Randomization in Cellular Automata

B. Hellouin de Menibus, V. Salo, G. Theyssier

Institut de Mathématiques de Marseille
(CNRS, Université Aix-Marseille)

Turku, October 5th 2016

Cellular Automata

- Q finite **alphabet**, configuration space $Q^{\mathbb{Z}}$

$$c = \cdots c_{-1} c_0 c_1 \cdots$$

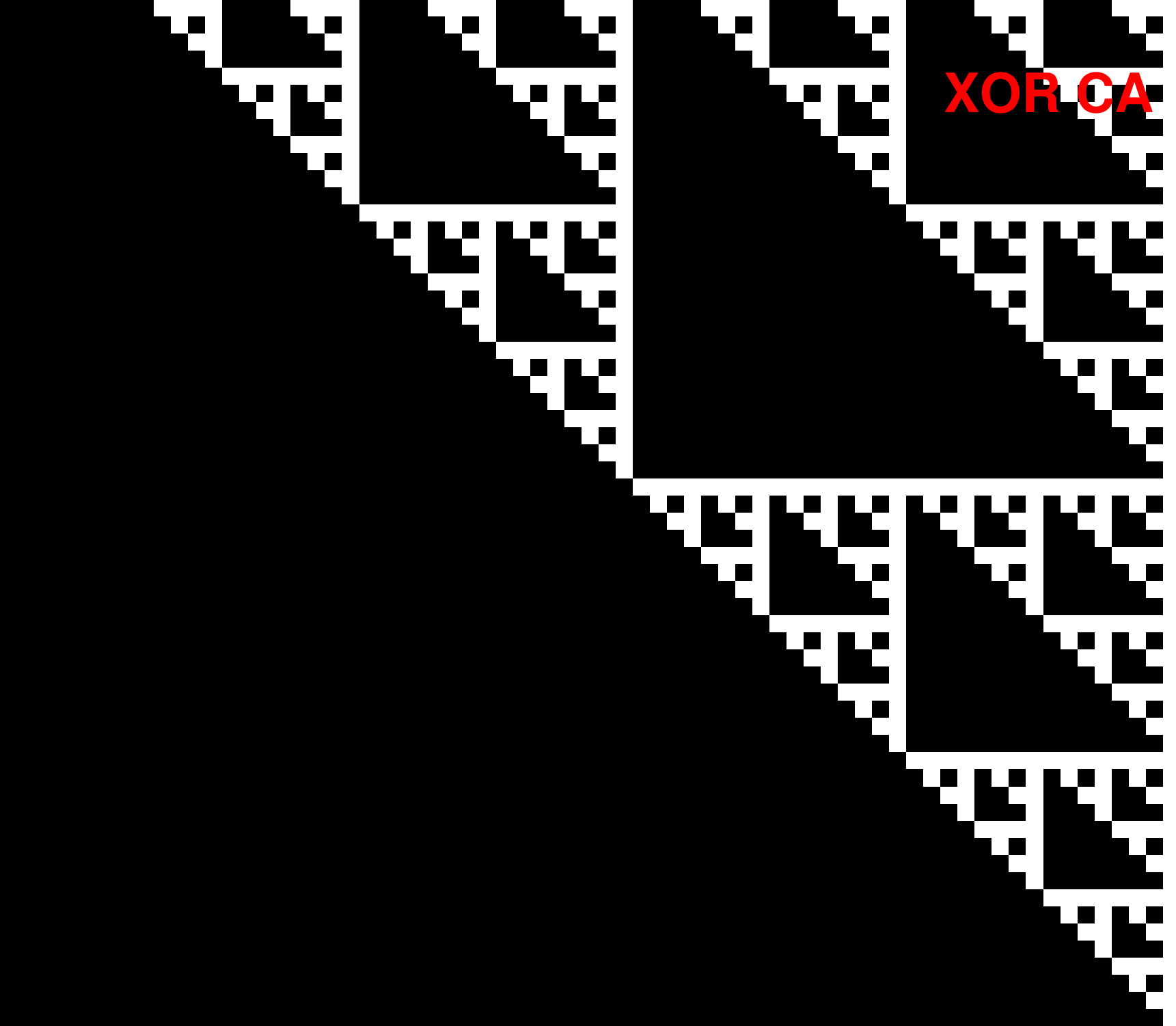
- **cellular automaton** $F : Q^{\mathbb{Z}} \to Q^{\mathbb{Z}}$

$$F(c)_z = f\left(j \in V \mapsto c_{z+j}\right)$$

$V \subseteq \mathbb{Z}$ finite **neighborhood**, $f : Q^V \to V$ **local rule**

- example with $Q = \{0, 1\}$: XOR CA

$$F(c)_z = c_z + c_{z+1} \bmod 2$$


XOR CA

CA and Probability Measures

- **cylinders** (base of open sets)

$$[u]_z = \{c \in Q^{\mathbb{Z}} : c_z \cdots c_{z+|u|-1} = u\}$$

CA and Probability Measures

- **cylinders** (base of open sets)

$$[u]_z = \{c \in Q^{\mathbb{Z}} : c_z \cdots c_{z+|u|-1} = u\}$$

- translation invariant **probability measure** μ
  - $\mu([u]_z) = \mu([u]_{z'}) = \mu(u) \in [0, 1]$
  - $\mu(u) = \sum_{q \in Q} \mu(uq) = \sum_{q \in Q} \mu(qu)$
  - $\mu(\epsilon) = 1$

CA and Probability Measures

- **cylinders** (base of open sets)

$$[u]_z = \{c \in Q^{\mathbb{Z}} : c_z \cdots c_{z+|u|-1} = u\}$$

- translation invariant **probability measure** μ
  - $\mu([u]_z) = \mu([u]_{z'}) = \mu(u) \in [0,1]$
  - $\mu(u) = \sum_{q \in Q} \mu(uq) = \sum_{q \in Q} \mu(qu)$
  - $\mu(\epsilon) = 1$
- **NDB**: **N**on-**D**egenerate **B**ernoulli measure μ

$$\mu(u) = \prod \mu(u_i)\ ,\ \mu(q) > 0\ \forall q \in Q$$

- example: uniform Bernoulli measure, $\mu_0(u) = \#Q^{-|u|}$

CA and Probability Measures

- **cylinders** (base of open sets)

$$[u]_z = \{c \in Q^{\mathbb{Z}} : c_z \cdots c_{z+|u|-1} = u\}$$

- translation invariant **probability measure** μ
  - $\mu([u]_z) = \mu([u]_{z'}) = \mu(u) \in [0,1]$
  - $\mu(u) = \sum_{q \in Q} \mu(uq) = \sum_{q \in Q} \mu(qu)$
  - $\mu(\epsilon) = 1$
- **NDB**: **N**on-**D**egenerate **B**ernoulli measure μ

$$\mu(u) = \prod \mu(u_i)\ ,\ \mu(q) > 0\ \forall q \in Q$$

- example: uniform Bernoulli measure, $\mu_0(u) = \#Q^{-|u|}$
- iteration: $F\mu(u) = \mu\big(F^{-1}([u])\big)$

