HAL open science

Characterizing Asymptotic Randomization in Abelian Cellular Automata

Benjamin Hellouin de Menibus, Ville Salo, Guillaume Theyssier

To cite this version:

Benjamin Hellouin de Menibus, Ville Salo, Guillaume Theyssier. Characterizing Asymptotic Randomization in Abelian Cellular Automata. Ergodic Theory and Dynamical Systems, 2018. hal-01491485v2

HAL Id: hal-01491485

https://hal.science/hal-01491485v2

Submitted on 8 Feb 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Characterizing Asymptotic Randomization in Abelian Cellular Automata

B. Hellouin de Menibus†, V. Salo‡, G. Theyssier§

† *Centro de Modelamiento Matemático (CMM), Universidad de Chile, Chile & Departamento de Matemáticas, Universidad Andrés Bello, Chile*
‡ *Centro de Modelamiento Matemático (CMM), Universidad de Chile, Chile*
§ *Institut de Mathématiques de Marseille (Université Aix Marseille, CNRS, Centrale Marseille), France*

(*Received March 2017*)

Abstract. Abelian cellular automata (CA) are CA which are group endomorphisms of the full group shift when endowing the alphabet with an abelian group structure. A CA randomizes an initial probability measure if its iterated images weak*-converge towards the uniform Bernoulli measure (the Haar measure in this setting). We are interested in structural phenomena, i.e. randomization for a wide class of initial measures (under some mixing hypotheses). First, we prove that an abelian CA randomizes in Cesàro mean if and only if it has no soliton, i.e. a nonzero finite configuration whose time evolution remains bounded in space. This characterization generalizes previously known sufficient conditions for abelian CA with scalar or commuting coefficients. Second, we exhibit examples of strong randomizers, i.e. abelian CA randomizing in simple convergence; this is the first proof of this behaviour to our knowledge. We show however that no CA with commuting coefficients can be strongly randomizing. Finally, we show that some abelian CA achieve partial randomization without being randomizing: the distribution of short finite words tends to the uniform distribution up to some threshold, but this convergence fails for larger words. Again this phenomenon cannot happen for abelian CA with commuting coefficients.

1. *Introduction*

Cellular automata, although extremely simple to define, provide a rich source of examples of dynamical systems which are not yet well understood. This is in particular true when taking a measure theoretic point of view and studying the evolution of a probability measure under iterations of a CA. The situation can be roughly depicted as follows: for non-surjective CAs, essentially all behaviors that

are not prohibited by immediate computability restrictions can happen [**4, 1, 6**]; for the surjective case, various forms of rigidity are observed (see [**21**] for an overview). In particular, since the pioneering work of Lind and Miyamoto on the 'addition modulo 2' CA [**19, 16**], many CAs of algebraic origin were shown to behave like randomizers [**8, 22, 23, 18, 13**], *i.e.* they converge in Cesàro mean or in density to the uniform Bernoulli measure from any initial probability measure from a large class $\mathcal{C}$. In [**19, 16**], the class $\mathcal{C}$ is Bernoulli measures of full support. It was later extended to full support Markov measures or N-step Markov processes, measures with complete connections and summable decay of correlations and harmonically mixing measures [**21**] and more [**24, 28**].

Apart from specific examples (like in [**17**]), the class of CA where randomizing behavior has been shown is essentially contained in that of 'linear' CA defined on an abelian group alphabet by

$$F(x)_i = \sum_{j \in V} \theta_j(x_{i+j}),$$

where θ_j are *commuting* endomorphisms (most of the time automorphisms or scalar coefficients). Furthermore, the type of convergence considered has always been Cesàro mean or convergence in density.

In this paper we consider the class of harmonically mixing measures and the class of abelian CAs which are like 'linear' CA described above but *without* the assumption of commutation of endomorphisms. Our first main result is a complete characterization of randomization in density in that setting.

> THEOREM (Theorem 2) — *An abelian CA F randomizes in density any harmonically mixing measure if and only if it does not possess a soliton, i.e. a nonzero finite configuration whose set of nonzero cells stays within a bounded diameter under iterations of the CA.*

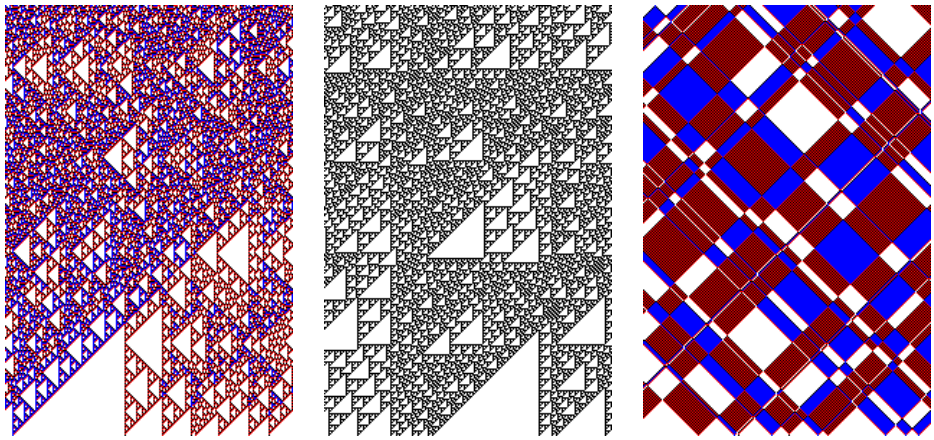
We show that this theorem extends the most general previous result [**23**] and allows us to easily prove randomization for particular examples, even in the setting of non-commutative coefficients [**17**], hence answering a question of [**21**].

Our approach uses tools from harmonic analysis using a similar approach to the work of Pivato and Yassawi on diffusion of characters [**22, 23**]. We rely on the abelian structure of the considered CA to reduce randomization to a combinatorial property of diffusivity. More precisely, we define a dual CA on the (Pontryagin) dual group and show that diffusion in the dual is equivalent to randomization and that the diffusion property is preserved by duality. Finally, we prove the equivalence between diffusivity and the absence of solitons, not by using the abelian structure but by general combinatorial properties of surjective CA. This allows us to go beyond the commuting coefficient case, which was treated in previous works by a careful analysis of binomial coefficients of the iterates of F.

We also prove the existence of a stronger form of randomization where taking subsequences of density 1 or Cesàro mean is not necessary:

THEOREM (Theorem 4) — *There exist abelian CAs that randomize in simple convergence any harmonically mixing measure.*

This answers a question of [**14**] (Question 59). Experiments on small surjective CAs [**12, 29**] suggest that this strong form of randomization is the most common, that it occurs as well on nonabelian CA, and even that randomization occurring only in density (or Cesàro mean) might be an artifact of abelian CAs. This confirms the importance of the non-commutative coefficients case, since we also prove that abelian CA with commuting coefficients cannot achieve such a strong form of randomization.



Strong randomizer Randomizer in density "Cellwise" randomizer

Figure 1. Three forms of randomization: F_2 (defined in Section 6.2), addition modulo 2, and $I_{\mathbb{Z}_2}$ (defined in Section 6.3). The direction of time is upward. The CA are iterated on an initial configuration drawn according to a Bernoulli measure with 95% white (state 0). The addition modulo 2 does not converge directly because the image measure is far from the uniform measure around times $t = 2^n$ (see Theorem 3). $I_{\mathbb{Z}_2}$ randomizes individual cells but not cylinders of length 2 (see Proposition 8).

The results above are stated as randomization for the class of harmonically mixing measures. We do not investigate when there are more randomized measures (as in [**24**]), however we show that there can not be fewer: if an abelian CA randomizes in density full-support Bernoulli measures, then it randomizes in density all harmonically mixing measures. Interestingly, the rigidity is even stronger for abelian CA with commutative coefficients: we prove that if the frequency of individual states is randomized (in density), then the CA is fully randomizing in density. In the case of non-commutative coefficients, we can have partial randomization: we give examples for any K of abelian CA which do randomize all cylinders up to size K but fail to randomize completely. This suggests that experimental work on randomization in general CA should be done with care: randomization might fail in non-obvious ways on long-range

correlations.

The paper is organized as follows: in Section 2 we recall basic definitions and tools about measure theoretic aspects of cellular automata; in Section 3 we study the evolution of ranks of characters under iterations of abelian CAs, the property of character diffusion and its link with randomization; in Section 4 we define the dual of an abelian CA, show that duality preserves diffusivity in density and link this property with the absence of solitons; in Section 5 we establish our main result, a characterization of randomization in density through the absence of solitons; in Section 6, we exhibit a class of examples of strong randomization and randomization up to fixed-length cylinder, and we show that these behaviors are specific to CA with non-commuting coefficients; finally, in Section 7 we give some directions for further research on this topic.

2. *Definitions and tools*

Throughout this paper we will state our results for dimension 1, but they extend straightforwardly to the d-dimensional case. Our convention on natural number is $0 \in \mathbb{N}$.

Let $\mathcal{A}$ be a finite alphabet. We define $\mathcal{A}^* = \bigcup_{n\in\mathbb{N}} \mathcal{A}^n$ to be the set of finite *words*, and $\mathcal{A}^{\mathbb{Z}}$ the set of (one-dimensional) *configurations*. For a finite set $U \subset \mathbb{Z}$ and $u \in \mathcal{A}^U$, define the *cylinder*:

$$[u]_U = \{x \in \mathcal{A}^{\mathbb{Z}} \ : \ x|_U = u\}.$$

For $u \in \mathcal{A}^n$ and $k \in \mathbb{Z}$, also define $[u]_k = [u]_{\{k,\dots,k+n-1\}}$ and $[u] = [u]_0$.

We endow $\mathcal{A}^{\mathbb{Z}}$ with the product topology, which is metrizable using the *Cantor distance*:

$$\forall x, y \in \mathcal{A}^{\mathbb{Z}}, d(x,y) = 2^{-\Delta(x,y)} \quad \text{where} \quad \Delta(x,y) = \min\{|i| : x_i \neq y_i\}.$$

The *shift map* is defined by

$$\forall x \in \mathcal{A}^{\mathbb{Z}}, \sigma(x) = (x_{i+1})_{i\in\mathbb{Z}}.$$

A *cellular automaton* is a pair $(\mathcal{A}, F)$ where $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ is a continuous function that commutes with the shift map (i.e. $F \circ \sigma = \sigma \circ F$). Equivalently, F is defined by a finite neighborhood $\mathcal{N} \subset \mathbb{Z}$ and a *local rule* $f : \mathcal{A}^{\mathcal{N}} \to \mathcal{A}$ in the sense that:

$$\forall x \in \mathcal{A}^{\mathbb{Z}}, \forall i \in \mathbb{Z}, F(x)_i = f(x_{i+\mathcal{N}}).$$

Let $(\mathcal{A}, +)$ be an abelian group and 0 its neutral element. A *finite configuration* is a configuration $x \in \mathcal{A}^{\mathbb{Z}}$ such that $x(i) = 0$ for all $i \in \mathbb{Z}$ except on a finite set. If x is a finite configuration, we define its *support* by $\mathrm{supp}(x) = \{i \in \mathbb{Z} : x(i) \neq 0\}$ and its *rank* by $\mathrm{rank}(x) = |\mathrm{supp}(x)|$. Note that the set of finite configurations is dense in $\mathcal{A}^{\mathbb{Z}}$. The notion of finite points makes sense also when $\mathcal{A}$ has no group structure, assuming a choice of zero element $0 \in \mathcal{A}$ has been made.

An *abelian cellular automaton* F is a cellular automaton which is an endomorphism for $(\mathcal{A}^{\mathbb{Z}}, +)$ (componentwise addition):

$$\forall x, y \in \mathcal{A}^{\mathbb{Z}}, F(x+y) = F(x) + F(y)$$

Equivalently, F is a finite sum of shifts composed with endomorphisms of $(\mathcal{A}, +)$. More precisely, there is a finite $\mathcal{N} \subset \mathbb{Z}$ and a collection $(\phi_i)_{i \in \mathcal{N}}$ of endomorphisms of $(\mathcal{A}, +)$ such that:

$$F = \sum_{i \in \mathcal{N}} \overline{\phi}_i \circ \sigma^i, \qquad \text{where} \qquad \overline{\phi}_i : \begin{array}{ccc} \mathcal{A}^{\mathbb{Z}} & \to & \mathcal{A}^{\mathbb{Z}} \\ x & \mapsto & \big(\phi_i(x(j))\big)_j \end{array}.$$

Note that the image of a finite configuration is always a finite configuration. In particular, $0 \in \mathcal{A}$ is a *quiescent state*, meaning $F(0^{\mathbb{Z}}) = 0^{\mathbb{Z}}$ where $0^{\mathbb{Z}}$ denotes the constant-0 configuration.

We also define addition on abelian CA by $F + F' : x \mapsto F(x) + F'(x)$.

We say that F has *commuting endomorphisms* if the endomorphisms ϕ_i commute pairwise. Supposing $\mathcal{A}$ is a vector space over a finite field $\mathbb{F}_p$ turns out to be a source of simple yet illustrative examples. As said above, we are particularly interested in the non-commuting case. We will illustrate our results with the two representatives F_2 and H_2 defined over $\mathcal{A} = \mathbb{F}_2^2$ by

$$F_2(x)_i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot x_i + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot x_{i+1}$$
$$H_2(x)_i = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot x_{i-1} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot x_i + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot x_{i+1}$$

where elements of $\mathcal{A}$ are seen as vectors and matrix notation is used to denote endomorphisms of $\mathcal{A}$.

