Separating Stochasticity and Randomness

Justin Miller

December 7th, 2021

Penn State Logic Seminar

https://math.dartmouth.edu/~jdmiller/files/talks/PSU21.pdf

What is Randomness?

It’s a well-known maxim in computer science that computers cannot generate a sequence of numbers which is "truly random."

But what does it mean for a sequence to be random? The natural idea is that an object is random if, with high probability, it is the end result of a random process. To formalize this, however, we instead say an object is not random if it is the result of a nonrandom process.

Historically, there are many different (and equivalent) formal definitions of what constitutes randomness. This inevitably leads to comparisons between them.

Probability Measures

We work in Cantor space, 2^ω.

A probability measure μ on 2^ω is a measure with the property $\mu(2^\omega) = 1$.

We will be most interested in the r-Bernoulli measure μ_r for real numbers r: given a finite binary string σ, let $|\sigma|$ denote the length of σ, and let $\#\sigma$ denote the number of 1's in σ. Then

$$\mu_r([\sigma]) = r^{\#\sigma}(1-r)^{|\sigma|-\#\sigma}$$

$\mu_{\frac{1}{2}}$ is the Lebesgue measure on the unit interval.

Martingales

Definition

A μ-martingale $m : 2^{<\omega} \to \mathbb{R}$ is a betting function for which expected value is preserved. In other words,

$$\mu([\sigma])m(\sigma) = \mu([\sigma 1])m(\sigma 1) + \mu([\sigma 0])m(\sigma 0)$$

We say m succeeds on a a set X if $\limsup_{n\to\infty} m(X \upharpoonright n) = \infty$.

X is μ-ML-Random (μ-1-Random) if no μ-c.e. μ-martingale succeeds on X. For noncomputable μ, we work with respect to any representation of μ. The specifics of representations are outside the scope of this talk, but essentially we are working with respect to an oracle which can computably approximate $\mu([\sigma])$ uniformly in σ.

Different Types of Randomness

If we require martingales to be computable rather than c.e., then the corresponding notion is μ-computable randomness.

If we additionally require that the $\limsup$ goes to infinity computably, the corresponding notion is μ-Schnorr randomness.

If we require our martingales to be computable but allow them to bet out of order, then we obtain the notion of μ-KL randomness.

Law of Large Numbers

The law of large numbers states that, as the number of iterations of some random process increases, the average of the outcomes approaches the expected value.

A set which is random with respect to the r-Bernoulli measure is thought of as the outcome of infinitely many independent r-Bernoulli trials, i.e. r-biased flips of a 0,1-sided coin. The expected value of one such flip is given by $r \cdot 1 + (1 - r) \cdot 0 = r$.

Thus, if our notion of randomness is correct, then the average number of 1's in a μ_r-random set should be r.

Asymptotic Density

Definition

For a set $X \in 2^\omega$ and $n \in \omega$,

$$\rho_n(X) = \frac{\#(X \upharpoonright n)}{n}$$

Then

$$\overline{\rho}(X) = \limsup_{n\to\infty} \rho_n(X), \;\; \underline{\rho}(X) = \liminf_{n\to\infty} \rho_n(X)$$

are called the upper density of X and the lower density of X respectively. If $\overline{\rho(X)} = \underline{\rho(X)}$, then we call this value the (asymptotic) density of X and denote it by $\rho(X)$.

The law of large numbers suggests that $\rho(X) = r$ for any set X which is μ_r-random. This is in fact true.

Sampling

Asymptotic density is not a particularly random property: the set of even numbers has density $\frac{1}{2}$, but is clearly not random. However, sufficiently random sets satisfy a stronger property: the density remains the same even if we sample a nice subset.

Definition

A selection (sampling) function is a partial function $f : 2^{<\omega} \to \{0, 1\}$. Then we use $f(X)$ to denote the set $\{n : f(X \upharpoonright n) = 1\}$.

The level of μ_r-randomness which X exhibits determines the selection functions f for which $\rho(f(X)) = r$.