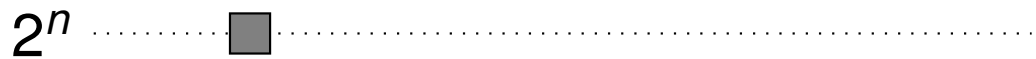
Example: XOR CA

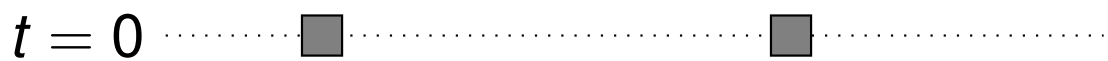
$F(c)_z = c_z + c_{z+1} \bmod 2$

Example: XOR CA

$F(c)_z = c_z + c_{z+1} \bmod 2$

- $F^{2^n}(c)_z = c_z + c_{z+2^n} \bmod 2$

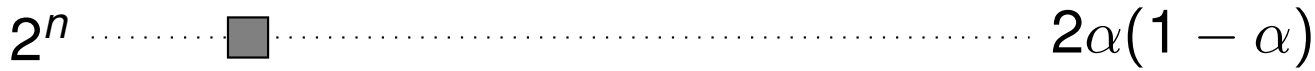


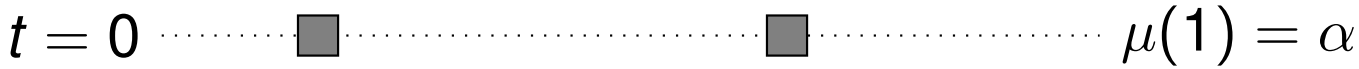


Example: XOR CA

$F(c)_z = c_z + c_{z+1} \bmod 2$

- $F^{2^n}(c)_z = c_z + c_{z+2^n} \bmod 2$
- μ Non Degenerate Bernoulli

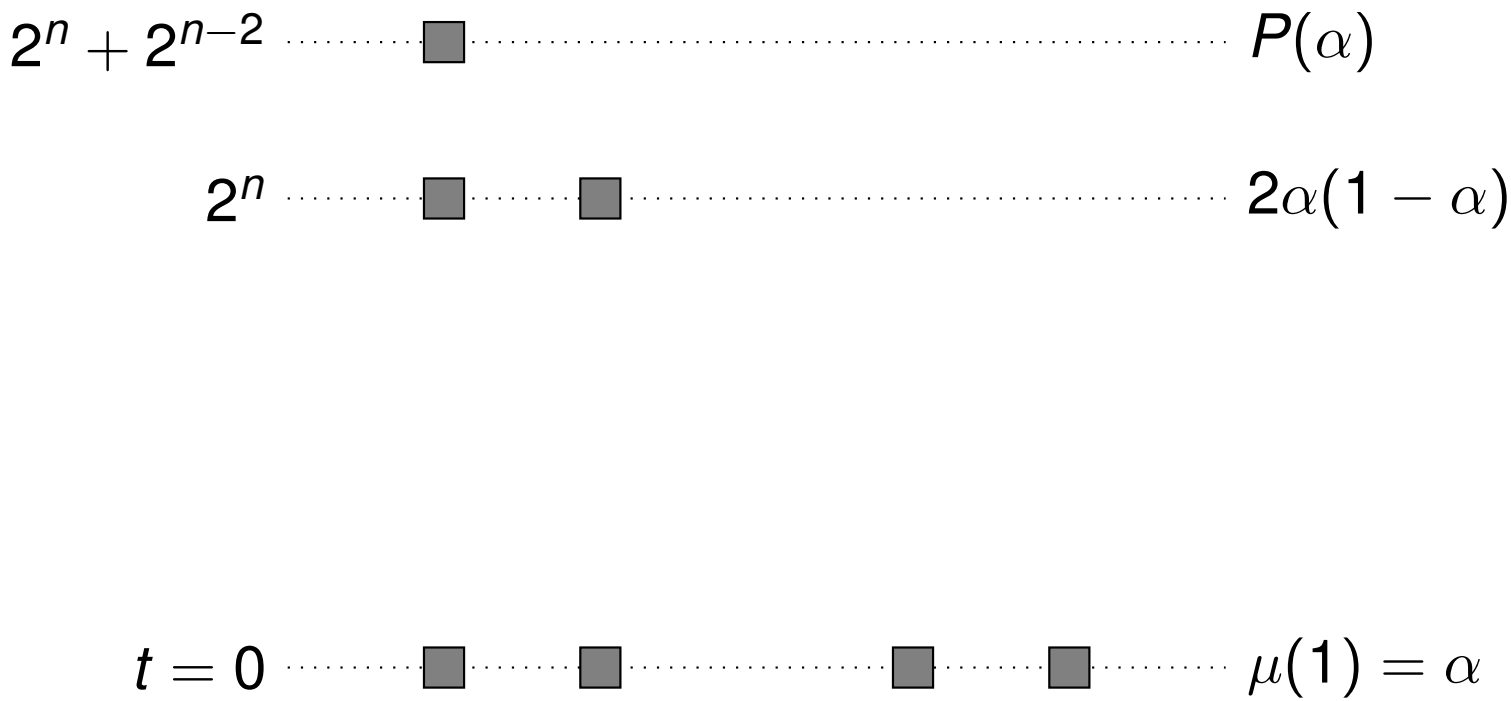




Example: XOR CA

$F(c)_z = c_z + c_{z+1} \bmod 2$

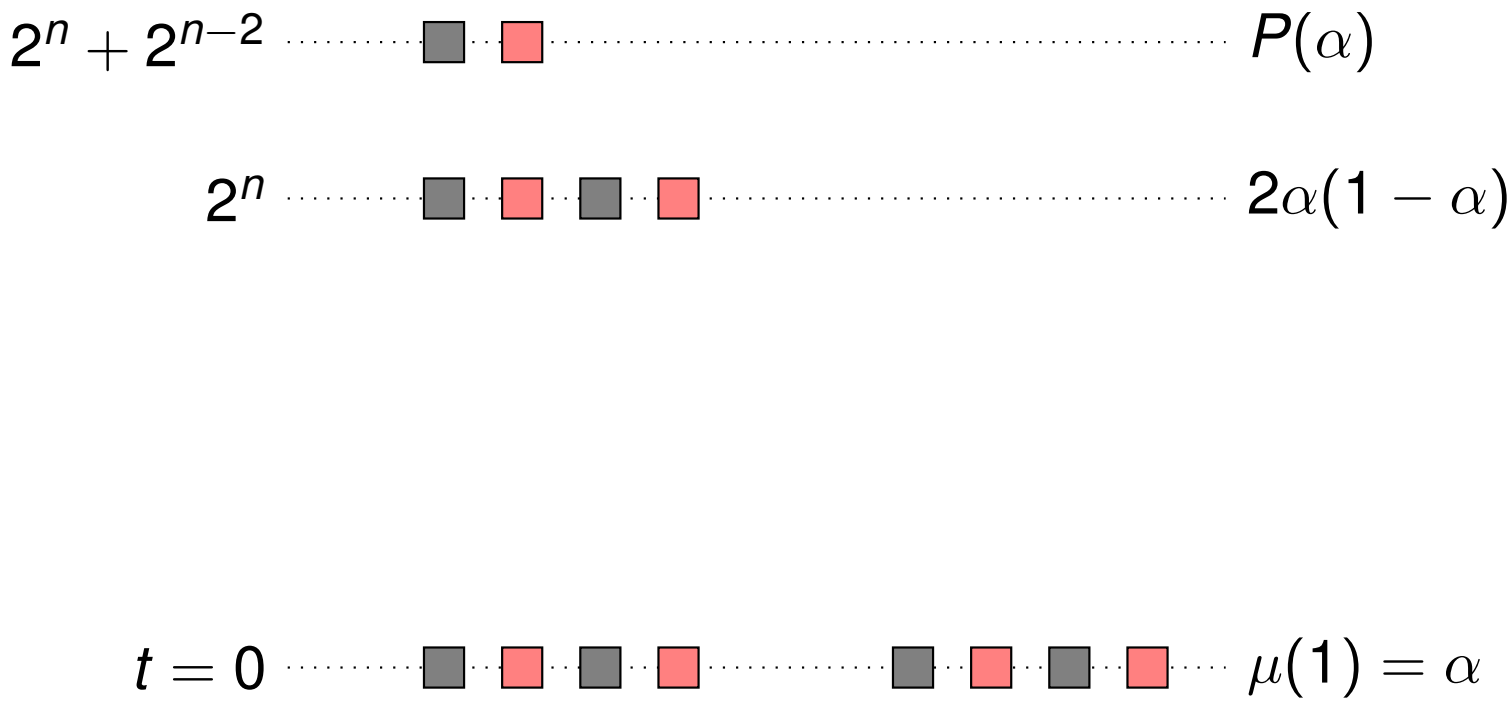
- $F^{2^n}(c)_z = c_z + c_{z+2^n} \bmod 2$
- μ Non Degenerate Bernoulli



Example: XOR CA

$F(c)_z = c_z + c_{z+1} \bmod 2$

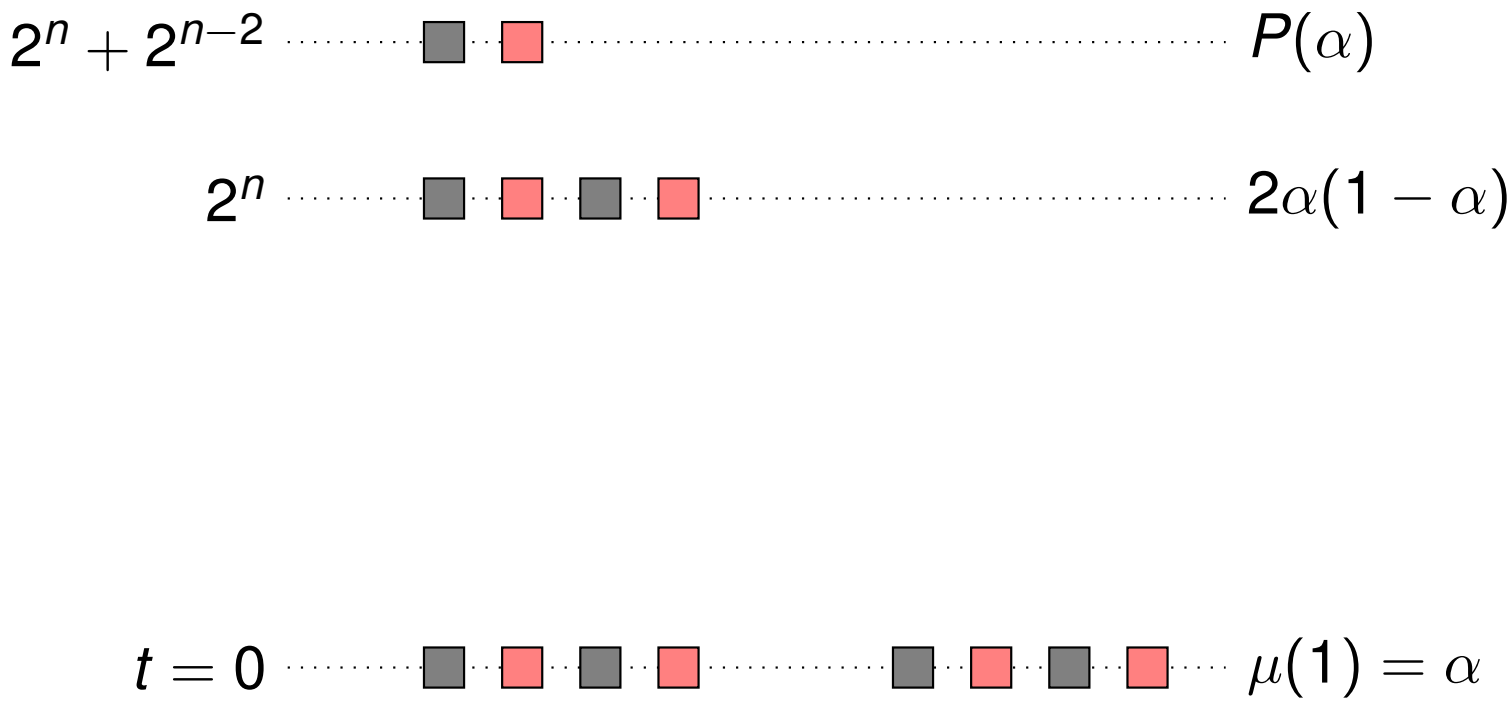
- $F^{2^n}(c)_z = c_z + c_{z+2^n} \bmod 2$
- μ Non Degenerate Bernoulli