2.1. *Cellular automata acting on probability measures* Let $\mathcal{M}(\mathcal{A}^{\mathbb{Z}})$ be the space of probability measures on the Borel sigma-algebra of $\mathcal{A}^{\mathbb{Z}}$. In particular, we consider $\mathcal{M}_\sigma(\mathcal{A}^{\mathbb{Z}})$, the subset of all σ-invariant measures. Here are a few examples that we mention throughout the paper:

Bernoulli measure Take $(\beta_i)_{i \in \mathcal{A}} \in [0,1]^{\mathcal{A}}$ such that $\sum_i \beta_i = 1$. Let β be the usual Bernoulli measure of parameters (β_i) on $\mathcal{A}$. The *Bernoulli measure* of parameters (β_i) on $\mathcal{A}^{\mathbb{Z}}$ is defined as $\mu = \otimes_{\mathbb{Z}} \beta$; that is, each cell is drawn in a i.i.d manner and distributed as a Bernoulli measure. In other words,

$$\forall u \in \mathcal{A}^*, \mu([u]) = \prod_{0 \le i < |u|} \beta_{u_i}.$$

A particularly important example is the uniform Bernoulli measure on $\mathcal{A}^{\mathbb{Z}}$, denoted λ, which is the Bernoulli measure of parameters $\left(\frac{1}{|\mathcal{A}|}\right)_{i \in \mathcal{A}}$.

Markov measure Let $(p_{i,j})_{i,j\in\mathcal{A}}$ be a nonnegative matrix satisfying $\sum_j p_{ij} = 1$ for all i, and $(\mu_i)_{i\in\mathcal{A}}$ an eigenvector associated with the eigenvalue 1 (the choice being unique if the matrix is irreducible). The associated *two-step Markov measure* is defined as

$$\forall u \in \mathcal{A}^*, \mu([u]) = \mu_{u_0} \prod_{0\leq i<|u|} p_{u_i u_{i+1}}.$$

This can be extended to n-step Markov measures.

The weak-* topology on $\mathcal{M}(\mathcal{A}^{\mathbb{Z}})$ is metrisable. A possible metric is given by the distance:

$$d_{\mathcal{M}}(\mu,\nu) = \sum_{k\in\mathbb{N}} \frac{1}{2^k} \max_{u\in\mathcal{A}^{2k+1}} |\mu([u]_{-k}) - \nu([u]_{-k})|.$$

A cellular automaton $(\mathcal{A}, F)$ yields a continuous action on the space of probability measures $\mathcal{M}(\mathcal{A}^{\mathbb{Z}})$:

$$\text{For any Borel set } U,\ F\mu(U) = \mu(F^{-1}U)$$

Given a subset $X \subseteq \mathbb{N}$ of natural numbers, its *lower density* is defined as $\liminf_n \frac{|\{i\in X, i\leq n\}|}{n}$. We prove a diagonalization lemma for sequences of lower density one, stating, informally, that the intersection of countably many sequences of lower density one "eventually has lower density one".

LEMMA 1. *Suppose that I is countable, and for all $n \in I$, $N_n \subset \mathbb{N}$ is a set with lower density one. Then there there exists a set $N \subset \mathbb{N}$ of lower density one such that for all $n \in I$, $N \cap [k,\infty) \subset N_n \cap [k,\infty)$ for all large enough k.*

Proof. We can assume $I = \mathbb{N}$. The intersection of finitely many sets of lower density one has lower density one. Thus, we may assume the N_n form a decreasing sequence (with respect to inclusion) by replacing each N_n by $N_0 \cap N_1 \cap \cdots \cap N_n$.

Now, let $m_0 = 0$ and pick an increasing sequence of natural numbers $(m_n)_{n\geq 1}$ such that $|N_n \cap [0,m)| \geq m(1-1/n)$ for all $m \geq m_n$, using the fact N_n has lower density one. Define $N \cap [m_{n-1}, m_n) = N_n \cap [m_{n-1}, m_n)$ for all n. Then

$$\begin{aligned}|N \cap [0,m)| &= |N_1 \cap [0,m_1)| + \cdots + |N_\ell \cap [m_{\ell-1}, m_\ell)| + |N_{\ell+1} \cap [m_\ell, m)| \\ &\geq |N_\ell \cap [0,m)| \\ &\geq m(1-1/\ell)\end{aligned}$$

where ℓ is maximal such that $m_\ell < m$, and where the first inequality follows because the N_n form a decreasing sequence under inclusion. □

Considering the iterated action of a cellular automaton on an initial measure μ, we distinguish various forms of convergence:

- $(F^t\mu)_{t\in\mathbb{N}}$ *converges* to ν if $F^t\mu \to \nu$ (for the weak-$*$ convergence); equivalently, $F^t\mu([u]) \to \nu([u])$ for every finite word u;

- $(F^t\mu)_{t\in\mathbb{N}}$ *converges in Cesàro mean* to ν if $\dfrac{1}{T}\displaystyle\sum_{t=0}^{T-1} F^t\mu \to \nu$; equivalently, if $\dfrac{1}{T}\displaystyle\sum_{t=0}^{T-1} F^t\mu([u]) \to \nu([u])$ for every finite word u;
- $(F^t\mu)_{t\in\mathbb{N}}$ *converges in density* to ν if there exists an increasing sequence $(\varphi(t))_{t\in\mathbb{N}}$ of lower density 1 such that $F^{\varphi(t)}\mu \to \nu$; equivalently by Lemma 1, if for every finite word u there exists an increasing sequence $(\varphi_u(t))_{t\in\mathbb{N}}$ of lower density 1 such that $F^{\varphi_u(t)}\mu([u]) \to \nu([u])$;
- $(F^t\mu)_{t\in\mathbb{N}}$ *converges on cylinders of support* $\subset \mathbb{U}$ to ν if $\mu(\cdot \mid \mathfrak{B}_{\mathbb{U}}) \to \nu(\cdot \mid \mathfrak{B}_{\mathbb{U}})$ where $\mathfrak{B}_{\mathbb{U}}$ is the Borel σ-algebra generated by the cylinders of support $\subset \mathbb{U}$ (this can be seen as convergence of measures of $\mathcal{M}(\mathcal{A}^{\mathbb{U}})$); equivalently, $F^t\mu([u]) \to \nu([u])$ for every word u with $\mathrm{supp}(u) \subset \mathbb{U}$.

Recall that, in a context where the alphabet is $\mathcal{A}$, λ is the uniform Bernoulli measure on $\mathcal{A}^{\mathbb{Z}}$.

DEFINITION 1 (RANDOMIZATION) *Let $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ be a cellular automaton and $\mathcal{M} \subset \mathcal{M}(\mathcal{A}^{\mathbb{Z}})$ be a class of initial measures.*

F strongly randomizes *$\mathcal{M}$ (resp. in Cesàro mean, in density, on cylinders of support $\mathbb{U}$) if, for all $\mu \in \mathcal{M}$, $(F^t\mu)_{t\in\mathbb{N}}$ converges to λ (resp. in Cesàro mean, in density, on cylinders of support $\mathbb{U}$).*

PROPOSITION 1. *Strong randomization implies all other forms of randomization, and randomization in Cesàro mean is equivalent to randomization in density for σ-invariant measures.*

Proof. The first point is clear. The second point stems from the fact that the uniform Bernoulli measure λ is an extremal point of $\mathcal{M}_\sigma(\mathcal{A}^{\mathbb{Z}})$ and $\mathcal{M}_\sigma(\mathcal{A}^{\mathbb{Z}})$ is compact. We prove this point by contraposition. Assume that $(F^t\mu)_{t\in\mathbb{N}}$ does not converge to λ in density. Then there must exist some $\varepsilon > 0$ and some sequence $(\varphi(t))$ of upper density $\alpha > 0$ such that $F^{\varphi(t)}\mu \notin B(\lambda,\varepsilon)$, where $B(\lambda,\varepsilon)$ is the open ball of radius ε centered on λ (otherwise for any $n > 0$ the set of times t with $F^t\mu \in B(\lambda, \frac{1}{n})$ would be of density 1 and by Lemma 1, $(F^t\mu)_{t\in\mathbb{N}}$ would converge to λ in density). Therefore there exists a sequence of times $(T_i)_{i\in\mathbb{N}}$ such that $\frac{T_i}{\varphi(T_i)} \to \alpha$. Then:

$$\frac{1}{\varphi(T_i)+1}\sum_{t=0}^{\varphi(T_i)} F^t\mu = \frac{1}{\varphi(T_i)+1}\sum_{t=0}^{T_i} F^{\varphi(t)}\mu + \frac{1}{\varphi(T_i)+1}\sum_{\substack{t=0\\ t\notin\varphi(\mathbb{N})}}^{\varphi(T_i)} F^t\mu.$$

Let $\mathcal{C}$ be the convex hull of $\mathcal{M}_\sigma(\mathcal{A}^{\mathbb{Z}})\backslash B(\lambda,\varepsilon)$. By compactness, this sequence admits accumulation points which must be of the form $\alpha\nu + (1-\alpha)\eta$ for some $\nu \in \mathcal{C}$ and $\eta \in \mathcal{M}_\sigma(\mathcal{A}^{\mathbb{Z}})$. However, since λ is extremal in $\mathcal{M}_\sigma(\mathcal{A}^{\mathbb{Z}})$, $\lambda \notin \mathcal{C}$, so that $\lambda \neq \nu$, and $\lambda \neq \alpha\nu + (1-\alpha)\eta$. In other words, the sequence $(\frac{1}{T+1}\sum F^t\mu)_{t\in\mathbb{N}}$ admits some accumulation point which is not λ, and we conclude. □

2.2. *Fourier theory*

DEFINITION 2 (CHARACTER) *A* character *of a topological group $\mathcal{G}$ is a continuous group homomorphism $\mathcal{G} \to \mathbb{T}^1$, where $\mathbb{T}^1$ is the unit circle group (under multiplication). Denote by $\widehat{\mathcal{G}}$ the group of characters of $\mathcal{G}$ under elementwise multiplication.*

The following result is well-known (see e.g. **[5]**, Lemma 4.1.3.):

PROPOSITION 2. *Any finite abelian group $\mathcal{G}$ is isomorphic to its dual $\widehat{G}$.*

If $\mathcal{A}$ is a finite abelian group, $\widehat{\mathcal{A}^{\mathbb{Z}}}$ is in bijective correspondance with the sequences of $(\widehat{\mathcal{A}})^{\mathbb{Z}}$ whose elements are all **1** except for a finite number. That is, $\chi \in \widehat{\mathcal{A}^{\mathbb{Z}}}$ can be written as $\chi(x) = \prod_{k\in\mathbb{Z}} \chi_k(x_k)$ where all but finitely many elements are equal to 1. In this context we call the elements of $\widehat{\mathcal{A}}$ *elementary characters*.

DEFINITION 3. *Let $\chi \in \widehat{\mathcal{A}^{\mathbb{Z}}}$ and $(\chi_i)_{i\in\mathbb{Z}}$ its decomposition in elementary characters. The* support *of χ is $\mathrm{supp}(\chi) = \{i \in \mathbb{Z} \ : \ \chi_i \neq 1\}$. Its* rank *is $\mathrm{rank}(\chi) = |\mathrm{supp}(\chi)|$.*

DEFINITION 4 (FOURIER COEFFICIENTS, OR FOURIER-STIELTJES TRANSFORM) *The* Fourier coefficients *of a measure $\mu \in \mathcal{M}(\mathcal{A}^{\mathbb{Z}})$ are given by:*

$$\widehat{\mu}[\chi] = \int_{\mathcal{A}^{\mathbb{Z}}} \chi d\mu$$

for all characters $\chi \in \widehat{\mathcal{A}^{\mathbb{Z}}}$. For a character $\chi = \prod_{k\in S} \chi_k$ (where $S = \mathrm{supp}(\chi)$), this can be rewritten as a finite sum:

$$\widehat{\mu}[\chi] = \sum_{u\in\mathcal{A}^S} \prod_{k\in S} \chi_k(u_k) \cdot \mu([u]_S)$$

The Fourier coefficients of μ completely characterize it. They also behave well with regard to convergence in (weak-*) topology:

THEOREM 1 (LÉVY'S CONTINUITY THEOREM) *Let G be a locally compact abelian group and $\mu_1, \mu_2, \ldots \mu_\infty \in \mathcal{M}(G)$. Then:*

$$\mu_n \to \mu_\infty \text{ in the weak-* topology} \quad \Longleftrightarrow \quad \forall \chi \in \widehat{G},\ \widehat{\mu_n}[\chi] \to \widehat{\mu_\infty}[\chi].$$

This theorem was first introduced in **[15]** (in French). It has been extended to locally compact abelian groups in **[20]**, and to more general settings which are out of the scope of this article.

DEFINITION 5 (HARMONICALLY MIXING MEASURE) *$\mu \in \mathcal{M}(\mathcal{A}^{\mathbb{Z}})$ is harmonically mixing if, for all $\varepsilon > 0$, there exists $R > 0$ such that $\mathrm{rank}(\chi) > R \implies \widehat{\mu}[\chi] < \varepsilon$.*

Throughout this paper, we sometimes omit to specify the class of initial measures, which is always the class of harmonically mixing measures.

PROPOSITION 3. *Let $\mathcal{A}$ be any finite abelian group. Any Bernoulli or (n-step) Markov measure on $\mathcal{A}^{\mathbb{Z}}$ with nonzero parameters is harmonically mixing.*

This is Propositions 6 and 8 and Corollary 10 in **[22]**.

3. *Character-diffusivity*

Let $\chi \in \widehat{\mathcal{A}^{\mathbb{Z}}}$ and let $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ be an abelian cellular automaton. Then $\chi \circ F$ is a character (composition of continuous group homomorphisms). One of the central ideas introduced in [**22**] is to focus on the evolution of the rank of characters under the action of F in order to establish randomization in density of harmonically mixing measures. They introduce the following notion of diffusivity over characters. We call it character-diffusivity to clearly distinguish it from the notion of diffusivity we will introduce later.

