Randomness relative to almost everything

Tomasz Steifer [1]

Joint (preliminary) work with Laurent Bienvenu and Valentino Delle Rose

[1]Institute of Fundamental Technological Research, Polish Academy of Sciences

April 29, 2021

A well-known theorem

Theorem (van Lambalgen)

$\boldsymbol{X} \bigoplus \boldsymbol{Y}$ is Martin-Löf random if and only if $\boldsymbol{X}$ and $\boldsymbol{Y}$ are Martin-Löf random relative to each other.

This has as an interesting consequence:

Observation

For every Martin-Löf random set $\boldsymbol{X}$ the set

$$\{\boldsymbol{Z} : \boldsymbol{X} \text{ is not Martin-Löf random relative to } \boldsymbol{Z}\}$$

is of measure zero.

Weaker notions of randomness

It is also known that the van Lambalgen theorem fails for some weaker notions of randomness, e.g, Schnorr and computable randomness.
Hence, a following question arises:

Question

Is there a computable (Schnorr) random $\boldsymbol{X}$ *such that*

$$\boldsymbol{\mu(\{Z : X \text{ is computable (Schnorr) random relative to } Z\}) < 1?}$$

Almost everywhere randomness

We introduce a following template:

Definition

We say that X is a.e. $\ldots$ random if

$$\mu(\{Z : X \text{ is } \ldots \text{ random relative to } Z\}) = 1.$$

When can we get separation between randomness and a.e. randomness?

Computable randomness

Definition (martingale)

A function $d : 2^{<\mathbb{N}} \to \mathbb{R}^{\geq 0}$ is called a martingale if for all $\sigma \in 2^{<\mathbb{N}}$:

$$d(\sigma) = \frac{d(\sigma 0) + d(\sigma 1)}{2}$$

A martingale d succeeds on a sequence X if

$$\limsup_{n \to \infty} d(X \upharpoonright n) = \infty.$$

Definition

A sequence $X \in 2^{\mathbb{N}}$ is called (partial) computably random if no (partial) total computable martingale succeeds on X.

Theorem

There exists $\boldsymbol{X}$ which is computably random but not a.e. computably random.

The proof combines two techniques - the Kucera-Gacs encoding and the fireworks.

Lemma (Space Lemma, Merkle-Mihailović)

Given a rational $\boldsymbol{\delta > 1}$ and $\boldsymbol{k \in \mathbb{N}^+}$, we can compute a length $\boldsymbol{l(\delta, k)}$ such that, for any martingale $\boldsymbol{d}$ and any $\boldsymbol{\sigma \in 2^{<\mathbb{N}}}$

$$\boldsymbol{|\{\tau \in 2^{l(\delta,k)} : d(\sigma\tau) \leq \delta d(\sigma)\}| \geq k.}$$

Lemma (Exact Computation lemma, Mayordomo 1994)

For every computable martingale $\boldsymbol{d}$, there exists an exactly computable martingale $\boldsymbol{d'}$ such that $\boldsymbol{d'}$ succeeds on every sequence on which $\boldsymbol{d}$ succeeds.

Fix a sequence of rationals $\beta_1, \beta_2, \ldots$ such that $\beta_i > 1$ for each i and $\prod_{i=1}^{\infty} \beta_i < \infty$ and consider a partition of $\mathbb{N}$ into intervals $[0, l(\beta_1, 2)), [l(\beta_1, 2), l(\beta_2, 2)), \ldots$

To get a computably random, we need to diagonalize against all exactly computable martingales $d_0, d_1, \ldots$. We start by diagonalizing against d_0, then after some time, we diagonalize against the mixture $d_0 + 2^{-1} d_1$ and so on. At each step we use a mixture of finite number of total computable martingales. This means that we can encode something on the way, e.g., an index of the next martingale or a bit of some A.

There is a strategy which decodes this information and succeeds on the sequence. This strategy is partial—a malicious demon may trick us into thinking that we have decoded an index of a total martingale, while giving us a partial one.

Can we have a probabilistic strategy which will be (total and succeeding) with positive probability? Yes, we can do it with fireworks.

Suppose we have just decoded an index of the next martingale $\boldsymbol{d_n}$ after reading $\boldsymbol{k}$ bits of $\boldsymbol{X}$. We do not know if $\boldsymbol{\delta = \sum_{i=0}^{n-1} 2^{-i}}$ is 'total' enough for us to make more decoding. The fireworks strategy is as follows. We randomly choose $\boldsymbol{m}$ from $\boldsymbol{[1, N_n]}$. We make a passive guess that $\boldsymbol{\delta}$ is 'bad', e.g., that it is partial somewhere on strings of length at most $\boldsymbol{2k}$. We continue to read $\boldsymbol{X}$ without betting anything. If the guess was wrong, we will known at some point.

