Normality and preservation of measure in cellular automata

Silvio Capobianco[1]

[1]Institute of Cybernetics at TUT

Theory Days at Saka
October 25–26–27, 2013

Joint work with Pierre Guillon (CNRS & IML Marseille)
and Jarkko Kari (Mathematics Department, University of Turku)

Revision: October 27, 2013

Introduction

- Cellular automata (CA) are uniform, synchronous model of parallel computation, where the next state of a point is a function of the current state of a finite neighborhood of the point.
- In dimension d, it is easy to define a notion of normality for configurations akin to that for real numbers.
- On more general structures such as free groups, however, several complications arise.
- We introduce a definition of normality with additional parameters, which still ensures that almost all configurations are normal.
- We use this to measure the amount by which a surjective CA on a non-amenable group may fail to be balanced (Bartholdi, 2010).

Cellular automata

A cellular automaton (CA) on a group G is a triple $\mathcal{A} = \langle Q, \mathcal{N}, f \rangle$ where:

- Q is a finite set of states.
- $\mathcal{N} = \{n_1, \ldots, n_k\} \subseteq G$ is a finite neighborhood.
- $f : Q^k \to Q$ is a finitary local function

The local function induces a global function $F : Q^G \to Q^G$ via

$$\begin{aligned} F_{\mathcal{A}}(c)(x) &= f\left(c(x \cdot n_1), \ldots, c(x \cdot n_k)\right) \\ &= f\left(c^x|_{\mathcal{N}}\right) \end{aligned}$$

where $c^x(g) = c(x \cdot g)$ for all $g \in G$.

The same rule induces a function over patterns with finite support:

$$f(p) : E \to Q \ , \ f(p)(x) = f\left(p^x|_{\mathcal{N}}\right) \ \forall p : E\mathcal{N} \to Q$$

Prodiscrete topology and product measure

The prodiscrete topology of the space Q^G of configurations is generated by the cylinders

$$C(E,p) = \{c : G \to Q \mid c|_E = p\}$$

The cylinders also generate a σ-algebra Σ_C, on which the product measure induced by

$$\mu_\Pi(C(E,p)) = |Q|^{-|E|}$$

is well defined.

- Σ_C is **not** the Borel σ-algebra unless G is countable.

Balancedness

Let E be a finite nonempty subset of G; let $\mathcal{A} = \langle Q, \mathcal{N}, f \rangle$ be a CA on G.
$\mathcal{A}$ is E-balanced if for every $p : E \to Q$,

$$|f^{-1}(p)| = |Q|^{|E\mathcal{N}|-|E|}$$

This is the same as saying that $\mathcal{A}$ preserves μ_Π, *i.e.*,

$$\mu_\Pi \left(F_{\mathcal{A}}^{-1}(U) \right) = \mu_\Pi \left(U \right)$$

for every measurable open $U \subseteq Q^G$.

Theorem (Maruoka and Kimura, 1976)
A CA on $\mathbb{Z}^d$ is surjective if and only if it is balanced.

A counterexample on the free group

Ceccherini-Silbertstein, Machì and Scarabotti, 1999:

Let $G = \mathbb{F}_2$ be the free group on two generators a, b.
Let $Q = \{0, 1\}$, $\mathcal{N} = \{1, a, b, a^{-1}, b^{-1}\}$, and

$$f(\alpha) = \begin{cases} 1 & \text{if } \alpha_a + \alpha_b + \alpha_{a^{-1}} + \alpha_{b^{-1}} = 3\,, \\ 1 & \text{if } \alpha_a + \alpha_b + \alpha_{a^{-1}} + \alpha_{b^{-1}} \in \{1, 2\} \text{ and } \alpha_1 = 1\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

