, 3\}$, then $\partial\mathbb{V} = \{0, 4\}$. Suppose $\mathbb{W} = \{5, 6\}$.

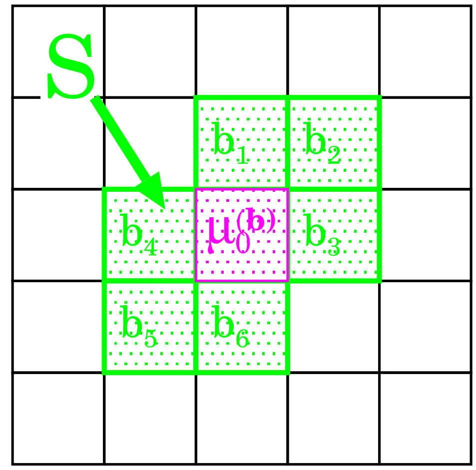
$$\boxed{\ldots}\boxed{\ldots}\boxed{\ldots}\boxed{b_0}\underbrace{\boxed{a_1}\boxed{a_2}\boxed{a_3}}_{\mathbb{V}}\boxed{b_4}\underbrace{\boxed{c_5}\boxed{c_6}}_{\mathbb{W}}\boxed{\ldots}\boxed{\ldots}\boxed{\ldots}$$

If $b_0, b_4 \in \mathcal{A}$, then for any $a_1, a_2, a_3 \in \mathcal{A}$ and any $c_5, c_6 \in \mathcal{A}$,

$$\frac{\mu[b_0, a_1, a_2, a_3, b_4, c_5, c_6]}{\mu[b_0, *, *, *, b_4]} \;=\; \frac{\mu[b_0, a_1, a_2, a_3, b_4]}{\mu[b_0, *, *, *, b_4]} \cdot \frac{\mu[b_4, c_5, c_6]}{\mu[b_4]}$$

In this case, $\mathsf{supp}\,(\mu)$ is a *topological Markov chain.*

Local Freedom



Let $\mathbb{S} = \partial\{0\} = \mathbb{B} \setminus \{0\}$ (the 'sphere').

If $\mathbf{b} \in \mathcal{A}^{\mathbb{S}}$, let $\mu_0^{(\mathbf{b})}$ be the conditional measure on $\mathcal{A}^{\{0\}}$.

μ is **locally free** if, for any $\mathbf{b} \in \mathcal{A}^{\mathbb{S}}$, $\mathsf{supp}\left(\mu_0^{(\mathbf{b})}\right)$ contains at least 2 elements.

Example: Let μ be a Markov chain on $\mathcal{A}^{\mathbb{Z}}$. Then $\mathbb{B} = \{-1, 0, 1\}$ and $\mathbb{S} = \{-1, 1\}$. μ is **locally free** if, for any $b_{(-1)}, b_1 \in \mathcal{A}$, there are a and $a' \in \mathcal{A}$ so that $a \neq a'$ and

$$\mu[b_{-1}, a, b_1] \quad \neq \quad 0 \quad \neq \quad \mu[b_{-1}, a', b_1].$$

Let $\mathbf{T} = [t_{a,b}]_{a,b \in \mathcal{A}}$ be the **admissible transition matrix** for $\mathsf{supp}(\mu)$ (ie. $t_{a,b} = 1$ iff $\mu[a,b] > 0$). Then

$$\Big(\mu \text{ is locally free} \Big) \iff \Big(\text{All entries of } \mathbf{T}^2 \text{ are at least } 2 \Big)$$

Example: Suppose μ has transition probability matrix $\mathbf{P}$. Then:

$$\left(\mathbf{P} = \begin{bmatrix} 1/2 & 1/2 & \\ & & 1 \\ 1/2 & & 1/2 \end{bmatrix} \right) \Longrightarrow \left(\mathbf{T}^2 = \begin{bmatrix} 1 & 1 & \\ & & 1 \\ 1 & & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & & 1 \\ 2 & 1 & 1 \end{bmatrix} \right)$$

$$\Longrightarrow \Big(\mu \text{ is not LF} \Big).$$

$$\left(\mathbf{P} = \begin{bmatrix} & 1/3 & 1/3 & 1/3 \\ 1/3 & & 1/3 & 1/3 \\ 1/3 & 1/3 & & 1/3 \\ 1/3 & 1/3 & 1/3 & \end{bmatrix} \right) \Longrightarrow \left(\mathbf{T}^2 = \begin{bmatrix} & 1 & 1 & 1 \\ 1 & & 1 & 1 \\ 1 & 1 & & 1 \\ 1 & 1 & 1 & \end{bmatrix}^2 = \begin{bmatrix} 3 & 2 & 2 & 2 \\ 2 & 3 & 2 & 2 \\ 2 & 2 & 3 & 2 \\ 2 & 2 & 2 & 3 \end{bmatrix} \right)$$

$$\Longrightarrow \Big(\mu \text{ is LF} \Big).$$

Theorem (Y&P, 2002)
Let $\mathcal{A} = \mathbb{Z}_{/p}$ (p prime). Let μ be a Markov random field. Then:

$$\Big(\mu \text{ is locally free} \Big) \Longrightarrow \Big(\mu \text{ is harmonically mixing} \Big).$$