If after reading $\boldsymbol{k'}$ bits we find out that the passive guess was wrong, we make a new passive guess that $\boldsymbol{\delta}$ is partial somewhere on strings of length at most $\boldsymbol{2k'}$.

We allow ourselves to make m wrong passive guesses, after which we make an active guess that δ is defined on all string of a certain length. In case of an active guess, we try to make some betting and to decode the next message.

If the active guess is correct then we are good. We might lose money in some cases but then we simply stop betting forever. On a 'nice' X we will bet, win and decode the next information.

If the active guess was wrong, then it is bad, because the strategy goes into a loop. But a standard fireworks reasoning tells us that we have $1/N_n$ probability of making a wrong active guess (conditioned on other random choices being fixed). If N_n grows fast enough, we get a positive probability of not making a wrong active choice anywhere while reading arbitrary sequence X.

How much randomness do we need to 'derandomize' a computably random?

Conjecture

There exists a set $\boldsymbol{X}$ which is computably random relative to some Martin-Löf random $\boldsymbol{Y}$ but is not computably random relative to any Demuth random.

We believe this is true but the proof is not yet written down.

Almost everywhere domination

Definition

A degree $\mathbf{a}$ is called uniformly almost everywhere dominating if $\mathbf{a}$ computes a function f such that

$$\mu\{Z : \forall g \in \omega^\omega (g \leq_T Z \Rightarrow g <^* f)\} = 1$$

A separation result

Theorem

If $\mathbf{a}$ *is a Turing degree which is uniformly almost everywhere dominating, then it contains some* $\boldsymbol{X}$ *which is a.e. computably random but not partial computably random. Moreover, such an* $\boldsymbol{X}$ *can be chosen to be facile, i.e., for each computable order function* $\boldsymbol{h}$

$$\forall_n \boldsymbol{K}((\boldsymbol{X} \upharpoonright \boldsymbol{n})|\boldsymbol{n}) <^+ \boldsymbol{h}(\boldsymbol{n}).$$

Proof idea: Let $\boldsymbol{h} \leq_{\boldsymbol{T}} \mathbf{a}$ be a.e. dominating function. Let $\boldsymbol{\delta}$ be a universal oracle martingale. For an oracle $\boldsymbol{Z}$ we consider $\boldsymbol{\delta}_{\boldsymbol{s}}^{\boldsymbol{Z}}$ given by simulating $\boldsymbol{h}(\boldsymbol{h}(\boldsymbol{s}))$ steps of $\boldsymbol{\delta}^{\boldsymbol{Z}}$. If the computations halts in that much steps, we copy the output. Otherwise, $\boldsymbol{\delta}_{\boldsymbol{s}}^{\boldsymbol{Z}}$ do not bet. Finally, at step $\boldsymbol{s}$ we diagonalize against an exactly computable version of $\int_{\boldsymbol{Z}} \boldsymbol{\delta}_{\boldsymbol{s}}^{\boldsymbol{Z}}$.

Theorem

Let $\mathbf{a}$ *be a Turing degree. If* $\mathbf{a}$ *is not uniformly almost everywhere dominating, then for every* $X \in \mathbf{a}$*, we have*

$$X \in \mathbf{aeSR} \Leftrightarrow X \in \mathbf{aeCR} \Leftrightarrow X \in \mathbf{MLR}$$

Let $X \in \mathbf{a}$ and suppose that X is not Martin-Löf random, i.e., $X \in \bigcap_n \mathcal{U}_n$ for $(\mathcal{U}_n)$ a sequence of uniformly effectively open sets with $\mu(\mathcal{U}_n) \leq 2^{-n}$. Consider the function t^X defined by $t^X(n) := \min\{s \mid X \in \mathcal{U}_n[s]\}$. Since $\mathbf{a}$ is not a.e. dominating, there exists a functional Γ such that

$$\mu\{Z \mid \Gamma^Z \text{is total and } \exists^\infty n\ \Gamma^Z(n) > t^X(n)\} > 0$$

When Γ^Z is total and $\Gamma^Z(n) > t^X(n)$ for infinitely many n, we have $X \in \mathcal{U}_n[\Gamma^Z(n)]$ for infinitely many n. Note that in that case $\mathcal{U}_n[\Gamma^Z(n)]$ is a clopen set which Z-uniformly computable in Z. This type of test characterizes Schnorr randomness: a sequence X is Schnorr random if and only if for every computable sequence of clopen sets $\mathcal{D}_n$ such that $\mu(\mathcal{D}_n) \leq 2^{-n}$, X belongs to only finitely $\mathcal{D}_n$.

Questions

Question

Is there a set $\boldsymbol{X}$ which is partial computably random but not a.e. computably random?

Question

Given $\boldsymbol{X}$ which is computably random but not a.e. computably random—what can we say about the oracles which 'derandomize' $\boldsymbol{X}$? How much randomness do we need?