New Directions in Randomness

Jason Rute

Pennsylvania State University

Computability, Complexity, and Randomness
June 22–26

Slides available at
www.personal.psu.edu/jmr71/

(Updated on June 22, 2015.)
Introduction
The goals

- To make you think about randomness in a new way.
- What is a randomness notion?
- What is a natural randomness notion?
- Can randomness be studied as a theory? Like the theory of groups?
- Can we axiomatize algorithmic randomness?
Organizing the randomness zoo
The Heidelberg zoo
The randomness zoo
Antoine Tavenaexs
Organizing the randomness zoo

Step 1: Organize by $\sigma$-ideals
Some randomness notions are not like the others

- Kurtz-like (green)
- Stochastic (blue)
- Partial randomness (purple/red)

This can largely be explained via $\sigma$-ideals.
**σ-ideals**

- A **σ-ideal** is a collection of sets closed downward and under countable unions.
- Each σ-ideal $I$ provides a notion of “small set” or “null set”.
- Examples:
  - meager sets
  - null sets
  - sets of Hausdorff dimension $\leq s$ (for a fixed $0 \leq s \leq 1$).
- Every “randomness” notion is associated with a σ-ideal $I$. 

Example: $\sigma$-ideals of Kurtz randomness

- $x \in 2^{\mathbb{N}}$ is Kurtz random (or weak random) if $x$ is not in any $\Pi^0_1$ null set.
- Common complaint: “Kurtz randomness is really a genericity notion.”

- Let $\text{Kurtz}^A$ be the set of $A$-Kurtz random sequences for the oracle $A$.
- Let $I_{\text{Kurtz}}$ be the $\sigma$-ideal of subsets of $2^{\mathbb{N}} \setminus \text{Kurtz}^A$ for some $A$.
- $I_{\text{Kurtz}}$ is the exactly the $\sigma$-ideal of subsets of $F_\sigma$ (i.e. $\Sigma^0_2$) null sets.
- These are the null sets associated with Riemann integrable functions, a.e. continuous functions, and Jordan-Peano measurable sets.
- $I_{\text{Kurtz}}$ is a sub-$\sigma$-ideal of both the ideals of meager sets and the ideal of null sets.

- Kurtz randomness is both a genericity notion and a randomness notion.
σ-ideals and their “randomness notions”

<table>
<thead>
<tr>
<th>σ-Ideal</th>
<th>Randomness (Genericity) notions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meager</td>
<td>weakly 1-generic, 1-generic</td>
</tr>
<tr>
<td>Subsets of $F_{\sigma}$-null</td>
<td>Kurtz, finite bounded, Kurtz$^{0'}$</td>
</tr>
<tr>
<td>(Lebesgue) null</td>
<td>Sch, CR, ML, W2R, 2R, etc.</td>
</tr>
<tr>
<td>μ-null</td>
<td>μ-Sch, μ-CR, μ-ML, μ-W2R, μ-2R, etc.</td>
</tr>
<tr>
<td>Hausdorff dimension $\leq s$</td>
<td>Sch-dim $&gt; s$, cdim $&gt; s$</td>
</tr>
<tr>
<td>Null s-dim. Hausdorff measure</td>
<td>strong $s$-randomness: $KM(x \upharpoonright n) \geq^+ s n$</td>
</tr>
<tr>
<td>Null s-dim. Riesz capacity</td>
<td>$s$-energy randomness: $\sum_n 2^{sn - KM(x \upharpoonright n)} &lt; \infty$</td>
</tr>
</tbody>
</table>

- It is not clear what the σ-ideals are for
  - the stochasticity notions
  - constructive dimension = 1
  - (weak) $s$-randomness
  - UD randomness

- However, they are clearly not the σ-ideal of Lebesgue null sets.
Organizing the randomness zoo

Step 1: Organize by $\sigma$-ideals

$\sigma$-ideal zoo

- Meager (W1G, 1G)
- NULL (SR, MLR)
- $\subseteq \text{null } F_\sigma$ (Kurtz)
- $s$-Riesz null (s-energy rand)
- $s$-Hausdorff null (strong s-rand)
- $\text{Hdim} \leq s$ (cdim $> s$)

From here on, we will focus on the $\sigma$-ideal of Lebesgue (or $\mu$-) null sets.
Organizing the randomness zoo

Step 2: Organize by computability
True randomness vs. algorithmic randomness

- $x$ is **truly random** if $x$ avoids every null set.
- Except for a pesky problem...