Example: XOR CA

$F(c)_z = c_z + c_{z+1} \bmod 2$

- $F^{2^n}(c)_z = c_z + c_{z+2^n} \bmod 2$
- μ Non Degenerate Bernoulli



- $F^{t_n}\mu \to_n \mu_0$ for a good choice of t_n

Randomization

- class $\mathcal{I}$ of initial measure (NDB$\subseteq \mathcal{I}$)

Randomization

- class $\mathcal{I}$ of initial measure (NDB$\subseteq \mathcal{I}$)

- **strong randomization:** for all $\mu \in \mathcal{I}$

$$\forall u, F^t\mu(u) \xrightarrow[t\to\infty]{} \mu_0(u)$$

Randomization

- class $\mathcal{I}$ of initial measure (NDB$\subseteq \mathcal{I}$)

- **strong randomization:** for all $\mu \in \mathcal{I}$

$$\forall u, F^t\mu(u) \xrightarrow[t\to\infty]{} \mu_0(u)$$

- **randomization:** for all $\mu \in \mathcal{I}$

$$\forall u, F^{t_n}\mu(u) \xrightarrow[n\to\infty]{} \mu_0(u)$$

(t_n) subsequence of $\mathbb{N}$ of density 1

Some Results on Randomization

- **Miyamoto 1979, Lind 1984**

  XOR CA is randomizing for NDB measures.

- **Ferrari-Maass-Martinez-Ney 2000**

  $F(c)_z = \alpha c_z + \beta c_{z+1} \bmod p^l$, $\alpha, \beta \neq 0 \bmod p$
  is randomizing for measures with quick correlation decay.

- **Pivato-Yassawi 2002**

  $F(c)_z = \sum_{j \in J} \alpha_j c_{z+j}$ on Abelian group + conditions on α_j
  is randomizing for harmonically mixing measures.

- **Pivato-Yassawi 2004**

  $F(c)_z = \sum_{j \in J} \phi_j(c_{z+j})$ on Abelian group with $|J| \geq 2$ and ϕ_j commuting automorphisms
  is randomizing for harmonically mixing measures.

This talk

- consider all **Abelian** CAs: $(Q, \oplus)$ Abelian group and

$$F(c \overline{\oplus} d) = F(c) \overline{\oplus} F(d)$$

  or equivalently

$$F(c)_z = \bigoplus_{i \in V} h_i(c_{z+i})$$

  with h_i endomorphisms of $(Q, \oplus)$

- **characterization** of randomization

- example of **strong** randomization

Diamond dynamics

- Remark: F randomizing $\Rightarrow$ F surjective

Diamond dynamics

- Remark: F randomizing $\Rightarrow$ F surjective
- **differences:** $\Delta(c,d) = \{z \in \mathbb{Z} : c(z) \neq d(z)\}$
- **diamond:** $c \diamond d \Leftrightarrow \Delta(c,d)$ finite non empty

Theorem (Moore-Myhill)

F surjectif $\Leftrightarrow \big(c \diamond d \Rightarrow F(c) \diamond F(d)\big)$

Diamond dynamics

- Remark: F randomizing $\Rightarrow$ F surjective
- **differences:** $\Delta(c,d) = \{z \in \mathbb{Z} : c(z) \neq d(z)\}$
- **diamond:** $c \diamond d \Leftrightarrow \Delta(c,d)$ finite non empty

Theorem (Moore-Myhill)

F surjectif $\Leftrightarrow \big(c \diamond d \Rightarrow F(c) \diamond F(d)\big)$

- **strong diffusion:** *nb. of differences grows to infinity*
  $\forall c,d : c \diamond d \Rightarrow \#\Delta(F^t(c), F^t(d)) \xrightarrow[t\to\infty]{} \infty$

Diamond dynamics

- Remark: F randomizing $\Rightarrow$ F surjective
- **differences:** $\Delta(c,d) = \{z \in \mathbb{Z} : c(z) \neq d(z)\}$
- **diamond:** $c \diamond d \Leftrightarrow \Delta(c,d)$ finite non empty

Theorem (Moore-Myhill)

F surjectif $\Leftrightarrow \big(c \diamond d \Rightarrow F(c) \diamond F(d)\big)$

- **strong diffusion:** *nb. of differences grows to infinity*
  $\forall c,d : c \diamond d \Rightarrow \#\Delta(F^t(c), F^t(d)) \xrightarrow[t\to\infty]{} \infty$
- **diffusion:** *same but removing "accidental" steps*
  $\forall c,d : c \diamond d \Rightarrow \#\Delta(F^{t_n}(c), F^{t_n}(d)) \xrightarrow[n\to\infty]{} \infty$
  (t_n) subsequence of $\mathbb{N}$ of density 1

Diamond dynamics

- Remark: F randomizing $\Rightarrow$ F surjective
- **differences:** $\Delta(c,d) = \{z \in \mathbb{Z} : c(z) \neq d(z)\}$
- **diamond:** $c \diamond d \Leftrightarrow \Delta(c,d)$ finite non empty

Theorem (Moore-Myhill)

F surjectif $\Leftrightarrow \big(c \diamond d \Rightarrow F(c) \diamond F(d)\big)$

- **strong diffusion:** *nb. of differences grows to infinity*
  $\forall c,d : c \diamond d \Rightarrow \#\Delta(F^t(c), F^t(d)) \xrightarrow[t\to\infty]{} \infty$
- **diffusion:** *same but removing "accidental" steps*
  $\forall c,d : c \diamond d \Rightarrow \#\Delta(F^{t_n}(c), F^{t_n}(d)) \xrightarrow[n\to\infty]{} \infty$
  (t_n) subsequence of $\mathbb{N}$ of density 1
- **glider:** *differences stay in a tube*
  $c \diamond d$ such that $\Delta(F^t(c), F^t(d)) \subseteq [\alpha t - \beta, \alpha t + \beta]$ for all t

Abelian Examples

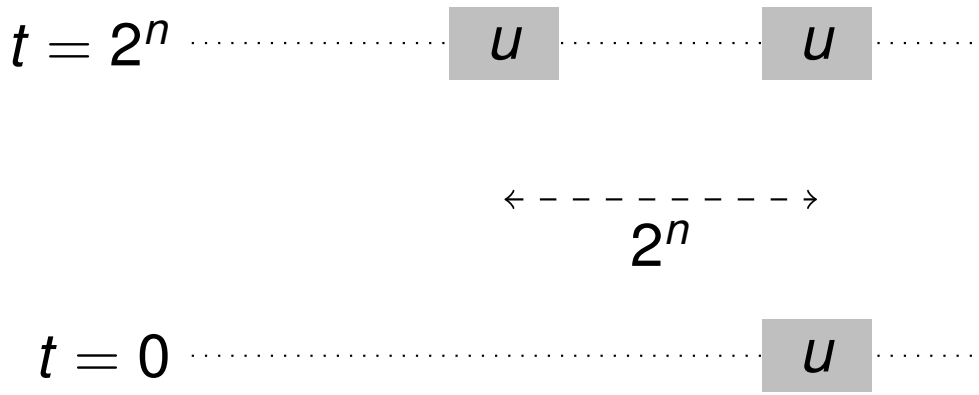
- enough to consider diamonds with $c \diamond d$ with $c = {}^{\omega}0^{\omega}$

Abelian Examples

- enough to consider diamonds with $c \diamond d$ with $c = {}^{\omega}0^{\omega}$
- XOR has a glider?

