Limit Measures for Affine Cellular Automata

Marcus Pivato (University of Houston)

Reem Yassawi (Trent University)

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

Preliminaries

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

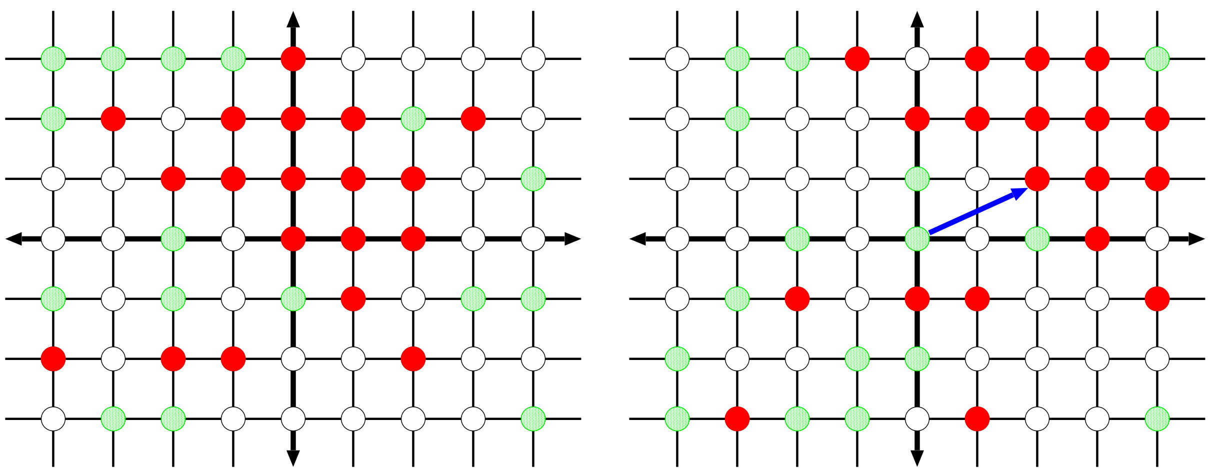
$\mathbb{M}$: a **lattice** (for example, $\mathbb{M} = \mathbb{N},\ \mathbb{Z},\ \mathbb{N}^d \times \mathbb{Z}^{D_2}$).

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

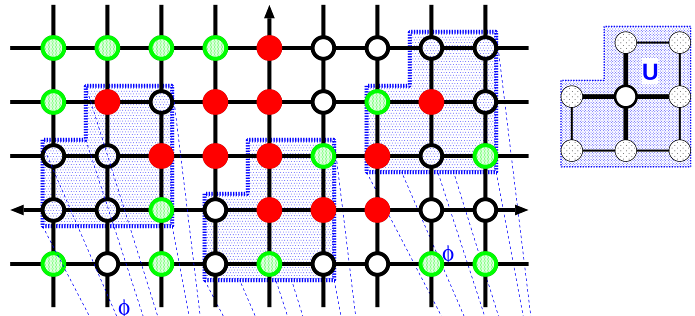
An element of $\mathcal{A}^{\mathbb{M}}$ will be written as $\mathbf{a} = [a_m]_{m \in \mathbb{M}}$.

$\mathbb{M}$ acts on itself by **translation**. This induces a **shift action** of $\mathbb{M}$ on $\mathcal{A}^{\mathbb{M}}$: for all $u \in \mathbb{M}$, and $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, define

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

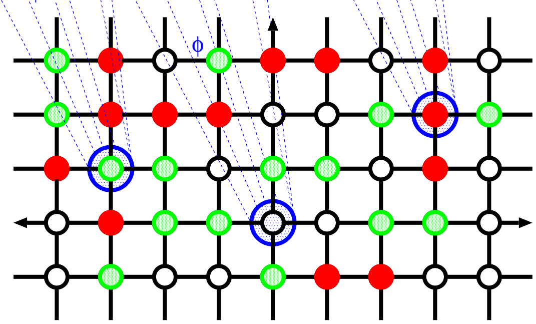


Cellular Automata



Neighbourhood:

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



Local transformation rule:

ϕ: $\mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$

The CA **induced by** ϕ is function Φ: $\mathcal{A}^{\mathbb{M}} \hookleftarrow$ so that, for any $[a_m|_{m\in\mathbb{M}}]$ in $\mathcal{A}^{\mathbb{M}}$,

$$\Phi(\mathbf{a}) = [b_m|_{m\in\mathbb{M}}], \quad \text{where, } \forall m \in \mathbb{M}, \quad b_m \;=\; \phi\left[a_{(u+m)}|_{u\in\mathbb{U}}\right].$$

Equivalently:

A CA is a *continuous transformation commuting with all shifts*:

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

Example: *Nearest-neighbour XOR*

Lattice: $\mathbb{M} = \mathbb{Z}$;

Neighbourhood: $\mathbb{U} = \{-1, +1\}$;

Alphabet: $\mathcal{A} = \{0, 1\} \cong \mathbb{Z}_{/2}$;

