Randomness and initial segment complexity for probability measures

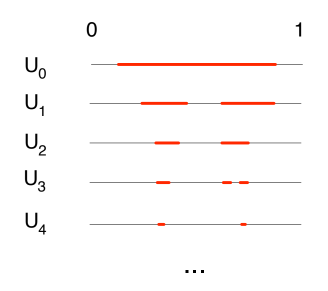
André Nies, University of Auckland
Joint work with Frank Stephan, NUS

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

STACS 2020
Montpellier, March 2020

Martin-Löf's randomness notion (1966)

- A Martin-Löf test is a uniformly recursively enumerable sequence $\langle U_m \rangle_{m \in \mathbb{N}}$ of open sets in the space $\{0,1\}^{\mathbb{N}}$ of infinite bit sequences such that $\lambda U_m \leq 2^{-m}$ for each m. Here λ is the uniform (product) measure giving both 0 and 1 the same probability.
- A bit sequence Z is Martin-Löf random if Z passes each ML-test, in the sense that Z is only in finitely many of the U_m.



Example of a ML-test. (We picture open sets as unions of intervals via binary representations.)

Characterization of ML-randomness via the initial segment complexity

Let $K(x)$ be the length of a shortest prefix free description of a binary string z. Given $Z \in \{0,1\}^{\mathbb{N}}$ and $n \in \mathbb{N}$, let $Z \upharpoonright n$ denote the initial segment $Z(0) \ldots Z(n-1)$.

Schnorr's Theorem informally says that

Z is ML-random $\iff$ each initial segment of Z is incompressible.

Theorem (Schnorr 1973)

Z is ML-random $\iff$ there is $b \in \mathbb{N}$ such that $\forall n\, K(Z \upharpoonright n) \geq n - b$.

Levin (1973) proved the analogous theorem for monotone string complexity.

Generalise to measures?

A probability measure μ on $\{0,1\}^{\mathbb{N}}$ can be seen as a statistical superposition of infinite bit sequences.

How do we define algorithmic randomness for such superpositions?

Plan

- We plan to study algorithmically defined randomness properties of probability measures μ on Cantor space $\{0,1\}^{\mathbb{N}}$.
- This should generalise the case of infinite bit sequences, which correspond to Dirac measures.
- We define initial segment complexity for measures.
- We relate the growth of initial segment complexity to randomness properties.

Randomness for infinite sequences of qubits

- Nies and Scholz, J. Math. Physics, 2019, introduced ML-randomness for infinite “sequences” of quantum bits;
- these sequences are states ρ on a C^*-algebra M_∞ from physics called the “CAR algebra”.
- They can be viewed as coherent sequences of density matrices $D_n \in M_{2^n}$. Here M_{2^n} is the algebra of $2^n \times 2^n$ matrices over $\mathbb{C}$. Coherence means that the partial trace of D_{n+1}, wrt last qubit, is D_n.
- $D_n = \rho \upharpoonright n$ is the n-th initial segment.
- Probability measures can be seen as states where all the matrices are diagonal.
- Our definition of randomness for measures is a special case of theirs by recent work of Bhojraj.

Martin-Löf absolutely continuous measures

Recall that a measure μ is continuous if it has no atoms, and absolutely continuous if $\mu(\mathcal{N}) = 0$ for each λ-null set $\mathcal{N}$.

Definition (Main)

A measure μ on $\{0,1\}^{\mathbb{N}}$ is called Martin-Löf absolutely continuous (ML-a.c., for short) if

$$\inf_m \mu(G_m) = 0 \text{ for each Martin-Löf-test } \langle G_m \rangle.$$

Fact

- The uniform measure λ is ML-a.c..
- Let $\mu = \sum_k c_k \delta_{Z_k}$ be a positive sum of Dirac measures. Then μ is ML-a.c. $\iff$ all Z_k are Martin-Löf-random.
- In particular δ_Z is ML-a.c. for each ML-random Z.

Definition (Recall)

A measure μ on Cantor space is called Martin-Löf absolutely continuous (ML-a.c., for short) if $\inf_m \mu(G_m) = 0$ for each Martin-Löf-test $\langle G_m \rangle$.

- It suffices to consider descending Martin-Löf-tests, because we can replace $\langle G_m \rangle$ by the Martin-Löf-test $\widehat{G}_m = \bigcup_{k>m} G_k$.
- So we can change the passing condition to $\lim_m G_m = 0$.

Since there is a universal ML-test, μ being ML-a.c. simply means that

$$\mu(\text{non-MLR}) = 0.$$

Solovay tests

The following test notions appears to be more general than ML-tests, but it in fact isn't.