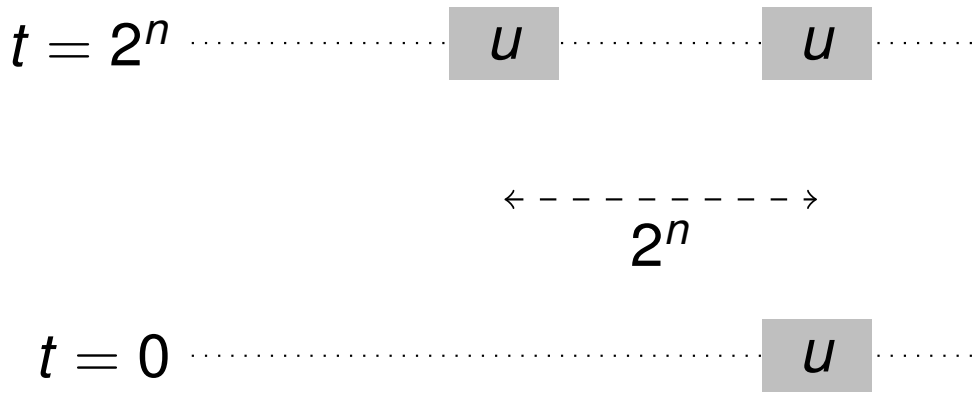
Abelian Examples

- enough to consider diamonds with $c \diamond d$ with $c = {}^{\omega}0^{\omega}$
- XOR has a glider? **NO!** $F^{2^n}(c)_z = c_z \oplus c_{z+2^n}$



Abelian Examples

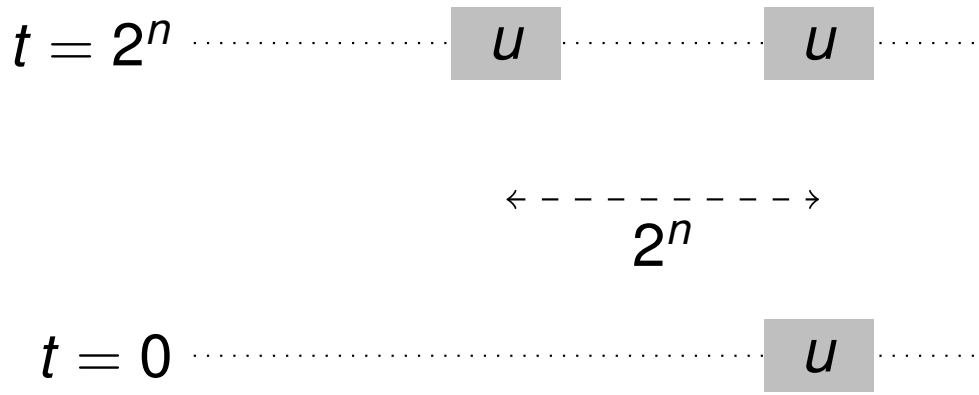
- enough to consider diamonds with $c \diamond d$ with $c = {}^{\omega}0^{\omega}$
- XOR has a glider? **NO!** $F^{2^n}(c)_z = c_z \oplus c_{z+2^n}$



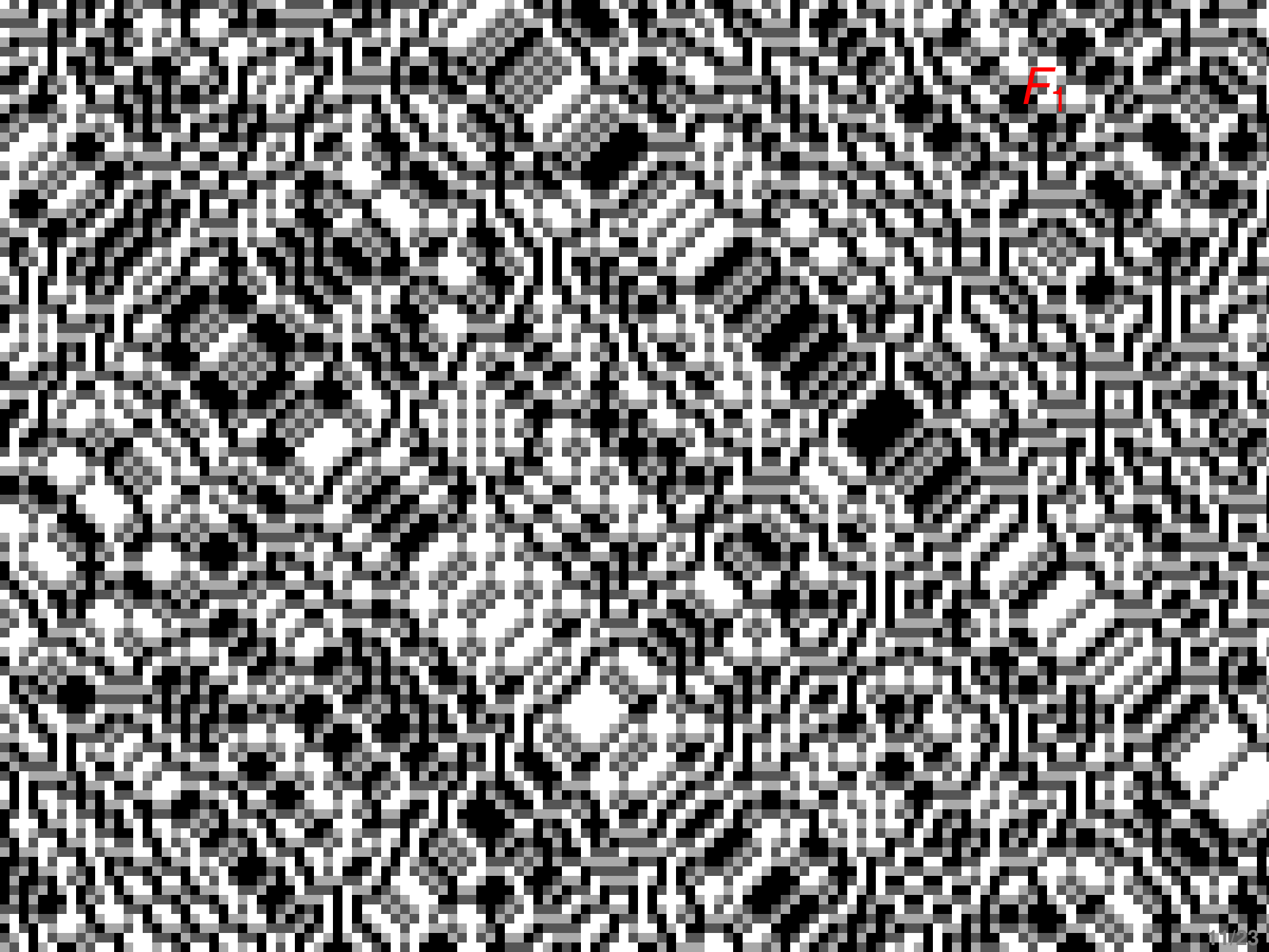
- XOR is strongly diffusive? **NO!** $F^{2^n}(c)_z = c_z \oplus c_{z+2^n}$