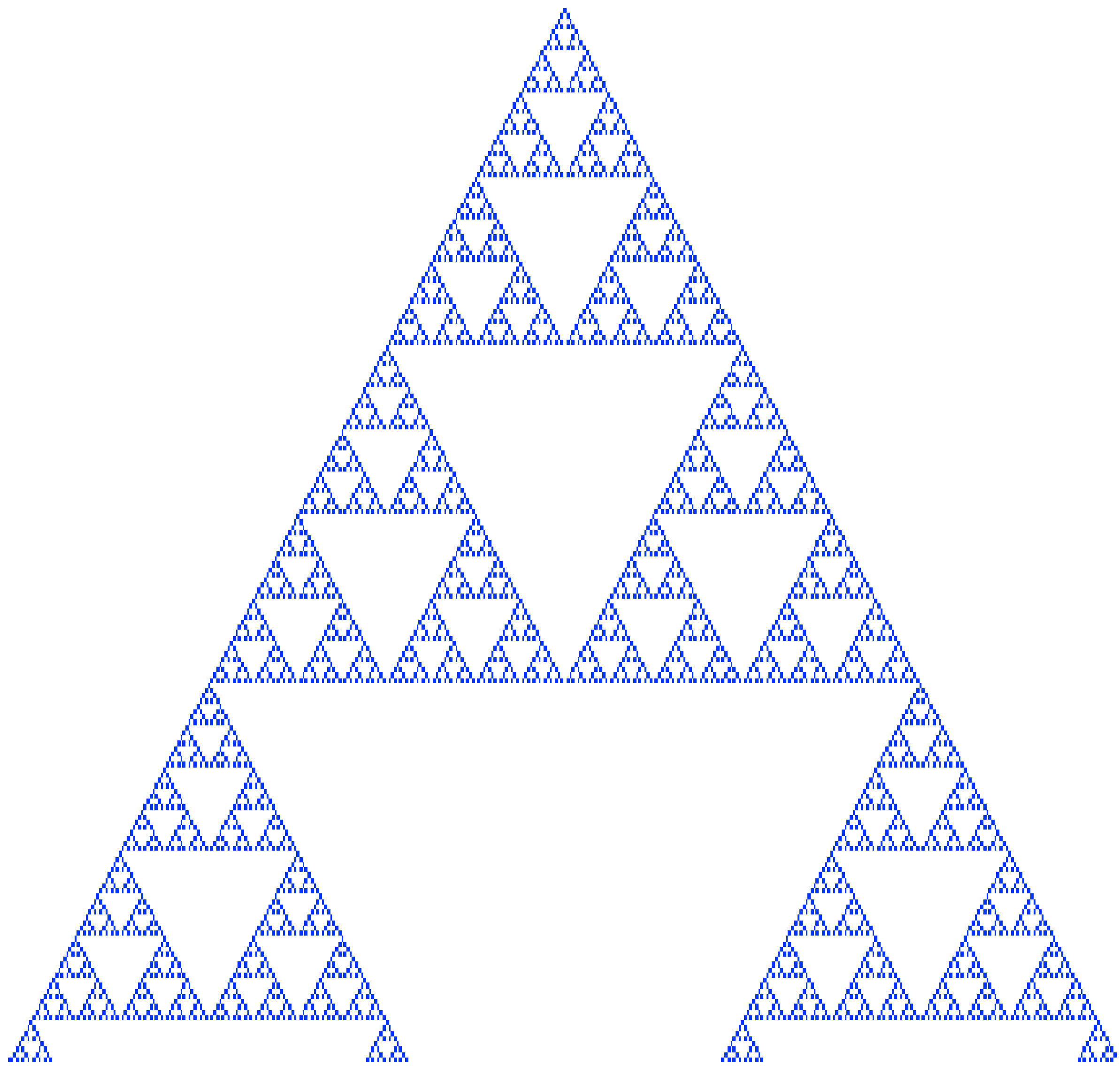
Local Map: $\phi(\mathbf{a}) \;=\; a_{-1} + a_1 \pmod 2$.

⟵ Space ⟶

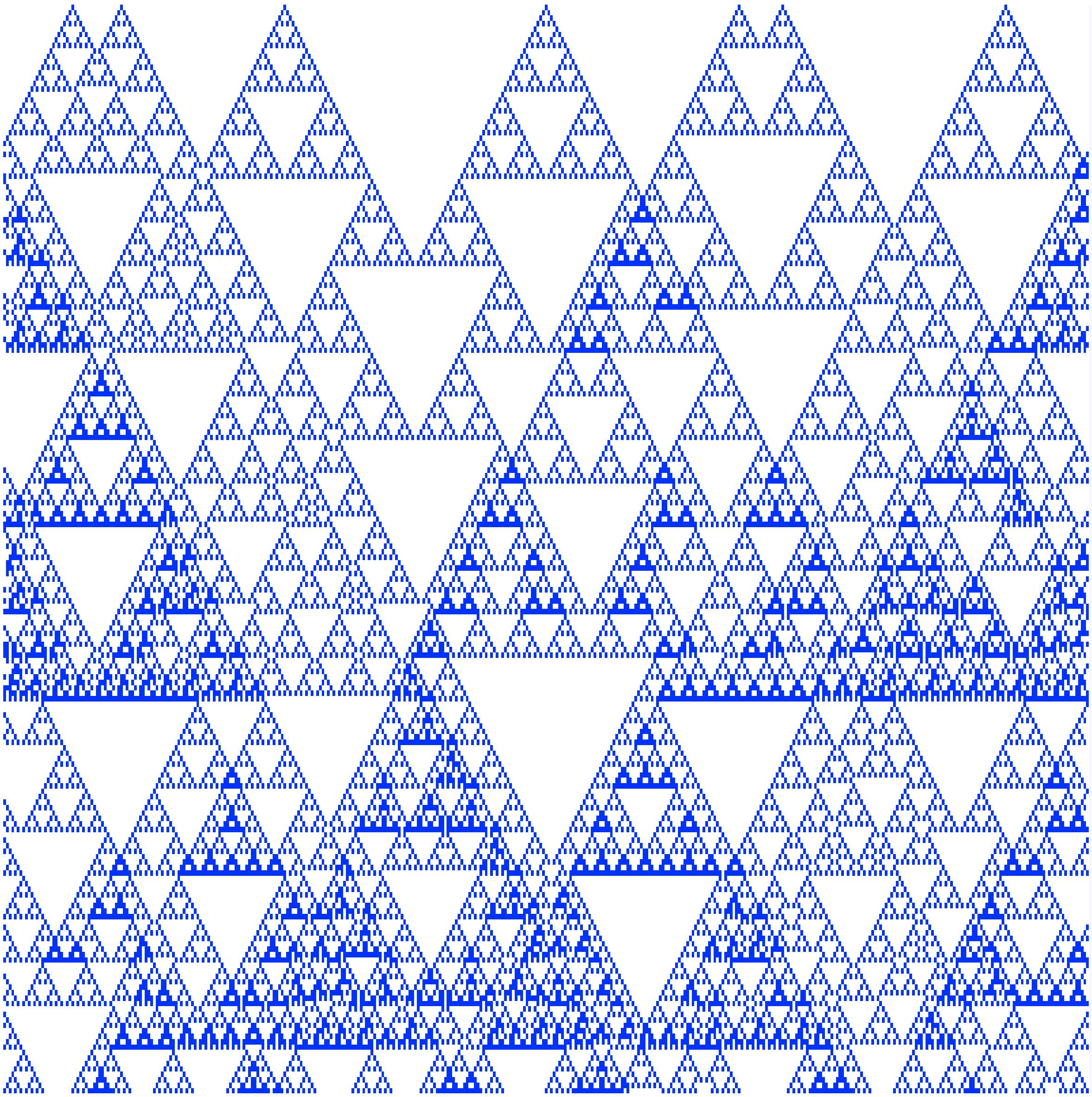
$\mathbb{U}$:	.	.	.	.	.	.	.	.	.	.	□	.	□	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	1	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	1	.	1	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	1	.	.	.	1	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	1	.	1	.	1	.	1	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	1	.	.	.	.	.	.	.	1	.	.	.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