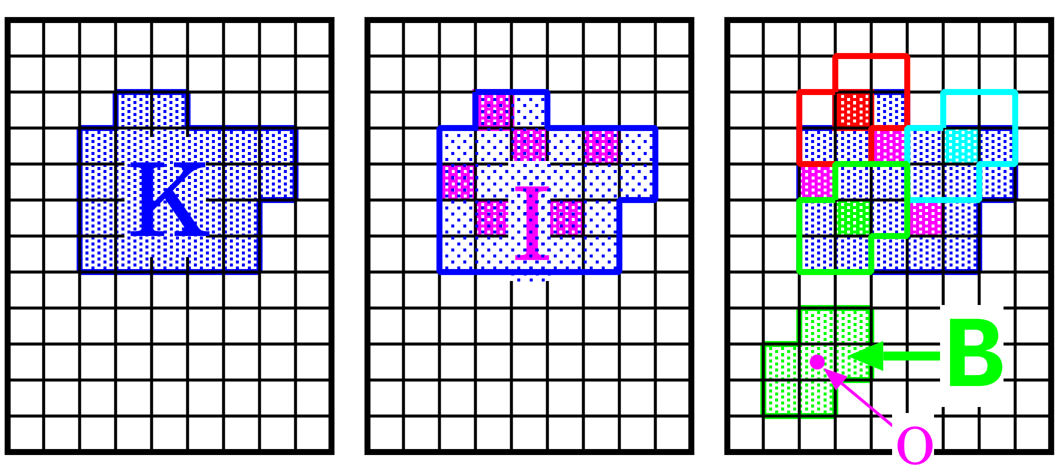
Proof: Let $\widehat{\mathcal{A}}$ be the dual group of $\mathcal{A}$. If $\chi \in \widehat{\mathcal{A}}$, let

$$\left\langle \chi, \mu_0^{(\mathbf{b})} \right\rangle \quad = \quad \sum_{a \in \mathcal{A}} \chi(a) \cdot \mu_0^{(\mathbf{b})}\{a\}.$$

Claim 1: *$\exists$ constant $c < 1$ so that, $\forall \chi \in \widehat{\mathcal{A}}$, and $\forall \mathbf{b} \in \mathcal{A}^{\mathbb{S}}$, $\left| \left\langle \chi, \mu_0^{(\mathbf{b})} \right\rangle \right| \leq c$.*

Claim 2: *$\exists$ constant B (determined by $\mathbb{B}$) so that, for any $\mathbb{K} \subset \mathbb{M}$, $\exists\ \mathbb{I} \subset \mathbb{K}$ so that:*

- *Elements of $\mathbb{I}$ are 'well-separated': $\forall\, i, j \in \mathbb{I}$, $(i - j) \notin \mathbb{B}$.*
- $|\mathbb{I}| \geq \dfrac{|\mathbb{K}|}{B}$.

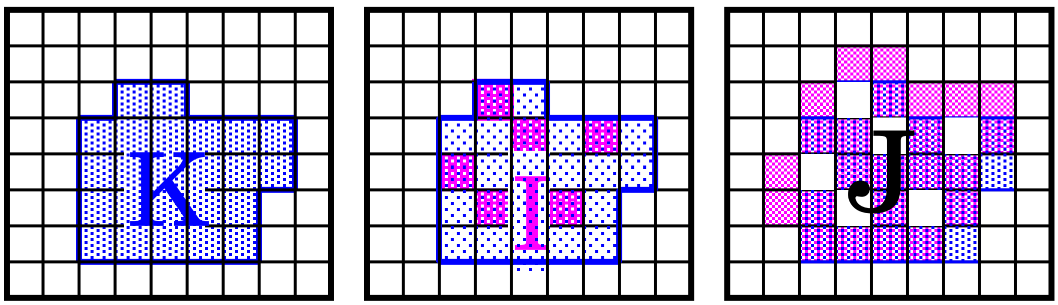


Let $\boldsymbol{\chi} = \bigotimes_{\mathsf{k}\in\mathbb{K}} \chi_k$ be a character ($\mathbb{K} \subset \mathbb{M}$ finite).

