Martin-Löf randomness and measure preservation in cellular automata

Silvio Capobianco

Institute of Cybernetics at TUT

Theory Days at Rogosi, Estonia
February 6–7–8, 2015

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

Revision: February 7, 2015
Introduction

- In 1966 Martin-Löf gave a formal answer to the question: what does it mean for a single object to be random?
- Martin-Löf’s ideas were expanded by Hertling and Weihrauch, who adapted them to a very large class of systems.
- Cellular automata (CA) are a synchronous model of parallel computation on regular grids, where the next state of a point depends on the current state of a finite, uniform neighborhood.
- Bartholdi, 2010: for an arbitrary group, either it can be split and reassembled into two copies of itself, or every surjective CA on it preserves the uniform produce measure on the space of configurations.
- The Hertling-Weihrauch methodology is applied, under suitable hypotheses, to define Martin-Löf randomness for configurations.
- We then extend a 2001 result by Calude et al. by proving a Bartholdi-like condition for amenability of groups.
Any one who considers arithmetic methods of producing random digits is, of course, in a state of sin. For, as has been pointed out several times, there is no such thing as a random number—there are only methods to produce random numbers, and a strict arithmetical procedure is of course not such a method.

John von Neumann
What does it mean to be random?

0000000000000000000000000000000000...
0101010101010101010101010101010101...
0100011011000001010011100101110111...
0011011010110101100001011010111110...
011011010110101100001011010111110...
Martin-Löf’s idea of randomness

The basic idea is:

a random sequence should possess every conceivable property of stochasticity

- This includes at least definitions such as incompressibility — as “very few” strings are compressible
- This also includes normality: every finite subsequence of given length should appear with the same asymptotic frequency.
- In particular, random sequences would display no “conceivable” regularities.

But what does “conceivable” mean?
Martin-Löf randomness for infinite words

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

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

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

$w$ 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.
Prodiscrete topology and product measure

The prodiscrete topology of the space $A^\omega$ of infinite words is generated by the fundamental cylinders

$$wA^\omega = \{ u \in A^\omega \mid u_{[0:|w|-1]} = w \} , \ w \in A^*$$

- Two infinite words are “near” if they have a “long” common prefix.
- Long prefix of $w + \text{M-L random word} = \text{M-L random word “near” } w$.
- Long prefix of $w + a^\omega = \text{non-M-L random word “near” } w$.

The fundamental cylinders also generate the Borel $\sigma$-algebra where the product measure induced by

$$\mu_\Pi(wA^\omega) = |A|^{-|w|}$$

is well defined.

Can we apply these concepts to more general objects?
Presentations of groups

Let $S$ be a set. Construct $S^{-1} = \{s^{-1} \mid s \in S\}$. Let $R \subseteq (S \cup S^{-1})^*$. The group $G$ has the presentation $\langle S \mid R \rangle$ if $G \cong F_S/K_R$, where:

- $F_S$ is the free group of the reduced words on $S \cup S^{-1}$. (Pairs $ss^{-1}$ or $s^{-1}s$ are recursively erased.)
- $K_R$ is the normal subgroup of $F_S$ generated by $R$.

$G$ is finitely generated (f.g.) if $S$ can be chosen finite.

The word problem for the group $G = \langle S \mid R \rangle$ is the set of words on $S \cup S^{-1}$ that represent the identity element of $G$.

- Decidability of the word problem depends on the group, but not on the presentation.
- The word problem is decidable for free groups, $\mathbb{Z}^d$, etc.
Computable groups

An admissible indexing of a group $G$ is a computable bijection $\phi : \mathbb{N} \to G$ such that there exists a computable function $m : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ satisfying

$$\phi(i) \cdot \phi(j) = \phi(m(i,j)) \quad \forall i, j \in \mathbb{N}$$

$G$ is computable if it has an admissible indexing.