Time ↓

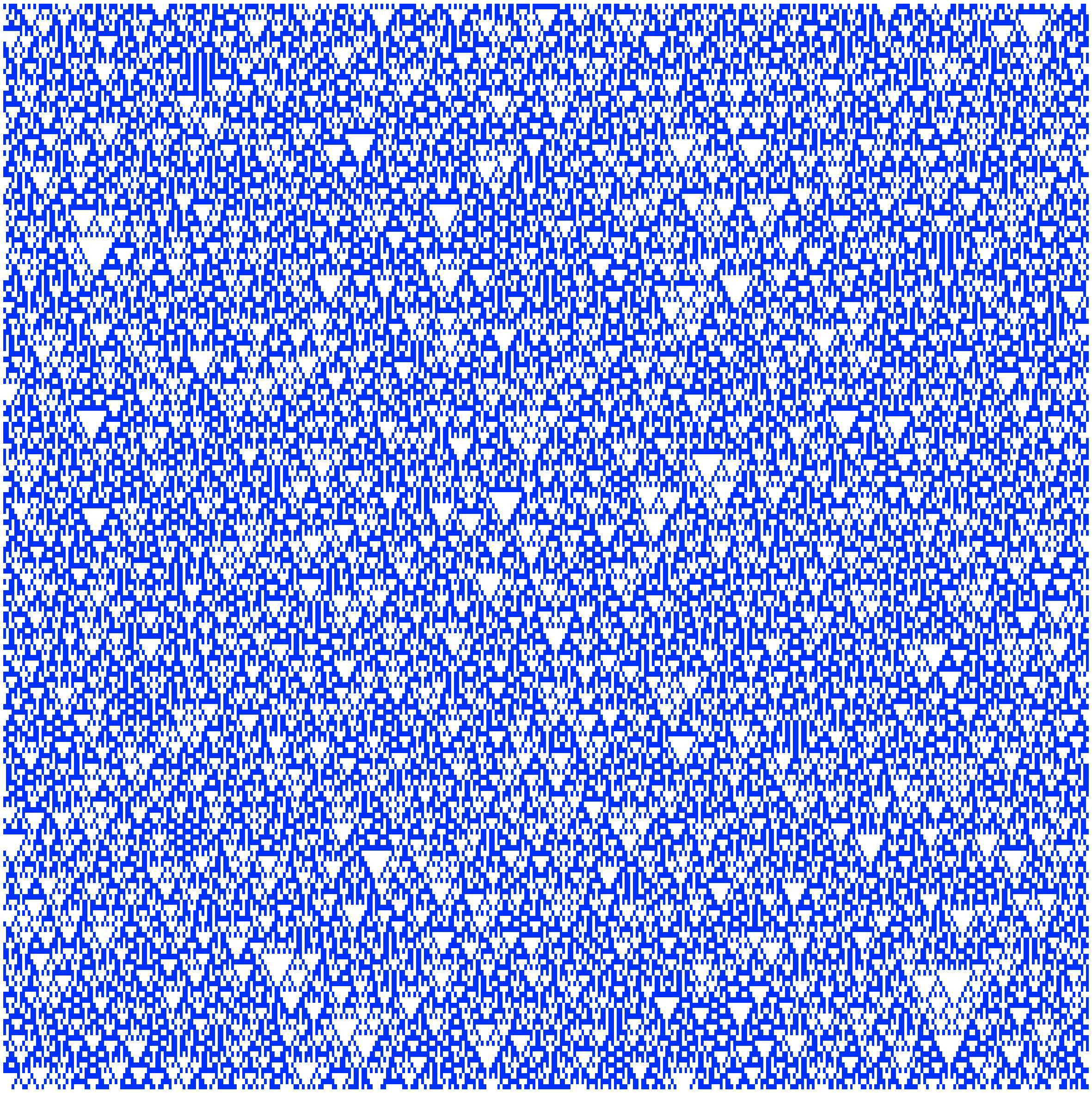
Initial Conditions: *Point mass*



Initial Conditions: *Isolated point masses*



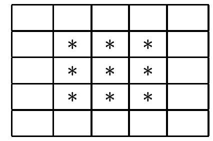
Initial Conditions: *Random*



Example: John H. Conway's *Game of Life*

Lattice: $\mathbb{M} = \mathbb{Z}^2$;

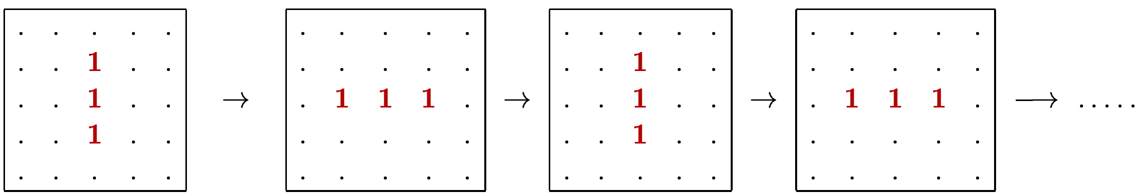
Neighbourhood: $\mathbb{U} = [-1..1] \times [-1..1]$;



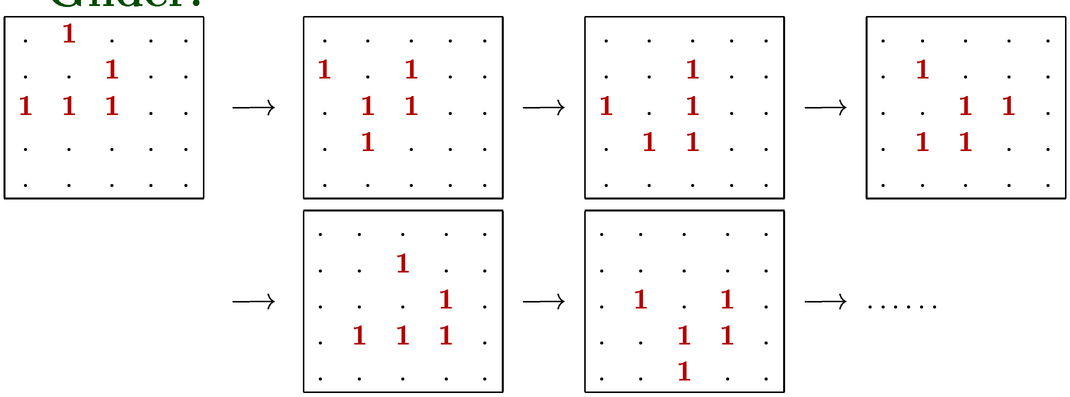
Alphabet: $\mathcal{A} = \{0, 1\}$;

Local Map:
$$\phi(\mathbf{a}) = \begin{cases} 1 & \text{if } a_0 = 1 \text{ and } \sum_{u \in \mathbb{U}} a_u = 3, 4 \\ 1 & \text{if } a_0 = 0 \text{ and } \sum_{u \in \mathbb{U}} a_u = 3, \\ 0 & \text{otherwise.} \end{cases}$$

Blinker:



Glider:



- Emergence of large scale, coherent structure.
- Universal computation.

Linear Cellular Automata

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

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

Cellular automaton Φ is **linear** if it is a group endomorphism.

Equivalently: $\phi : \underbrace{\mathcal{A}^{\mathbb{U}}}_{\text{Product group}} \longrightarrow \mathcal{A}$ is a homomorphism.