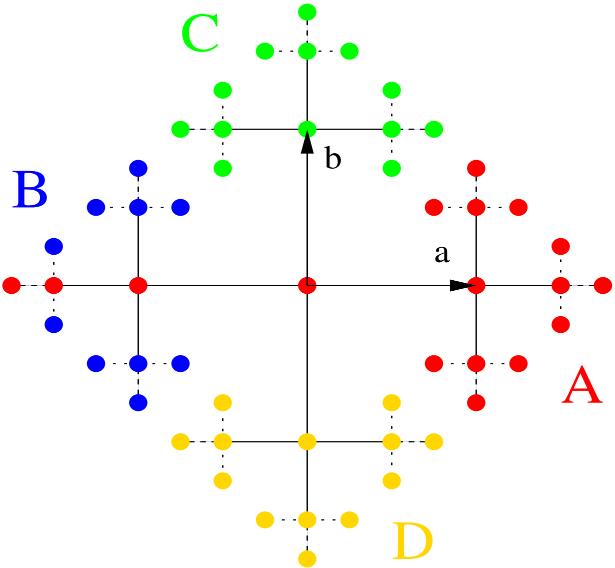
$\mathcal{A}$ is not balanced:

- There are 18 in 32 patterns $\alpha : \mathcal{N} \to \{1\}$ such that $f(\alpha) = 1$.

However, $\mathcal{A}$ is surjective:

- Let $E \in \mathcal{PF}(G)$ and let $m = \max\{\|g\| \mid g \in E\}$.
- Each $g \in E$ with $\|g\| = m$ has three neighbors outside E.
- This allows an argument by induction.

A paradoxical decomposition of $\mathbb{F}_2$



Paradoxical groups

A paradoxical decomposition of a group G is a partition $G = \bigsqcup_{i=1}^{n} A_i$ such that, for suitable $\alpha_1, \ldots, \alpha_n \in G$,

$$G = \bigsqcup_{i=1}^{k} \alpha_i A_i = \bigsqcup_{i=k+1}^{n} \alpha_i A_i$$

A bounded propagation 2:1 compressing map on G is a function $\phi : G \to G$ such that, for a finite propagation set S,

- $\phi(g)^{-1} g \in S$ for every $g \in G$ (bounded propagation) and
- $|\phi^{-1}(g)| = 2$ for every $g \in G$ (2:1 compression)

A group has a paradoxical decomposition if and only if it has a bounded propagation 2:1 compression map.
Such groups are called paradoxical.

A bounded propagation 2:1 compressing map for $\mathbb{F}_2$

Let us "invert" the paradoxical decomposition:

- $H = \{g \in G \mid w_m = a^{-1}\} \cup \{a^n \mid n \geq 0\} = A^{-1}$
- $I = \{g \in G \mid w_m = a\} \setminus \{a^n \mid n \geq 0\} = B^{-1}$
- $J = \{g \in G \mid w_m = b^{-1}\} = C^{-1}$
- $K = \{g \in G \mid w_m = b\} = D^{-1}$

so that $\mathbb{F}_2 = H \sqcup I \sqcup J \sqcup K = H \sqcup Ia^{-1} = J \sqcup Kb^{-1}$. Put:

- $\phi(g) = g$ if $g \in H$
- $\phi(ga) = g$ if $g \in Ia^{-1}$
- $\phi(g) = g$ if $g \in J$
- $\phi(gb) = g$ if $g \in Kb^{-1}$

Then ϕ is a bounded-propagation 2:1 compressing map with $S = \{1, a, b\}$.

Amenable groups

A group G is amenable if there exists a finitely additive probability measure $\mu : \mathcal{P}(G) \to [0, 1]$ such that:

$$\mu(gA) = \mu(A) \text{ for every } g \in G, A \subseteq G$$

- Subgroups of amenable groups are amenable.
- Quotients of amenable groups are amenable.
- Abelian groups are amenable.

The Tarski alternative

Let G be a group. **Exactly one of the following happens.**

1. G is amenable.
2. G is paradoxical.

Bartholdi's theorem (2010)

Let G be a group. The following are equivalent.