Stochasticity

A set X is r-Church stochastic if $f(X)$ is finite or $\rho(f(X)) = r$ for all total computable selection functions f. If X is μ_r-computably random, then it is r-Church stochastic.

A set X is r-MWC stochastic if $f(X)$ is finite or $\rho(f(X)) = r$ for all partial computable selection functions f. If X is μ_r-ML random, then it is r-MWC stochastic.

X is r-KL stochastic if $f(X)$ is finite or $\rho(f(X)) = r$ for all non-monotonic computable selection functions. If X is KL-random, then it is r-KL stochastic.

Injection Stochasticity

A special case of KL stochasticity is injection stochasticity, which is stochasticity with respect to non-monotonic selection functions which ignore the input. (I.e., uniform KL stochasticity.)

Astor proved that r-injection stochasticity corresponds with intrinsic density r.

Definition

The absolute upper density of X is

$$\overline{P}(X) = \sup_{\pi}\{\overline{\rho}(\pi(X)) : \pi \text{ a computable permutation}\}$$

The absolute lower density, $\underline{P}(X)$, is defined similarly for the lim inf. If these are equal, we denote the quantity by $P(X)$ and call it the intrinsic density of X.

Intrinsic Density and Randomness

If X is μ_r-ML random, then it has intrinsic density r. Is the converse true?

The answer is no. It is not hard to show that if A has intrinsic density $\frac{1}{2}$, then $A \oplus A$ has intrinsic density $\frac{1}{2}$ as well. However, $A \oplus A$ is not random by Van Lambalgen's Theorem, which says that $A \oplus B$ is only random if A and B are relatively random to each other.

Separating Randomness and Stochasticity

While this shows that there are sets which have intrinsic density but are not random, it is a structural fact. If A is random, $A \oplus A$ can still trivially compute A, and therefore can compute a random. We have not shown any difference in computational properties between the two notions.

This will be our goal. We shall prove that, for almost all r, there is an r-computable set of intrinsic density r. As a corollary, this set will not be able to compute any μ_r-random set. To do this, we first need to develop some machinery.

The Into Operation

Definition

Given two sets

$$A = \{a_0 < a_1 < a_2 < \dots\}$$

and

$$B = \{b_0 < b_1 < b_2 < \dots\}$$

we define the set $B \triangleright A$, or "B into A," to be

$$\{a_{b_0} < a_{b_1} < a_{b_2} < \dots\}$$

As an example: If E is the set of even numbers and T is the set of multiples of three, then $E \triangleright T$ is the set of multiples of six.

Into and Asymptotic Density

Lemma

$\rho(B \triangleright A) = \rho(B)\rho(A)$

Proof Sketch.

We will be able to estimate the limsup for $B \triangleright A$ with

$$\limsup_{n\to\infty} \frac{n+1}{a_{b_n}+1} \cdot \frac{b_n+1}{b_n+1} \leq (\limsup_{n\to\infty} \frac{b_n+1}{a_{b_n}+1})(\limsup_{n\to\infty} \frac{n+1}{b_n+1})$$

The latter term will be the limsup for B, and the former will be no greater than the limsup for A. The liminf will be similar, and as both B and A have density we are done. $\square$

$\mathtt{Into}$ and Intrinsic Density

The following theorem is central to our argument. We shall use it to combine sets and manipulate intrinsic density.

Theorem

If A has intrinsic density α and B has intrinsic density β relative to A, then $B \triangleright A$ has intrinsic density $\alpha\beta$.

To prove this, we need to introduce another operation.

The `Within` Operation

Definition

Given two sets

$$A = \{a_0 < a_1 < a_2 < \dots\}$$

and

$$B = \{b_0 < b_1 < b_2 < \dots\}$$

we define the set $B \lhd A$, or "B within A," to be

$$\{n : a_n \in B\}$$

In other words, $B \cap A \subseteq A$, so there is some set X such that $X \rhd A$. We use $B \lhd A$ to represent this set X.