DEFINITION 6 (CHARACTER DIFFUSION) *Let $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ be an abelian cellular automaton. We say F* strongly diffuses *a character $\chi \in \widehat{\mathcal{A}^{\mathbb{Z}}}$ if $\operatorname{rank}(\chi \circ F^t) \to \infty$, and* diffuses χ in density *if if the convergence occurs along an increasing sequence of times of lower density one. We say F is* strongly character-diffusive *if it strongly diffuses every nontrivial character, and define* character-diffusivity in density *analogously.*

DEFINITION 7. *A measure μ is* strongly nonuniform *if $\mu[\chi] \neq 0$ for all characters $\chi \in \widehat{\mathcal{A}^{\mathbb{Z}}}$.*

EXAMPLE 1. *A Bernoulli measure $\mu = \otimes\beta$ whose parameters are all equal except one is strongly nonuniform. Assume that $\beta(a) = c$ for all $a \in \mathcal{A}$ except for $\beta(a') \neq c$. Let χ_k be a nontrivial elementary character, i.e. a character of $\mathcal{A}$.*

$$\mu[\chi_k] = \sum_{a\in\mathcal{A}} \beta(a)\chi_k(a) = (\beta(a') - c)\chi_k(0) + c\sum_{a\in\mathcal{A}} \chi_k(a) = \beta(a') - c \neq 0$$

by hypothesis. It follows that for every character $\chi = \prod_k \chi_k$, we have $\mu[\chi] = \prod_k \mu[\chi_k] \neq 0$ where we are using the fact that μ is a Bernoulli measure.

An example of a non-strongly nonuniform measure is any measure of the form $\lambda \times \mu$ on $(\mathcal{A} \times \mathcal{B})^{\mathbb{Z}}$, where λ is the uniform Bernoulli measure on $\mathcal{A}^{\mathbb{Z}}$.

The following proposition completes Theorem 12 of [**22**] by giving an equivalence between character-diffusivity and randomization. It also shows that randomization is a structural phenomenon, in the sense that it cannot happen on individual initial measures without happening on a large class.

DEFINITION 8. *A Bernoulli measure $\otimes\beta$ is* nondegenerate *if the support of β has nontrivial intersection with at least two cosets of every proper subgroup of $\mathcal{A}$.*

PROPOSITION 4. *Let F be an abelian cellular automaton. The following are equivalent:*

(i) F is character-diffusive ;

(ii) F randomizes the class of harmonically mixing measures;

(iii) F randomizes the class of nondegenerate Bernoulli measures;

(iv) F randomizes some strongly nonuniform Bernoulli measure.

This equivalence holds for all three kinds of character-diffusivity and randomization, that is: strong character-diffusivity/randomization, character-diffusivity/randomization

in density, and character-diffusivity for characters of support $\subset \mathbb{U}$/randomization on cylinders of support $\subset \mathbb{U}$ for any $\mathbb{U} \subset \mathbb{Z}$.

Proof.

$(i) \Rightarrow (ii)$**:** Assume F is strongly character-diffusive . Let μ be a harmonically mixing measure and χ any nontrivial character of $\mathcal{A}^{\mathbb{Z}}$. Since F is strongly character-diffusive , $\mathrm{rank}(\chi \circ F^t) \underset{t\to\infty}{\longrightarrow} \infty$. Since μ is harmonically mixing, it follows that $F^t\mu[\chi] = \mu[\chi \circ F^t] \underset{t\to\infty}{\longrightarrow} 0 = \lambda[\chi]$. Since this is true for any character χ, we have by Lévy's continuity theorem that $F^t\mu \underset{t\to\infty}{\longrightarrow} \lambda$.

For randomization in density, do the same proof, where each convergence is taken along a subsequence of upper density 1.

For randomization for characters of support $\subset \mathbb{U}$, the same argument shows that $F^t\mu[\chi] = \mu[\chi \circ F^t] \underset{t\to\infty}{\longrightarrow} 0 = \lambda[\chi]$ for any nontrivial character χ with support in $\mathbb{U}$. There is a bijection between the characters of support $\subset \mathbb{U}$ and $\widehat{\mathcal{A}^{\mathbb{U}}}$, and a conditional measure $\mu(\cdot \mid \mathfrak{B}_{\mathbb{U}})$ can be seen as a measure of $\mathcal{M}(\mathcal{A}^{\mathbb{U}})$. Applying Lévy's continuity theorem to $\mathcal{A}^{\mathbb{U}}$, it follows that $F^t\mu(\cdot \mid \mathfrak{B}_{\mathbb{U}}) \to \lambda(\cdot \mid \mathfrak{B}_{\mathbb{U}})$.

$(ii) \Rightarrow (iii)$**:** We prove that any nondegenerate Bernoulli measure $\mu = \otimes\beta$ is harmonically mixing. First note that for any elementary character $\chi_0 \neq \mathbf{1}$, we have:

$$\mu[\chi_0] = \int_{\mathcal{A}^{\mathbb{Z}}} \chi d\mu = \sum_{a\in\mathcal{A}} \chi_0(a)\beta(a).$$

We claim that there exist $a, b \in \mathcal{A}$ such that $\beta(a), \beta(b) > 0$ and $\chi_0(a) \neq \chi_0(b)$. To see this, let $K \leq \mathcal{A}$ be the kernel of χ_0. Since $\chi_0 \neq \mathbf{1}$, $\chi_0(g) \neq 1$ for some $g \in \mathcal{A}$, and thus $K < \mathcal{A}$. Then by the assumption that β is nondegenerate, there exist a, b in the support of β such that $aK \neq bK$. Thus $\beta(a), \beta(b) > 0$ and $\chi_0(a) \neq \chi_0(b)$.

Now the existence of a, b shows that $\sum_{a\in\mathcal{A}} \chi_0(a)\beta(a)$ is a non-trivial convex combination of points on the unit circle, so by the strict convexity of the unit circle, $\mu[\chi_0]$ is a non-extremal point of the unit disk, that is to say $|\mu[\chi_0]| < 1$.

Define $m = \max\{|\mu[\chi_0]| \ : \ \chi_0 \in \widehat{\mathcal{A}}\backslash\mathbf{1}\} < 1$. For any character $\chi = \prod_{i\in\mathbb{Z}} \chi_i$,

$$|\mu[\chi]| = \left|\prod_{i\in\mathbb{Z}} \mu[\chi_i]\right| \leq m^{\mathrm{rank}(\chi)},$$

where the first equality comes from the fact that μ is a Bernoulli measure. This implies that μ is harmonically mixing.

$(iii) \Rightarrow (iv)$**:** See e.g. the first measure in Example 1.

$(iv) \Rightarrow (i)$**:** Assume F is not strongly character-diffusive and take a character $\chi \neq \mathbf{1}$ such that $\mathrm{rank}(F^t \circ \chi) \nrightarrow \infty$. This means that there exists $C \in \mathbb{N}$ and a subsequence φ such that $\mathrm{rank}(\chi \circ F^{\varphi(t)}) \leq C$. Since there is a finite number of elementary characters, we have for any strongly nonuniform Bernoulli measure μ:

$$|F^{\varphi(t)}\mu[\chi]| \geq m^C \quad \text{where} \quad m = \min\{|\mu[\chi_0]| : \chi_0 \in \widehat{A}\} > 0.$$

Therefore $F^t\mu[\chi] \nrightarrow 0$, which implies that $F^t\mu \nrightarrow \lambda$. We conclude by contraposition.

For randomization in density, do the same proof along a sequence of times with positive upper density.

For randomization of cylinders of support $\subset \mathbb{U}$, we can do the same proof for any character of support $\subset \mathbb{U}$. □

REMARK 1. *The strongly nonuniform hypothesis is necessary to prevent the following kind of counterexample: take $\mathcal{A} = (\mathbb{Z}/2\mathbb{Z})^2$, $F' = F \times Id$ where F is a strongly randomizing cellular automaton on $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{Z}}$ (such as F_2, as we prove later) and $\mu = \nu \times \lambda$ where ν is any harmonically mixing measure and λ is the uniform Bernoulli measure on $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{Z}}$. Then F' strongly randomizes μ, but does not strongly randomize any measure whose second component is nonuniform.*

DEFINITION 9 (DEPENDENCY FUNCTION) *To any abelian CA $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ we associate a* dependency function*:*

$$\forall (t,i) \in \mathbb{N} \times \mathbb{Z},\ \Delta_F(t,i) = \left\{ \begin{array}{ccc} \mathcal{A} & \to & \mathcal{A} \\ q & \mapsto & F^t(x_q)_i \end{array} \right.$$

where x_q is the configuration worth q at position 0 and 0 everywhere else.

Notice that by linearity, we have:

$$\forall x \in \mathcal{A}^{\mathbb{Z}},\ \forall t \in \mathbb{N},\ F^t(x)_z = \sum_{j \in \mathbb{Z}} \Delta_F(t, z-j)(x_j), \tag{1}$$

where only a finite number of terms are nonzero.

In the following lemma, we prove that the support of the image of a fixed character at time t is entirely determined by the local dependency diagram.

LEMMA 2. *Let F be an abelian cellular automaton, and χ be a character whose support is included in $[0,m]$ for $m \geq 0$. If there are (t_1, z_1) and (t_2, z_2) such that:*

$$\forall z \in [0,m],\ \Delta_F(t_1, z_1 + z) = \Delta_F(t_2, z_2 + z)$$

then

$$-z_1 \in \mathrm{supp}(\chi \circ F^{t_1}) \Leftrightarrow -z_2 \in \mathrm{supp}(\chi \circ F^{t_2})$$

Proof. By Equation 1,

$$\begin{aligned}\chi \circ F^t(x) &= \prod_{i\in\mathbb{Z}} \chi_i \left(\sum_{j\in\mathbb{Z}} \Delta_F(t, i-j)(x_j) \right) \\ &= \prod_{i\in\mathbb{Z}} \prod_{j\in\mathbb{Z}} \chi_i \circ \Delta_F(t, i-j)(x_j) \\ &= \prod_{j\in\mathbb{Z}} \left(\prod_{k\in\mathbb{Z}} \chi_{k+j} \circ \Delta_F(t,k) \right)(x_j)\end{aligned}$$

where the last step is obtained by rewriting the sum: $k = i - j$. It follows:

$$\begin{aligned}-z_1 \in \operatorname{supp}(\chi \circ F^{t_1}) &\Leftrightarrow \prod_{k\in\mathbb{Z}} \chi_{k-z_1} \circ \Delta_F(t_1, k) \neq 0 \\ &\Leftrightarrow \prod_{k\in\mathbb{Z}} \chi_{k-z_2} \circ \Delta_F(t_2, k) \neq 0 \\ &\Leftrightarrow -z_2 \in \operatorname{supp}(\chi \circ F^{t_2})\end{aligned}$$

where the second step uses the hypothesis of the lemma and the fact that $\chi_{k-z_1} = 0$ whenever $k - z_1 \notin [0, m]$. □

Given an abelian CA F and $t \in \mathbb{N}$, denote by $d(t)$ the number of non-trivial dependencies of F at time t:

$$d(t) = \left|\{z \in \mathbb{Z} : \Delta_F(t, z) \neq 0\}\right| \quad \text{(the zero map)}$$

Following **[22, 23]**, we introduce *isolated bijective dependencies* which provide useful lower-bounds on the rank of image of characters under the action of F.

DEFINITION 10 (ISOLATED DEPENDENCY) *For $k \geq 1$, a k-isolated dependency is a pair $(t, z) \in \mathbb{N} \times \mathbb{Z}$ such that:*

1. *$\Delta_F(t, z)$ is a bijective dependency;*
2. *$\Delta_F(t, z + i) = 0$ for $1 \leq i \leq k$.*

We denote by $S_k(t)$ the set of k-isolated dependencies at time t (i.e. of the form (t, z)) and $s_k(t) = |S_k(t)|$.

This concept of k-isolated dependencies is also used in **[24]** to define dispersion mixing measure and dispersive CA. The main techniques of **[22]** (proof of Therorem 15) and **[23]** (V-separating sets) is essentially to use s_k as a lower bound for the rank of characters under the iteration of an abelian CA.

PROPOSITION 5. *Let F be an abelian cellular automaton, $\chi \neq \mathbf{1}$ a character, and k the diameter of $\operatorname{supp}(\chi)$. Then we have:*

$$\forall t \in \mathbb{N},\ s_{k-1}(t) \leq \operatorname{rank}(\chi \circ F^t) \leq \operatorname{rank}(\chi) \cdot d(t)$$

Proof. The rank being invariant by translation, we can suppose that $\mathrm{supp}(\chi) \subset [0, k-1]$ and that $\chi_0 \neq \mathbf{1}$. By Equation 1, we have:

$$\chi \circ F^t(x) = \prod_{i=0}^{k-1} \prod_{j \in \mathbb{Z}} \chi_i \circ \Delta_F(t, i-j)(x_j) = \prod_{j \in \mathbb{Z}} \left(\prod_{i=0}^{k-1} \chi_i \circ \Delta_F(t, i-j) \right)(x_j).$$

First, we have

$$j \in \mathrm{supp}(\chi \circ F^t) \Rightarrow \exists i, \chi_i \circ \Delta_F(t, i-j) \neq 1 \Rightarrow \exists i \in \mathrm{supp}(\chi), \Delta_F(t, i-j) \neq 0.$$

Therefore we get the upper bound $\mathrm{rank}(\chi \circ F^t) \leq \mathrm{rank}(\chi) \cdot d(t)$.

Second, if $(t, -j)$ is $k-1$-isolated, then $j \in \mathrm{supp}(\chi \circ F^t)$. Indeed:

$$(\chi \circ F^t)_j = \prod_{i=0}^{k-1} \chi_i \circ \Delta_F(t, i-j) = \chi_0 \circ \Delta_F(t, -j).$$

We deduce that $s_{k-1}(t) \leq \mathrm{rank}(\chi \circ F^t)$. □

EXAMPLE 2. *By Propositions 4 and 5, having $s_k(t) \longrightarrow_t +\infty$ for all k is a sufficient condition for randomization, but it is not necessary. For instance, take $F' = F \times (\sigma^N \circ F)$ where F is any abelian CA that randomizes in density. By Corollary 1 below, F' is randomizing in density. However, when N is large enough that F and $\sigma^N \circ F$ have disjoint neighborhoods, F' has no bijective dependency, and therefore $s_k(t) = 0$ for all k and t.*

On the other hand, having many bijective dependencies is not enough if they are not well-isolated. For example, one can check that H_2 satisfies $s_1(t) = t - 2$ but it is not randomizing, as shown in Section 5.