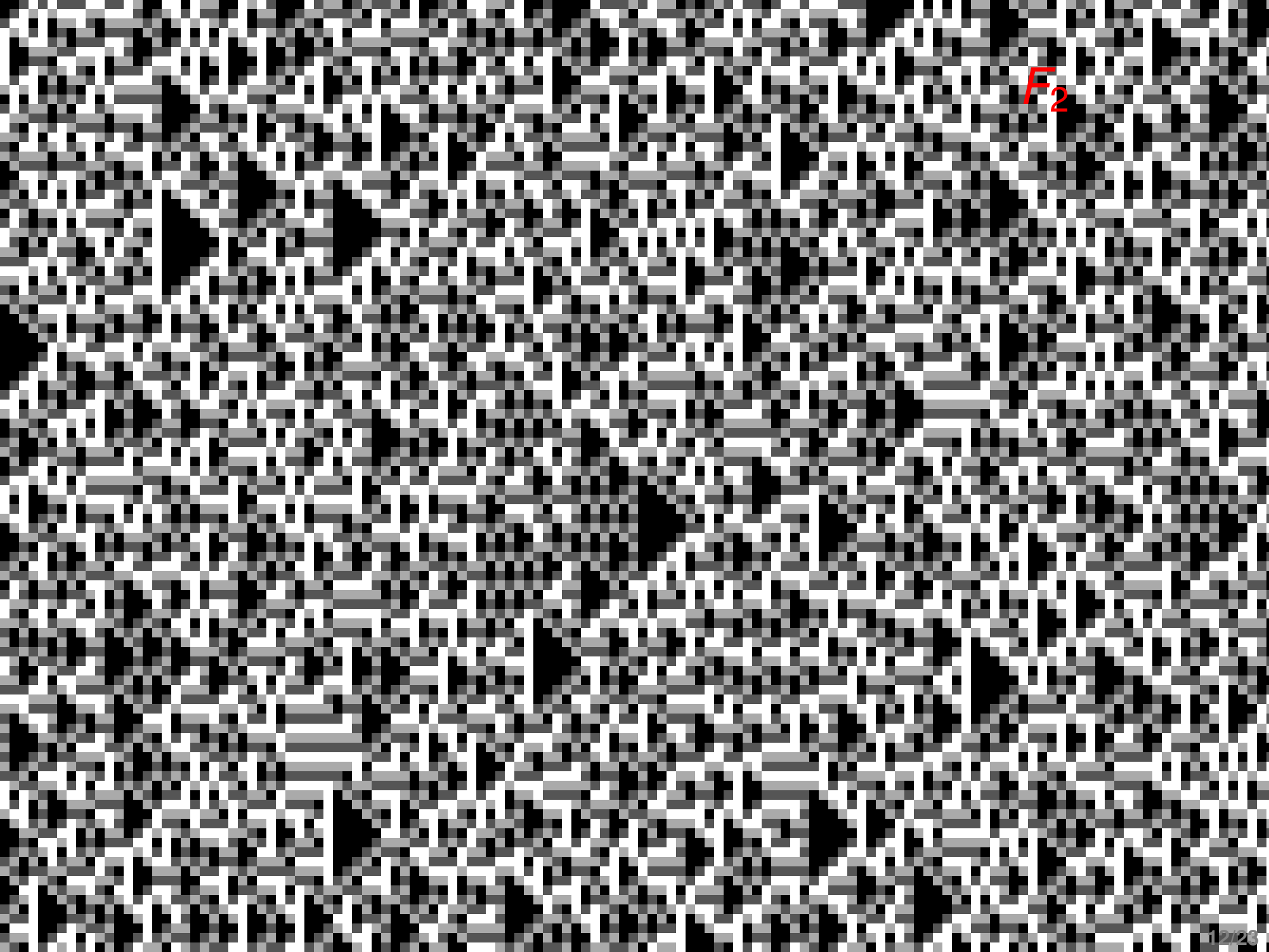
Abelian Examples

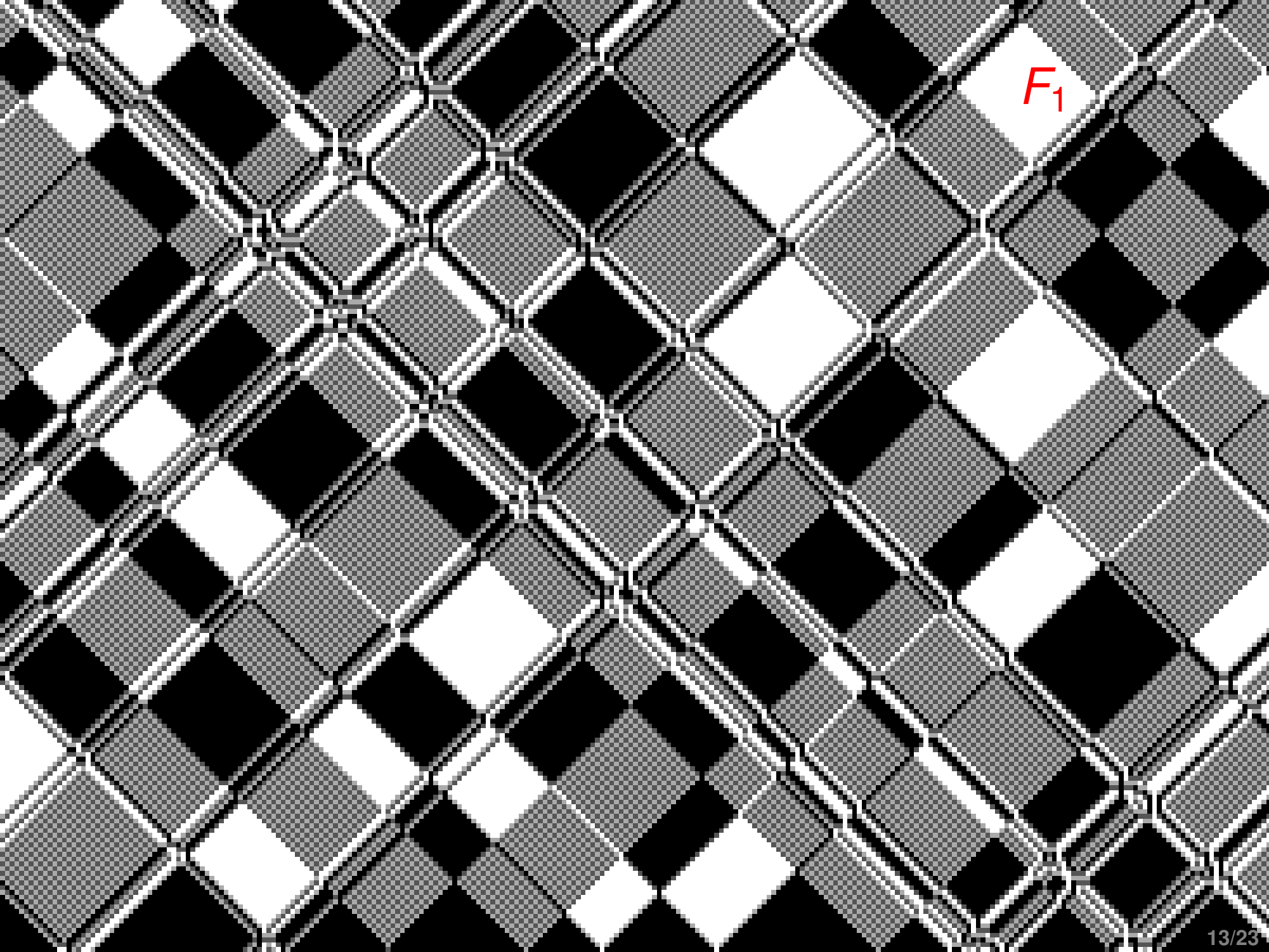
- enough to consider diamonds with $c \diamond d$ with $c = {}^{\omega}0^{\omega}$
- XOR has a glider? **NO!** $F^{2^n}(c)_z = c_z \oplus c_{z+2^n}$

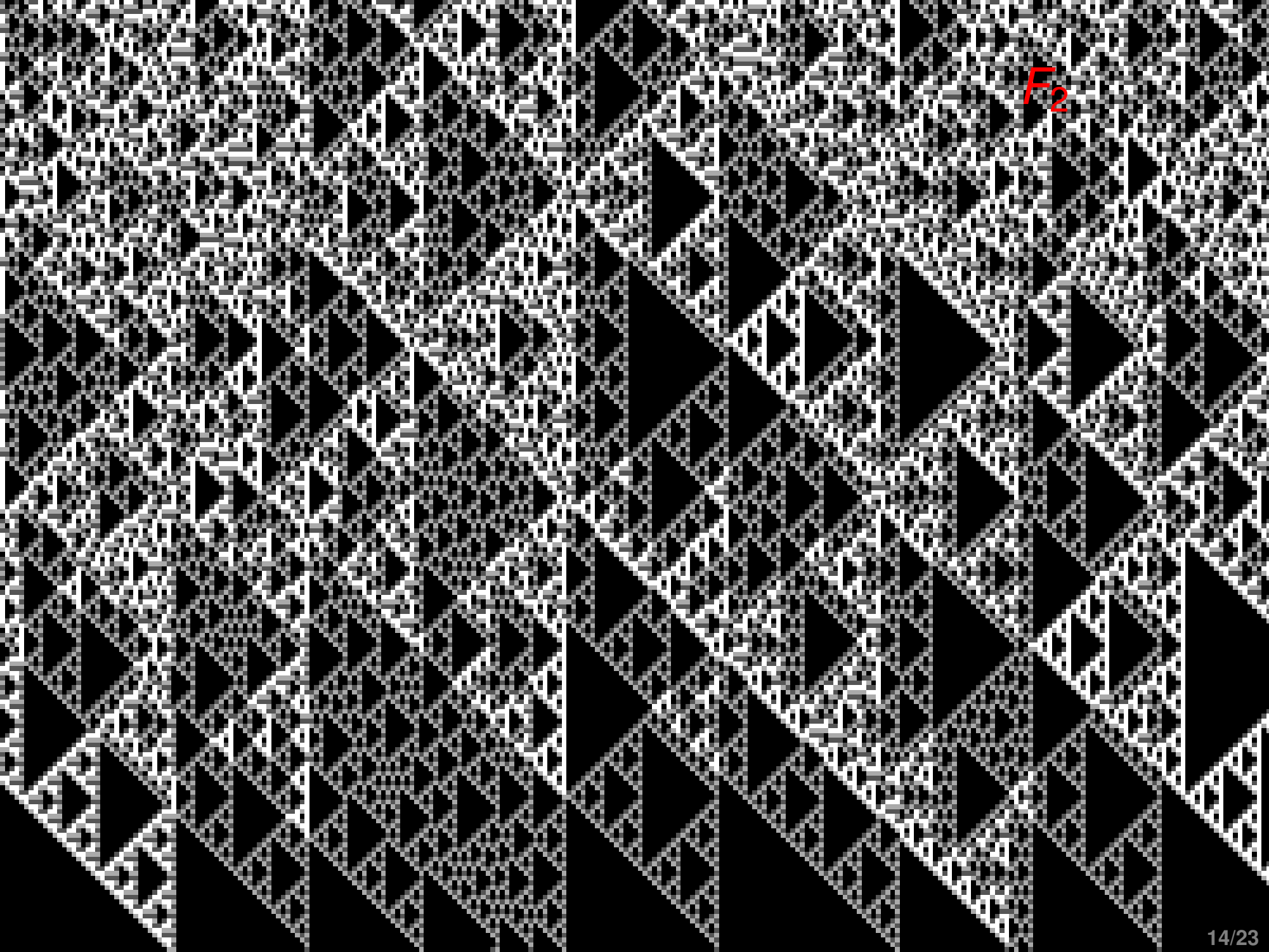


- XOR is strongly diffusive? **NO!** $F^{2^n}(c)_z = c_z \oplus c_{z+2^n}$
- examples with $(Q, \oplus) = \mathbb{Z}_2^2$
  1. $F_1(c)_z = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot c_{z-1} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot c_z + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot c_{z+1}$
  2. $F_2(c)_z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot c_z + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot c_{z+1}$


F_1


F_2


F_1


F_2

Main Theorem

Theorem

Let F be an Abelian CA, then the following are equivalent:

1. F has no glider
2. F is diffusive
3. F is randomizing for harmonically mixing measures
4. F is randomizing for NDB measures

Corollaries

For Abelian CA:

1. F and G randomizing $\Rightarrow$ $F \times G$ randomizing
2. F randomizing and reversible $\Rightarrow$ F^{-1} randomizing
3. F positively expansive $\Rightarrow$ F randomizing
4. F randomizing $\Rightarrow$ all its subautomata are randomizing
5. randomizing μ NDB $\Leftrightarrow$ randomizing μ harmonically mixing

Corollaries

For Abelian CA:

1. F and G randomizing $\Rightarrow$ $F \times G$ randomizing
2. F randomizing and reversible $\Rightarrow$ F^{-1} randomizing
3. F positively expansive $\Rightarrow$ F randomizing
4. F randomizing $\Rightarrow$ all its subautomata are randomizing
5. randomizing μ NDB $\Leftrightarrow$ randomizing μ harmonically mixing

Question

Are the above statements still true for non-Abelian CA?