Fact: $\mathcal{A} = \mathbb{Z}_{/n}$ is a ring under multiplication. Any LCA can be written as a 'polynomial of shift maps':

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

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

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

$\mathbf{a}$:			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		

$\Big($ LCA composition $\Big) \Longleftrightarrow \Big($ Polynomial multiplication $\Big)$

$$\boldsymbol{\phi}(x) = \sum_{u\in\mathbb{U}} \varphi_u \cdot x^u \qquad \text{(formal polynomial with `powers' in } \mathbb{M})$$

$$\Phi \;=\; \sum_{u\in\mathbb{U}} \varphi_u \cdot \boldsymbol{\sigma}^u \;=\; \boldsymbol{\phi}(\boldsymbol{\sigma}) \qquad \text{(corresponding LCA).}$$

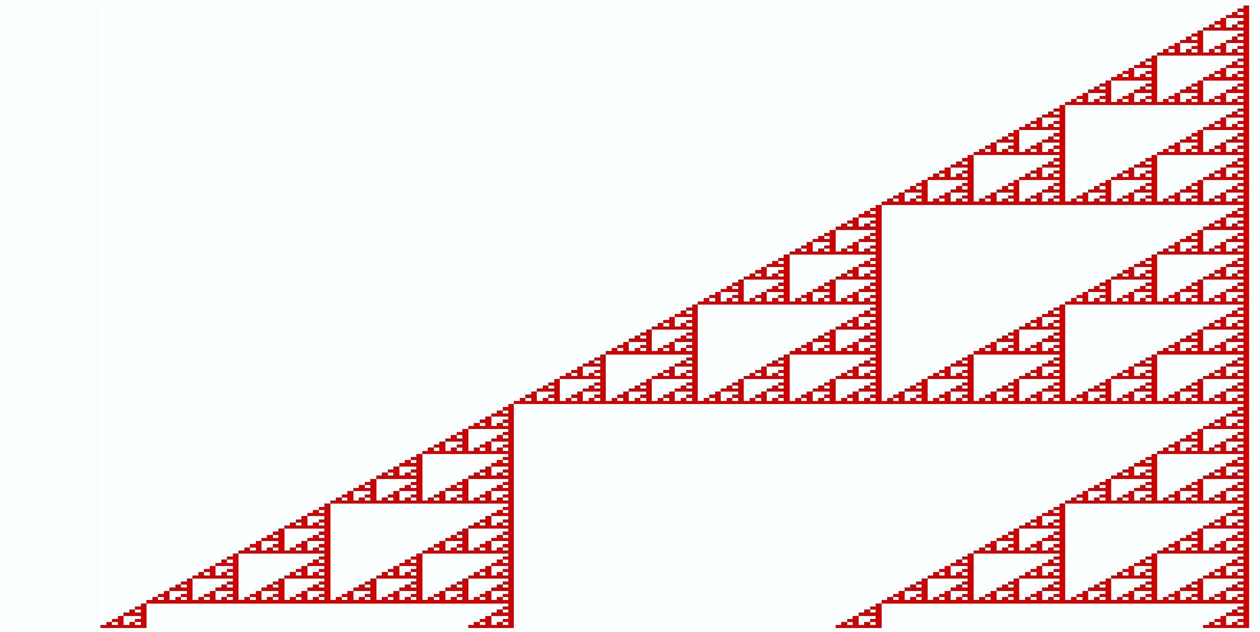
Then: $\Phi \circ \Phi \;=\; (\boldsymbol{\phi}\cdot\boldsymbol{\phi})(\boldsymbol{\sigma})$, $\qquad \Phi\circ\Phi\circ\Phi \;=\; \boldsymbol{\phi}^3(\boldsymbol{\sigma})$, etc.

Example: $\mathcal{A} = \mathbb{Z}_{/2}$; $\quad \mathbb{M} = \mathbb{Z}$; $\quad \phi(\mathbf{a}) = a_0 + a_1 \pmod 2$.

$$\begin{array}{rcccl}
\Phi & = & (\boldsymbol{\sigma}^0+\boldsymbol{\sigma}^1)^1 & = & \boldsymbol{\sigma}^0 + \boldsymbol{\sigma}^1 \\
\Phi^{\circ 2} & = & (\boldsymbol{\sigma}^0+\boldsymbol{\sigma}^1)^2 & = & \boldsymbol{\sigma}^0 + \boldsymbol{\sigma}^2 \\
\Phi^{\circ 3} & = & (\boldsymbol{\sigma}^0+\boldsymbol{\sigma}^1)^3 & = & \boldsymbol{\sigma}^0 + \boldsymbol{\sigma}^1 + \boldsymbol{\sigma}^2 + \boldsymbol{\sigma}^3 \\
\Phi^{\circ 4} & = & (\boldsymbol{\sigma}^0+\boldsymbol{\sigma}^1)^4 & = & \boldsymbol{\sigma}^0 + \boldsymbol{\sigma}^4 \\
\Phi^{\circ 5} & = & (\boldsymbol{\sigma}^0+\boldsymbol{\sigma}^1)^5 & = & \boldsymbol{\sigma}^0 + \boldsymbol{\sigma}^1 + \boldsymbol{\sigma}^4 + \boldsymbol{\sigma}^5 \\
\Phi^{\circ 6} & = & (\boldsymbol{\sigma}^0+\boldsymbol{\sigma}^1)^6 & = & \boldsymbol{\sigma}^0 + \boldsymbol{\sigma}^2 + \boldsymbol{\sigma}^4 + \boldsymbol{\sigma}^6 \\
\Phi^{\circ 7} & = & (\boldsymbol{\sigma}^0+\boldsymbol{\sigma}^1)^7 & = & \boldsymbol{\sigma}^0 + \boldsymbol{\sigma}^1 + \boldsymbol{\sigma}^2 + \boldsymbol{\sigma}^3 + \boldsymbol{\sigma}^4 + \boldsymbol{\sigma}^5 + \boldsymbol{\sigma}^6 + \boldsymbol{\sigma}^7 \\
\Phi^{\circ 8} & = & (\boldsymbol{\sigma}^0+\boldsymbol{\sigma}^1)^8 & = & \boldsymbol{\sigma}^0 + \boldsymbol{\sigma}^8 \\
 & \vdots & \vdots & \vdots &
\end{array}$$

- Pascal's triangle, mod 2.

$\Phi = \boldsymbol{\sigma}^0 + \boldsymbol{\sigma}^1$;   **Initial Conditions:** *Point mass*



Affine Cellular Automata

$\Phi(\mathbf{a}) = \Psi(\mathbf{a}) + \mathbf{c}$, where

- Ψ is a linear CA (the **linear part** of Φ);
- $\mathbf{c} \in \mathcal{A}^{\mathbb{M}}$ is a constant configuration $(\forall m \in \mathbb{M}, c_m = c)$.