4. *Duality, Diffusivity and Solitons*

In the last section, we saw that the iterated images of characters under the action of a CA is key to understanding its action on probability measures. It turns out that the action of abelian CA on characters can be seen as a CA on the dual group, and that furthermore this dual CA shares many properties with the original CA.

Remember that any character χ of $\widehat{G^{\mathbb{Z}}}$ can be written as a finite product of cellwise (elementary) characters: $\chi(x) = \prod_{z \in \mathcal{N}} \chi_z(x_z)$ for some finite set $\mathcal{N} \subset \mathbb{Z}$ and $\chi_z \in \widehat{G}$. To such a χ we associate $\Psi(\chi)$, the configuration of $\widehat{G}^{\mathbb{Z}}$ defined by:

$$\Psi(\chi)(z) = \begin{cases} \chi_z & \text{if } z \in \mathcal{N} \\ 1 & \text{else.} \end{cases}$$

Note that $\Psi\left(\widehat{G^{\mathbb{Z}}}\right)$ is exactly the set of finite configurations of $\widehat{G}^{\mathbb{Z}}$.

DEFINITION 11 (DUAL CA) *Let F be an abelian CA over $G^{\mathbb{Z}}$. It can be written as*

$$F(x)_z = \sum_{i \in \mathcal{N}} \phi_i(x_{z+i})$$

where $\mathcal{N} \subset \mathbb{Z}$ is finite and ϕ_i are endomorphisms of G. We define $\widehat{F}$ over the finite configurations of $\widehat{G}^{\mathbb{Z}}$ by:

$$\widehat{F}(\Psi(\chi)) = \Psi(\chi \circ F).$$

Since $\widehat{F}$ is uniformly continuous and shift-invariant on finite configurations, it can be extended by continuity to a cellular automaton $\widehat{G}^{\mathbb{Z}} \to \widehat{G}^{\mathbb{Z}}$; this is the dual CA of F, and is an abelian CA for the group $(\widehat{G}, \times)$.

More concretely, if $\chi(x) = \prod_{z \in A} \chi_z(x_z)$, we have:

$$\widehat{F}(\Psi(\chi)) = \begin{cases} x_z \mapsto \prod_{i \in \mathcal{N}} \chi_{z-i}\big(\phi_i(x_z)\big) & \text{if } z \in A + \mathcal{N} \\ 1 & \text{else.} \end{cases}$$

Then, for any $c \in \widehat{G}^{\mathbb{Z}}$ we can define:

$$\widehat{F}(c)_z = \prod_{i \in \mathcal{N}} \gamma_i(c_{z-i}) \tag{2}$$

where γ_i is the endomorphism of $\widehat{G}$ defined by:

$$\gamma_i(\chi) = g \mapsto \chi \circ \phi_i(g).$$

When $G = \mathbb{F}_p^d$, the dual of a CA is obtained (up to conjugacy) by applying a mirror operation and transposing the matrix corresponding to each coefficient. Indeed, the map:

$$\begin{array}{ccc} G & \to & \widehat{G} \\ a & \mapsto & \chi_a \end{array} \qquad \text{where} \qquad \chi_a : b \in \mathcal{A} \mapsto e^{\frac{2i\pi}{p} < a, b >},$$

where $< a, b >$ denotes the scalar product of a and b seen as d-dimensional vectors, is an isomorphism. Through that isomorphism, we have that $\chi_a \circ M = \chi_{M^t a}$ for any endomorphism $M : \mathcal{A} \to \mathcal{A}$, and the result comes from Equation (2).

In particular, our examples F_2 and H_2 are flip conjugate to their own dual since all their coefficients are symmetric matrices. H_2 is actually conjugate to its dual since it is left-right symmetric.

We do not know whether an abelian CA F is always flip conjugate to its dual $\widehat{F}$; however, we show in the remainder of this section that they are dynamically close enough that properties like randomization or diffusion are preserved by duality.

LEMMA 3. *Let Φ_1 and Φ_2 be two abelian CA over $G^{\mathbb{Z}}$. Then we have $\widehat{\Phi_1 \circ \Phi_2} = \widehat{\Phi_2} \circ \widehat{\Phi_1}$. As a consequence:*

- *$\widehat{F^t} = \left(\widehat{F}\right)^t$ for any $t > 0$,*
- *$\widehat{F \circ \sigma} = \widehat{F} \circ \sigma^{-1}$,*
- *If F is reversible, then $\widehat{F}$ is also reversible and $\widehat{F^{-1}} = \left(\widehat{F}\right)^{-1}$.*

Furthermore, $\widehat{\widehat{F}} = F$ up to a canonical isomorphism.

Proof. By definition of dual CAs, we have for any $\chi \in \widehat{G^{\mathbb{Z}}}$:

$$\widehat{\Phi_1 \circ \Phi_2}(\Psi(\chi)) = \Psi(\chi \circ \Phi_1 \circ \Phi_2) = \widehat{\Phi_2}(\Psi(\chi \circ \Phi_1)) = \widehat{\Phi_2} \circ \widehat{\Phi_1}(\Psi(\chi)).$$

Since $\Psi\left(\widehat{G^{\mathbb{Z}}}\right)$ is dense in $\widehat{G}^{\mathbb{Z}}$ we deduce that $\widehat{\Phi_1 \circ \Phi_2} = \widehat{\Phi_2} \circ \widehat{\Phi_1}$ on the whole space.

For the last point, it is well-known that $\widehat{\widehat{G^{\mathbb{Z}}}} \simeq G^{\mathbb{Z}}$ through the canonical isomorphism $\psi : g \mapsto (\chi \mapsto \chi(g))$ (see e.g. [**5**], Lemma 4.1.4). Then we check that $\widehat{\widehat{F}} : \psi(g) \mapsto \psi(g) \circ \widehat{F} = \psi(F(g))$, so that $\widehat{\widehat{F}} \simeq F$ up to this isomorphism. □

In the following two technical lemmas and in the remainder of the section, we stress when our results do not require the CA to be abelian, even though we will only apply them to abelian CA.

LEMMA 4. *Let F be a CA with quiescent state 0. Then for any finite configuration x, $\mathrm{rank}(F(x)) \leq |\mathcal{N}| \cdot \mathrm{rank}(x)$.*

In particular, if F is abelian and χ is a character , $\mathrm{rank}(\chi \circ F) \leq |\mathcal{N}| \cdot \mathrm{rank}(\chi)$.

Proof. Since 0 is quiescent, the only nonzero cells in $F(x)$ belong to $\mathrm{supp}(x) + \mathcal{N}$. It follows that $\mathrm{rank}(F(x)) \leq |\mathcal{N}| \cdot \mathrm{rank}(x)$. The second statement follows by applying the result to $\widehat{F}$, noticing that F and $\widehat{F}$ have the same neighbourhood size by Equation 2. □

The converse lemma holds for reversible CA:

LEMMA 5. *Let F be a reversible CA with quiescent state 0. There exists a constant $C > 0$ such that for any finite configuration x, $\mathrm{rank}(F(x)) \geq C \cdot \mathrm{rank}(x)$.*

In particular, if F is abelian, there exists $C > 0$ such that $\mathrm{rank}(\chi \circ F) \geq C \cdot \mathrm{rank}(\chi)$ for any character χ.

Proof. Apply Lemma 4 on F^{-1}. The second point uses the last point of Lemma 3. □

DEFINITION 12. *A CA F with a quiescent state 0 is* strongly diffusive *(resp. diffusive in density) if for any finite configuration c, we have $\mathrm{rank}\big(F^t(c)\big) \to \infty$ (resp. on a subsequence of density 1).*

LEMMA 6. *An abelian CA F is strongly character-diffusive (resp. character-diffusive in density) if and only if $\widehat{F}$ is strongly diffusive (resp. diffusive in density).*

Proof. $\widehat{F}(\Psi(\chi)) = \Psi(\chi \circ F)$ and $\mathrm{rank}(\chi) = \mathrm{rank}\big(\Psi(\chi)\big)$. □

DEFINITION 13 (SOLITON) *Let F be an abelian CA. A* soliton *is a finite configuration $c \neq \overline{0}$ such that $F^p(c) = \sigma^q(c)$ for some $p \geq 1$ and $q \in \mathbb{Z}$.*

Intuitively, having a soliton is the opposite of being diffusive (even in density). In the remainder of the section we will develop this intuition and prove a series of technical results about solitons that will be culminate in the characterization of randomization in density in the next section.

First note that all the configurations in the orbit of a soliton have bounded rank. Conversely, we can extract a soliton from any orbit of finite configurations whose rank is bounded on a set of time steps of positive density:

PROPOSITION 6. *Let $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ be a surjective cellular automaton with a quiescent state 0. Assume that F is not diffusive in density. Then F admits a soliton.*

Proof. There is a finite initial configuration x and an increasing sequence $(T_n)_{n\in\mathbb{N}}$ of positive upper density such that $\mathrm{rank}(F^{T_n}(x))$ is bounded. Without loss of generality, assume that $\mathrm{rank}(F^{T_n}(x)) = k$ for all n. Denote $i_1(T_n), \ldots, i_k(T_n)$ the nonzero coordinates at time T_n.

Now let $m \in \{1, \ldots, k\}$ be the maximum integer such that there exists an integer M such that the subsequence:

$$(T_{\varphi(n)})_{n\in\mathbb{N}} = \{n \in \mathbb{N} : i_m(T_n) - i_1(T_n) \leq M\}$$

has positive upper density. In particular $(T_{\varphi(n)})_{n\in\mathbb{N}}$ has positive upper density. We distinguish two cases.

$\boxed{m = k:}$ $F^{T_{\varphi(n)}}(x)_{[i_1(T_{\varphi(n)}),i_k(T_{\varphi(n)})]}$ can take at most $|\bigcup_{j=0}^{M} \mathcal{A}^j| = \sum_{j=0}^{M} |\mathcal{A}|^j$ different values. By the pidgeonhole principle, we can find two integers $a < b$ such that

$$F^{T_{\varphi(a)}}(x)_{[i_1(T_{\varphi(a)}),i_k(T_{\varphi(a)})]} = F^{T_{\varphi(b)}}(x)_{[i_1(T_{\varphi(b)}),i_k(T_{\varphi(b)})]}.$$

But this means that $F^{T_{\varphi(b)}}(x) = \sigma^{i_1(T_{\varphi(b)})-i_1(T_{\varphi(a)})} \circ F^{T_{\varphi(a)}}(x)$, so we have found a soliton.

$\boxed{m < k:}$ First, by the same argument as above, $F^{T_{\varphi(n)}}(x)_{[i_1(T_{\varphi(n)}),i_m(T_{\varphi(n)})]}$ can only take a finite number of values, so at least one of these words appear with positive density. Denote w the corresponding word and $(T_{\varphi'(n)})_{n\in\mathbb{N}}$ the corresponding subsequence. We now prove that the configuration

$$\cdots 0 \cdot 0 \cdot 0 \cdot w \cdot 0 \cdot 0 \cdot 0 \cdots$$

is a soliton.

Take $N \in \mathbb{N}$ such that $\frac{1}{N}$ is a lower bound on the density of $(T_{\varphi'(n)})_{n\in\mathbb{N}}$ and let r be the radius of F. By construction of m, the times $T_{\varphi'(n)}$ where $i_{m+1}(T_{\varphi'(n)}) - i_m(T_{\varphi'(n)}) \leq 2rN$ have upper density 0. Therefore we extract from the sequence $(T_{\varphi'(n)})_{n\in\mathbb{N}}$ a new subsequence $(T_{\varphi''(n)})_{n\in\mathbb{N}}$ corresponding to times t where $i_{m+1}(t) - i_m(t) > 2rN$ with the same upper density. In particular, we can find some n such that $T = T_{\varphi''(n+1)} - T_{\varphi''(n)} \leq N$.

As shown in Figure 2, only two disjoint areas can contain nonzero values in $F^{T_{\varphi''(n+1)}}(x)$:

- the interval $[i_1(T_{\varphi''(n)}) - rT, i_m(T_{\varphi''(n)}) + rT]$,
  which contains $f^T\left(0^{2rT} \cdot w \cdot 0^{2rT}\right)$;
- the interval $[i_{m+1}(T_{\varphi''(n)}) - rT, i_k(T_{\varphi''(n)}) + rT]$
  which contains $f^T\left(0^{2rT} \cdot F^{T_{\varphi''(n)}}(x)_{[i_{m+1}(T_{\varphi''(n)}),i_k(T_{\varphi''(n)})]} \cdot 0^{2rT}\right)$.

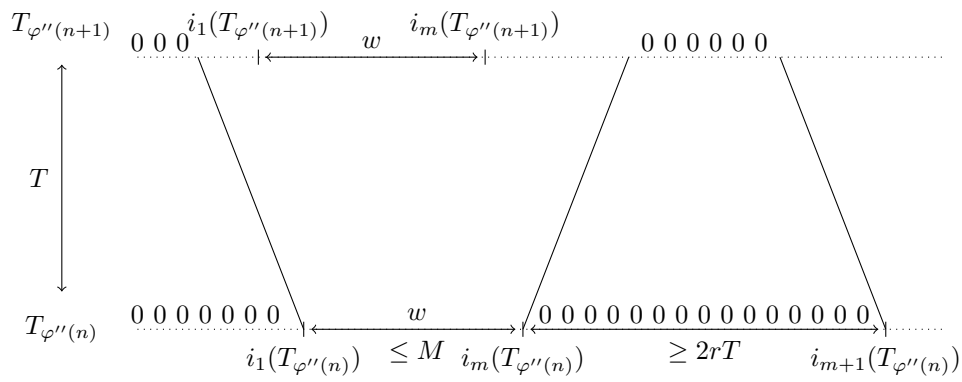


Figure 2. The finite configuration defined by w is a soliton.