1. G is amenable.
2. Every surjective cellular automaton on G is balanced.

Question:

How much does preservation of product measure fail on paradoxical groups?

A strategy for an answer:

find a CA $\mathcal{A}$ and a measurable set U such that
the difference between $\mu_\Pi(U)$ and $\mu_\Pi(F_{\mathcal{A}}^{-1}(U))$ is "large"

SC, P. Guillon, J. Kari. Surjective cellular automata far from the Garden of Eden. *Disc. Math. Theor. Comp. Sci.* **15:3** (2013), 41–60.
`www.dmtcs.org/dmtcs-ojs/index.php/dmtcs/article/view/2336`

A surjective, non-balanced CA

Guillon, 2011: improves Bartholdi's counterexample.

Let G be a non-amenable group, ϕ a bounded propagation 2:1 compressing map with propagation set S.
Define on S a total ordering $\preceq$.
Define a CA $\mathcal{A}$ on G by $Q = (S \times \{0,1\} \times S) \sqcup \{q_0\}$, $\mathcal{N} = S$, and

$$f(u) = \begin{cases} q_0 & \text{if } \exists s \in S \mid u_s = q_0, \\ (p, \alpha, q) & \text{if } \exists!(s,t) \in S \times S \mid s \prec t, u_s = (s, \alpha, p), u_t = (t, 1, q), \\ q_0 & \text{otherwise.} \end{cases}$$

Then $\mathcal{A}$, although clearly non-balanced, is surjective.

- For $j \in G$ it is $j = \phi(js) = \phi(jt)$ for exactly two $s, t \in S$ with $s \prec t$.
- If $c(j) = q_0$ put $e(js) = e(jt) = (s, 0, s)$.
- If $c(j) = (p, \alpha, q)$ put $e(js) = (s, \alpha, p)$ and $e(jt) = (t, 1, q)$.
- Then $F(e) = c$.

The Guillon CA on $\mathbb{F}_2$

Consider the bounded propagation 2:1 compressing map ϕ on $\mathbb{F}_2$.

- $S = \{1, a, b\} = \mathcal{N}$: we sort $1 \prec a \prec b$.
- $Q = S \times \{0, 1\} \times S \sqcup \{q_0\}$ has 19 elements.
- ϕ has $19^3 = 6859$ entries, but only few yield a non-q_0 value:
  - $\phi\left((1, 0, 1), (a, 1, 1), (1, 0, 1)\right) = (1, 0, 1)$
  - $\phi\left((1, 1, 1), (a, 1, 1), (1, 0, 1)\right) = (1, 1, 1)$
  - $\phi\left((1, 0, a), (a, 1, 1), (1, 0, 1)\right) = (a, 0, 1)$
  - ...

  but $\phi\left((1, 0, a), (a, 1, 1), (b, 1, 1)\right) = q_0$.

What is normality?

Consider the definition for real numbers:

- A real number $x \in [0,1)$ is normal in base b if the sequence of its digits in base b is equidistributed.
- x is normal if it is normal in every base b

A similar definition holds for sequences $w \in Q^{\mathbb{N}}$:

- Let $\mathrm{occ}(u,w) = \{i \geq 0 \mid w_{[i:i+|u|-1]} = u\}$.
- w is m-normal if for every $u \in Q^m$,

$$\lim_{n\to\infty} \frac{|\mathrm{occ}(u,w) \cap \{0,\ldots,n-1\}|}{n} = |Q|^{-m}$$

- w is normal if it is m-normal for every $m \geq 1$.

Theorem (Niven and Zuckerman, 1951)
x is m-normal in base b iff it is 1-normal in base b^m.

- Similarly, w is m-normal over Q iff it is 1-normal over Q^m.

How common is normality?

Theorem (cf. Hardy and Wright)
The set of normal $x \in [0, 1)$ has Lebesgue measure 1.

Theorem
The set of normal words over Q has product measure 1.