- We may write $g_i$ instead of $\phi(i)$.
- If $G$ is computable, then there is also a computable function $\iota : \mathbb{N} \to \mathbb{N}$ such that $g_i^{-1} = g_{\iota(i)}$ for every $i \in \mathbb{N}$.

**Theorem** (Rabin, 1960)

A f.g. group is computable if and only if it has decidable word problem.
Prodiscrete topology and product measure on $A^G$

The **prodiscrete topology** of the space $A^G$ of configurations over $G$ with values in $A$ is generated by the cylinders

$$C(E, p) = \{c \in A^G \mid c|_E = p\}$$

where $E \in \mathcal{P} \mathcal{F}(G)$ and $p : E \to A$ is a pattern.

- Two configurations are “near” if they are equal on a “large” finite set.
- Parallel with infinite words: $wA^\omega = C(\{0, \ldots, |w| - 1\}, w)$.

The cylinders also generate a $\sigma$-algebra $\Sigma_C$, on which the **product measure** induced by

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

is well defined.
Enumerating the cylinders

Let $A = \{a_0, \ldots, a_{k-1}\}$ be a $k$-ary alphabet.
Let $\phi : \mathbb{N} \to G$ be an admissible indexing.

1. First, we enumerate the elementary cylinders

$$B_{ki+j} = C(g_i, a_j) = \{c \in A^G \mid c(g_i) = a_j\}$$

which form a subbasis of the prodiscrete topology.

2. Next, we define a bijection $\Psi : \mathcal{P}(G) \to \mathbb{N}$ by

$$\Psi(X) = \sum_{i \in X} 2^i$$

(so that $\Psi(\emptyset) = 0$)

3. 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 computable group. Let $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a recursive bijection. Let $\mathcal{U} = \{U_i\}_{i \geq 0}$, $\mathcal{V} = \{V_j\}_{j \geq 0} \subseteq \mathcal{P}(A^G)$ be families of open sets.

- $\mathcal{U}$ is $\mathcal{V}$-computable if there exists a r.e. $T \subseteq \mathbb{N}$ such that
  \[ U_i = \bigcup_{\pi(i,j) \in T} V_j \quad \forall i \geq 0 \]

- $\mathcal{U}$ is a Martin-Löf $\mu_{\Pi}$-test if it is $B'$-computable and
  \[ \mu_{\Pi}(U_n) \leq 2^{-n} \quad \forall n \geq 0 \]

- $c \in A^G$ fails $\mathcal{U}$ if $c \in \bigcap_{n \geq 0} U_n$.
- $c$ is M-L $\mu_{\Pi}$-random if it does not fail any M-L $\mu_{\Pi}$-test.

For an admissible indexing $\phi : \mathbb{N} \to G$ the following are equivalent:

1. $c \in A^G$ is Martin-Löf $\mu_{\Pi}$-random.
2. $c \circ \phi \in A^\omega$ is Martin-Löf random.
Cellular automata

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

- $A$ is a finite alphabet.
- $\mathcal{N} = \{n_1, \ldots, n_m\} \subseteq G$ is a finite neighborhood.
- $f : A^m \rightarrow A$ is a finitary local update rule.

The local function induces a global transition function $F : A^G \rightarrow A^G$ via

$$F_A(c)(x) = f(c(x \cdot n_1), \ldots, c(x \cdot n_m)) = f(c^x|_\mathcal{N})$$

where $c^x = \lambda(y : G).c(x \cdot y)$.

The same rule induces a function over patterns:

$$f(p) : E \rightarrow A \quad f(p)(x) = f(p^x|_\mathcal{N}) \quad \forall p : E\mathcal{N} \rightarrow A$$
Balancedness

Let $E \in \mathcal{P}\mathcal{F}(G)$ and let $A = \langle A, \mathcal{N}, f \rangle$ be a CA on $G$.