Equivalently: Local map $\phi = \psi + c$, where $\psi : \mathcal{A}^{\mathbb{U}} \longrightarrow \mathcal{A}$ is a homomorphism, and $c \in \mathcal{A}$ is a constant.

Invariant Measure

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

- μ is **stationary** if $\boldsymbol{\sigma}^m \mu = \mu$ for all $m \in \mathbb{M}$.
- μ is **Φ-invariant** if $\Phi\mu = \mu$.

Question: *What stationary measures are Φ-invariant?*

Cesàro Averages

If it exists, $\mu_\infty \;=\; \mathbf{wk}^*\!-\!\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} \Phi^n \mu$ is Φ-invariant.

Question: *Does μ_∞ exist? What is it?*

The Haar Measure

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

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

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

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

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

- $\mathcal{H}^{aar}$ is the 'most random' measure on $\mathcal{A}^{\mathbb{M}}$.
- $\mathcal{H}^{aar}$ is Φ-invariant for any affine CA Φ.

Question: *When does* $\mu_\infty = \mathcal{H}^{aar}$*?*

('Asymptotic randomization'.)

Cesàro Limit Measures for ACA

Theorem (Lind, 1984) $\mathcal{A} = \mathbb{Z}_{/2}$; $\mathbb{M} = \mathbb{Z}$; $\Phi = \boldsymbol{\sigma}^{-1} + \boldsymbol{\sigma}^{1}$.
If μ *is a nontrivial* **Bernoulli measure**, *then* $\mu_\infty = \mathcal{H}aar$.

Lind showed that the stronger limit, '$\mathbf{wk}^*\text{–}\lim_{n\to\infty} \Phi^N \mu = \mathcal{H}aar$', is *not* true. The subsequence $\left\{\Phi^{(2^n)}\mu\big|_{n\in\mathbb{N}}\right\}$ does *not* converge to $\mathcal{H}aar$.

Theorem (P. Ferrari, P. Ney, A. Maass & S. Martínez, 1998)

- $q = p^n$, *with* p *prime;* $\mathcal{A} = \mathbb{Z}_{/q}$; $\mathbb{M} = \mathbb{N}$.
- $\Phi = \varphi_0 \cdot \boldsymbol{\sigma}^0 + \varphi_1 \cdot \boldsymbol{\sigma}^1$, $(\varphi_0, \varphi_1$ *relatively prime to* $p)$.
- μ a **Markov measure**; *all transition probabilities nonzero.*

Then $\mu_\infty = \mathcal{H}aar$.

(Ferrari *et al.* have a similar result when μ is a **g**-measure)

Theorem (A. Maass & S. Martínez, 1999)

- $\mathcal{A} = \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}$; $\mathbb{M} = \mathbb{N}$.
- Φ *has local map* $\phi\left[(x_0, y_0);\ (x_1, y_1)\right] = (y_0,\ x_0 + y_1)$.
- μ a **Markov measure**; *all transition probabilities nonzero.*

Then $\mu_\infty = \mathcal{H}aar$.

Limit Measures for ACA

Theorem 1: (Yassawi & P, 2001)

- $\mathcal{A} = \mathbb{Z}_{/n}$ *($n \in \mathbb{N}$).* $\mathbb{M} = \mathbb{Z}^D \times \mathbb{N}^d$ *($d, D \geq 0$).*
- $\Phi : \mathcal{A}^{\mathbb{M}} \circlearrowleft$ *affine CA so that, for each prime divisor p of n, at least two coefficients of Φ are prime to p.*
- *μ a stationary* **Markov random field** *with full support.*

Then $\mu_\infty = \mathcal{H}aar$.

Examples:

- $n = p$ is prime; Φ has two or more nontrivial coefficients.
- μ a Bernoulli measure; all $a \in \mathcal{A}$ have nonzero probability.
- $\mathbb{M} = \mathbb{Z}$ and μ is an N-step Markov measure; all $(N+1)$-words have nonzero probability.

It suffices to prove Theorem 1 in the linear case:

Lemma: *Let Ψ be an ACA with linear part Φ.*

$$\left(\mathbf{wk}^*\text{–}\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} \Phi^n \mu = \mathcal{H}aar\right) \Longrightarrow \left(\mathbf{wk}^*\text{–}\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} \Psi^n \mu = \mathcal{H}aar\right).$$

Bernoulli Measures

Let ρ be a probability distribution on $\mathcal{A}$.

The corresponding **Bernoulli measure** on $\mathcal{A}^{\mathbb{Z}}$ is defined:

For any $\mathbf{b} = (b_0, b_1, \ldots, b_N) \in \mathcal{A}^{[0..N]}$,

$$\mu[\mathbf{b}] \;=\; \rho(b_0) \cdot \rho(b_1) \cdot \ldots \cdot \rho(b_N).$$

('Rolling dice'.)

Markov Measures

For all $a \in \mathcal{A}$, let $\mathbf{p}_a$ be a **transition probability** distribution over $\mathcal{A}$. Let ρ be another probability distribution such that

$$\sum_{a \in \mathcal{A}} \rho(a) \cdot \mathbf{p}_a \;=\; \rho.$$

The corresponding **Markov measure** on $\mathcal{A}^{\mathbb{Z}}$ is defined:

For any $\mathbf{b} = (b_0, b_1, \ldots, b_N) \in \mathcal{A}^{[0..N]}$,

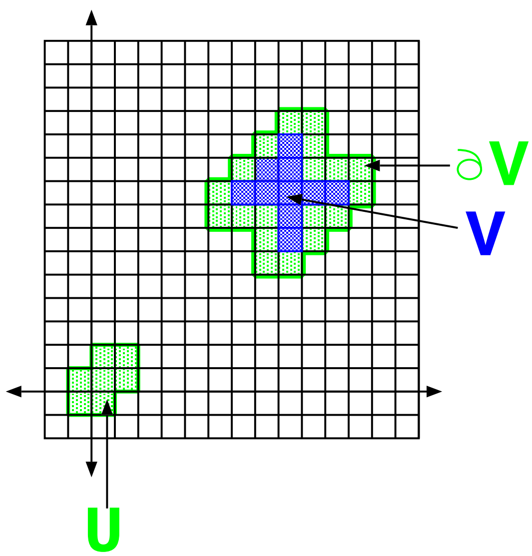
$$\mu[\mathbf{b}] \;=\; \rho(b_0) \cdot \mathbf{p}_{b_0}(b_1) \cdot \mathbf{p}_{b_1}(b_2) \cdot \ldots \cdot \mathbf{p}_{b_{N-1}}(b_N)$$

('Weak causality'.)

Markov Random Fields

$\mathbb{M} = \mathbb{Z}^D \times \mathbb{N}^d$.