Indeed, any cell outside of these regions can be written as $f^T(0^{2rT+1}) = 0$ since 0 is quiescent. Consider the different possibilities for the value of $i_1(T_{\varphi''(n+1)})$:

- if $i_1(T_{\varphi''(n+1)}) < i_1(T_{\varphi''(n)}) - rT$, then $F^{T_{\varphi''(n+1)}}(x)_{i_1(T_{\varphi''(n+1)})} = f^T(0^{2rT+1}) = 0$ which is a contradiction;
- if $i_1(T_{\varphi''(n+1)}) > i_1(T_{\varphi''(n)}) + rT$, then $F^{T_{\varphi''(n)}}(x)_{[i_1(T_{\varphi''(n)})\pm rT]}$ is a nonzero word whose image under f^T is zero. This means F is not preinjective (two different configurations that differ on a finite subset of cells have same image), so by the Garden-of-Eden theorem **[11, 3]** it is not surjective, a contradiction.

Therefore we have $i_1(T_{\varphi''(n+1)}) \in [i_1(T_{\varphi''(n)}) \pm rT]$. In particular, the interval $I = [i_1(T_{\varphi''(n)}) - rT,\ i_m(T_{\varphi''(n)}) + rT]$ contains all $i_\ell(T_{\varphi''(n+1)})$ for $\ell \leq m$. Using a similar argument, $i_{m+1}(T_{\varphi''(n+1)}) \in [i_{m+1}(T_{\varphi''(n)}) \pm rT]$, so that I does not contain any $i_\ell(T_{\varphi''(n+1)})$ for $\ell > m$.

From this we conclude that for some constant C:

$$F^T\left(0^{2rT} \cdot w \cdot 0^{2rT}\right) = 0^C \cdot w \cdot 0^{2rT-C}$$

and therefore we have found a soliton. □

The remainder of this section is dedicated to proving the following proposition.

PROPOSITION 7. *Let F be an abelian CA. Then F has a soliton if and only if $\widehat{F}$ has a soliton.*

To prove this proposition, we need a series of lemmas. For an abelian CA F, a finite fixed point is just a fixed point which is also a finite configuration. A finite fixed point is non-trivial if it is not the configuration everywhere equal to 0.

LEMMA 7. *Let F be an abelian CA and denote by X_F the set of spatially periodic fixed points:*

$$X_{F,n} = \{x : \sigma^n(x) = x \text{ and } F(x) = x\} \qquad X_F = \bigcup_n X_{F,n}.$$

F has a non-trivial finite fixed point if and only if X_F is infinite. In this case we actually have $|X_{F,n}| = 2^{\Omega(n)}$.

REMARK 2. *This remark holds in dimension d if one replaces the infiniteness assumption by $|X_{F,n}| = 2^{\Omega(n^d)}$.*

Proof. First suppose that $F(x) = x$ where x is a nontrivial finite configuration, and denote by u a finite word containing the nonzero part of x. Let r be the radius of F and $k = |u| + 2r$. Consider the set of finite words:

$$W_n = \left\{ w \in \mathcal{A}^n \ : \ \begin{array}{l} \forall i, 0 \leq i < \left\lfloor \frac{n}{k} \right\rfloor \Rightarrow \ w_{[ki,k(i+1)-1]} = 0^k \text{ or } w_{[ki,k(i+1)-1]} = 0^r u 0^r \\ \text{and} \\ w_{k\cdot\left\lfloor \frac{n}{k} \right\rfloor,n} = 0 \end{array} \right\}.$$

Any periodic configuration made of concatenated copies of some word in W_n (excepting 0^n) is a nontrivial fixed point and $|W_n| = 2^{\lfloor \frac{n}{k} \rfloor}$. Therefore we have $|X_{F,n}| = 2^{\Omega(n)}$.

Conversely, suppose X_F is infinite. Then, since $X_{F,n} \subset X_{F,kn}$ for $k \in \mathbb{N}^+$, $n \mapsto |X_{F,n}|$ is not bounded from above. For some n, $X_{F,n}$ must contain at least 2 distinct configurations x_1 and x_2 such that $x_1|_{[1,r]} = x_2|_{[1,r]}$ and $x_1|_{[n-r+1,n]} = x_2|_{[n-r+1,n]}$ by the pidgeonhole principle. It follows that the configuration

$$x : z \in \mathbb{Z} \mapsto \begin{cases} 0 & \text{if } z \leq 0 \text{ or } z > n \\ x_1(z) - x_2(z) & \text{else} \end{cases}$$

is a non-trivial finite fixed point. □

LEMMA 8. *Let G be an abelian group. For any endomorphism $h : G \to G$, define its dual $\widehat{h}$ by $\widehat{h}(\chi) = \chi \circ h$ for any character $\chi \in \widehat{G}$. Then we have $|\ker(h)| = |\ker(\widehat{h})|$.*

Proof. We have $\chi \in \ker(\widehat{h}) \Leftrightarrow \chi \circ h = 1 \Leftrightarrow \mathrm{Im}(h) \subset \ker(\chi)$. Therefore the restriction

$$\chi \mapsto \chi|_{(G/\operatorname{Im} h)}$$

is a bijection between $\ker(\widehat{h})$ and $(\widehat{G/\operatorname{Im} h})$. Since $\left|(\widehat{G/\operatorname{Im} h})\right| = |G/\operatorname{Im} h| = |\ker h|$ by Proposition 2, we conclude. □

LEMMA 9. *Let F be an abelian CA over alphabet G. F has a non-trivial finite fixed point if and only if $\widehat{F}$ has a non-trivial finite fixed point.*

Proof. For any $n \in \mathbb{N}$ with $n \geq 1$, let h_n be the endomorphism of G^n defined as follows. For any $u \in G^n$, let $x^u \in G^{\mathbb{Z}}$ be the (spatially) periodic point of period u, i.e. $x^u_i = u_{i \mod n}$ for all i. For each $u \in G^n$, define

$$h_n(u) = (F(x^u) - x^u)_{[0,n-1]}.$$

h_n captures the action of the CA $F - Id$ on spatially periodic configurations of period n. In particular we have $|\ker(h_n)| = |X_{F,n}|$. Now consider its dual $\widehat{h_n}$, which is an endomorphism of $\widehat{G^n} = (\widehat{G})^n$. For any $\chi = \prod_{1 \leq i \leq n} \chi_i$,

$$\widehat{h_n}(\chi) : u \mapsto \prod_{i=1}^{n} \chi_i(F(x^u) - x^u)_i = \prod_{i=1}^{n} \chi_i \circ F(x^u)_i \cdot (\chi_i(x^u)_i)^{-1}$$
$$= (\widehat{F}(x^\chi) \cdot x^{1/\chi})(x^u)$$

by definition of $\widehat{F}$, and where again we define the periodic point $x^\chi \in \widehat{G}^{\mathbb{Z}}$ by $x_i^\chi = \chi_{i \mod n}$. Therefore we have $|\ker(\widehat{h_n})| = |X_{\widehat{F},n}|$, similarly as above.

Now, by Lemma 8, we have $|\ker(h_n)| = |\ker(\widehat{h_n})|$ and therefore $|X_{F,n}| = |X_{\widehat{F},n}|$. We conclude by Lemma 7. □

Proof (of Proposition 7). Suppose F has a soliton x, that is, $F^p(x) = \sigma^q(x)$ for $p \geq 1$ and $q \in \mathbb{Z}$. Then x is a finite fixed point for the abelian CA $\sigma^{-q} \circ F^p$. By Lemma 9 we deduce that $\widehat{\sigma^{-q} \circ F^p}$ also has a finite fixed point y. Using Lemma 3, we can rewrite this as $\left(\widehat{F}\right)^p(y) = \sigma^{-q}(y)$, which shows that y is actually a soliton of $\widehat{F}$.

Applying the same reasoning, a soliton in $\widehat{F}$ implies a soliton in $\widehat{\widehat{F}}$, and $\widehat{\widehat{F}} = F$ up to a canonical isomorphism by Lemma 3. □

EXAMPLE 3. *Note that the smallest solitons of F and $\widehat{F}$ need not be of the same size. For example, consider the CA F defined over the alphabet $\mathbb{F}_2^2$ defined by:*

$$F(x)_z = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot x_z + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot x_{z+1}.$$

F acts like the identity on any configuration whose second components are all 0. In particular it admits solitons of rank 1. However, its dual, obtained up to conjugacy by mirroring and transposing the coefficients:

$$\widehat{F}(x)_z = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot x_{z-1} + \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot x_z$$

has no soliton of rank 1. Indeed, take any finite configuration x supported in $[i, j]$ for $i \leq u$ and such that $x_i \neq 0, x_j \neq 0$. Notice that:

$$F(x)_i = \begin{pmatrix} (x_i)_1 \\ (x_i)_1 + (x_i)_2 \end{pmatrix} \neq 0 \qquad \textit{and} \qquad F(x)_{j+1} = \begin{pmatrix} 0 \\ (x_j)_2 \end{pmatrix}.$$

In particular, if $(x_j)_2 \neq 0$, then x cannot be a soliton.

Now take any finite x of rank 1, assuming $x_0 \neq 0$. If $(x_0)_2 \neq 0$ then x is not a soliton by the previous argument. If $(x_0)_2 = 0$ then $\widehat{F}(x)$ is a finite configuration of rank 1 such that $\widehat{F}(x)_0 = \begin{pmatrix} (x_0)_1 \\ (x_0)_1 \end{pmatrix}$ and is not a soliton.

Finally, it is easy to check that the configuration

$$y = \cdots \begin{pmatrix} 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdots$$

is a fixed point, and therefore a soliton, of $\widehat{F}$.

5. *Characterization of Randomization in Density*

We are now ready to prove our first main result, which is a combinatorial characterization of randomization in density by the absence of solitons.

THEOREM 2. *Let F be an abelian CA. The following are equivalent:*

(i) F randomizes in density any harmonically mixing measure;

(ii) F has no soliton;

(iii) F is diffusive in density;

(iv) For some strongly nonuniform Bernoulli measure μ, the sequence $(F^t\mu)_{t\in\mathbb{N}}$ admits λ as an accumulation point.

Proof. Write the dual claims of $(i),(ii),(iii),(iv)$ for $\hat{F}$ as $(j),(jj),(jjj),(jv)$, respectively. Then

$$(i) \overset{Prop.\ 4}{\Longleftrightarrow} (jjj) \overset{Prop.\ 6}{\Longleftrightarrow} (jj) \overset{Prop.\ 7}{\Longleftrightarrow} (ii) \overset{Prop.\ 6}{\Longleftrightarrow} (iii),$$

so the first three claims are equivalent, and are also equivalent to (jj). Moreover, it is clear that $(i) \Rightarrow (iv)$. We prove $(iv) \Rightarrow (jj)$. Suppose (jj) does not hold, and let $\chi \in \widehat{G}^{\mathbb{Z}}$ be a soliton for $\widehat{F}$. Solitons are finite nonzero configurations, so we can consider $\chi \in \widehat{G^{\mathbb{Z}}}$ to be a nontrivial character satisfying that $\mathrm{rank}(\widehat{F}^t(\chi))$ is bounded from above by some m. Since μ is strongly nonuniform and Bernoulli, there exists $\varepsilon > 0$ such that $\mu[\chi'] \geq \varepsilon^{\mathrm{rank}\,\chi'}$. In particular, $F^t\mu[\chi] = \mu[\widehat{F}^t(\chi)] \geq \varepsilon^m$ for all t. Since $\lambda[\chi] = 0$, $F^t\mu[\chi]$ does not have λ as an accumulation point.

□

Before giving some general consequences of this theorem and applying it to the commutative case, let's use it on our examples.

EXAMPLE 4. *The CA H_2 admits a soliton:*

$$\cdots \begin{pmatrix}0\\0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\0\end{pmatrix}\cdots$$

and therefore it is not randomizing in density.

*On the contrary, we show that F_2 has no soliton and therefore is randomizing in density (it is actually strongly randomising, see Section 6.2). This is an alternative proof to the result of [**17**] where it was proven through a delicate analysis of F_2 using binomial coefficients and Lucas' Lemma. Our proof is illustrated in Figure 3. It is easy to show by induction that:*

$$\forall c \in \mathcal{A}^{\mathbb{Z}}, \forall n \in \mathbb{N}, \forall z \in \mathbb{Z},\ F_2^{2^{n+1}}(c)_z + F_2^{2^n}(c)_{z+2^n} + c_z = 0 \bmod 2.$$

Suppose by contradiction that F_2 has a soliton c such that $F^p(c) = \sigma^q(c)$. Therefore there is a constant M such that any nonzero cell of the space-time diagram $(F^t(c))_{t\in\mathbb{N}}$ is at horizontal distance at most M of the real line $L = \{(z,t) : pz + qt = 0\}$. In other words, $F^t(c)_z \neq 0 \Rightarrow |pz + qt| < pM$. Now take n such that $2^n > 2M$ and any $|z| \leq M$ and distinguish three cases:

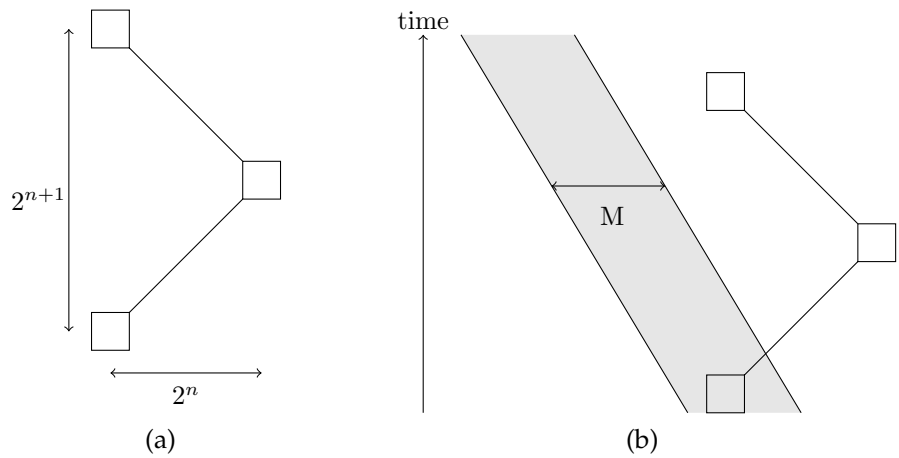


Figure 3. The direction of time is upward. (a) Any three cells in these relative positions in the space-time diagram of F_2 sum to zero (cancelling shape). (b) The space-time diagram of a soliton is zero except around a space-time line, and we can always position a cancelling shape that does not sum to zero.