Then $\boldsymbol{\chi} \;=\; \boldsymbol{\chi}_{\mathbb{I}} \cdot \boldsymbol{\chi}_{\mathbb{K}\setminus\mathbb{I}}$, where

$$\boldsymbol{\chi}_{\mathbb{I}}(\mathbf{a}) \;=\; \prod_{i\in\mathbb{I}} \chi_i(a_i), \quad \text{and} \quad \boldsymbol{\chi}_{\mathbb{K}\setminus\mathbb{I}}(\mathbf{a}) \;=\; \prod_{k\in\mathbb{K}\setminus\mathbb{I}} \chi_k(a_k).$$

Let $\mathbb{J} \;=\; (\partial\,\mathbb{I}\,) \cup (\,\mathbb{K} \setminus \mathbb{I}\,)$.



Fix $\mathbf{b} \in \mathcal{A}^{\mathbb{J}}$. Then $\mu_{\mathbb{I}}^{(\mathbf{b})}$ is a product measure:

$$\text{For any } \mathbf{a} \in \mathcal{A}^{\mathbb{I}}, \quad \mu_{\mathbb{I}}^{(\mathbf{b})}[\mathbf{a}] \quad = \quad \prod_{i\in\mathbb{I}} \mu_i^{(\mathbf{b})}[a_i].$$

$$\text{Thus,} \quad \left\langle \boldsymbol{\chi}_{\mathbb{I}},\ \mu_{\mathbb{I}}^{(\mathbf{b})} \right\rangle \;=\; \prod_{i\in\mathbb{I}} \left\langle \chi_i,\ \mu_i^{(\mathbf{b})} \right\rangle.$$

$$\text{Thus,} \quad \left|\left\langle \boldsymbol{\chi}_{\mathbb{I}},\ \mu_{\mathbb{I}}^{(\mathbf{b})} \right\rangle\right| \;=\; \prod_{i\in\mathbb{I}} \left|\left\langle \chi_i,\ \mu_i^{(\mathbf{b})} \right\rangle\right| \quad \leq \quad \prod_{i\in\mathbb{I}} c \quad \text{(Claim 1).}$$
$$= \; c^{|\mathbb{I}|} \quad \leq \quad c^{|\mathbb{K}|/B} \qquad \text{(Claim 2).}$$

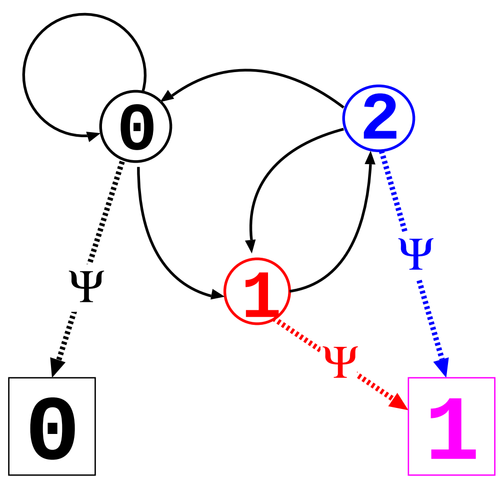
$$\text{Thus,} \quad \left|\left\langle \boldsymbol{\chi},\ \mu^{(\mathbf{b})} \right\rangle\right| \;=\; \left|\boldsymbol{\chi}_{\mathbb{K}\setminus\mathbb{I}}(\mathbf{b})\right| \cdot \prod_{i\in\mathbb{I}} \left|\left\langle \chi_i,\ \mu_i^{(\mathbf{b})} \right\rangle\right| \quad \leq \quad 1 \cdot c^{|\mathbb{K}|/B}.$$

This holds for all $\mathbf{b} \in \mathcal{A}^{\mathbb{J}}$. Thus, $|\langle \boldsymbol{\chi},\ \mu\rangle| \;\leq\; c^{|\mathbb{K}|/B}$, and $c^{|\mathbb{K}|/B} \to 0$ as $\mathsf{rank}\,[\boldsymbol{\chi}] = |\mathbb{K}| \to \infty$, because $|c| < 1$. $\square$

Sofic Shifts

A **sofic shift** is the image of a SFT under a block map Ψ.

The Even Sofic Shift



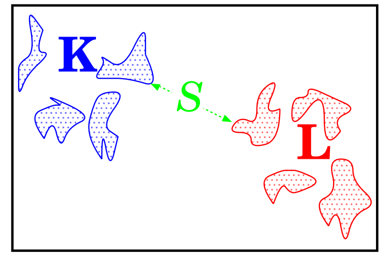
$$\mathbf{a} = [\ldots 0,1,2,1,2,0,0,0,0,1,2,0,0,1,2,1,2,1,2,0,0,\ldots]$$
$$\Psi(\mathbf{a}) = [\ldots 0,1,1,1,1,0,0,0,0,1,1,0,0,1,1,1,1,1,1,0,0,\ldots]$$

Proposition: (Y&P, 2001)
Let μ be the measure of maximal entropy on the Even Shift. Then μ is not harmonically mixing.