Basic Properties

- $A = A \rhd \omega$
- $A = \omega \rhd A$
- $(B \rhd A) \sqcup (\overline{B} \rhd A) = A$
- $\rhd$ is associative
- $\omega = A \lhd A$

- $(B \lhd A) \sqcup (\overline{B} \lhd A) = \omega$
- If $B \subseteq A$, $(B \lhd A) \rhd A = A \cap B$.
- $\lhd$ is not associative
- $(B \rhd A) \lhd A = B$
- $A \oplus B = (A \rhd E) \sqcup (B \rhd O)$

A Set Calculus

In proving theorems using these operations, we often use technical lemmas about their behavior which say nothing about stochasticity or randomness.

Lemma

For any sets A, B, C:

- $\rho(B \triangleright A) = \rho(B)\rho(A)$.
- $(A \triangleleft C) \triangleleft (B \triangleleft C) = A \triangleleft (B \cap C)$.
- $(A \triangleleft C) \triangleleft (B \triangleleft C) = (A \triangleleft B) \triangleleft (C \triangleleft B)$.
- *If $C \cap E$ is infinite and coinfinite and*

$$\rho((A \triangleright E) \triangleleft (C \cap E)) = \rho((B \triangleright \overline{E}) \triangleleft (C \cap \overline{E})) = r$$

then $\rho((A \oplus B) \triangleleft C) = r$

Within and Intrinsic Density

Theorem

If C is computable and $P(A) = \alpha$, $P(A \triangleleft C) = \alpha$.

The proof technique for this result is used to prove the main `Into` theorem.

Back to the `Into` Theorem

Theorem

If A has intrinsic density α and B has intrinsic density β relative to A, then $B \triangleright A$ has intrinsic density $\alpha\beta$.

Proof of Theorem

Proof.

Suppose not. Then there is a computable permutation π such that $\rho(\pi(B \triangleright A)) \neq \alpha\beta$.

Define an A-computable permutation f such that $f(B \triangleright A) = B$ modulo a set of density 0 and an A-computable permutation g such that $g(\pi(B \triangleright A)) = \pi(B \triangleright A) \triangleleft \pi(A)$ modulo a set of density 0. Then $\rho(g(\pi(f^{-1}(B)))) = \beta$, so by the A-intrinsic density of B, $\rho(\pi(B \triangleright A) \triangleleft \pi(A)) = \beta$.

However, by the asymptotic density theorem for `Into` and the fact that $P(A) = \alpha$,

$$\rho(\pi(B \triangleright A)) = \rho((\pi(B \triangleright A) \triangleleft \pi(A)) \triangleright \pi(A)) = \rho(\pi(B \triangleright A) \triangleleft \pi(A))\rho(\pi(A)) = \alpha\beta$$

This is a contradiction. $\square$

Intersections

Corollary

If A has intrinsic density α and B has intrinsic density β relative to A, then $A \cap B$ has intrinsic density $\alpha\beta$.

Proof.

By the relativized form of the `Within` theorem, $B \triangleleft A$ has intrinsic density β relative to A. By the `Into` theorem, $A \cap B = (B \triangleleft A) \triangleright A$ has intrinsic density $\alpha\beta$. $\square$

Unions

We shall construct sets using the `Into` theorem, then combine them using disjoint unions.

Theorem (Essentially Jockusch and Schupp, 2012)

Suppose $\{S_i\}_{i\in\mathbb{N}}$ *is a countable sequence of sets. If all of the following occur:*

- *The* S_i*'s are disjoint*
- S_i *has intrinsic density for all* i
- *the limit of the density of the tail of this sequence goes to* 0 *as* i *goes to infinity*

then the union has defined intrinsic density and it is the sum of the densities of the S_i*'s.*

Powers of Two

Theorem (Van Lambalgen, 1990)

Any set random with respect to $\mu_{\frac{1}{2}}$ can be decomposed into countably many sets which are random with respect to $\mu_{\frac{1}{2}}$ relative to any combination of the others.