$q = 0$**:** *Since* $|z - 2^n| > M$*, we have* $c_{z-2^n} = 0$ *and* $F_2^{2^{n+1}}(c)_{z-2^n} = 0$*, so that* $F_2^{2^n}(c)_z = 0$*. This is true for every* z *such that* $|z| \leq M$*, so* $F_2^{2^n}(c) = 0$*, a contradiction.*

$q = -p$**:** *Assume* $p = -q = 1$*.* $c_{z+2^{n+1}} = 0$ *and* $F_2^{2^n}(c)_{z+2^{n+1}+2^n} = 0$*, so that* $F_2^{2^{n+1}}(c)_{z+2^{n+1}} = 0$*. At time* 2^{n+1}*, this applies to every* z *such that* $|p(z + 2^{n+1}) - q(2^{n+1})| = |z| \leq M$*, so* $F_2^{2^{n+1}}(c) = 0$*, a contradiction.*

otherwise, $F_2^{2^{n+1}}(c)_z = F_2^{2^n}(c)_{z+2^n} = 0$ *when* n *is large enough, so that* $c_z = 0$ *for all* $|z| \leq M$*, a contradiction.*

DEFINITION 14 (POSITIVE EXPANSIVENESS) *A CA is* positively expansive *if there is some finite* $W \subseteq \mathbb{Z}$ *such that for any pair of distinct configurations* $x, y \in \mathcal{A}^{\mathbb{Z}}$*:*

$$\exists t \in \mathbb{N},\ \exists z \in W,\ F^t(x)_z \neq F^t(y)_z.$$

More generally, for $\alpha \in \mathbb{R}$*, we say that* F *is* positively expansive in direction α *if there is some finite* $W \subseteq \mathbb{Z}$ *such that for any pair of distinct configurations* $x, y \in \mathcal{A}^{\mathbb{Z}}$*,*

$$\exists t \in \mathbb{N},\ \exists z \in W,\ F^t(x)_{z+\lceil \alpha t \rceil} \neq F^t(y)_{z+\lceil \alpha t \rceil}$$

See **[25, 7]** for further developments on directional dynamics in cellular automata.

In the next result, for a CA $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ and a subalphabet $\mathcal{B} \subset \mathcal{A}$ such that $F(\mathcal{B}^{\mathbb{Z}}) \subseteq \mathcal{B}^{\mathbb{Z}}$, the corresponding *subautomaton* of F is $F' = F|_{\mathcal{B}^{\mathbb{Z}}}$.

COROLLARY 1. *Let* F *and* G *be abelian CA. Then:*

- *if* F *and* G *are randomizing then so is* $F \times G$*;*
- *if* F *is randomizing then all its subautomata are;*

- *if F is randomizing and reversible, then so is F^{-1};*
- *if F has a direction of positive expansivity then it is randomizing;*

where randomizing means randomizing in density any harmonically mixing measure.

Proof. This corollary follows from Theorem 2 by the following elementary observations on solitons:

- a soliton in $F \times G$ implies a soliton in either F or G;
- a soliton in a subautomaton of F is a soliton for F;
- a soliton for F^{-1} is a soliton for F;
- a positively expansive CA cannot admit a soliton. Indeed, take a CA F with a direction of positive expansiveness α and assume for the sake of contradiction that it admits a soliton c: $F^p(c) = \sigma^q(c)$. For any finite $W \subset \mathbb{Z}$, take the two distinct configurations $x = 0$ and $y = \sigma^k(c)$ for $|k|$ large enough and $\text{sign}(k) = \text{sign}(q/p - \alpha)$, and check that $F^t(x)_{z+\lceil \alpha t \rceil} = F^t(y)_{z+\lceil \alpha t \rceil} = 0$ for every $t \in \mathbb{N}$ and $z \in W$.

□

REMARK 3. *A CA with local rule $f : \mathcal{A}^m \to \mathcal{A}$ is bipermutive if $m \geq 2$ and the maps $x \mapsto f(x, a_1, \ldots, a_{m-1})$ and $x \mapsto f(a_1, \ldots, a_{m-1}, x)$ are permutations of $\mathcal{A}$ for any $a_1, \ldots, a_{m-1} \in \mathcal{A}$. Since bipermutivity implies the existence of a direction of positive expansivity [**2**], the above corollary implies that any bipermutive abelian CA randomizes in density any harmonically mixing measure. This generalizes Theorem 9 of [**23**], where the authors consider abelian CA of the form*

$$F = \sum_{i \in \mathcal{N}} \overline{\phi}_i \circ \sigma^i$$

where $|\mathcal{N}| \geq 2$ and $\overline{\phi}_i$ are commuting automorphisms. We do not need this hypothesis here, and for instance we prove that the following CA over $\mathbb{F}_2^2$ is randomizing in density:

$$F(c)_z = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot c_z + \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot c_{z+1}.$$

6. *Other forms of randomization*

In this section we consider other forms of randomization that have been less studied in the literature. First we prove that, in the case of abelian CAs whose coefficients are commuting endomorphisms, only randomization in density can happen. Then we provide examples of abelian CA that exhibit strong randomization and randomization for cylinders up to some fixed length.

6.1. *Abelian CAs with commuting coefficients* The case of abelian CAs with commuting coefficients is in many regards similar to the case of scalar coefficients. These CAs have more rigidity in their time evolution than general abelian CAs: the image of a single cell at time t can be determined directly through the use of the binomial theorem and modular arithmetic of binomial coefficients. In particular, when t is some power of the order of the group, the number of bijective dependencies is bounded, which explains why these CAs cannot randomize strongly.

LEMMA 10. *Let p be a prime number and $l \geq 0$. Let $(\mathcal{X}, +, \times)$ be a commutative ring of characteristic p^l, i.e. such that for any $X \in \mathcal{X}$:*

$$p^l \cdot X = 0$$

where 0 is the neutral element for $+$.

Then, for any $n \geq 0$ and any elements $X_i \in \mathcal{X}$, $1 \leq i \leq k$, we have this equality in $\mathcal{X}$:

$$\left(\sum_{i=1}^{k} X_i\right)^{p^{n+l-1}} = \left(\sum_{i=1}^{k} X_i^{p^n}\right)^{p^{l-1}}$$

Proof. First by the binomial theorem we have:

$$\left(\sum_{i=1}^{k} X_i\right)^{p^n} = \left(X_1 + \sum_{i=2}^{k} X_i\right)^{p^n} = X_1^{p^n} + \left(\sum_{i=2}^{k} X_i\right)^{p^n} + p \cdot Y$$

for some Y because, by Kummer's theorem, p divides $\binom{p^n}{i}$ for $0 < i < p^n$. By a direct induction we deduce:

$$\left(\sum_{i=1}^{k} X_i\right)^{p^n} = \sum_{i=1}^{k} X_i^{p^n} + p \cdot Y'$$

for some Y'. Now, applying again the binomial theorem we get:

$$\begin{aligned}
\left(\sum_{i=1}^{k} X_i\right)^{p^{n+l-1}} &= \left(\sum_{i=1}^{k} X_i^{p^n} + p \cdot Y'\right)^{p^{l-1}} \\
&= \left(\sum_{i=1}^{k} X_i^{p^n}\right)^{p^{l-1}} + \sum_{j=1}^{p^{l-1}} \binom{p^{l-1}}{j} \cdot p^j \cdot (Y')^j \cdot \left(\sum_{i=1}^{k} X_i^{p^n}\right)^{p^{l-1}-j} \\
&= \left(\sum_{i=1}^{k} X_i^{p^n}\right)^{p^{l-1}} + p^{l-1} \cdot Z
\end{aligned}$$

because by Kummer's theorem p^l divides $\binom{p^{l-1}}{j} \cdot p^j$ for any $1 \leq j \leq p$. Then the desired equality is shown since $p^l \cdot Z' = 0$. □

Now we prove that abelian CA cannot randomize strongly, and cannot randomize some cylinders without randomizing in density.

THEOREM 3. *There is no strongly randomizing abelian CA with commuting endomorphisms. Moreover, for any abelian group G, there exists an $N \in \mathbb{N}$ such that, for any abelian CA F over G with commuting endomorphisms, the following are equivalent:*

(i) F randomizes in density;

(ii) $\operatorname{rank}\big(F^N(c)\big) \geq 2$ for any finite configuration c of rank 1;

(iii) F randomizes in density on cylinders of length 1,

where as usual the class of initial measures is the set of harmonically mixing measures.

Proof. If p is a prime number, a *p-group* is a group G' where the order of every element $g \in G'$ is a power of p. By the decomposition theorem for finite abelian groups, they can be written as a direct product of finite p-groups for distinct primes p. Using this fact together with Corollary 1, it is enough to consider the case where G is a p-group (because an abelian CA on $G_1 \times G_2$ where G_1 and G_2 have relatively prime orders is a Cartesian product of abelian CAs on G_1 and G_2 respectively).

As usual, we write F as

$$F = \sum_{i \in \mathcal{N}} \overline{\phi}_i \circ \sigma^i.$$

Consider the commutative ring generated by the $\overline{\phi}_i$ and the shift map under addition and composition. This ring has characteristic p^l for some l because we considered a p-group as the alphabet. By Lemma 10, we get

$$\forall n \in \mathbb{N},\ F^{p^{n+l-1}} = \left(\sum_{i \in \mathcal{N}} (\overline{\phi}_i)^{p^n} \circ \sigma^{ip^n} \right)^{p^{l-1}} = \sum_{j \in \mathcal{N}'} (\gamma_j)^{p^n} \circ \sigma^{jp^n}, \tag{3}$$

where

$$\mathcal{N}' = \{n_1 + \cdots + n_{p^{l-1}} : n_i \in \mathcal{N}\}$$

and each γ_j is a sum of compositions of some ϕ_i that do not depend on n. The number of terms in the right-hand expression is bounded independently of n, so the number of dependencies of F^t is bounded on an infinite sequence of times and so F cannot be strongly randomizing by Proposition 5 (it cannot even strongly randomize cylinders of size 1).

For the second part of the proposition, consider $N = p^{n_0+l-1}$ for some n_0 such that $p^{n_0} > |G|$. This choice of N guaranties that, for any endomorphism h of G, we have $\ker(h^{p^{n_0}}) = \ker(h^{p^n})$ for any $n \geq n_0$ (because the sequence $\ker(h^i)$ increases strictly until it stabilizes). We have the following alternatives:

(a) *There is c of rank 1 such that $\operatorname{rank}\big(F^N(c)\big) = 0$.* In particular, F is not surjective. We claim that there is some $g \in G$ such that $F^{-t}([g])$ is empty for any large enough t. From the claim we deduce that F doesn't randomize cylinders of length 1 starting from the uniform Bernoulli measure. We now prove the claim: suppose that $F^{-t}([g])$ is never empty, whatever g and t. Then consider

any finite word $g_1 \cdots g_k$ and take n large enough so that $p^n > k$. By Equation 3 and by choice of n we get that for any configuration c, $F^{p^{n+l-1}}(c)_i$ depends only on $c_{|i+V_n}$ where $V_n \subseteq \mathbb{Z}$ is such that $1+V_n$, $2+V_n$,..., $k+V_n$ are two-by-two disjoint sets. Therefore from the assumption that $F^{-p^{n+l-1}}([g_i]) \neq \emptyset$ for any $1 \leq i \leq k$ and by linearity of F we deduce that there is some c with $F^{p^{n+l-1}}(c) \in [g_1 \cdots g_k]$. Since the choice of $g_1 \cdots g_k$ was arbitrary, we proved that F is surjective which is a contradiction.

(b) $\mathrm{rank}\big(F^N(c)\big) > 0$ *for any* c *of rank* 1*, but there is* d *of rank* 1 *such that* $\mathrm{rank}\big(F^N(d)\big) = 1$. By Equation 3, there is some $g \in G$ and a $j \in \mathcal{N}'$ such that $g \notin \ker(\gamma_j^{p^{n_0}})$ but $g \in \ker(\gamma_{j'}^{p^{n_0}})$ for all $j' \neq j$. As said before, the choice of n_0 ensures that for any $n \geq n_0$ we have $g \notin \ker(\gamma_j^{p^n})$ but $g \in \ker(\gamma_{j'}^{p^n})$ for all $j' \neq j$. Hence, using the formula for $F^{p^{n+l-1}}$, we deduce $\mathrm{rank}\big(F^{p^{n+l-1}}(d)\big) = 1$ for any $n \geq n_0$. In that case F admits a soliton of size 1.

(c) *For any* c *of rank* 1, $\mathrm{rank}\big(F^N(c)\big) \geq 2$. For the same reason as in the previous case we deduce $\mathrm{rank}\big(F^{p^{n+l-1}}(c)\big) \geq 2$ for any $n \geq n_0$. But Equation 3 above shows that the nonzero cells in $F^{p^{n+l-1}}(c')$ belong to the set $\mathcal{N}'_n = \{jp^n : j \in \mathcal{N}'\}$ for any c' of rank 1. We deduce that for any d of rank m and n large enough, $F^{p^{n+l-1}}(d)$ contains 2 nonzero cells distant from each other by at least $p^n - m$ cells. Therefore F does not have any soliton and it randomizes harmonically mixing measures in density by Theorem 2.