The proof is based on the Chernoff bound:

- Let $Y_0, \ldots, Y_{n-1}$ be independent nonnegative random variables.
- Let $S_n = Y_0 + \ldots + Y_{n-1}$, $\mu = \mu(n) = \mathbb{E}(S_n)$.
- For every $\delta \in (0, 1)$,

$$\mathbb{P}\left(S_n < \mu \cdot (1 - \delta)\right) < e^{-\frac{\mu\delta^2}{2}}$$

Normality for d-dimensional configurations

It is still sensible to define normality for $c \in \mathbb{Z}^d$ as follows:

- Let $E = E(n_1, \ldots, n_d) = \prod_{i=1}^{d} \{0, \ldots, n_i - 1\}$.
- $c : \mathbb{Z}^d \to Q$ is E-normal if for every $p : E \to Q$,

$$\lim_{n \to \infty} \frac{1}{(2n+1)^d} \cdot |\{x \in \mathbb{Z}^d \mid \|x\| \leq n \,,\, c^x|_E = p\}| = \frac{1}{|Q|^{|E|}}$$

- It is still true that the set U of normal configurations has $\mu_\Pi(U) = 1$.
- And it is still true that c is $E(k_1 n_1, \ldots, k_d n_d)$-normal on Q if and only if it is $E(n_1, \ldots, n_d)$-normal in $Q^{E(k_1, \ldots, k_d)}$.

So the set U of normal configurations seems a good candidate . . .

What seems easy . . . usually only seems so

But: **why** is this sensible?

- Every E such as above is a coset for some subgroup of $\mathbb{Z}^d$.
- Also, a subgroup of finite index of $\mathbb{Z}^d$ is isomorphic to $\mathbb{Z}^d$.

This is **not** true for arbitrary groups!

- If G is free on two generators, and $H \leq G$ has index 2, then H is free on three generators!

So, if we define E-normality as in the previous slide, but on arbitrary groups:

- either we need to change the underlying group —which spoils the Niven-Zuckerman property,
- or we risk getting overlapping blocks —which voids use of Chernoff bound!

The solution: (Kari, 2012)

only patch a portion of the group!

Normal configurations, modulo some conditions

Let G be an arbitrary infinite group.

- Let $E \in \mathcal{PF}(G)$ be nonempty.
- Let $h : \mathbb{N} \to G$ be injective.

We define the lower density, upper density, and density of $U \subseteq G$ according to h, as the lower limit $\mathrm{dens\,inf}_h$, upper limit $\mathrm{dens\,sup}_h$, and (if exists) limit dens_h of

$$\frac{|U \cap \{h(0), \ldots, h(n-1)\}|}{n}$$

We say $c : G \to Q$ is h-E-normal if for every pattern $p : E \to Q$,

$$\mathrm{dens}_h \, \mathrm{occ}(p, c) = |Q|^{-|E|}$$

where $\mathrm{occ}(p, c) = \{g \in G \mid c^g|_E = p\}$.

Sanity check

If $E \subseteq F$ and c is h-F-normal, then it is also h-E-normal.

- The vice versa is false: for $h(n) = n$, $\ldots 010101 \ldots$ is h-$\{0\}$-normal and h-$\{1\}$-normal but not h-$\{0,1\}$-normal.

Also, the following are equivalent:

1. c is h-E-normal.
2. For every $p : E \to Q$, $\mathrm{dens\,inf}_h\, \mathrm{occ}(p, c) \geq |Q|^{-|E|}$.
3. For every $p : E \to Q$, $\mathrm{dens\,sup}_h\, \mathrm{occ}(p, c) \leq |Q|^{-|E|}$.

A key lemma

Let $\mathcal{A} = \langle Q, \mathcal{N}, f \rangle$ be a nontrivial CA on G. Suppose that:

- $\mathcal{A}$ has a spreading state q_0,
  i.e., if $\alpha(x) = q_0$ for some $x \in \mathcal{N}$, then $f(\alpha) = q_0$;
- s, t are two distinct elements of $\mathcal{N}$; and
- $h : \mathbb{N} \to G$ is injective.