Question: Do LCA asymptotically randomize measures on sofic shifts?

We need a condition weaker than harmonic mixing.

Dispersion Mixing

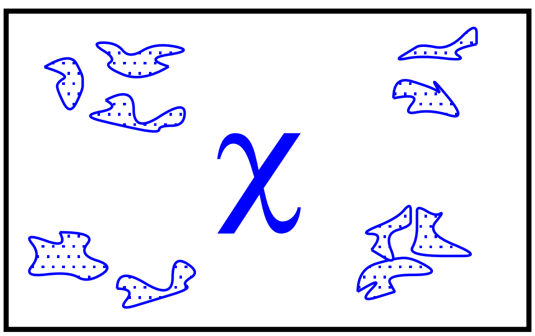


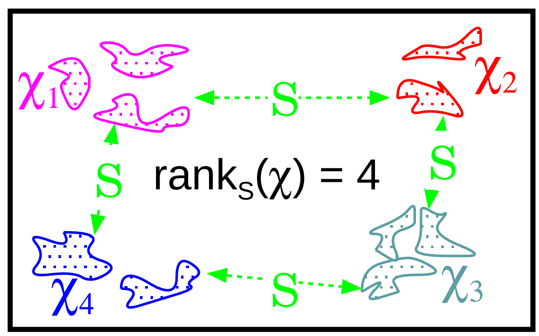
Let $S > 0$. Subsets $\mathbb{K}$, $\mathbb{L} \subset \mathbb{Z}^D$ are S**-separated** if

$$\min\{|\mathsf{k} - \ell| \ ; \ \mathsf{k} \in \mathbb{K} \text{ and } \ell \in \mathbb{L}\} \quad \geq \quad S.$$

Characters $\boldsymbol{\chi} \ = \ \bigotimes_{\mathsf{k}\in\mathbb{K}} \chi_{\mathsf{k}}$ and $\boldsymbol{\lambda} \ = \ \bigotimes_{\ell\in\mathbb{L}} \lambda_\ell$ are S**-separated** if $\mathbb{K}$ and $\mathbb{L}$ are S-separated. Define:

$$\mathsf{rank}_S(\chi) \quad = \quad \max\left\{ \begin{array}{l} R \ ; \ \exists\, \boldsymbol{\chi}_1, \ldots, \boldsymbol{\chi}_R \text{ mutually } S\text{-separated,} \\ \qquad \text{so that } \boldsymbol{\chi} = \boldsymbol{\chi}_1 \otimes \cdots \otimes \boldsymbol{\chi}_R \end{array} \right\}.$$





The measure μ is **dispersion mixing** (DM) if, for every $\epsilon > 0$, there are $S, R > 0$ so that, for any character $\boldsymbol{\chi}$,

$$\Big(\mathsf{rank}_S(\boldsymbol{\chi}) \ > \ R \Big) \Longrightarrow \Big(|\langle \boldsymbol{\chi}, \mu \rangle| \ < \ \epsilon \Big).$$

Proposition: *Let μ be a mixing N-step Markov measure on $\mathcal{A}^{\mathbb{Z}}$.*

1. *μ is DM.* *(and $\mathsf{supp}(\mu)$ is a subshift of finite type).*

2. *If $\Psi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{B}^{\mathbb{Z}}$ is a block map, and $\nu = \Psi(\mu)$, then ν is also DM.* *(and $\mathsf{supp}(\mu)$ is a sofic shift).* ______ □

Example: The measure of max. entropy on the Even Shift is DM.

Dispersive Cellular Automata

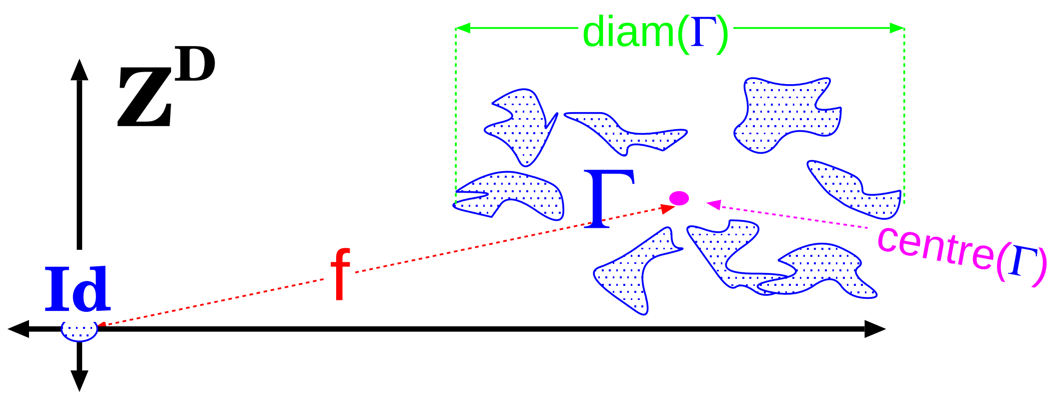
If Φ is an LCA and $\boldsymbol{\chi}$ is a character, then $\boldsymbol{\chi} \circ \Phi$ is also a character.