- Our “solution” is to consider **algorithmic** null sets.
- However, what type of algorithmic?
Levels of computability in algorithmic randomness

Poly-time randomness notions
- Poly-time Schnorr random
- Poly-time random
- ...

Computable randomness notions
- Schnorr random
- Computably random
- Martin-Löf random
- Weak 2-random
- 2-random
- ...

Higher randomness notions
- $\Delta^1_1$ random
- $\Pi^1_1$ MLR random
- $\Pi^1_1$ random
- ...

Forcing randomness notions
- Solovay genericity
- ...
- “Pointless” randomness notions
  - True randomness

From now on, we will just work at the computable level.
Organizing the randomness zoo

Step 3: Mark the minimal sufficient randomness notion in each computability level
Schnorr randomness is sufficient

- A **μ-Schnorr test** is a computable sequence of $\Sigma^0_1$ sets such that $\mu(U_n) \leq 2^{-n}$ and $\mu(U_n)$ is computable in $n$.
- $x$ is **μ-Schnorr random** if $x \notin \bigcap_n U_n$ for any $\mu$-Schnorr test.

- Schnorr randomness is closely connected to constructive mathematics.
- See the slides for my VAI 2015 talk (available on my webpage).
- Schnorr null sets where first called “null sets in the sense of Brouwer.”
- Constructively provable a.e. theorems are true for Schnorr randomness.
Schnorr randomness is minimally sufficient

- Schnorr randomness is the minimal randomness notion for working with **computable measurable objects**.

**Definition**

A function \( f : 2^\mathbb{N} \rightarrow \mathbb{R} \) is **\( L^1 \)-computable** if there is a computable sequence of rational step functions \( f_n \) such that

\[
\|f_n - f\|_1 = \int |f_n - f| \, d\mu \leq 2^{-n}.
\]

- Only on Schnorr randomness is the convergence of \( f_n(x) \) guaranteed.
- Moreover, if the computable sequence \( g_n \) also converges rapidly to \( f \) in \( L^1 \), then \( \lim_n g_n(x) = \lim_n f_n(x) \) for all Schnorr randoms \( x \).
- This is one of many such similar examples.
Other computability notions

There is no obvious reason why these ideas cannot be extended to lower and higher computability notions.

Conjectures

1. **Poly-time Schnorr randomness** is the minimal sufficient randomness notion with respect to poly-time computability.

2. **Higher Schnorr randomness** (i.e. $\Delta^1_1$ randomness) is the minimal sufficient randomness notion with respect to higher computability.

These conjectures extend to basically every idea in this talk.
Organizing the randomness zoo

Step 4: Separate the wheat from the chaff, the sheep from the goats, the good randomness notions from the bad
Work with many randomness notions at once

- Why prove a theorem for one randomness notion when you can prove it for all of them?

- For example, the theorem:

  *Schnorr randomness satisfies the strong law of large numbers.*

  holds for all stronger randomness notions (CR, MLR, W2R, 2R, etc.).

- However, many theorems of randomness are not of this form.

- For example,

  *Schnorr randomness is closed under computable permutations of bits.*

  is not satisfied by partial computable randomness (PCR) even though PCR is stronger than Schnorr randomness.
The rest of this talk is devoted to developing a system of axioms which are sufficient for working with randomness in practice.

The randomness notions satisfying these axioms are the natural ones.

The unnatural ones should be demoted to footnotes in our zoo.
Properties desired of an algorithmic randomness notion
A very informal guiding principle

- A natural randomness notion should be sufficient for working constructively with Brownian motion
Brownian motion is given by the Wiener measure on $C[0,1]$ or $C[0,\infty)$.