Proof Sketch

1. no glider $\Leftrightarrow$ diffusivity

Proof Sketch

1. no glider $\Leftrightarrow$ diffusivity

2. harmonic analysis (inspired from Pivato-Yassawi)
   - characters: $\chi : Q^{\mathbb{Z}} \to \mathbb{C}$ continuous group morphism
   - Fourier coefficients: $\mu[\chi] = \int \chi d\mu$
   - $F\mu[\chi] = \mu[\chi \circ F]$
   - study $\chi \circ F^n$ to understand $F^n\mu$
   - harmonically mixing (HM) measures

Proof Sketch

1. no glider $\Leftrightarrow$ diffusivity

2. harmonic analysis (inspired from Pivato-Yassawi)
   - characters: $\chi : Q^{\mathbb{Z}} \to \mathbb{C}$ continuous group morphism
   - Fourier coefficients: $\mu[\chi] = \int \chi d\mu$
   - $F\mu[\chi] = \mu[\chi \circ F]$
   - study $\chi \circ F^n$ to understand $F^n\mu$
   - harmonically mixing (HM) measures

3. dual F^*: action of F on characters
   - F^* diffusive $\Leftrightarrow$ F randomizing
   - F^* has a glider $\Leftrightarrow$ F has a glider

Measures and Characters

- **character** of $Q^{\mathbb{Z}}$ = finite product of elementary characters

$$\chi(c) = \prod_z \chi_z(c_z) \text{ where } \chi_z : Q \to \mathbb{C} \text{ are almost all trivial}$$

- $\mathrm{dom}(\chi) = \{z : \chi_z \neq \overline{1}\}$, $\mathrm{rank}(\chi) = \#\,\mathrm{dom}(\chi)$

Measures and Characters

- **character** of $Q^{\mathbb{Z}}$ = finite product of elementary characters

$$\chi(c) = \prod_z \chi_z(c_z) \text{ where } \chi_z : Q \to \mathbb{C} \text{ are almost all trivial}$$

- $\mathrm{dom}(\chi) = \{z : \chi_z \neq \overline{1}\}$, $\mathrm{rank}(\chi) = \#\,\mathrm{dom}(\chi)$
- μ is **harmonically mixing** if

$$\mu[\chi] \to 0 \text{ when } \mathrm{rank}(\chi) \to \infty$$

Measures and Characters

- **character** of $Q^{\mathbb{Z}}$ = finite product of elementary characters

$$\chi(c) = \prod_z \chi_z(c_z) \text{ where } \chi_z : Q \to \mathbb{C} \text{ are almost all trivial}$$

- $\mathrm{dom}(\chi) = \{z : \chi_z \neq \overline{1}\}$, $\mathrm{rank}(\chi) = \#\,\mathrm{dom}(\chi)$
- μ is **harmonically mixing** if

$$\mu[\chi] \to 0 \text{ when } \mathrm{rank}(\chi) \to \infty$$

Theorem (Pivato-Yassawi 2002)

All NDB measures and all full support Markov measures are harmonically mixing.

Measures and Characters

- **character** of $Q^{\mathbb{Z}}$ = finite product of elementary characters

$$\chi(c) = \prod_z \chi_z(c_z) \text{ where } \chi_z : Q \to \mathbb{C} \text{ are almost all trivial}$$

- $\mathrm{dom}(\chi) = \{z : \chi_z \neq \overline{1}\}$, $\mathrm{rank}(\chi) = \#\,\mathrm{dom}(\chi)$
- μ is **harmonically mixing** if

$$\mu[\chi] \to 0 \text{ when } \mathrm{rank}(\chi) \to \infty$$

Theorem (Pivato-Yassawi 2002)

All NDB measures and all full support Markov measures are harmonically mixing.

- for μ HM, $\mathrm{rank}(\chi \circ F^n) \to \infty \Rightarrow F^n\mu[\chi] \to 0$

Duality

- group Q **isomorphic** to $\hat{Q}$ (group of characters $Q \to \mathbb{C}$)
- $q \in Q \mapsto \chi_q \in \hat{Q}$

Duality

- group Q **isomorphic** to $\hat{Q}$ (group of characters $Q \to \mathbb{C}$)
- $q \in Q \mapsto \chi_q \in \hat{Q}$
- characters of $Q^{\mathbb{Z}}$ seen as finite configurations of $Q^{\mathbb{Z}}$:

$$c \in Q^{\mathbb{Z}} \mapsto \phi(c) = \left(c' \mapsto \prod_z \chi_{c_z}(c'_z)\right)$$

Duality

- group Q **isomorphic** to $\hat{Q}$ (group of characters $Q \to \mathbb{C}$)
- $q \in Q \mapsto \chi_q \in \hat{Q}$
- characters of $Q^{\mathbb{Z}}$ seen as finite configurations of $Q^{\mathbb{Z}}$:

$$c \in Q^{\mathbb{Z}} \mapsto \phi(c) = \left(c' \mapsto \prod_z \chi_{c_z}(c'_z)\right)$$

Dual CA

$\hat{F} : Q^{\mathbb{Z}} \to Q^{\mathbb{Z}}$ such that $\phi(c) \circ F = \phi(\hat{F}(c))$ for any c finite.

Duality

- group Q **isomorphic** to $\hat{Q}$ (group of characters $Q \to \mathbb{C}$)
- $q \in Q \mapsto \chi_q \in \hat{Q}$
- characters of $Q^{\mathbb{Z}}$ seen as finite configurations of $Q^{\mathbb{Z}}$:

$$c \in Q^{\mathbb{Z}} \mapsto \phi(c) = \left(c' \mapsto \prod_z \chi_{c_z}(c'_z)\right)$$

Dual CA

$\hat{F} : Q^{\mathbb{Z}} \to Q^{\mathbb{Z}}$ such that $\phi(c) \circ F = \phi(\hat{F}(c))$ for any c finite.

- *e.g.* $Q = \mathbb{Z}_p^k$ and $F(c)_z = M_{-1} \cdot c_{z-1} + M_0 \cdot c_z + M_1 \cdot c_{z+1}$

Duality

- group Q **isomorphic** to $\hat{Q}$ (group of characters $Q \to \mathbb{C}$)
- $q \in Q \mapsto \chi_q \in \hat{Q}$
- characters of $Q^{\mathbb{Z}}$ seen as finite configurations of $Q^{\mathbb{Z}}$:

$$c \in Q^{\mathbb{Z}} \mapsto \phi(c) = \left(c' \mapsto \prod_z \chi_{c_z}(c'_z)\right)$$

Dual CA

$\hat{F} : Q^{\mathbb{Z}} \to Q^{\mathbb{Z}}$ such that $\phi(c) \circ F = \phi(\hat{F}(c))$ for any c finite.

- *e.g.* $Q = \mathbb{Z}_p^k$ and $F(c)_z = M_{-1} \cdot c_{z-1} + M_0 \cdot c_z + M_1 \cdot c_{z+1}$
- $\chi_q = q' \mapsto \lambda^{<q,q'>}$ ($\lambda^p = 1$, $\lambda \neq 1$)

Duality

- group Q **isomorphic** to $\hat{Q}$ (group of characters $Q \to \mathbb{C}$)
- $q \in Q \mapsto \chi_q \in \hat{Q}$
- characters of $Q^{\mathbb{Z}}$ seen as finite configurations of $Q^{\mathbb{Z}}$:

$$c \in Q^{\mathbb{Z}} \mapsto \phi(c) = \left(c' \mapsto \prod_z \chi_{c_z}(c'_z)\right)$$

Dual CA

$\hat{F} : Q^{\mathbb{Z}} \to Q^{\mathbb{Z}}$ such that $\phi(c) \circ F = \phi(\hat{F}(c))$ for any c finite.