Φ is **dispersive** if, for any $S > 0$, and any $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$, there is subset $\mathbb{J} \subset \mathbb{N}$ of density 1 so that $\displaystyle\lim_{\mathbb{J} \ni j \to \infty} \mathsf{rank}_S \left(\boldsymbol{\chi} \circ \Phi^j \right) = \infty$.

Theorem: *If Φ is dispersive and μ is DM, then Φ asymptotically randomizes μ.*

Bipartite CA & Dispersion

If $\Gamma = \displaystyle\sum_{\mathsf{g} \in \mathbb{G}} \gamma_{\mathsf{g}} \cdot \boldsymbol{\sigma}^{\mathsf{g}}$ is an LCA, then $\mathsf{diam}\,[\Gamma] = \max\left\{ |\mathsf{g} - \mathsf{h}| \ ; \ \mathsf{g}, \mathsf{h} \in \mathbb{G} \right\}$.



$$\mathsf{centre}\,(\Gamma) = \frac{1}{\mathrm{card}\,[\mathbb{G}]} \sum_{\mathsf{g} \in \mathbb{G}} \mathsf{g}$$ is the centroid of $\mathbb{G}$ (as subset of $\mathbb{R}^D$).

Let $\mathcal{A} = \mathbb{Z}_{/p}$ for $p \geq 5$. Φ is **bipartite** if $\Phi = \mathbf{Id} + \Gamma \circ \boldsymbol{\sigma}^{\mathsf{f}}$, where $|\mathsf{centre}\,(\Gamma)| < 1$ and $\mathsf{diam}\,[\Gamma] \leq \frac{1}{2} \cdot |\mathsf{f}|$. For example:

$$\Phi = 1 + \boldsymbol{\sigma} = 1 + \underbrace{\mathbf{Id}}_{\mathsf{diam}[\Gamma]=0} \circ \boldsymbol{\sigma}^1, \qquad \text{or} \quad \Phi = 1 + \boldsymbol{\sigma}^2 + \boldsymbol{\sigma}^3 = 1 + \underbrace{(1 + \boldsymbol{\sigma})}_{\mathsf{diam}[\Gamma]=1} \circ \boldsymbol{\sigma}^2$$

Theorem: *If Φ is bipartite then Φ is dispersive.*

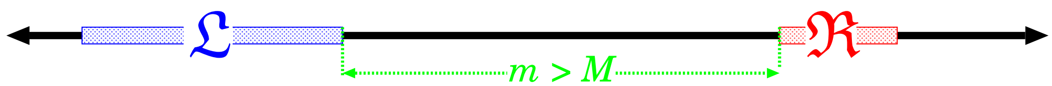
(similar results for $p = 2$ or $p = 3$.)

Uniform Mixing & Dispersion Mixing

Measure μ on $\mathcal{A}^{\mathbb{Z}}$ is **uniformly mixing** (UM) if, for any $\epsilon > 0$, there $\exists$ $M > 0$ so that, for any cylinder subsets $\mathfrak{L} \subset \mathcal{A}^{(-\infty..0]}$ and $\mathfrak{R} \subset \mathcal{A}^{[0..\infty)}$, and any $m > M$,

$$\mu\left[\boldsymbol{\sigma}^m(\mathfrak{L}) \cap \mathfrak{R}\right] \underset{\epsilon}{\sim} \mu\left[\mathfrak{L}\right] \cdot \mu\left[\mathfrak{R}\right] \tag{1}$$

("$x \underset{\epsilon}{\sim} y$" means $|x - y| < \epsilon$.)



Example: Any mixing Markov measure is uniformly mixing.

μ is **harmonically bounded** (HB) if there is some $C < 1$ so that $|\langle \boldsymbol{\chi}, \mu \rangle| < C$ for all $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{Z}}}$ except $\boldsymbol{\chi} = \mathbb{1}$.

Example: Any system with 'high enough' entropy is HB.

Theorem: *If μ is UM and HB then μ is DM.*

A **quasi-Markov measure** is a mixing Markov measure, or the image of a mixing Markov measure under a block map.

Example: The measure of max. entropy on the Even Shift is quasi-Markov.