- A Solovay test is a sequence $\langle S_n \rangle$ of uniformly Σ^0_1 sets such that $\sum_k \lambda S_k < \infty$. (Before, we required $\lambda S_k \leq 2^{-k}$.)
- A measure μ passes such a test if $\lim_k \mu(S_k) = 0$.

Proposition

A measure μ is ML-a.c. $\iff$ μ passes each Solovay test.

Proof:

- by the known equivalence for bit sequences, the set $\limsup_k S_k = \{Z \colon \exists^\infty k\, [Z \in S_k]\}$ only consists of non-MLR sequences.
- So $\mu(\limsup_k S_k) = 0$.

Descriptive complexity of initial segments for measures

x will denote a (finite) bit string.

- Let $C(\mu \upharpoonright n) = \sum_{|x|=n} C(x)\mu[x]$ be the μ-average of all the $C(x)$ over all strings x of length n.
- In a similar way we define $K(\mu \upharpoonright n)$.

Fact

Let λ denote the uniform measure. We have $C(\lambda \upharpoonright n) \geq n - 1$.

Pf.: $C(\lambda \upharpoonright n) = \sum_{r=0}^{n+d} \sum_{x:|x|=n \wedge C(x) \geq r} 2^{-n} \geq$
$\sum_{r=0}^{n} [\sum_{|x|=n} 2^{-n} - \sum_{|x|=n, C(x)<r} 2^{-n}] \geq n+1 - \sum_{r \leq n} 2^{-n+r} \geq n-1.$

Both implications of Schnorr's theorem fail

We say that μ has complex initial segments if $K(\mu \upharpoonright n) \geq^+ n$. The analog of Levin-Schnorr fails for measures in both directions.

Proposition

There is a ML-a.c. measure μ such that for each $\theta \in (0, 1)$, $K(\mu \upharpoonright n) \leq^+ n - n^\theta$. ($\leq^+$ means up to a constant.)

We falsify the converse implication of L-S by the following.

Theorem

There are a ML random bit sequence X and a non-ML random Y such that, for all n, $K(X \upharpoonright n) + K(Y \upharpoonright n) \geq^+ 2n$.

Corollary

The measure $\mu = \frac{1}{2}(\delta_X + \delta_Y)$ has complex initial segments but is not ML-a.c.

Strong Chaitin randomness for measures

Recall that a measure μ on Cantor space is called Martin-Löf absolutely continuous if $\inf_m \mu(G_m) = 0$ for each Martin-Löf-test $\langle G_m \rangle$.

$Z \in \{0,1\}^{\mathbb{N}}$ is called strongly Chaitin random if there is $d \in \mathbb{N}$ such that $K(Z \upharpoonright n) \geq n + K(n) - d$ for infinitely many n.

This is equivalent to ML-randomness relative to the halting problem by Miller (2010).

Theorem

Suppose that for some r, we have $K(\mu \upharpoonright n) \geq n + K(n) - r$ for infinitely many n. Then μ is ML-a.c.
Similar under the hypothesis $C(\mu \upharpoonright n) \geq n - r$ for infinitely many n.

The uniform measure on the space of measures

- The "uniform" probability measure $\mathbb{P}$ on the space $\mathcal{M}(\{0,1\}^{\mathbb{N}})$ of probability measures on Cantor space has been studied by Mauldin and Monticino (1995).
- Idea: if $\mu[x]$ has been determined for a string x, choose $\mu[x0] \leq \mu[x]$ uniformly at random.
- The algorithmic theory has been developed in Culver's PhD thesis (Notre Dame, 2015). μ is ML-random wrt $\mathbb{P} \Rightarrow \mu$ is continuous.

Proposition

μ is Martin-Löf-random wrt to $\mathbb{P} \Rightarrow \mu$ is ML-a.c.

- $\lambda(G) = \int \mu(G) d\mathbb{P}(\mu)$ for each open G.
- Use this to show: if $\langle G_m \rangle$ is a Martin-Löf-test such that $\inf_m \mu(G_m) > 0$, then μ is not Martin-Löf-random w.r.t. $\mathbb{P}$.

K-triviality for measures

Definition

A measure μ is called K-trivial if $\exists b \forall n \, K(\mu \restriction n) \leq K(n) + b$.

For Dirac measures δ_A this means that A is K-trivial in the usual sense.

Theorem

Suppose μ is K-trivial. Then μ is concentrated on its atoms.