$\mathbb{U} \subset \mathbb{M}$ finite 'neighbourhood of 0' e.g. $\mathbb{U} = [-1...1]^D \times \{0,1\}^d$.



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

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

μ is a **Markov random field** if, for any $\mathbb{V} \subset \mathbb{M}$, and any $\mathbf{a} \in \mathcal{A}^{\partial(\mathbb{V})}$, events occuring *inside* $\mathbb{V}$ are independent of events *outside*, relative to conditional measure $\mu_{\mathbf{a}}$. That is:

If:
- $\mathbb{W}_{in} \subset \mathbb{V}$ and $\mathbf{b}_{in} \in \mathcal{A}^{\mathbb{W}_{in}}$;
- $\mathbb{W}_{out} \subset \mathbb{M} \setminus cl(\mathbb{V})$ and $\mathbf{b}_{out} \in \mathcal{A}^{\mathbb{W}_{out}}$;

Then: $\mu_{\mathbf{a}}[\mathbf{b}_{in} \smile \mathbf{b}_{out}] = \mu_{\mathbf{a}}[\mathbf{b}_{in}] \cdot \mu_{\mathbf{a}}[\mathbf{b}_{out}]$.

- μ is **stationary** if it is invariant under all shifts.
- μ has **full support** if $\mu[\mathbf{a}] > 0$ for every $\mathbf{a} \in \mathcal{A}^{\mathbb{U}}$.

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 $\mathcal{A}^{\mathbb{Z}}$:

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

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

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

$$\boldsymbol{\chi}(\mathbf{a}) \;=\; \exp\left(\frac{2\pi\mathbf{i}}{n} \sum_{m\in\mathbb{M}} \chi_m a_m\right) \;=\; \mathcal{E}\left(\sum_{m\in\mathbb{M}} \chi_m a_m\right)$$

(**coefficients** $\chi_m \in \mathbb{Z}_{/n}$; *all but finitely many are zero).*

The **rank** of χ is the number of nonzero coefficients.

Example: $\mathsf{rank}\,[\boldsymbol{\zeta}] \;=\; 1$ and $\mathsf{rank}\,[\boldsymbol{\xi}] \;=\; 3$.

Characters and Measures

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

Theorem 2: $\mu_1, \mu_2, \ldots$ *a sequence of measures on* $\mathcal{A}^{\mathbb{M}}$;

$$\left(\mathbf{wk}^*\!-\!\lim_{n\to\infty} \mu_n \; = \; \mathcal{H}aar \right) \quad \Longleftrightarrow \quad \left(\lim_{n\to\infty} \widehat{\mu}_n[\boldsymbol{\chi}] \; = \; 0, \;\; \textit{for all } \boldsymbol{\chi} \neq \mathbb{1} \right)$$

Harmonic Mixing

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

$$\text{For all characters } \boldsymbol{\chi}, \quad \Big(\mathsf{rank}\,[\chi] > R \Big) \Longrightarrow \Big(|\widehat{\mu}[\chi]| < \epsilon \Big)$$

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

Theorem 3.0: *The set of HM measures is an* **ideal** *of the Banach algebra* $\left(\mathcal{M}_{\mathcal{EAS}}\left[\mathcal{A}^{\mathbb{M}};\mathbb{C}\right],+,*\right)$, *closed under the total variation norm, but dense in the weak* topology.*

Theorem 3.1: *Suppose:*

- $\mathbb{M} = \mathbb{Z}^D \times \mathbb{N}^d$;
- μ *is a* **stationary Markov random field** *on* $\mathcal{A}^{\mathbb{M}}$ *with full support;*

Then μ *is harmonically mixing.*

Example: A fully supported N-step Markov process on $\mathcal{A}^{\mathbb{Z}}$ is HM.

Harmonic Mixing

A special case of **Theorem 3.1** is:

Theorem: *Suppose:*

- $\mathcal{A} = \mathbb{Z}_{/p}$, *p prime;*
- μ *is a Bernoulli measure;* $\mu[a] > 0$ *for all* $a \in \mathcal{A}$.

Then μ *is harmonically mixing.*

Proof: If $\boldsymbol{\chi}(\mathbf{a}) = \prod_{m \in \mathbb{M}} \mathcal{E}(\chi_m a_m)$ and $\mu = \bigotimes_{m \in \mathbb{M}} \mu_0$, then

$$\begin{aligned} |\widehat{\mu}[\boldsymbol{\chi}]| &= \left| \int_{\mathcal{A}^{\mathbb{M}}} \boldsymbol{\chi}[\mathbf{a}] \, d\mu[\mathbf{a}] \right| \\ &= \left| \prod_{m \in \mathbb{M}} \left(\int_{\mathcal{A}} \mathcal{E}(\chi_m a_m) \; d\mu_0[a_m] \right) \right| \\ &= \prod_{\chi_m \neq 0} \left| \int_{\mathcal{A}} \mathcal{E}(\chi_m a_m) \; d\mu_0[a_m] \right| \\ &\leq \prod_{\chi_m \neq 0} C \quad = \quad C^{\mathsf{R}}, \end{aligned}$$

where $C := \max_{c \in [1..p]} \left| \int_{\mathcal{A}} \mathcal{E}(c \cdot a) \; d\mu_0[a] \right| < 1$, and $\mathsf{R} = \mathsf{rank}[\boldsymbol{\chi}]$.

Thus, as $\mathsf{R} \to \infty$, $|\widehat{\mu}[\boldsymbol{\chi}]| \leq C^{\mathsf{R}} \to 0$. □

Characters and LCA

Suppose:
$$\begin{cases} \bullet\ \boldsymbol{\chi}(\mathbf{a}) \ = \ \mathcal{E}\left(\sum_{m\in\mathbb{M}} \chi_m a_m\right) \text{ is a character.} \\ \bullet\ \Phi \ = \ \sum_{u\in\mathbb{U}} \varphi_u \cdot \boldsymbol{\sigma}^u \text{ is a linear CA.} \end{cases}$$

Then:

- $\boldsymbol{\xi} = \boldsymbol{\chi} \circ \Phi : \mathcal{A}^{\mathbb{M}} \longrightarrow \mathbb{T}^1$ is also a character.
- Obtain coefficients of $\boldsymbol{\xi}$ by 'convolving' coefficients of $\boldsymbol{\chi}$ and Φ:

$$\forall m \in \mathbb{M}, \text{ let } \ \xi_k \ = \sum_{\substack{m,n\in\mathbb{M} \\ n+m=k}} \chi_n \cdot \varphi_m. \qquad \text{Then } \boldsymbol{\xi}(\mathbf{a}) \ = \mathcal{E}\left(\sum_{m\in\mathbb{M}} \xi_m a_m\right).$$

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

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

Cesàro Density

If $\mathbb{J} \subset \mathbb{N}$, the **Cesàro density** of $\mathbb{J}$ is the limit

$$\lim_{N\to\infty} \frac{1}{N} \operatorname{card}\left[j \in \mathbb{J} \; ; \; j \leq N \right]$$

(if the limit exists)

Examples:

- $\{3n \; ; \; n \in \mathbb{N}\}$; density $1/3$.
- $\left\{n^2 \; ; \; n \in \mathbb{N}\right\}$; density 0.
- $\{2^n \; ; \; n \in \mathbb{N}\}$; density 0.
- **Prime Numbers:** density 0.
- **Composite Numbers:** density 1.