If $c : G \to Q$ is h-$\{s, t\}$-normal, then $F_{\mathcal{A}}(c)$ is not h-1-normal.

- There are $2|Q| - 1$ patterns $p : \{s, t\} \to Q$ with $p(s) = q_0$ or $p(t) = q_0$ (or both): each of these has density $1/|Q|^2$.
- Thus, $\mathrm{dens}_h(q_0, F_{\mathcal{A}}(c)) \geq (2|Q| - 1)/|Q|^2 > 1/|Q|$.

In particular, if c is h-E-normal for some $E \in \mathcal{PF}(G)$ containing $\mathcal{N}$, then $F_{\mathcal{A}}(c)$ is not h-1-normal.

The set of non-normal configurations

For $p : E \to Q$, $k \geq 1$, and $h : \mathbb{N} \to G$ injective, let

$$L_{h,p,k,n} = \left\{ c : G \to Q \;\middle|\; \frac{|\{i < n \mid h(i) \in \mathrm{occ}(p,c)\}|}{n} \leq \frac{1}{|Q|^{|E|}} - \frac{1}{k} \right\} .$$

$\mathrm{dens\,inf}_h \, \mathrm{occ}(p,c) < |Q|^{-|E|}$ if and only if there exists $k \geq 1$ such that

$$c \in \limsup_n L_{h,p,k,n} = \bigcap_{n \geq 1} \bigcup_{m \geq n} L_{h,p,k,m} \stackrel{\mathrm{def}}{=} L_{h,p,k}$$

which is Σ_C-measurable. Then

$$L_{h,E} = \bigcup_{p \in Q^E, k \geq 1} L_{h,p,k}$$

is the set of all the configurations $c \in Q^G$ that are not h-E-normal.

When is it the case that $\mu_\Pi(L_{h,E}) = 0$?

A full set of normal configurations

Suppose that the sets $h(i)E$, $i \geq 0$, are pairwise disjoint.

- The random variables

$$Y_i = \left[c^{h(i)} \Big|_E = p \right]$$

  are i.i.d. Bernoulli of parameter $t = |Q|^{-|E|}$.

- Set $S_n = Y_0 + \ldots + Y_{n-1}$. Then for $\delta = |Q|^{|E|}/k$,

$$L_{h,p,k,n} = \{c : G \to Q \mid S_n < n \cdot |Q|^{-|E|} \cdot (1 - |Q|^{|E|}/k)\}$$

  and the Chernoff bound yields

$$\mu_\Pi(L_{h,p,k,n}) = \mathbb{P}\left(\{S_n < \mu \cdot (1 - \delta)\}\right) < e^{-\frac{|Q|^{|E|}}{2k^2} n}$$

- By the Borel-Cantelli lemma, all the $L_{h,p,k}$ are null sets.

If it fails, it fails catastrophically

Let G be a non-amenable group.

- Let $\mathcal{A} = \langle Q, \mathcal{N}, f \rangle$ be the Guillon CA.
- Let $E \supseteq \mathcal{N} \cup \{1\}$.
- Let $h : \mathbb{N} \to G$ s.t. the $h(i)E$, $i \geq 0$, are pairwise disjoint.
- Then μ_Π-almost every $c \in Q^G$ is h-E- and h-1-normal …
- … but the Guillon CA has a spreading state …
- … so none of their preimages can be h-E-normal!

Hence, the set U of h-E-normal configurations satisfies

$$\mu_\Pi(U) = 1 \text{ and } \mu_\Pi\left(F_{\mathcal{A}}^{-1}(U)\right) = 0$$

Conclusions and future work

- We provide a notion of “relativized normality” which mimics the usual notion of normality for infinite words.
- This notion allows to prove a very remarkable result in cellular automata theory.
- Are there injective CA which are not balanced?
(If no such CA exists, then Gottschalk’s conjecture is true.)

Thank you for attention!

Any questions?