Normality, randomness, and the Garden of Eden

Silvio Capobianco

Institute of Cybernetics at TUT

Institute of Cybernetics at TUT
October 15, 2013

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

Revision: November 17, 2013

Introduction

- Cellular automata (CA) are uniform, synchronous model of parallel computation on uniform grids, where the next state of a point is a function of the current state of a finite neighborhood of the point.
- The Garden-of-Eden theorem provides a necessary condition for the global function of a CA in dimension d to be surjective.
- Also, surjective d-dimensional CA are balanced—every pattern of a given shape has the same number of pre-images.
- Notably, on more complex grids such implications are not respected.
- Bartholdi's theorem characterizes amenable groups (a class introduced by von Neumann) as those where all surjective CA are balanced.
- We measure the amount by which a surjective CA on a non-amenable group may fail to be balanced.

The Banach-Tarski paradox (1924)

A closed ball U in the 3-dimensional Euclidean space
can be decomposed into two disjoint subsets X, Y,
both piecewise congruent to U.

This is due to a series of facts:

- The axiom of choice.
- The group of rotations of the 3-dimensional space has a free subgroup on two generators.
- The pieces of the decomposition are not Lebesgue measurable.

What is the role of the group?

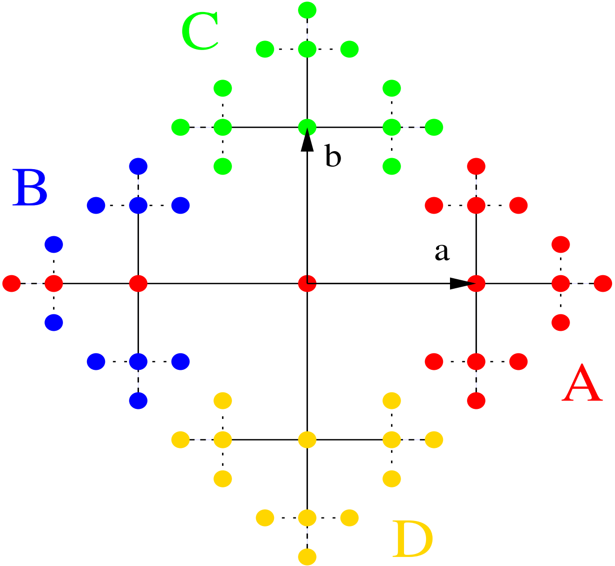
Amenable groups

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.
- A group whose finitely generated subgroups are all amenable, is amenable.

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.

Examples of paradoxical groups

- The free group on two generators is paradoxical.
- Every group with a paradoxical subgroup is paradoxical.
- In particular, every group with a free subgroup on two generators is paradoxical.
- The converse of the previous point is false!
  (von Neumann's conjecture; disproved by Ol'shanskii, 1980)
- In fact, there exist paradoxical groups where every element has finite order. (Adian, 1983)

The Tarski alternative

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

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

Are there other ways to express that?

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:

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

The Garden-of-Eden theorem

A cellular automaton is pre-injective if it satisfies the following condition:

$$\text{if } 0 < |\{g \in G \mid c(g) \neq e(g)\}| < \infty$$
$$\text{then } F_{\mathcal{A}}(c) \neq F_{\mathcal{A}}(e)$$

Theorem (Moore's Garden-of-Eden theorem, 1962)
A surjective cellular automaton on $G = \mathbb{Z}^d$ is pre-injective.

Theorem (Myhill, 1963)
A pre-injective cellular automaton on $G = \mathbb{Z}^d$ is surjective.

A counterexample on the free group

Let $G = \mathbb{F}_2$, $Q = \{0, 1\}$, $\mathcal{N} = \{1_G, a, b, a^{-1}, b^{-1}\}$, and f the majority rule.

$\mathcal{A}$ is not pre-injective.

- The configuration which has value 1 only on 1_G is updated into the all-0 configuration.

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.

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.*,

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

for every open $U \in \Sigma_C$.

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

Martin-Löf randomness for infinite words

A sequential Martin-Löf test (briefly, M-L test) is a recursively enumerable $U \subseteq \mathbb{N} \times Q^*$ such that the level sets $U_n = \{x \in Q^* \mid (n, x) \in U\}$ satisfy the following conditions:

1. For every $n \geq 1$, $U_{n+1} \subseteq U_n$.
2. For every $n \geq 1$ and $m \geq n$, $|U_n \cap Q^m| \leq |Q|^{m-n}/(|Q|-1)$.
3. For every $n \geq 1$ and $x, y \in Q^*$, if $x \in U_n$ and $y \in xQ^*$ then $y \in U_n$.

$w \in Q^{\mathcal{N}}$ fails a sequential M-L test U if $w \in \bigcap_{n \geq 0} U_n Q^{\mathbb{N}}$.

w is Martin-Löf random if w does not fail any sequential M-L test.