- *e.g.* $Q = \mathbb{Z}_p^k$ and $F(c)_z = M_{-1} \cdot c_{z-1} + M_0 \cdot c_z + M_1 \cdot c_{z+1}$
- $\chi_q = q' \mapsto \lambda^{<q,q'>}$ ($\lambda^p = 1$, $\lambda \neq 1$)
- $\hat{F}(c)_z = M_1^T \cdot c_{z-1} + M_0^T \cdot c_z + M_{-1}^T \cdot c_{z+1}$

Proof Tool: Dependencies

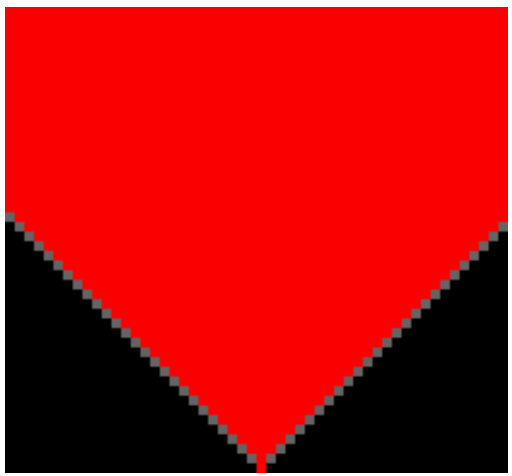
- δ_z^t: how cell z at time t depends on cell 0 at time 0

$$\delta_z^t : q \mapsto F^t({}^\omega 0 q 0^\omega)_z$$

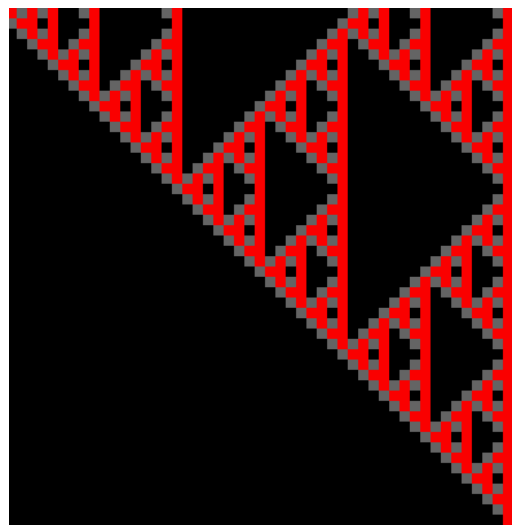
Proof Tool: Dependencies

- δ_z^t: how cell z at time t depends on cell 0 at time 0

$$\delta_z^t : q \mapsto F^t({}^\omega 0 q 0^\omega)_z$$



F_1

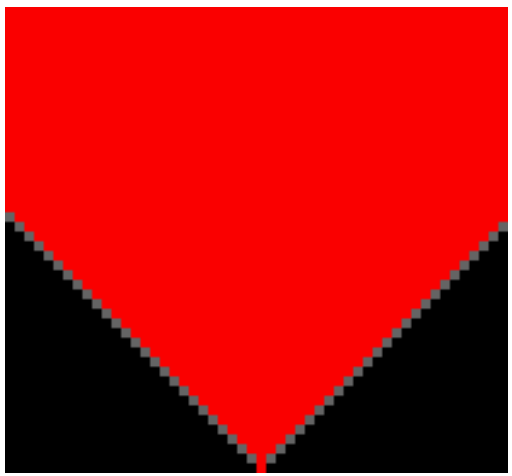


F_2

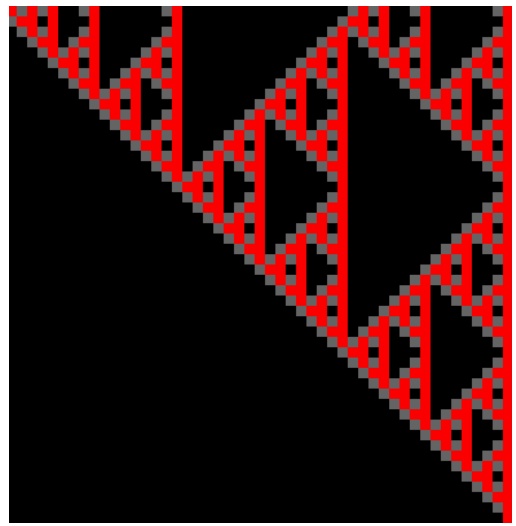
Proof Tool: Dependencies

- δ_z^t: how cell z at time t depends on cell 0 at time 0

$$\delta_z^t : q \mapsto F^t({}^\omega 0 q 0^\omega)_z$$



F_1



F_2

- k-isolated dependencies: δ_z^t **bijective** / $\delta_{z-1}^t, \ldots, \delta_{z-k}^t$ **null**

$$\Rightarrow F^t({}^\omega 0 u 0^\omega)_z \neq 0 \text{ when } |u| \leq k \text{ and } u_0 \neq 0$$

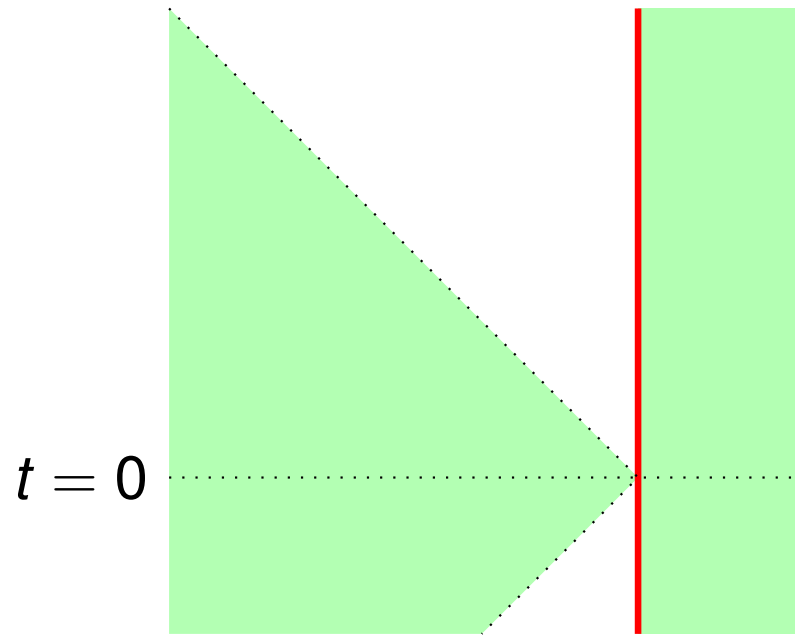
A strongly randomizing/diffusive CA

$$F_2(c)_z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot c_z + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot c_{z+1}$$

A strongly randomizing/diffusive CA

$$F_2(c)_z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot c_z + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot c_{z+1}$$

Known dependencies:

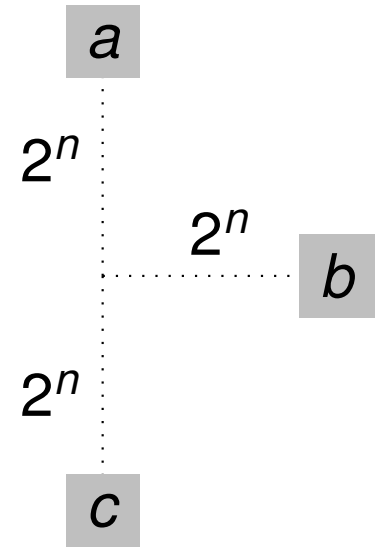


red $=$ bijective / green $=$ null

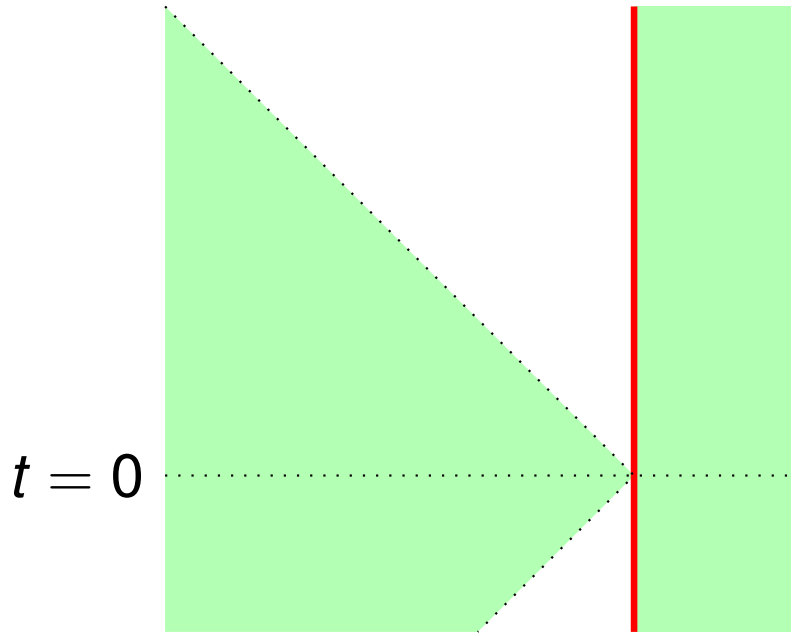
A strongly randomizing/diffusive CA

$$F_2(c)_z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot c_z + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot c_{z+1}$$

Known dependencies:



$a \oplus b \oplus c = 0$

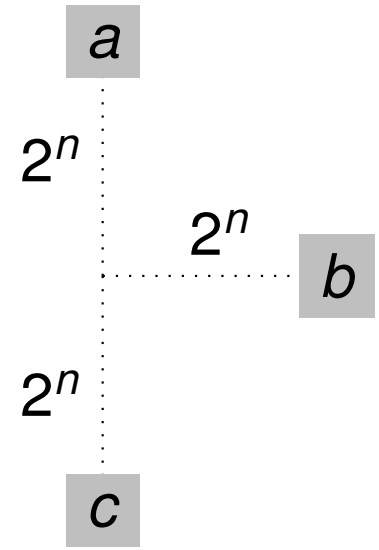


red = bijective / green = null

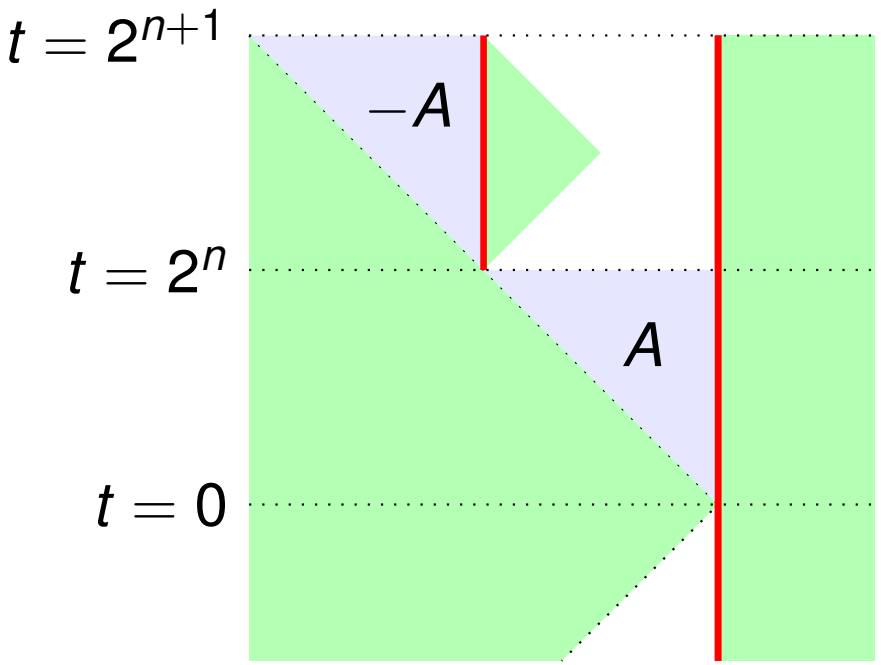
A strongly randomizing/diffusive CA

$$F_2(c)_z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot c_z + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot c_{z+1}$$

Known dependencies:



$$a \oplus b \oplus c = 0$$

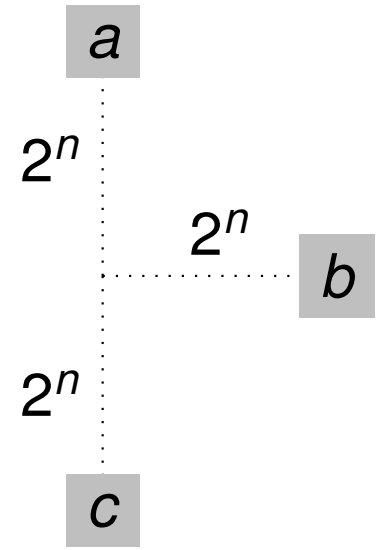


red = bijective / green = null

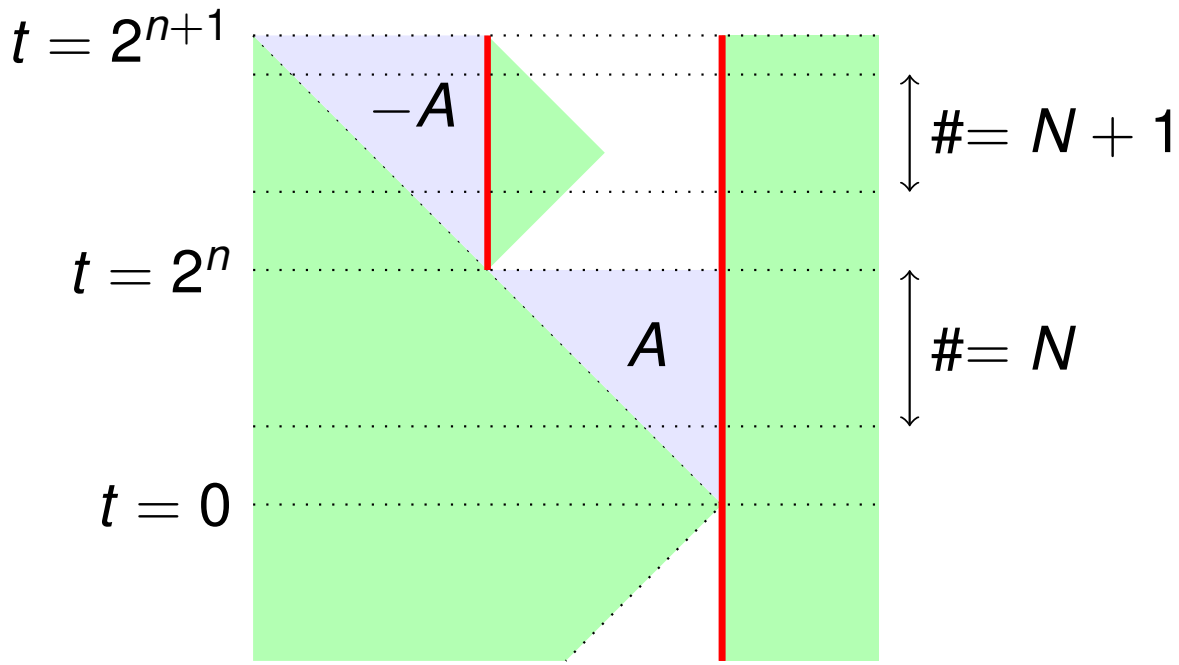
A strongly randomizing/diffusive CA

$$F_2(c)_z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot c_z + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot c_{z+1}$$

Known dependencies:



$$a \oplus b \oplus c = 0$$



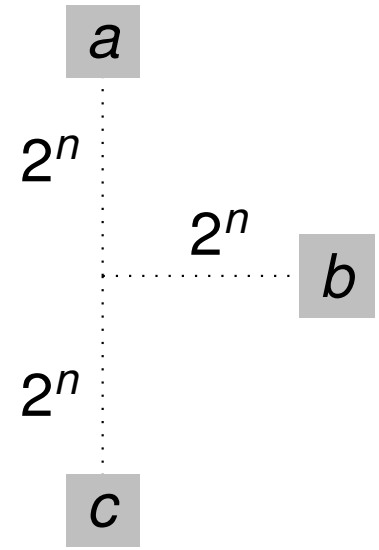
red = bijective / green = null

- *k*-separated dependencies

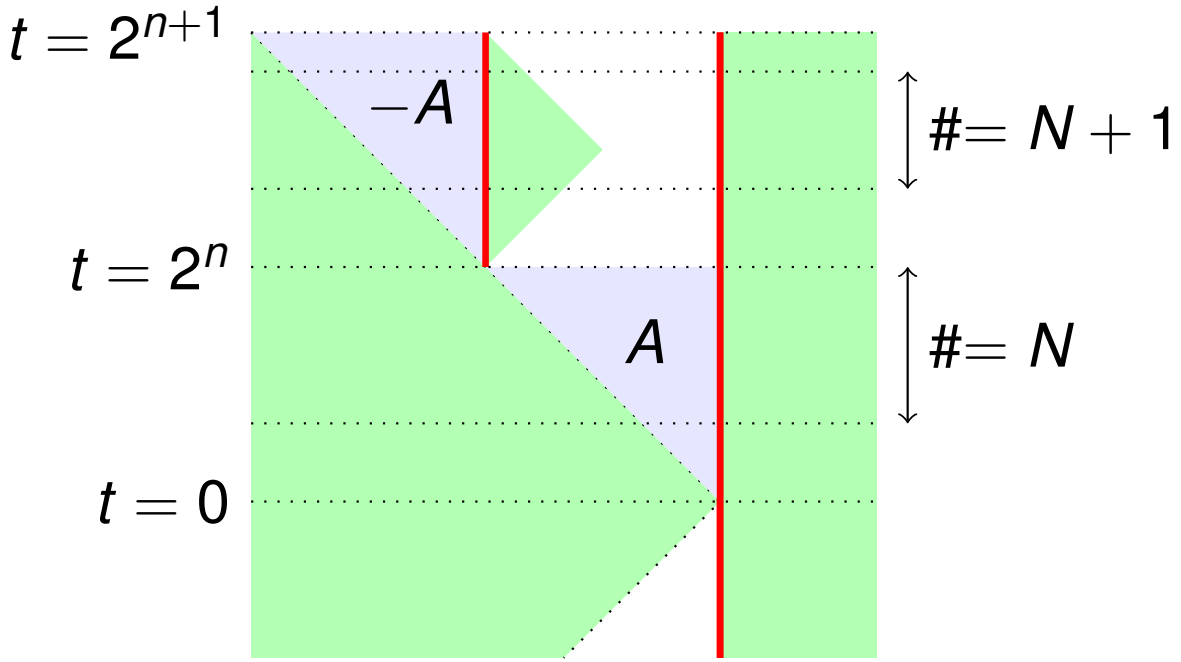
A strongly randomizing/diffusive CA

$$F_2(c)_z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot c_z + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot c_{z+1}$$

Known dependencies:



$$a \oplus b \oplus c = 0$$



red $=$ bijective / green $=$ null

- ***k*-separated dependencies** + reversibility!

“Super-Abelian” case

- Abelian $F(c)_z = \bigoplus_{i \in V} h_i(c_{z+i})$ with h_i commuting

- All previously cited results are in this case.

“Super-Abelian” case

- Abelian $F(c)_z = \bigoplus_{i \in V} h_i(c_{z+i})$ with h_i commuting
- All previously cited results are in this case.
- $Q = \mathbb{Z}_{p^l}^k$
- **lemma:** $F^{p^{n+l-1}}(c)_z = \left(\sum_{i \in V} h_i^{p^n}(c_{z+ip^n}) \right)^{p^{l-1}}$
- **corollary 1:** no strong randomization
- **corollary 2:** decision algorithm for randomization

Thank you!