- $A$ is **$E$-balanced** if for every $p : E \rightarrow A$,
  
  $$|f^{-1}(p)| = |A||E\mathcal{N}| - |E|$$

- $A$ is **balanced** if it is $E$-balanced for every $E \in \mathcal{P}\mathcal{F}(G)$.

Equivalently, $A$ is balanced if it preserves the product measure, i.e.,

$$\mu_\Pi (F_A^{-1}(U)) = \mu_\Pi (U) \quad \forall U \in \Sigma \text{ open}$$

**Theorem.** If $G = \mathbb{Z}^d$ then the following are equivalent:

1. $A$ is surjective.
2. $A$ is balanced. (Maruoka and Kimura, 1976)
3. For every $c \in A^{\mathbb{Z}^d}$, if $c$ is M-L $\mu_\Pi$-random then so is $F_A(c)$. (Calude, Hertling, Jürgensen and Weihrauch, 2001)
A counterexample on the free group

Let $G = \mathbb{F}_2$, $A = \{0, 1\}$, $\mathcal{N} = \{1_G, a, b, a^{-1}, b^{-1}\}$, and

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

$A$ is not balanced.

- The pattern 1 has 18 preimages instead of 16.

However, $A$ is surjective.

- Let $E \in \mathcal{P} \mathcal{F}(G)$ 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 group is paradoxical if it has a paradoxical decomposition.

Equivalently, $G$ is paradoxical if it has a bounded propagation $2:1$ compressing map, i.e., 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)
Amenable groups

von Neumann, 1929:
A group $G$ is amenable if there exists a \textit{finitely} additive probability measure $\mu : \mathcal{P}(G) \to [0, 1]$ such that:

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

- Abelian groups are amenable.
- Groups with a free subgroup on two generators are not amenable.

\textbf{The Tarski alternative} (1929, 1938)
Let $G$ be a group. \textbf{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 pre-injective. (Informally, a CA is pre-injective if it cannot erase finitely many errors in finite time.)
3. Every surjective cellular automaton on $G$ is balanced.

How much does preservation of product measure fail on paradoxical groups?
An extension to Calude’s theorem

Let $G$ be an amenable, f.g. group with decidable word problem.
Let $A = \langle A, N, f \rangle$ be a CA on $G$.

- Finiteness of neighborhood and decidability of word problem:
  If $U$ is $B'$-computable then so is $F_A^{-1}(U)$.
- Preservation of product measure:
  If $A$ is surjective and $U$ is a M-L $\mu_{\Pi}$-test, then so is $F_A^{-1}(U)$.
- Consequently:
  If $A$ is surjective and $F_A(c)$ fails $U$, then $c$ fails $F_A^{-1}(U)$.

Summarizing:

for an amenable f.g. computable group,
the image of a M-L $\mu_{\Pi}$-random configuration by a surjective CA
is also M-L $\mu_{\Pi}$-random
Normality

An infinite word \( w \in A^\omega \) is \( m \)-normal if for every \( u \in A^m \)

\[
\lim_{n \to \infty} \frac{\left| \{ i < n \mid w_{[i:i+m-1]} = u \} \right|}{n} = \frac{1}{|A|^m}
\]

M-L random infinite words are \( m \)-normal for every \( m \geq 1 \).

**Theorem** (Niven and Zuckerman, 1951)

\( w \) is \( m \)-normal as a word on \( A \) iff it is 1-normal as a word on \( A^m \).

Let \( h : \mathbb{N} \to G, \ E \subseteq G, \ 0 < |E| < \infty \).

We say that \( c \in A^G \) is \( h\)-\( E \)-normal if the infinite word

\[
w \in (A^E)^\omega : \ w(i) = \left. c^{h(i)} \right|_E = c_{h(i)E} \forall i \geq 0
\]

is 1-normal. For \( E = \{1\} \) we say \( h\)-1-normal.
Lemma 1

Let $\mathcal{A} = \langle A, \mathcal{N}, f \rangle$ be a CA on $G$, such that $1 < |A|, |\mathcal{N}|$.