Theorem: *Any high-entropy quasi-Markov measure is UM and HB, therefor dispersion mixing.*

Example: The measure of max.entropy on the Even Shift is DM.

$$\Big(\textbf{LCA composition}\Big) \Longleftrightarrow \Big(\textbf{Polynomial multiplication}\Big)$$

Example: Suppose $\mathbb{M} = \mathbb{Z}$ and $\phi(\mathbf{a}) = a_0 + a_1$. Then

$$\begin{array}{rcccl}
\Phi & = & (1+\boldsymbol{\sigma})^1 & = & 1 + \boldsymbol{\sigma} \\
\Phi^{\circ 2} & = & (1+\boldsymbol{\sigma})^2 & = & 1 + 2\boldsymbol{\sigma} + \boldsymbol{\sigma}^2 \\
\Phi^{\circ 3} & = & (1+\boldsymbol{\sigma})^3 & = & 1 + 3\boldsymbol{\sigma} + 3\boldsymbol{\sigma}^2 + \boldsymbol{\sigma}^3 \\
\Phi^{\circ 4} & = & (1+\boldsymbol{\sigma})^4 & = & 1 + 4\boldsymbol{\sigma} + 6\boldsymbol{\sigma}^2 + 4\boldsymbol{\sigma}^3 + \boldsymbol{\sigma}^4 \\
\Phi^{\circ 5} & = & (1+\boldsymbol{\sigma})^5 & = & 1 + 5\boldsymbol{\sigma} + 10\boldsymbol{\sigma}^2 + 10\boldsymbol{\sigma}^3 + 5\boldsymbol{\sigma}^4 + \boldsymbol{\sigma}^5 \\
 & \vdots & & &
\end{array}$$

Suppose $\mathcal{A} = \mathbb{Z}_{/2}$; thus $\phi(\mathbf{a}) = a_0 + a_1 \pmod 2$.

$$\begin{array}{rcccl}
\Phi & = & (1+\boldsymbol{\sigma})^1 & = & 1 + \boldsymbol{\sigma} \\
\Phi^{\circ 2} & = & (1+\boldsymbol{\sigma})^2 & = & 1 + \boldsymbol{\sigma}^2 \\
\Phi^{\circ 3} & = & (1+\boldsymbol{\sigma})^3 & = & 1 + \boldsymbol{\sigma} + \boldsymbol{\sigma}^2 + \boldsymbol{\sigma}^3 \\
\Phi^{\circ 4} & = & (1+\boldsymbol{\sigma})^4 & = & 1 + \boldsymbol{\sigma}^4 \\
\Phi^{\circ 5} & = & (1+\boldsymbol{\sigma})^5 & = & 1 + \boldsymbol{\sigma} + \boldsymbol{\sigma}^4 + \boldsymbol{\sigma}^5 \\
\Phi^{\circ 6} & = & (1+\boldsymbol{\sigma})^6 & = & 1 + \boldsymbol{\sigma}^2 + \boldsymbol{\sigma}^4 + \boldsymbol{\sigma}^6 \\
\Phi^{\circ 7} & = & (1+\boldsymbol{\sigma})^6 & = & 1 + \boldsymbol{\sigma} + \boldsymbol{\sigma}^2 + \boldsymbol{\sigma}^3 + \boldsymbol{\sigma}^4 + \boldsymbol{\sigma}^5 + \boldsymbol{\sigma}^6 + \boldsymbol{\sigma}^7 \\
 & \vdots & & &
\end{array}$$

In general:

If $\boldsymbol{\phi}(x) = \sum_{u \in \mathbb{U}} \varphi_u \cdot x^u$ is a formal polynomial with 'powers' in $\mathbb{M}$,

and $\Phi = \sum_{u \in \mathbb{U}} \varphi_u \cdot \boldsymbol{\sigma}^u = \boldsymbol{\phi}(\boldsymbol{\sigma})$ is the corresponding LCA,

Then: $\Phi \circ \Phi = (\boldsymbol{\phi} \cdot \boldsymbol{\phi})(\boldsymbol{\sigma})$, $\Phi \circ \Phi \circ \Phi = \boldsymbol{\phi}^3(\boldsymbol{\sigma})$, etc.

Lucas Theorem

If $n \in \mathbb{N}$, let $\left[n^{[i]}|_{i=0}^{\infty}\right]$ be the **binary expansion** of n.

Example: Let $n = 19_{\text{dec}} = \ldots 0010011_{\text{bin}}$. Thus, $n^{[0]} = 1$, $n^{[1]} = 1$, $n^{[2]} = 0$, $n^{[3]} = 0$, $n^{[4]} = 1$, $n^{[5]} = 0$, etc.