Theorem 4: Let $\mathcal{A}$ be a finite abelian group.

- Φ: *A* **diffusive** *linear CA on* $\mathcal{A}^{\mathbb{M}}$;
- μ: *A* **harmonically mixing** *measure on* $\mathcal{A}^{\mathbb{M}}$.

Then $\exists\, \mathbb{J} \subset \mathbb{N}$ *of Cesàro density 1 so that* $\mathbf{wk}^*\!\!-\!\!\lim_{\substack{j\to\infty \\ j\in\mathbb{J}}} \Phi^j \mu \;=\; \mathcal{H}aar.$

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

Proof: Follows from Theorem 2 and definitions of 'diffusive' and 'harmonic mixing'. □

Theorem 5: $\mathbb{M} = \mathbb{Z}^D \times \mathbb{N}^d$; $\quad \mathcal{A} = \mathbb{Z}_{/n}$.
For each prime divisor p *of* n*, suppose at least two coefficients of* Φ *are prime to* p*. Then* Φ *is diffusive.*

Theorem 1 follows from Theorems 3.1, 4, and 5.

Proof Sketch for Theorem 5:

Every $n \in \mathbb{N}$ has a p**-ary expansion**: $\mathbb{P}(\mathrm{n}) = \{ n^{[i]} \}_{i=0}^{\infty} \in [0..p)^{\mathbb{N}}$, such that $n = \sum_{i=0}^{\infty} n^{[i]} p^i$.

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

Lucas' Theorem:

For any $N,\ n \in \mathbb{N}$,
$$\begin{bmatrix} N \\ n \end{bmatrix}_p = \prod_{k=0}^{\infty} \begin{bmatrix} N^{[k]} \\ n^{[k]} \end{bmatrix}_p ,$$
where $\binom{0}{0} := 1$ *and* $\binom{a}{b} := 0$ *for any* $b > a > 0$.

Write "$n \ll N$" whenever $n^{[i]} \leq N^{[i]}$ for each $i \in \mathbb{N}$.

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

Proof Sketch for Theorem 5: Suppose (for simplicity) $\mathcal{A} = \mathbb{Z}_{/2}$, $\mathbb{M} = \mathbb{Z}$, and $\Phi = \boldsymbol{\sigma}^{\ell_0} + \boldsymbol{\sigma}^{\ell_1} + \boldsymbol{\sigma}^{\ell_2}$, for $\ell_1 < \ell_2 < \ell_3$ in $\mathbb{Z}$. Then: $\Phi = \Phi_0 \circ \boldsymbol{\sigma}^{\ell_0}$, where $\Phi_0 = \mathbf{Id} + \boldsymbol{\sigma}^{m_1} \left(\mathbf{Id} + \boldsymbol{\sigma}^{m_2} \right)$, with $\ell_1 = \ell_0 + m_1$ and $\ell_2 = \ell_0 + m_1 + m_2$.

Composing with $\boldsymbol{\sigma}^{\ell_0}$ does not affect the diffusion property; hence, assume WOLOG that $\Phi = \Phi_0$.

$$\left(\text{Recall:} \quad \Phi = \mathbf{Id} \ + \ \boldsymbol{\sigma}^{m_1} (\mathbf{Id} \ + \ \boldsymbol{\sigma}^{m_2}) \right)$$

By Lucas' Theorem, $\begin{bmatrix} N \\ n \end{bmatrix}_2 = \begin{cases} 1 & if \ \ n \ll N \\ 0 & if \ \ n \not\ll N \end{cases}$.

$$\text{Thus,} \quad \Phi^N = \sum_{k_1=0}^{N} \begin{bmatrix} N \\ k_1 \end{bmatrix}_2 \boldsymbol{\sigma}^{m_1 k_1} (1 + \boldsymbol{\sigma}^{m_2})^{k_1}$$

$$= \sum_{k_1 \ll N} \boldsymbol{\sigma}^{m_1 k_1} \left(\sum_{k_2 \ll k_1} \boldsymbol{\sigma}^{m_2 k_2} \right)$$

$$= \sum_{k_1 \ll N} \sum_{k_2 \ll k_1} \boldsymbol{\sigma}^{m_1 k_1 + m_2 k_2}.$$

If Φ is *not* diffusive, $\exists\ \boldsymbol{\chi}$ so that rank $\left[\boldsymbol{\chi} \circ \Phi^N\right]$ is bounded by some $\mathsf{R} \in \mathbb{N}$ on a subset $\mathbb{B} \subset \mathbb{N}$ of nonzero density.

$$\text{Suppose} \quad \boldsymbol{\chi}(\mathbf{a}) = \mathcal{E}\left(\sum_{q \in \mathcal{Q}} a_q \right), \quad (\mathcal{Q} \subset \mathbb{Z} \text{ finite subset}).$$

Thus, for all $N \in \mathbb{N}$,

$$\boldsymbol{\chi} \circ \Phi^N(\mathbf{a}) = \mathcal{E}\left[\sum_{q \in \mathcal{Q}} \sum_{k_1 \ll N} \sum_{k_2 \ll k_1} a_{(k_1 m_1 + k_2 m_2 + q)} \right].$$

(here, $\mathbf{a} = [a_m|_{m \in \mathbb{M}}] \in \mathcal{A}^{\mathbb{M}}$.)

$$\left(\boldsymbol{\chi} \circ \Phi^N(\mathbf{a}) \;=\; \mathcal{E}\left[\sum_{q \in \mathcal{Q}} \sum_{k_1 \ll N} \sum_{k_2 \ll k_1} a_{(k_1 m_1 + k_2 m_2 + q)} \right] \right) \qquad (\dagger)$$

If $\mathsf{rank}\left[\boldsymbol{\chi} \circ \Phi^N\right] < \mathsf{R}$, then all but R of the terms in $(\dagger)$ must *cancel out*, through equations of the form:

$$k_1 m_1 + k_2 m_2 + q \quad = \quad k_1^* m_1 + k_2^* m_2 + q^* \quad (*)$$

for $k_2 \ll k_1 \ll N, \quad k_2^* \ll k_1^* \ll N, \quad$ and $q, q^* \in \mathcal{Q}$.

```
                        ⟵  Γ  ⟶
      N : ...1 1  1   1  1   1          1  1  1  1  1 1  1  1  1  1 1 1   1   1 1 1
     k1 :  ...                          1  1        1           1  1   1   1   1 1
     k2 :  ...                          1           1           1      1       1 1
(q − q1) : ...                                                       1 1 1   1 1 1 1
   2^jr :  ...               1
                             ↑          ↑                            ↑ ↑ ↑ ↑ ↑ ↑ ↑ ↑
                             jr ...  ... jr−Γ ...                 ... 7 6 5 4 3 2 1 0
```