To sum up, we have $(c) \Rightarrow (i)$ while (a) and (b) are both incompatible with (i). Since (c) corresponds to (ii), we have shown that $(i) \Leftrightarrow (ii)(\Leftrightarrow (c))$. Since clearly $(i) \Rightarrow (iii)$, we now prove that $(iii) \Rightarrow (c)$.

If F randomizes in density on cylinders of length 1, then F is character-diffusive on characters or rank 1 (by Proposition 5) which means that $\widehat{F}$ has no soliton of size 1. It is straightforward to check by Equation 2 that an abelian CA with commuting endomorphisms has a dual with commuting endomorphisms, and therefore the above alternative (a/b/c) applies also to $\widehat{F}$. In other words, $\widehat{F}$ satisfies (c), which implies that it admits no solitons. This means in turn that F must satisfy (c) as well. The theorem follows. □

REMARK 4. *In [23] the authors consider abelian CA with integer coefficients (i.e. endomorphisms of the form* $a \mapsto n \cdot a$*); such a CA is called* proper *if for any prime divisor* p *of the order of the alphabet there are at least* 2 *coefficients not divisible by* p*. Theorem 6 of [23] shows that proper CA are randomizing in density. This is a particular case of the above theorem. Indeed, if* F *is proper and taking* N *from the theorem, it is easy to check that* F^N *is proper and that this is equivalent to* $\mathrm{rank}(F^N(c)) \geq 2$ *for any finite configuration of rank* 1*.*

6.2. *Strong Randomization* We now give examples of strongly randomizing abelian cellular automata. They are all defined over the alphabet $\mathcal{A} = \mathbb{Z}_p^2$ where p

is a prime number. In this section we denote by π_1 and π_2 the projections on the first and second component of the alphabet respectively.

We also denote $n \cdot g = \underbrace{g + \cdots + g}_{n \text{ times}}$ and $\overline{0}$ the neutral element of the group $\left(\mathcal{A}^{\mathbb{Z}}, +\right)$ (*i.e.* the configuration everywhere equal to $(0,0)$).

LEMMA 11. *If two abelian CA F and G over $\mathcal{A}^{\mathbb{Z}}$ commute, then for any $n \geq 0$ we have:*

$$(F+G)^{p^n} = F^{p^n} + G^{p^n}$$

Proof. Due to the structure of the group $\mathcal{A} = \mathbb{Z}_p^2$, for any configuration $c \in \mathcal{A}^{\mathbb{Z}}$ we have $p \cdot c = \overline{0}$. Therefore for any CA F, we have that $p \cdot F$ is the constant map equal to $\overline{0}$.

Now, from the binomial formula and from the fact that p divides $\binom{p}{n}$ for any $1 < n < p$, we deduce that:

$$(F+G)^p = F^p + G^p.$$

The lemma follows by an easy induction. □

Extending example F_2 from Section 2, we now consider for each prime $p \geq 2$ and all $c \in \mathcal{A}^{\mathbb{Z}}$:

$$F_p(c)_z = \left(\pi_1(c_{z+1}) + \pi_2(c_z), \pi_1(c_z)\right)$$
$$G_p(c)_z = \left(\pi_1(c_{z+1}) + \pi_1(c_z) + \pi_2(c_z), \pi_1(c_z)\right)$$

In the remainder of the section we prove that F_p and G_p are strongly diffusive for any prime $p \geq 2$.

These cellular automata are reversible and in fact also time-symmetric *i.e.* the product of two involutions **[9]**. For instance the inverse of F_p is:

$$F_p^{-1}(c)_z = \left(\pi_2(c_z), \pi_1(c_z) - \pi_2(c_{z+1})\right).$$

Since they are reversible, we extend their dependency diagrams to negative times, which means that $\Delta_\Phi(t,z)$ is defined for any $(t,z) \in \mathbb{Z}^2$ where Φ denotes F_p or G_p.

Note that both F_p and its inverse can be defined with neighborhood $\{0,1\}$. The same is true for G_p.

LEMMA 12. *For any $n \geq 0$, any $t \in \mathbb{Z}$ and any $z \in \mathbb{Z}$ we have:*

$$\Delta_{F_p}(2p^n + t, z) = \Delta_{F_p}(p^n + t, p^n + z) + \Delta_{F_p}(t, z)$$
$$\Delta_{G_p}(2p^n + t, z) = \Delta_{G_p}(p^n + t, p^n + z) + \Delta_{G_p}(p^n + t, z) + \Delta_{G_p}(t, z)$$

Proof. First, it is straightforward to check that $F_p^2 = (\sigma \circ F_p) + I$ (where I denotes the identity map over $\mathcal{A}^{\mathbb{Z}}$). Hence, using Lemma 11, we get the identity $F_p^{2p^n} = (\sigma_{p^n} \circ F_p^{p^n}) + I$. For every configuration c, $t \in \mathbb{Z}$ and $z \in \mathbb{Z}$ we have $F_p^{2p^n+t}(c)_z = F_p^{p^n+t}(c)_{p^n+z} + c_z$, which proves the Lemma.

The same proof scheme applies to Δ_{G_p}. □

LEMMA 13. *Let Φ be either F_p or G_p. For any $t \in \mathbb{Z}$ we have:*

1. *$\Delta_\Phi(t,z)$ is the constant map equal to $(0,0)$ when $z > 0$ or $z < -|t|$*
2. *$\Delta_\Phi(t,0)$ is a bijection.*

Proof. First both Φ and Φ^{-1} have neighborhood $\{0,1\}$. So the first item is straightforward by induction.

Second, by definition, $\Delta_\Phi(0,0)$ is a bijection. We can check that:

$$\Delta_{F_p}(1,0) : (g,h) \mapsto (h,g),\ \Delta_{G_p}(1,0) : (g,h) \mapsto (g+h,g),\ \Delta_{G_p}(2,0) : (g,h) \mapsto (h,g+h),$$

which are bijections. Applying Lemma 12 with $n = 0$, we get by straightforward induction that $\Delta_{F_p}(t+2,0) = \Delta_{F_p}(t,0)$ and $\Delta_{G_p}(t+3,0) = \Delta_{G_p}(t,0)$. We proved the second item. □

Much of the structure of Δ_Φ can be understood when focusing on particular "triangular" zones of $\mathbb{Z}^2$ at various scales. For $k \geq 0$ and n large enough so that $p^n - k > k$, we define the corresponding zone as:

$$T_{n,k} = \{(t,z) : k < t < p^n - k \text{ and } -t < z < k\}$$

LEMMA 14. *Let Φ be either F_p or G_p. Let $k \geq 0$ and n such that $p^n - k > k$. Then for any $(t,z) \in T_{n,k}$ and any $j \geq 1$ we have:*

$$\Delta_\Phi(t,z) = \Delta_\Phi(t + j \cdot p^n, z - j \cdot p^n).$$

In particular, if χ is a character whose support is of diameter at most k, then for any t with $k < t < p^n - k$ we have:

$$\mathrm{rank}(\chi \circ \Phi^{t+j\cdot p^n}) \geq \mathrm{rank}(\chi \circ \Phi^t) + 1$$

The lemma is illustrated in Figure 4.

Proof. For the first assertion consider some $(t,z) \in T_{n,k}$. From Lemma 13, we have that both $\Delta_\Phi(t-p^n, z-p^n)$ and $\Delta_\Phi(t, z-p^n)$ are the constant map equal to $(0,0)$. Therefore the following identities obtained from Lemma 12

$$\begin{aligned}\Delta_{F_p}(t+p^n, z-p^n) &= \Delta_{F_p}(t-p^n, z-p^n) + \Delta_{F_p}(t,z)\\ \Delta_{G_p}(t+p^n, z-p^n) &= \Delta_{G_p}(t-p^n, z-p^n) + \Delta_{G_p}(t, z-p^n) + \Delta_{G_p}(t,z)\end{aligned}$$

can in both cases be simplified to:

$$\Delta_\Phi(t,z) = \Delta_\Phi(t+p^n, z-p^n).$$

This prove the case $j = 1$. The same idea shows the induction step on j:

$$\Delta_\Phi(t + j\cdot p^n, z - j\cdot p^n) = \Delta_\Phi(t + (j+1)\cdot p^n, z - (j+1)\cdot p^n).$$

For the second assertion, apply Lemma 2 on the first assertion. We get that $-z \in \mathrm{supp}(\chi\circ\Phi^t)$ if and only if $-z + j\cdot p_n \in \mathrm{supp}(\chi\circ\Phi^{t+j\cdot p^n})$. Furthermore, we also have $0 \in \mathrm{supp}(\chi \circ \Phi^{t+j\cdot p^n})$ since 0 is a k-isolated bijective dependency by Lemma 13. Accounting for both contributions, we get $\mathrm{rank}(\chi \circ \Phi^{t+j\cdot p^n}) \geq \mathrm{rank}(\chi \circ \Phi^t) + 1$. □

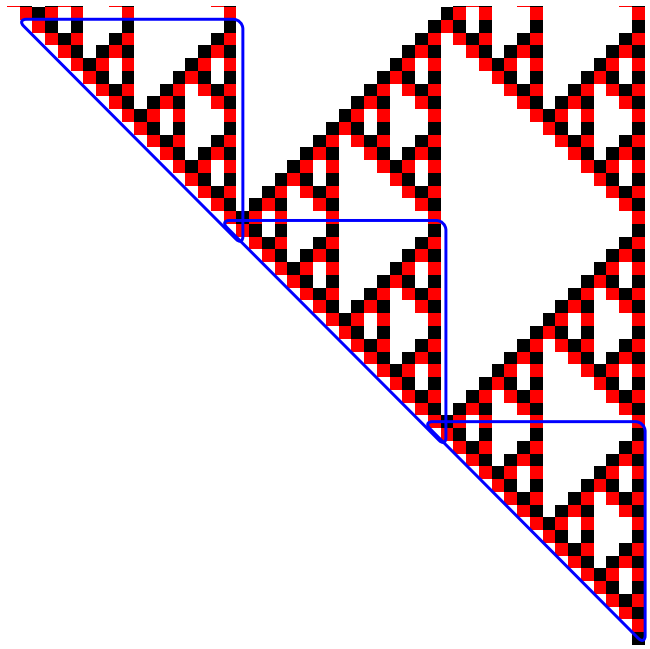


Figure 4. A representation of $\Delta_{F_2}(i,t)$ for $i \in \mathbb{Z}$ and $t \in \mathbb{N}$. The direction of time is upward. Thick blue lines indicate triangular zones $T_{4,0}$ and its translations by $(j \cdot 2^4, -j \cdot 2^4)$ for $j = 1, 2$.

THEOREM 4. *F_p and G_p strongly randomize the harmonically mixing measures.*

Proof. We prove that F_p and G_p are strongly character-diffusive, and Proposition 4 implies the result.

Denote by Φ either F_p or G_p. Φ is reversible and denote C the diameter of the neighborhood of Φ^{-1}. By Lemma 5, $\mathrm{rank}(\chi \circ \Phi) \geq C \cdot \mathrm{rank}(\chi)$ for any character χ. Since Φ^{-t} can be defined by a neighborhood of diameter $C \cdot t$, $\mathrm{rank}(\chi \circ \Phi^t) \geq C \cdot t \cdot \mathrm{rank}(\chi)$ for any character χ. In particular, for any $m \geq 0$, any $T \geq 0$, and any character χ_0 of rank at least $C \cdot m \cdot T$, we have $\mathrm{rank}\,(\chi_0 \circ \Phi^t) \geq m$ for $1 \leq t \leq T$.

Let χ be any non-trivial character and let k be the diameter of its support. Denote by $R(t) = \mathrm{rank}(\chi \circ \Phi^t)$. We are going to show that $R(t) \to \infty$, which implies the claim since the choice of χ is arbitrary.

First, let n_0 be large enough and t_0 such that $k < t_0 < p^{n_0} - k$. By successive applications of Lemma 14, we get

$$R\big(t_0 + (p-1)p^{n_0} + (p-1)p^{n_0+1} + \cdots + (p-1)p^{n_0+m}\big) \geq m.$$

Since $p^{n_0+m+1} = \sum_{j=0}^{m}(p-1)p^{n_0+j} + p^{n_0}$ we deduce that

$$p^{n_0+m+1} - \big(t_0 + \sum_{j=0}^{m}(p-1)p^{n_0+j}\big) \leq p^{n_0} - t_0$$

so that as soon as $m \geq C \cdot M \cdot (p^{n_0} - t_0)$ it follows $R(p^{n_0+m+1}) \geq M$ by Lemma 5. Therefore:

$$R(p^n) \to_n \infty. \tag{4}$$

Now define the predicate $P_{t_0,n,m}$ as the conjunction of the following conditions:

1. $k \leq t_0 \leq p^n - k$;
2. $\forall t, t_0 \leq t \leq p^n - k : R(t) \geq m$;
3. $R(p^n - k) \geq C \cdot (m+1) \cdot (t_0 + k)$.

First, since $R(t) \geq 1$ for any t (from Lemma 13), we have by Equation (4) above and Lemma 4 that $P_{k,n,1}$ holds for n large enough.

Furthermore, if $P_{t_0,n,m}$, then $P_{t_0+p^n,n',m+1}$ for all large enough n'. Indeed, condition 1 is obviously true for $n' > n$, condition 3 is true for any large enough n' from (4) above and Lemma 4. Finally, condition 2 is obtained from Lemma 14: for any $j \geq 1$,

1. for $j \cdot p^n + t_0 \leq t \leq (j+1) \cdot p^n - k$, $R(t) \geq R(t - j \cdot p^n) + 1 \geq m + 1$;
2. for $(j+1) \cdot p^n - k \leq t \leq (j+1) \cdot p^n + t_0$ we have $R(t) \geq m+1$ because $R((j+1) \cdot p^n - k) \geq R(p^n - k) \geq C \cdot (m+1) \cdot (t_0 + k)$.