Define $\mathcal{L}(N) = \left\{ \ell \in \mathbb{N}\,; \quad \ell^{[i]} \leq N^{[i]},\ \forall i \in \mathbb{N} \right\}$.

Example:

$$\begin{aligned}
\mathcal{L}(19_{\text{dec}}) &= \mathcal{L}(10011_{\text{bin}}) \\
&= \left\{ 0_{\text{bin}}, 1_{\text{bin}}, 10_{\text{bin}}, 11_{\text{bin}}, 10000_{\text{bin}}, 10001_{\text{bin}}, 10010_{\text{bin}}, 10011_{\text{bin}} \right\} \\
&= \left\{ 0_{\text{dec}}, 1_{\text{dec}}, 2_{\text{dec}}, 3_{\text{dec}}, 16_{\text{dec}}, 17_{\text{dec}}, 18_{\text{dec}}, 19_{\text{dec}} \right\}.
\end{aligned}$$

Lucas Theorem for binomial coefficients, mod 2:

$$\begin{bmatrix} N \\ n \end{bmatrix}_2 = \begin{cases} 1 & \text{if } n \in \mathcal{L}(N)\,; \\ 0 & \text{if } n \notin \mathcal{L}(N)\,. \end{cases}$$

Consequence: If $\Phi = 1 + \boldsymbol{\sigma}$, then

$$\Phi^N = (1+\boldsymbol{\sigma})^N = \sum_{n=0}^{N} \begin{bmatrix} N \\ n \end{bmatrix}_2 \boldsymbol{\sigma}^n = \sum_{n \in \mathcal{L}(N)} \boldsymbol{\sigma}^n.$$

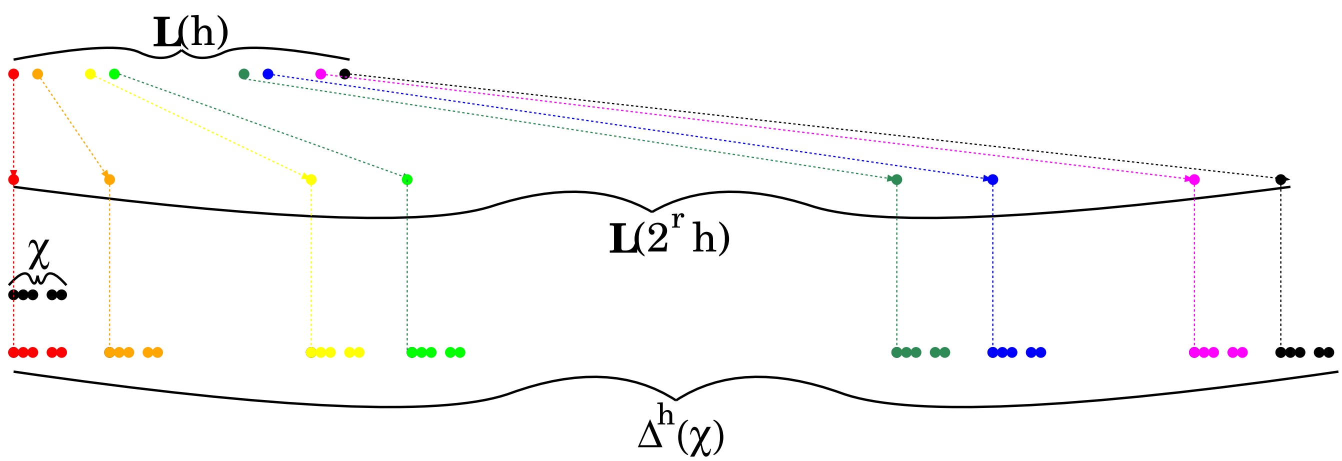
Example:

$$\Phi^{19} = 1 + \boldsymbol{\sigma} + \boldsymbol{\sigma}^2 + \boldsymbol{\sigma}^3 \quad + \quad \boldsymbol{\sigma}^{16} + \boldsymbol{\sigma}^{17} + \boldsymbol{\sigma}^{18} + \boldsymbol{\sigma}^{19}.$$

Lucas Mixing

Let $\boldsymbol{\chi} = \chi_0 \otimes \chi_1 \otimes \ldots \otimes \chi_K \in \widehat{\mathcal{A}^{\mathbb{Z}}}$. If $H \in \mathbb{N}$, define

$$\boldsymbol{\Delta}^H(\boldsymbol{\chi}) = \bigotimes_{h \in \mathcal{L}(H)} \boldsymbol{\chi} \circ \boldsymbol{\sigma}^{2^r \cdot h}, \qquad \text{where } r = \lceil \log_2(K) \rceil.$$



Example: Let $\boldsymbol{\chi} = \xi_0 \otimes \xi_1 \otimes \xi_2 \otimes \xi_3$, where $\xi_k(\mathbf{a}) = (-1)^{a_k}$.