- If $\eta : \mathbb{N} \to \mathbb{N}$ is a computable bijection, then w is M-L random if and only if $w \circ \eta$ is M-L random.
- It is well known (cf. [Martin-Löf, 1966]) that M-L random words are normal.

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 $u \in Q^m$,

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

Theorem (Niven and Zuckerman, 1951)
w is m-normal over Q iff it is 1-normal over Q^m.

Enumerating the cylinders

Suppose G is finitely generated and has decidable word problem.

- Then there is a computable bijection $\phi : \mathbb{N} \to G$.
- Also, there is a computable function $m : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that, for all i and j, if $\phi(i) = g$ and $\phi(j) = h$, then $\phi(m(i,j)) = g \cdot h$.

Then we can enumerate the cylinders as follows:

- First, we enumerate the elementary cylinders:

$$B_{|Q|i+j} = C(g_i, q_j) = \{c : G \to Q \mid c(\phi(i)) = q_j\}$$

- Next, we define a bijection $\Psi : \mathcal{PF}(G) \to \mathbb{N}$ as $\Psi(X) = \sum_{i \in X} 2^i$ (so that $\Psi(\emptyset) = 0$)
- Finally, we enumerate the cylinders as:

$$B'_n = \bigcap_{i \in \Psi^{-1}(n+1)} B_i$$

Martin-Löf randomness for configurations

Let G be a f.g. group with decidable word problem.

- We say that $\mathcal{U}$ is $\mathcal{V}$-computable if there exists a r.e. $A \subseteq \mathbb{N}$ such that

$$U_i = \bigcup_{\pi(i,j)\in A} V_j \;\; \forall i \geq 0$$

  where $\pi(i,j) = (i+j)(i+j+1)/2 + j$.
- A B'-computable family $\mathcal{U} = \{U_n\}_{n\geq 0}$ of open subsets of Q^G is a Martin-Löf μ_Π-test if $\mu_\Pi(U_n) \leq 2^{-n}$ for every $n \geq 0$.
  $c \in Q^G$ fails $\mathcal{U}$ if $c \in \bigcap_{n\geq 0} U_n$.
- c is M-L μ_Π-random if it does not fail any M-L μ_Π-test.

Two important facts about Martin-Löf randomness

Theorem (Hertling and Weihrauch)
Let $\phi : \mathbb{N} \to G$ an admissible indexing.
$c \in Q^G$ is M-L μ_Π-random if and only if $c \circ \phi \in Q^{\mathbb{N}}$ is M-L random.

Theorem (Calude *et al.*, 2001)
Let $\mathcal{A} = \langle Q, \mathcal{N}, f \rangle$ be a CA on $\mathbb{Z}^d$. The following are equivalent:

1. $\mathcal{A}$ is surjective.
2. For every $c : \mathbb{Z}^d \to Q$, if c is M-L μ_Π random then so is $F_\mathcal{A}(c)$.

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 pre-injective.
3. Every surjective cellular automaton on G preserves the product measure.

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

The amount of a failure

Theorem (Capobianco, Guillon and Kari)
Let G be a non-amenable group.
There exist an alphabet Q, a subset U of Q^G such that

$$\mu_\Pi(U) = 1\,,$$

and a surjective cellular automaton $\mathcal{A}$ over G with alphabet Q such that

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

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 $F(e) = c$.

End of the game?

At this point, one might be tempted to reason as such:

- Let G be a non-amenable group with decidable word problem.
- Let c be a Martin-Löf random configuration for Guillon's CA.
- There exist some points $g \in G$ where $c(g) = q_0$.
- As $|S| \geq 2$, $F_{\mathcal{A}}(c)$ cannot have isolated q_0's.
- Therefore, $F_{\mathcal{A}}(c)$ cannot be random.

This argument, albeit convincing, is **wrong**.

- To say that $F_{\mathcal{A}}(c)$ has no isolated occurrences of q_0, means that there are some patterns that do not occur in $F_{\mathcal{A}}(c)$.
- But c, being random, is also rich ...
- ... and a rich configuration contains all the preimages of every non-orphan pattern!

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 $p : E \to Q$,

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

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, what is to be done?

The idea:

- Patch the group with patches of a given shape.
- See the state of patches as macrostates.
- Show that μ_Π-almost every configuration is normal with respect to the macrostates.

The problem:

- If we want to fill the group without having the patches overlap, we may be forced to change the underlying group.

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 $\operatorname{dens\,inf}_h$, upper limit $\operatorname{dens\,sup}_h$, and (if exist) limit dens_h of

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

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

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

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

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 $\mathcal{A}$ has a spreading state q_0.
- Let s, t be two distinct elements of $\mathcal{N}$.
- Let $h : \mathbb{N} \to G$ be injective.

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

- 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 $\mu_\Pi(L_{h,E}) = 0$?