We have shown that for any m there exists t_0 such that for any large enough n' we have $P_{t_0,n',m}$. This in particular implies $R(t) \geq m$ for all $t \geq t_0$. We conclude that $R(t) \to \infty$. □

6.3. *Randomizing only up to fixed-length cylinders* We now define a family of cellular automata that randomize finite cylinders up to a certain length, but no further. The alphabet is G^2 where G is any finite abelian group. Define:

$$I_G(c)_z = \big(-[\pi_1(c_{z-1}) + \pi_1(c_{z+1}) + \pi_2(c_z)], \pi_1(c_z)\big).$$

Notice that $I_{\mathbb{Z}_2} = H_2$.

PROPOSITION 8. *I_G randomizes cylinders of length 1, but not cylinders of length 2.*

LEMMA 15. *For $t > 0$, we have:*

$$\Delta_{I_G}(t,z) = (g,h) \mapsto \begin{cases} 0 & \textit{if} \quad |z| > t \\ ((-1)^t g, 0) & \textit{if} \quad |z| = t \\ ((-1)^t g, (-1)^{t+1} h) & \textit{if} \quad |z| < t, t+z = 0 \mod 2 \\ ((-1)^t h, (-1)^{t+1} g) & \textit{if} \quad |z| < t, t+z = 1 \mod 2 \end{cases}$$

Proof. By straightforward induction. □

Now we use Proposition 4 in conjunction with the following proposition to prove the announced result.

PROPOSITION 9. *I_G is strongly diffusive on characters of rank 1, but not on characters of length 2.*

Proof. Let χ be a character of rank 1, i.e. $\chi(x) = \chi_0(x_0)$ with $\chi_0 \neq \mathbf{1}$. For $t > 0$:

$$\begin{aligned}\chi \circ I_G^t(x) &= \chi_0\left(\sum_{z=-t}^{t} \Delta_{I_G}(t,z)(x_{-z})\right)\\ &= \prod_{z=-t}^{t} \chi_0 \circ \Delta_{I_G}(t,z)(x_{-z})\end{aligned}$$

χ_0 is nontrivial and by the previous Lemma, $\Delta_{I_G}(t,z)$ is an isomorphism when $|z| < t$. We deduce that $\chi_0 \circ \Delta_{I_G}(t,z)$ is nontrivial whenever $|z| < t$ and therefore $\mathrm{rank}(\chi \circ I_G^t(x)) \geq 2t - 1 \to \infty$: I_G strongly diffuses characters of rank 1.

For the second point, take any elementary character $\eta_0 \in \widehat{G}$ and define another character $\eta : x \mapsto \eta_0(\pi_1(x_0) + \pi_2(x_1))$. Then, by a straightforward computation:

$$\begin{aligned}\eta \circ I_G(x) =& \eta_0\big(-[\pi_1(x_{-1}) + \pi_1(x_1) + \pi_2(x_0)] + \pi_1(x_1)\big)\\ =& \eta_0\big(-\pi_1(x_{-1}) - \pi_2(x_0)\big) = \sigma^{-1} \circ \eta(x)^{-1}\end{aligned}$$

which means η a soliton for $\widehat{F}$ of rank 2. □

Now we introduce the cellular automaton $I_{G,n}$, which consists in applying the local rule of I_G on the neighbourhood $\{z_{-n}, z_0, z_n\}$:

$$I_{G,n}(c)_z = \big(-[\pi_1(c_{z-n}) + \pi_1(c_{z+n}) + \pi_2(c_z)], \pi_1(c_z)\big)$$

Intuitively, a space-time diagram for $I_{G,n}$ consists of n intertwined space-time diagrams for I_G.

THEOREM 5. *For any $n \geq 1$, $I_{G,n}$ randomizes cylinders of length n, but does not randomize cylinders of length $n+1$.*

It is obvious (straightforward induction) that:

LEMMA 16.

$$\Delta_{I_{G,n}}(t,z) = \begin{cases} \Delta_{I_G}(t, z/n) & \textit{if } z = 0 \mod n \\ 0 & \textit{otherwise} \end{cases}$$

so that we can use Lemma 15. As in the previous case, we use Proposition 4 in conjunction with the following:

PROPOSITION 10. *$I_{G,n}$ is strongly character-diffusive on characters of support $\subset [0, n-1]$, but not on characters of support $\{0, n\}$.*

Proof. Let χ be a nonzero character of support $\subset [0, n-1]$, that is, $\chi = \prod_{i=0}^{n-1} \chi_i$; without loss of generality assume $\chi_0 \neq \mathbf{1}$. We have for any $t > 0$:

$$\begin{aligned}\chi \circ I^t_{G,n}(x) &= \prod_{i=0}^{n-1} \chi_i \left(\sum_{z=-t}^{t} \Delta_{I_{G,n}}(t, z+i)(x_{-z}) \right) \\ &= \prod_{z=-t}^{t} \left(\prod_{i=0}^{n-1} \chi_i \circ \Delta_{I_{G,n}}(t, z+i) \right) (x_{-z})\end{aligned}$$

Now for any z such that $z = 0 \mod n$, the corresponding term in the previous equation is $\chi_0 \circ \Delta_{I_{G,n}}(t, z)$ by Lemma 16, and this term is an isomorphism when $t < z < t$ by Lemma 15. Therefore $\mathrm{rank}(\chi \circ I^t_{G,n}) \geq 2 \left\lfloor \frac{t}{n} \right\rfloor - 1 \to \infty$.

For the second point, take any nontrivial elementary character $\eta_0 \in \widehat{G}$ and define another character $\eta : x \mapsto \eta_0(\pi_1(x_0) + \pi_2(x_n))$. This is a soliton for $\widehat{F}$ of support $\{0, n\}$ by Lemma 16 and the same proof as Proposition 9. □

7. *Open problems*

Building upon the approach of [**22, 23**] we completely characterized randomization in density for abelian CAs. Furthermore, we provided examples of other forms of randomization, most notably strong randomization (in simple convergence), that can only happen for abelian CA whose coefficient are noncommuting endomorphisms.

As mentioned by several authors, the most important research direction for randomization in CA is to develop tools and techniques to go beyond the abelian case: CA with a nonabelian group structure or nonlinear CA [**13, 14**]. There is some experimental evidence pointing at nonlinear randomization candidates [**12, 29**]. The class of bipermutive CA, although it does not encompass all candidates, has some relevant related work: the set of invariant well-behaved (i.e. Gibbs) measures is limited to the uniform Bernoulli measure ([**14**], Corollary 46) and it exhibits a topological analogue to randomization [**27**]. Apart from the existence of examples, one can ask in the general case whether randomization is a structural property (see Proposition 4), whether it is preserved by elementary operations and whether it is implied by some topological properties like positive expansivity (see Corollary 1).

We believe that several intermediate questions raised by the present work are worth being considered:

- Is strong randomization of an abelian CA equivalent to strong randomization of its dual?
- What is the importance of reversibility in the above examples of strong randomization? Our proof relies on reversibility and the smoothness it implies on the evolution of rank of characters. Can a reversible abelian CA be randomizing in density but not strongly randomizing? What are the examples of strongly randomizing non-reversible abelian CA?

- The notions of soliton and diffusivity can be defined for arbitrary CAs using diamonds (like in the notion of pre-injectivity): a pair (x, y) such that $\Delta(x, y) \subseteq \mathbb{Z}$ (the set of positions where x and y differ) is finite. We can define a soliton as a diamond (x, y) such that $\Delta(F^t(x), F^t(y))$ has a bounded diameter (independent of t). On the contrary diffusivity can be defined as the property of having $|\Delta(F^t(x), F^t(y))| \to \infty$ for any diamond (x, y). What are the links with topological properties like positive expansivity, pre-expansivity†, mixing or transitivity? Are there links with randomization beyond abelian CAs? The results of **[26]** can be useful for that line of research.

- Theorem 3 gives a procedure to test randomization in density for abelian CA with commuting coefficients because the constant N can be explicitely computed. Is there an algorithm to decide the presence of a soliton in abelian CA? What about solitons in general CAs (again formalizing through diamonds as above)?

8. *Acknowledgments*
We are grateful to the anonymous referee for her/his help to improve this paper and correct several mistakes of the previous version. Benjamin Hellouin de Menibus acknowledges the financial support of Basal project No. PFB-03 CMM, Universidad de Chile.

References

[1] Laurent Boyer, Martin Delacourt, Victor Poupet, Mathieu Sablik, and Guillaume Theyssier. μ-limit sets of cellular automata from a computational complexity perspective. *Journal of Computer and System Sciences*, 81(8):1623–1647, 2015.

[2] Gianpiero Cattaneo, Michele Finelli, and Luciano Margara. Investigating topological chaos by elementary cellular automata dynamics. *Theoretical Computer Science*, 244(1):219–241, 2000.

[3] Tullio Ceccherini-Silberstein and Michel Coornaert. *Cellular Automata and Groups*. Springer, 2010.

[4] Benjamin Hellouin de Menibus and Mathieu Sablik. Characterization of sets of limit measures of a cellular automaton iterated on a random configuration. *Ergodic Theory and Dynamical Systems*, pages 1–50, 001 2016.

[5] Anton Deitmar. *A First Course in Harmonic Analysis*. Universitext. Springer Verlag, 2002.

[6] Martin Delacourt and Benjamin Hellouin de Menibus. Construction of μ-limit sets of two-dimensional cellular automata. In *32nd International Symposium on Theoretical Aspects of Computer Science, STACS 2015, March 4-7, 2015, Garching, Germany*, pages 262–274, 2015.

[7] Martin Delacourt, Victor Poupet, Mathieu Sablik, and Guillaume Theyssier. Directional dynamics along arbitrary curves in cellular automata. *Theoretical Computer Science*, 412(30):3800–3821, 2011.

† Positive pre-expansivity, introduced in **[10]**, is the property of being positively expansive on diamonds. A reversible CA can be positively pre-expansive (but never positively expansive) like the example F_2 of this paper. Corollary 1 states that, for abelian CA, a direction of positive expansivity implies randomization in density: this implication actually holds for directions of positive pre-expansivity.

[8] Pablo A. Ferrari, Alejandro Maass, Servet Martinez, and Peter Ney. Cesàro mean distribution of group automata starting from measures with summable decay. *Ergodic Theory and Dynamical Systems*, 20(6), 1999.

[9] Anahí Gajardo, Jarkko Kari, and Andrés Moreira. On time-symmetry in cellular automata. *Journal of Computer and System Sciences*, 78(4):1115–1126, 2012.

[10] Anahí Gajardo, Vincent Nesme, and Guillaume Theyssier. Pre-expansivity in cellular automata. *CoRR*, abs/1603.07215, 2016.

[11] Gustav Arnold Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Mathematical Systems Theory*, 3:320–375, 1969.

[12] Benjamin Hellouin de Menibus. *Asymptotic behaviour of cellular automata: computation and randomness*. PhD thesis, Aix-Marseille University, 2010.

[13] Bernard Host, Alejandro Maass, and Servet Martínez. Uniform Bernoulli measure in dynamics of permutative cellular automata with algebraic local rules. *Discrete and Continuous Dynamical Systems*, 9(6):1423–1446, 2003.

[14] Jarkko Kari and Siamak Taati. Statistical mechanics of surjective cellular automata. *Journal of Statistical Physics*, 160(5):1198–1243, 2015.

[15] Paul Lévy. Sur la détermination des lois de probabilité par leurs fonctions caractéristiques. *Comptes-rendus de l'Académie des Sciences*, 175:854–856, 1922.

[16] D.A. Lind. Applications of ergodic theory and sofic systems to cellular automata. *Physica D: Nonlinear Phenomena*, 10(1–2):36 – 44, 1984.

[17] Alejandro Maass and Servet Martínez. *Time averages for some classes of expansive one-dimensional cellular automata*, pages 37–54. Springer Netherlands, Dordrecht, 1999.

[18] Alejandro Maass, Servet Martínez, Marcus Pivato, and Reem Yassawi. Asymptotic randomization of subgroup shifts by linear cellular automata. *Ergodic Theory and Dynamical Systems*, 26:1203–1224, 8 2006.

[19] Munemi Miyamoto. An equilibrium state for a one-dimensional life game. *Journal of Mathematics of Kyoto University*, 19(3):525–540, 1979.

[20] K. R. Parthasarathy, R. Ranga Rao, and S. R. S. Varadhan. Probability distributions on locally compact abelian groups. *Illinois J. Math.*, 7(2):337–369, 06 1963.

[21] Marcus Pivato. Ergodic theory of cellular automata. In Robert A. Meyers, editor, *Encyclopedia of Complexity and Systems Science*, pages 2980–3015. Springer New York, New York, NY, 2009.

[22] Marcus Pivato and Reem Yassawi. Limit measures for affine cellular automata. *Ergodic Theory and Dynamical Systems*, 22:1269–1287, 2002.

[23] Marcus Pivato and Reem Yassawi. Limit measures for affine cellular automata II. *Ergodic Theory and Dynamical Systems*, 30:1–20, 2003.

[24] Marcus Pivato and Reem Yassawi. Asymptotic randomization of sofic shifts by linear cellular automata. *Ergodic Theory and Dynamical Systems*, 26(4):1177–1201, 08 2006.

[25] Mathieu Sablik. Directional dynamics for cellular automata: a sensitivity to initial condition approach. *Theoretical Computer Science*, 400(1-3):1–18, 2008.

[26] Ville Salo. Subshifts with sparse projective subdynamics. *CoRR*, abs/1605.09623, 2016.

[27] Ville Salo and Ilkka Törmä. Commutators of bipermutive and affine cellular automata. In *International Workshop on Cellular Automata and Discrete Complex Systems*, pages 155–170. Springer Berlin Heidelberg, 2013.

[28] Marcelo Sobottka. Right-permutive cellular automata on topological Markov chains. *Discrete and Continuous Dynamical Systems - Series A (DCDS-A)*, 20(4):1095–1109, 2008.

[29] Siamak Taati. Statistical equilibrium in deterministic cellular automata. *arXiv preprint arXiv:1505.06464*, 2015.