Idea: Let $\Gamma \in \mathbb{N}$. If $\mathbb{B} \subset \mathbb{N}$ has nonzero density, then $\exists\ N \in \mathbb{B}$ such that $\mathbb{P}(N)$ has at least $\mathsf{R}+1$ 'gaps' of at least Γ consecutive 0's, ending in a 1. Suppose the terminating 1's in these 'gaps' occur at positions $j_0,\ j_1,\ \ldots, j_{\mathsf{R}}$. Set $q^* = \min[\mathcal{Q}]$. By Pigeonhole Principle, $\exists\ r \in [0...\mathsf{R}]$ so that $(*)$ holds with $k_1^* = 2^{j_r}$ and $k_2^* = 0$; ie.

$$k_1 m_1 + k_2 m_2 + q \quad = \quad 2^{j_r} m_1 + 0 \cdot m_2 + q^*$$

for some $k_2 \ll k_1 \ll N$ and $q \in \mathcal{Q}$. Rewrite this as:

$$m_1 2^{j_r} \quad = \quad k_1 m_1 + k_2 m_2 + (q - q^*) \quad (**)$$

Now, $k_2 \ll k_1 \ll N$, and $k_1 < 2^{j_r}$, so, because of the 'gap', we must have $k_2 \leq k_1 < 2^{j_r - \Gamma}$. If Γ is big enough, then $(**)$ is impossible. Contradiction. ______ □

Noncyclic Abelian Groups

Let $\mathcal{A}$ be a *noncyclic* abelian group; eg. $\mathcal{A} = \left(\mathbb{Z}_{/p^r}\right)^J$, where $r, J \in \mathbb{N}$ and p is prime.

$$\left(\text{Linear CA} \right) \iff \left(\text{polynomials over a ring of matrices} \right)$$

$$\left(\text{Composition of LCA} \right) \iff \left(\begin{array}{l} \text{Noncommutative} \\ \text{polynomial multiplication} \end{array} \right)$$

- Cannot apply binomial theorem to CA iterates.
- Diffusion is much harder to characterize.
- *Ad hoc* methods can be used in some cases.

Theorem: $\mathcal{A} = \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}$; $\mathbb{M} = \mathbb{N}$; Φ *has local map*

$$\phi\left[(x_0, y_0);\ (x_1, y_1)\right] \;=\; (y_0,\ x_0 + y_1).$$

Then Φ *is diffusive.* *Thus, if* μ *is HM, then* $\mu_\infty \;=\; \mathcal{H}^{\mathrm{ar}}$.

Nonabelian groups:

Let $\mathcal{G}$ be a *nonabelian* group.

Define **multiplicative** CA over $\mathcal{G}^{\mathbb{M}}$, analogous to linear CA.

Structure theory of $\mathcal{G}$ yields structure theory for MCA.

If $\mathcal{N} \subset \mathcal{G}$ is a normal subgroup, and $\mathcal{Q} = \mathcal{G}/\mathcal{N}$, then an MCA on $\mathcal{G}^{\mathbb{M}}$ can be decomposed as a **skew product** of:

- A multiplicative CA Θ: $\mathcal{Q}^{\mathbb{M}} \longrightarrow \mathcal{Q}^{\mathbb{M}}$; and...
- A **relative CA**: a continuous, shift-invariant map
$$\Psi : \mathcal{Q}^{\mathbb{M}} \times \mathcal{N}^{\mathbb{M}} \longrightarrow \mathcal{N}^{\mathbb{M}}$$
determined by a 'local map' $\psi : \mathcal{Q}^{\mathbb{U}} \times \mathcal{N}^{\mathbb{U}} \longrightarrow \mathcal{N}$.

If Θ is diffusive and Ψ is 'relatively diffusive', then HM measures on $\mathcal{G}^{\mathbb{M}}$ converge to Haar under iteration of Φ.

Example: *Quaternions*

- $\mathcal{G} = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$; $\mathcal{N} = \{\pm 1\} \cong \mathbb{Z}_{/2}$; $\mathcal{Q} \cong \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}$.
- $\Phi : \mathcal{G}^{\mathbb{Z}} \longrightarrow \mathcal{G}^{\mathbb{Z}}$ has local map $\phi(q_0, q_1, q_3, q_4) = q_3 \cdot q_0^3 \cdot q_2^5 \cdot q_1^{-1}$.
- λ: HM measure on $\mathcal{N}^{\mathbb{Z}}$; ν: HM measure on $\mathcal{Q}^{\mathbb{Z}}$;

If $\mu = \lambda \otimes \nu$, measure on $\mathcal{G}^{\mathbb{Z}}$, then $\mu_\infty = \mathcal{H}\!\mathit{aar}$.

Nonconvergence to Haar

Harmonic mixing $\iff$ 'randomness' in the initial conditions.

If μ describes initial conditions that are 'highly ordered', then $\Phi^n\mu$ does *not* converge to $\mathcal{H}\!aar$ in density. For example...

μ **has small support**:

- **Shift-invariant subgroups** of $\mathcal{A}^{\mathbb{M}}$.
- **Substitution systems** (eg. 'q-automata', the Morse sequence)
- 'Regular' **finite rank systems** (eg. many Toeplitz sequences)

μ **has strong recurrence properties**:

- Some **Sturmian shifts** (ie. quasiperiodic initial conditions).
- 'Recurrent' **finite rank systems** (eg. certain 'Chacon' type systems)

Question: Is *non*convergence to Haar generic when μ is...

- Quasiperiodic?
- Finite rank?
- Singular spectrum?
- Zero entropy?

Open Problems

Other Monoids: What if $\mathbb{M}$ is nonabelian group/monoid?

- Free group/monoid: no problem.
- Discrete subgroup of Lie group?
- **Example:** discrete isometry group of hyperbolic space?

Other measures:

- Most Markov random fields are harmonically mixing.
- Weaker 'randomness' conditions are insufficient for HM.
- **Example:** $\exists\mu$ such that $(\mathcal{A}^{\mathbb{Z}}, \mu, \boldsymbol{\sigma})$ is a **K**-automorphism, but μ is *not* HM.
- Necessary conditions for harmonic mixing?

Permutative Automata:

- The most 'chaotic' class of cellular automata.
- Affine & multiplicative automata are a subclass.
- Invariant/limit measures of *non*algebraic permutative CA?