**Generalization**

Randomness should generalize to all computable probability spaces $(\Omega, \mathcal{P})$. 
Extendable to other spaces

- Schnorr randomness, Martin-Löf randomness, weak-n-randomness, $n$-randomness are all naturally extendable to other spaces.
- Computable randomness also has a consistent extension to other probability spaces (R.).
  - A **measure bounded integral test** on $(X, \mu)$ is a lowersemicomputable function $t : X \to [0, \infty]$ and a computable measure $\nu$ such that
    \[ \int_A t(x) \, d\mu(x) \leq \nu(A) \quad (A \subseteq X \text{ measurable}). \]
  - $x \in X$ is **$\mu$-computably random** if $t(x) < \infty$ for all measure bounded integral tests $t$.
- For some of the more combinatorial randomness notions (e.g. partial computable randomness or Kolmogorov-Loveland randomness) it is not so clear.
Invariant under isomorphisms

- Brownian motion can be transformed via a number of isomorphisms.
- For example, if $B(t)$ is a BM, then the following are BMs:
  $$-B(t) \quad \text{and} \quad tB(1/t).$$
- Moreover, all the standard constructions of BM are isomorphisms between other probability spaces and the Wiener measure.

**Preservation under isomorphisms**

If $I: (\Omega_1, P_1) \simeq (\Omega_2, P_2)$ is an effectively measurable isomorphism, then $\omega$ is $P_1$-random if and only if $I(\omega)$ is $P_2$-random.
Invariant under isomorphisms

- Schnorr randomness, Martin-Löf randomness, weak-n-randomness, \( n \)-randomness are all invariant under isomorphisms.
- Computable randomness is also invariant under isomorphisms (R.).
- Partial computable randomness is not invariant under permutations of bits.
Randomness preservation

- The probability distribution of $B(1)$ is the Gaussian measure on $\mathbb{R}$.
- In other words, the Gaussian measure is the push-forward of the Wiener measure along the map $B \mapsto B(1)$.

**Preservation of randomness**

Assume $T: (\Omega, \mathcal{P}) \to (X, \mathcal{P}_T)$ is an effectively measurable map. If $\omega$ is $\mathcal{P}$-random, then $T(\omega)$ is $\mathcal{P}_T$-random. (Here $\mathcal{P}_T$ is the pushforward measure of $\mathcal{P}$ along $T$.)
Randomness preservation

- Schnorr randomness, Martin-Löf randomness, weak-n-randomness, \( n \)-randomness all satisfy randomness preservation.
- Computable randomness does not (Bienvenu/Porter; R.).
- Although, I will have more to say about this in a bit...
The Gaussian measure and the Lebesgue measure on \( \mathbb{R} \) are equivalent measures, i.e. they have the same null sets.

"Effectively equivalent" measures have the same randoms.
Equivalent measures share randoms

- This property can be stated with the following two properties.

1. If $x$ is $\mu$-random and $\mu \leq c\nu$ for some constant $c$, then $x$ is $\nu$-random.
2. Assume $\mu \ll \nu$ with an $L_1(\nu)$-computable density $f = \frac{d\mu}{d\nu}$, that is

   $$
   \mu(A) = \int_A f \, d\nu \quad (A \subseteq X).
   $$

   Then, $x$ is $\mu$-random iff both $x$ is $\nu$-random and $f(x) > 0$

- The standard randomness notions satisfy both of these:
  - SR, CR, MLR, $n$-random, weak $n$-random
No randomness from nothing

- Again consider that a Gaussian distribution can be found from a Brownian distribution.

**No randomness from nothing (a.k.a no randomness ex nihilo)**

Assume $T: (\Omega, P) \rightarrow (X, P_T)$ is an effectively measurable map. If $x$ is $P_T$-random, then there is a $P$-random $\omega$ such that $x = T(\omega)$. 
No randomness from nothing

- No-randomness-from-nothing holds for Martin-Löf randomness, \( n \)-randomness, weak 2-randomness, difference randomness.