Thus, $r = \lceil \log_2(3) \rceil = 2$.

Let $H = 4$. Then $\mathcal{L}(4) = \{0, 4\}$, so

$$\begin{aligned}
\boldsymbol{\Delta}^4(\boldsymbol{\chi}) &= \boldsymbol{\chi} \circ \boldsymbol{\sigma}^{2^r \cdot 0} \otimes \boldsymbol{\chi} \circ \boldsymbol{\sigma}^{2^r \cdot 4} = \boldsymbol{\chi} \circ \boldsymbol{\sigma}^0 \otimes \boldsymbol{\chi} \circ \boldsymbol{\sigma}^{2^2 \cdot 4} \\
&= \boldsymbol{\chi} \otimes \boldsymbol{\chi} \circ \boldsymbol{\sigma}^{16} \\
&= \xi_0 \otimes \xi_1 \otimes \xi_2 \otimes \xi_3 \otimes \xi_{16} \otimes \xi_{17} \otimes \xi_{18} \otimes \xi_{19}.
\end{aligned}$$

Measure μ is **Lucas mixing** (LM) if:

For all $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{Z}}}$, there is a subset $\mathbb{H} \subset \mathbb{N}$ of density 1 so that

$$\lim_{\mathbb{H} \ni H \to \infty} \langle \boldsymbol{\Delta}^H(\boldsymbol{\chi}), \mu \rangle = 0.$$

Theorem: *Any DM measure is LM*
In particular, any high-entropy quasi-Markov measure is LM.

LM & Asymptotic Randomization

Theorem *Let* $\Phi = 1 + \boldsymbol{\sigma}$. *Then*

$$\Big(\Phi \textit{ asymptotically randomizes } \mu \Big) \iff \Big(\mu \textit{ is LM} \Big).$$

Let $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{Z}}}$. For $\forall\ m \in \mathbb{N}$, let $\boldsymbol{\chi}^m = \boldsymbol{\chi} \circ \Phi^m$.

Lemma: There is a subset $\mathbb{N}_{\boldsymbol{\chi}}$ of density 1 so that, $\forall\ N \in \mathbb{N}_{\boldsymbol{\chi}}$:

1. $N = M + 2^r \cdot H$ for some M, r, and H.
2. $\boldsymbol{\chi} \circ \Phi^N = \boldsymbol{\Delta}^H \left(\boldsymbol{\chi}^M\right)$

Proof: Observe: $19 = 3 + 16 = 3 + 2^4$, and

$$\begin{aligned}
\mathcal{L}(19) &= \{0,1,2,3\} \sqcup \{16,17,18,19\} \\
&= \Big(\{0,1,2,3\} + 0\Big) \sqcup \Big(\{0,1,2,3\} + 16\Big) \\
&= \{0,1,2,3\} + \{0,16\} \quad = \quad \mathcal{L}(3) + 2^4 \cdot \{0,1\} \\
&= \mathcal{L}(3) + 2^4 \cdot \mathcal{L}(1).
\end{aligned}$$

Claim: *Let* $r,\ H \in \mathbb{N}$. *If* $M < 2^r$, *and* $N = M + 2^r \cdot H$, *then*

$$\mathcal{L}(N) = \mathcal{L}(M) + 2^r \cdot \mathcal{L}(H). \qquad \square$$

Consequence:

$$\begin{aligned}
\Phi^N &= \sum_{n \in \mathcal{L}(N)} \boldsymbol{\sigma}^n \quad = \quad \sum_{m \in \mathcal{L}(M)} \sum_{h \in \mathcal{L}(H)} \boldsymbol{\sigma}^{m + 2^r h} \\
&= \sum_{h \in \mathcal{L}(H)} \left(\sum_{m \in \mathcal{L}(M)} \boldsymbol{\sigma}^m \right) \circ \boldsymbol{\sigma}^{2^r h} \quad = \quad \sum_{h \in \mathcal{L}(H)} \Phi^M \circ \boldsymbol{\sigma}^{2^r h}
\end{aligned}$$

Now, suppose $\boldsymbol{\chi} = \chi_0 \otimes \ldots \otimes \chi_K$, and $N = M + 2^r \cdot H$. Then for 'most' M, r, and H,

$$\boldsymbol{\chi} \circ \Phi^N = \bigotimes_{h \in \mathcal{L}(H)} \left(\boldsymbol{\chi} \circ \Phi^M\right) \circ \boldsymbol{\sigma}^{2^r h} = \bigotimes_{h \in \mathcal{L}(H)} \boldsymbol{\chi}^M \circ \boldsymbol{\sigma}^{2^r h} = \boldsymbol{\Delta}^H \left(\boldsymbol{\chi}^M\right). \square$$