- Suppose $\mathcal{A}$ has a spreading state $q_0$,
  i.e., if $\alpha(x) = q_0$ for some $x \in \mathcal{N}$, then $f(\alpha) = q_0$.
- Let $s, t$ be two distinct elements of $\mathcal{N}$.
- Let $h : \mathbb{N} \rightarrow G$ be injective.
- If $c : G \rightarrow A$ 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 $E \in \mathcal{P}\mathcal{F}(G)$ with $\mathcal{N} \subseteq E$,
  then $F_{\mathcal{A}}(c)$ is not $h$-1-normal.
A surjective CA with a spreading state

Guillon, 2011: improves Bartholdi’s counterexample.

Let $\phi : G \rightarrow G$ be a b.p. 2:1 compressing map with propagation set $S$. Define on $S$ a total ordering $\preceq$.

Set $A = (S \times \{0, 1\} \times S) \cup \{q_0\}$, $\mathcal{N} = S$, 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 $A = \langle A, \mathcal{N}, f \rangle$, 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 $F_A(e) = c$. 
Relative randomness

$u \in A^\omega$ is M-L random relatively to $v \in A^\omega$ if it is M-L random when computability is considered according to Turing machines with oracle $v$.

- This is a tightening of the definition: by allowing more Turing machines, we increase the number of M-L tests to pass.

**Theorem** (van Lambalgen, 1987)
Let $u, v \in A^\omega$ and let $w$ be the interleaving of $u$ and $v$:

$$w(i) = \begin{cases} u(j) & \text{if } i = 2j, \\ v(j) & \text{if } i = 2j + 1. \end{cases}$$

The following are equivalent:

1. $w$ is M-L random.
2. $u$ and $v$ are M-L random relatively to each other.
Lemma 2

Let $G$ be an infinite f.g. group with decidable word problem. For every $E \subseteq G$ with $0 < |E| < \infty$ there exists a computable $h : \mathbb{N} \rightarrow G$ 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 $n \neq m$. (In particular: $h$ is injective.)
3. For any alphabet $A$, every M-L $\mu_\Pi$-random $c \in A^G$ is $h$-$E$-normal. (This follows from van Lambalgen’s theorem and the previous points.)
An extension to Bartholdi’s theorem

Let $G$ be a paradoxical, f.g. group with decidable word problem.
Let $\mathcal{A}$ be the Guillon CA.

- Construct $h$ as by Lemma 2 with $E = \mathcal{N} \cup \{1\}$.
- Let $c \in A^G$ be a M-L $\mu_{\Pi}$-random configuration.
- By Lemma 2, $c$ is both $h$-$E$- and $h$-$1$-normal.
- But by Lemma 1, $F_{\mathcal{A}}(c)$ cannot be $h$-$1$-normal . . .
- . . . thus not M-L $\mu_{\Pi}$-random either!

Summarizing:

on every paradoxical f.g. computable group,
there exists a surjective CA such that, given any configuration,
at most one between it and its image is M-L $\mu_{\Pi}$-random

In particular, if $U$ is the set of M-L $\mu_{\Pi}$-random configurations, then

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

- Martin-Löf definition of randomness can be extended to several systems, including configurations over computable groups.
- A computable finitely generated group $G$ is paradoxical if and only if there is a surjective CA on $G$ such that every Martin-Löf random configuration has a nonrandom image and only nonrandom preimages.
- For arbitrary paradoxical groups, we actually show a set $U$ of full measure and a surjective CA $A$ such that $F^{-1}_A(U)$ is a null set. (cf. C., Guillon and Kari, 2013)
- Do pre-injective, non-surjective CA exist on arbitrary paradoxical groups? (This holds if $F_2 \leq G$, cf. Ceccherini-Silberstein et al, 1999)
- Are there injective CA which are not balanced?
Bibliography


Thank you for attention!

Any questions?