Theorem (R.)

- No-randomness-from-nothing holds for computable randomness.
- However, it does not hold for Schnorr randomness:
  - If \( x \) is not CR, then there is a measure-preserving almost-everywhere computable map \( T \) such that the preimage of \( x \) under \( T \) is empty.

Theorem (R.)

- Martin-Löf randomness is the smallest randomness notion satisfying both no-randomness-from-nothing and randomness preservation.

- It is interesting (but not damning!) that NRFN fails for SR.
Van Lambalgen and combining measures

- A Brownian motion on $[0,1]$ can be **constructed** by “gluing together” two independent BM on $[0,1/2]$.
- And vice versa, a Brownian motion on $[0,1]$ can be **decomposed** into two independent BM on $[0,1/2]$.

**Van Lambalgen’s theorem**

$(\omega_1, \omega_2)$ is $P_1 \times P_2$-random iff $\omega_1$ is $P_1$-random and $\omega_2$ is $P_2$-random independently of $\omega_1$. 
Independence

Van Lambalgen’s theorem

\((\omega_1, \omega_2)\) is \(P_1 \times P_2\)-random iff \(\omega_1\) is \(P_1\)-random and \(\omega_2\) is \(P_2\)-random independently of \(\omega_1\).

- “Independent” is often taken one of two ways:
  - \(\omega\) is \(P\)-random \textbf{relative} to \(A\) means there is no test \(T^A\) computable from \(A\) that derandomizes \(\omega\).
  - \(\omega\) is \(P\)-random \textbf{uniformly relative} to \(A\) means there is no computably indexed family of tests \(\{T^B\}\), one test for each oracle \(B\), such that \(T^A\) derandomizes \(\omega\).

- For Martin-Löf and \(n\)-randomness, relative and uniformly relative are the same.

- (Others have suggested that “independent” should mean whatever makes van Lambalgen’s theorem holds.)
Properties desired of an algorithmic randomness notion

Van Lambalgen’s theorem

- Martin-Löf randomness and $n$-randomness satisfy van Lambalgen’s theorem with both **uniform relativization** and **relativization** (because they are the same!).

- The following satisfy van Lambalgen’s theorem for **uniform relativization**:
  - Schnorr randomness (Miyabe; Miyabe and R.)
  - Demuth randomness (Diamondstone, Greenberg, Turetsky)

- For computable randomness
  - One direction is true for **uniform relativization** (Miyabe and R.).
  - The other direction fails for both types of relativization (Bauwens, last week!)

- For other types of randomness, the details are not fully worked out.
Van Lambalgen’s theorem gives other results

Notice that one can construct a Brownian motion with two steps:

1. Choose a value $a$ at $t = 1$ from a Gaussian distribution.
2. Connect $(0,0)$ to $(1,a)$ via a Brownian bridge ending at $a$

The distribution in the second step is computable uniformly from the chosen $a$.

Using this idea we can, in many cases, recover randomness preservation for computable randomness and no-randomness-from-nothing for Schnorr randomness.
Generalized van Lambalgen’s theorem

- Let \((\Omega_1, P_1)\) be a computable probability measure.
- Let \(P(\cdot | \omega)\) be a **computable kernel**, that is a family of probability measures on the space \(\Omega_2\) such that the map \(\omega \mapsto P(\cdot | \omega)\) is effectively measurable.
- Combine \(P_1\) and \(P(\cdot | \omega)\) into one probability space \((\Omega_1 \times \Omega_2, P)\) via

\[
P(A \times B) = \int_A P(B | \omega_1) \, dP_1(\omega_1).
\]

Generalized van Lambalgen’s theorem

\((\omega_1, \omega_2)\) is \(P\)-random iff \(\omega_1\) is \(P_1\)-random and \(\omega_2\) is \(P(\cdot | \omega_1)\)-random independently of \(\omega_1\).

Besides interpreting "independently", we also have to figure out what "\(P(\cdot | \omega_1)\)-random" means since this measure may not be computable.