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 $\delta \in (0,1)$,

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

In particular, if the Y_i's are Bernoulli trials with probability p, and $0 < \varepsilon < \min(p, 1-p)$, then for $\delta = \varepsilon / p$

$$\sum_{0 \leq k < n \cdot (p-\varepsilon)} \binom{n}{k} p^k (1-p)^{n-k} < e^{-\frac{\varepsilon^2 n}{2p}} .$$

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

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

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

In conclusion: μ_Π-almost every $c : G \to Q$ is h-E-normal

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 ...
- ...so none of their preimages can be h-E-normal!

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

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

Back to randomness

Let G be an amenable group and let $\mathcal{A} = \langle Q, \mathcal{N}, f \rangle$ be a CA on G.

- If $\mathcal{U}$ is B'-measurable then so is $F_{\mathcal{A}}^{-1}(\mathcal{U})$.
- If $\mathcal{A}$ is surjective and $\mathcal{U}$ is a M-L μ_Π-test, then so is $F_{\mathcal{A}}^{-1}(\mathcal{U})$.
- In these hypotheses, if $F_{\mathcal{A}}(c)$ fails $\mathcal{U}$, then c fails $F_{\mathcal{A}}^{-1}(\mathcal{U})$.

Summarizing:

if G is amenable, $\mathcal{A}$ is surjective, and c is M-L μ_Π-random, then $F_{\mathcal{A}}(c)$ is M-L μ_Π-random

Fixing a flaw

$a \in Q^{\mathbb{N}}$ is M-L random relatively to $b \in Q^{\mathbb{N}}$ if it is M-L random when computability is considered according to Turing machines with oracle b.

Theorem (van Lambalgen, 1987)
Let $a, b \in Q^{\mathbb{N}}$ and

$$c(n) = \begin{cases} a(k) & \text{if } n = 2k\,, \\ b(k) & \text{if } n = 2k+1\,. \end{cases}$$

The following are equivalent:

1. c is M-L random.
2. a is M-L random, and b is M-L random relatively to a.
3. b is M-L random, and a is M-L random relatively to b.

Another catastrophic failure!

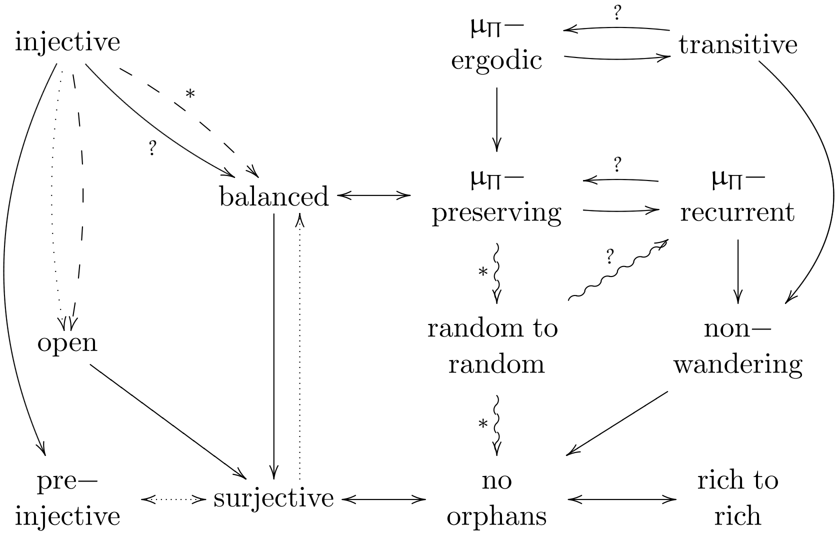
Let G be an infinite f.g. group with decidable word problem.
For every nonempty $E \in \mathcal{PF}(G)$ there exists a computable injective function $h : \mathbb{N} \to G$ such that:

1. $h(\mathbb{N})$ is a recursive subset of G with infinite complement.
2. $h(n)E \cap h(m)E = \emptyset$ for every $n \neq m$.
3. For any alphabet Q, every M-L μ_Π-random configuration $c : G \to Q$ is h-E-normal. (This follows from van Lambalgen's theorem.)

Let then $\mathcal{A}$ be the Guillon CA.

- Construct h as above with $E = \mathcal{N} \cup \{1\}$.
- Let $c : G \to Q$ be a M-L μ_Π-random configuration.
- Because of the above lemma, $F_{\mathcal{A}}(c)$ cannot be random.
- For the same reason, none of the preimages of c can be random.

A diagram of implications



Conclusions and future work

- The characterizations of surjective CA listed in [Calude et al., 2001] actually hold on arbitrary amenable groups—and precisely on those.
- Among those, preservation of the product measure is the one that fails catastrophically on paradoxical groups.
- Does Myhill's theorem fail for paradoxical groups? (This problem seems **very** difficult!)
- Are there injective CA which are not balanced? (If no such CA exists, then Gottschalk's conjecture is true.)
- Does there exists a CA that sends a nonrich configuration into a rich one?

Thank you for attention!

Any questions?