Use that $\forall c \; \exists d \; \forall n$

$$\exists^{\leq d} \text{ strings } x \text{ of length } n \text{ with } K(x) \leq K(n) + c.$$

Ergodic measures

- T denotes the shift operator on $\{0,1\}^{\mathbb{N}}$. A measure ρ is shift-invariant if $\rho(A) = \rho(T^{-1}(A))$ for each Borel A.
- A shift-invariant measure ρ is ergodic if every ρ-integrable function f with $f \circ T = f$ is constant ρ-a.s.
- For ergodic ρ, the entropy $H(\rho)$ is defined as $\lim_n H_n(\rho)$, where
$$H_n(\rho) = -\frac{1}{n} \sum_{|w|=n} \rho[w] \log \rho[w].$$
- $H(\lambda) = 1$ and this is the maximum possible entropy,

SMB Theorem (1950s)

For $n \geq 0$, for $Z \in \{0,1\}^{\mathbb{N}}$ let $h_n^\rho(Z) = -\frac{1}{n} \log \rho[Z \upharpoonright n]$.

This is the weighted log-likelihood random variable.
Note that $H_n(\rho) = E_\rho h_n^\rho$ where E_ρ denotes the expectation w.r.t. ρ.

Theorem (Shannon-McMillan-Breiman theorem)

Let ρ be an ergodic measure.
For ρ-a.e. $Z \in \{0,1\}^{\mathbb{N}}$ we have $\lim_n h_n^\rho(Z) = H(\rho) := \lim_n H_n(\rho)$.

Algorithmic version:
If ρ is computable, then the conclusion holds for ρ-ML-random Z by results of Hochman (2009, implicit) and Hoyrup (2012).

Recall: for $n \geq 0$, for $Z \in \{0,1\}^{\mathbb{N}}$ let $h_n^\rho(Z) = -\frac{1}{n} \log \rho[Z \upharpoonright n]$.

We say that a measure μ is ML-a.c. relative ρ if $\mu(G_m) \to 0$ for each ρ-ML test $\langle G_m \rangle$.

Proposition (Effective SMB theorem for measures)

Let ρ be a computable ergodic measure. Suppose that there is D such that $h_n^\rho \leq D$ for each n. If μ is ML-a.c. w.r.t. ρ then $\lim_n E_\mu h_n^\rho = H(\rho)$, where $E_\mu h_n^\rho = \sum_{|x|=n} h_n^\rho(x)\mu([x])$.

Example (Boundedness condition is necessary)

Let $p_k = 2^{-k^4}/c$ where c is chosen so that $\sum_{k \geq 1} p_k = 1$. Let ρ be the measure associated with the corresponding binary renewal process: $\rho(10^k 1 \prec Z \mid Z_0 = 1) = p_k$ for each $k \geq 1$.
Then there is a computable measure $\mu \ll \rho$ such that $E_\mu h_n^\rho \to \infty$.

A measure version of Brudno's Theorem

The weighted asymptotic initial segment complexity of a ML-a.c. measure relative to ρ obeys some positive lower bound.

Proposition

Let ρ be a computable ergodic measure, and suppose μ is a Martin-Löf a.c. measure with respect to ρ. Then

$$\lim_n \frac{1}{n} K(\mu \upharpoonright n) = \lim_n \frac{1}{n} C(\mu \upharpoonright n) = H(\rho).$$

Recall that we obtained a ML-a.c. measure μ such that $K(\mu \upharpoonright n) \leq^+ n - n^\theta$ for any $\theta \in (0,1)$. Since $H(\lambda) = 1$, we now see that we cannot subtract, say, $n/4$ instead of n^θ.

Summary and open questions

$$\begin{tikzcd}
\mu \text{ is a.c.} \arrow[ddr] & \forall n\, C(\mu \restriction n) \geq^+ n \arrow[d] & \mu \text{ is MLR w.r.t. } \mathbb{P} \arrow[ddl] \\
 & \exists^\infty n\, C(\mu \restriction n) \geq^+ n \arrow[d] & \\
 & \mu \text{ is ML-a.c.} \arrow[d] & \\
 & \lim_n \frac{1}{n} C(\mu \restriction n) = 1 &
\end{tikzcd}$$

Culver: μ MLR w.r.t. $\mathbb{P} \Rightarrow \mu$ is orthogonal to λ, and hence not a.c. The middle column of the diagram is strict, via examples that are Dirac measures.

Future research: improve the diagonal arrows in the diagram.

Study the case of randomness relative to a general ergodic computable ρ.

THANKS!

References:

- Martin-Löf random quantum states, with Volkher Scholz, J.Math Physics 2019, arxiv.org/abs/1709.08422
- Paper 55 on your USB, updated on arxiv.org/abs/1902.07871
- Logic Blogs 2017, 2020 accessible from my home page