- It could mean using \(P(\cdot | \omega_1)\) as an oracle.
- It could mean using \(P(\cdot | \omega_1)\) uniformly as an oracle.
Generalized van Lambalgen’s theorem

- Generalized van Lambalgen’s theorem holds for
  - Martin-Löf randomness (Takahashi)
  - Schnorr randomness (R., using uniform relativization)
Van Lambalgen’s theorem for maps

- Assume $T: (\Omega, \mathbf{P}) \to (X, \mathbf{P}_T)$ is an effectively measurable map.
- Assume the conditional probability $x \mapsto \mathbf{P} (\cdot \mid T = x)$ is effectively measurable as a map from $(X, \mathbf{P}_T)$ to measures.

$\begin{align*}
\left( \begin{array}{l}
\omega \text{ is } \mathbf{P}\text{-random} \\
\text{and } x = T(\omega)
\end{array} \right) \iff 
\left( \begin{array}{l}
x \text{ is } \mathbf{P}_T\text{-random} \quad \text{and}
\\
\omega \text{ is } \mathbf{P} (\cdot \mid T = x)\text{-random independent of } x
\end{array} \right)
\end{align*}$

- The $\Rightarrow$ direction is a stronger version of randomness preservation.
- The $\Leftarrow$ version is a stronger version of no-randomness-from-nothing.
- It also lets one prove that if $P \ll Q$ with an $L^1$-computable density function $f$, then $x$ is $P$-random if and only if $x$ is $Q$-random and $f(x) > 0$. 
Proposed axioms of randomness
Proposed axioms of randomness

Tentative randomness axioms

- \( \langle x, \mu, a \rangle \in \mathcal{R} \) means \( x \) is \( \mu \)-random independent of \( a \).

- Axiom 1: For all \( \mu \) and \( a \), \( \mu \{ x : \langle x, \mu, a \rangle \in \mathcal{R} \} = 1 \).

- Axiom 2: If \( \langle x, \mu, a \rangle \in \mathcal{R} \), then \( x \) is \( \mu \)-Schnorr random uniformly relativized to \( a \).

- Axiom 3: If \( b \) is computable uniformly in \((a, \mu)\), then \( \langle x, \mu, a \rangle \in \mathcal{R} \) implies \( \langle x, \mu, b \rangle \in \mathcal{R} \).

- Axiom 4: If \( \mu \) is computable uniformly in \( a \), \( T : \Omega \to \Omega \) is \( \mu \)-effectively measurable uniformly in \( a \), and \( y \mapsto \mu(\cdot | T = y) \) is \( \mu_T \)-effectively measurable uniformly in \( a \), then

\[
\begin{align*}
\left( \langle x, \mu, a \rangle \in \mathcal{R} \quad \text{and} \quad y = T(x) \right) & \iff \left( \langle y, \mu_T, a \rangle \in \mathcal{R} \quad \text{and} \quad \langle x, \mu(\cdot | T = y), (y, a) \rangle \in \mathcal{R} \right).
\end{align*}
\]
These axioms are a work in progress.

However, I can already do cool things with them.

I have a new randomness reducibility as well.

It treats randoms as infinitesimally small point masses and compares their relative masses.

It says, for example, if \( x \in 2^\mathbb{N} \) is random on the Lebesgue measure, then \( 0x \) is exactly half as random as \( x \).

There are now more questions than answers.
Other randomness axioms

- van Lambalgen two related axiomatizations of randomness.
- Alex Simpson is currently developing a set theoretic axiomatization of randomness based on independence.
Closing Thoughts
New directions in randomness

- I hope I made you think about algorithmic randomness in new and interesting ways.
- I hope I inspired the poly-time randomness folks and the higher randomness folks to consider how much of this applies to their world.
- I hope those interested in Schnorr and computable randomness found some interesting new theorems.
Thank You!

These slides will be available on my webpage:

http://www.personal.psu.edu/jmr71/

Or just Google™ me, “Jason Rute”.

P.S. I am on the job market.