This is essentially verifying the intuition that random sets are the output of countably many independent Bernoulli variables.

Theorem

There is a countable, disjoint sequence of sets $\{A_i\}_{i\in\omega}$ such that A_i has intrinsic density $\frac{1}{2^{i+1}}$. Furthermore, this satisfies the requirements of Jockusch and Schupp's result.

Proof Sketch.

Let X be 1-Random. Then by Van Lambalgen's theorem and the fact that 1-Randoms have intrinsic density $\frac{1}{2}$, we have countably many sets X_n all with intrinsic density relative to any combination of the rest. Then define B_0 to be all of the naturals, $A_n = \overline{X_n} \triangleright B_n$, and $B_{n+1} = X_n \triangleright B_n$. $\square$

Avoiding Randomness

Theorem

If r is random with respect to $\mu_{\frac{1}{2}}$, then r computes a set of intrinsic density r.

Proof.

Let r be random with respect to $\mu_{\frac{1}{2}}$ and let B_r be the set corresponding to its binary expansion to avoid confusion. We use B_r in place of X to construct the sequence from the previous theorem.

Then by the theorem of Jockusch and Schupp, $A = \bigcup_{n \in B_r} A_n$ will have intrinsic density the sum of the densities of the A_n's for $n \in B_r$. However, as B_r is the binary expansion of r and each A_n has intrinsic density $\frac{1}{2^{n+1}}$, these sum to r, completing the proof. $\square$

Note that no μ_r-random set can be r-computable, so this set cannot compute any μ_r-random set.

MWC and Church Stochasticity

What about other notions of stochasticity? It is natural to ask if the above techniques can be used to provide a similar separation between randomness and other notions of stochasticity.

However, there are some key structural differences between MWC and Church stochasticity and injection stochasticity which will cause the above argument to fail. We will state the results in terms of MWC stochasticity, but they will apply to Church stochasticity as well.

Differences in Stochasticity

Lemma

If A is MWC stochastic for some real other than 1, then $A \oplus A$ is not MWC stochastic.

Lemma

There exist disjoint sets A and B such that both are 0-MWC stochastic, but $A \sqcup B$ is not MWC stochastic.

Lemma

(Bienvenu) There exist disjoint sets A and B such that both are $\frac{1}{2}$-MWC stochastic, but $A \sqcup B$ is not MWC stochastic.

Similarities in Stochasticity

Theorem

If A is r-MWC stochastic and C is computable, then $A \triangleleft C$ is r-MWC stochastic.

Theorem

If A is α-MWC stochastic relative to B and B is β-MWC stochastic relative to A, then $B \triangleright A$ is $\alpha\beta$-MWC stochastic.

This second theorem looks similar to the `Into` theorem for intrinsic density. However, notice that there is an extra relativization requirement on A. It is unknown if this is necessary.

Theorem

If A is α-MWC stochastic relative to B and B is β-MWC stochastic relative to A, then $A \cap B$ is $\alpha\beta$-MWC stochastic.

Unions

Theorem
If A is α-MWC stochastic relative to B, and B is β-MWC stochastic relative to A, then $A \cup B$ is $\alpha + \beta - \alpha\beta$-MWC stochastic.

Theorem
If A is α-MWC stochastic relative to B, and B is β-MWC stochastic relative to A, then $A \sqcup (B \triangleright \overline{A})$ is $\alpha + \beta - \alpha\beta$-MWC stochastic.

Constructing MWC stochastic sets

Theorem

Every $\mu_{\frac{1}{2}}$-random set X computes a set of r-MWC stochasticity, where r is any real in the unit interval equal to a finite sum of powers of 2.

Proof.

We construct A_n and B_n from X as in the intrinsic density case. Van Lambalgen's Theorem ensures we have the relativization necessary even for the additional requirements. Then we verify that any finite union of the A_n's is of the form necessary to apply the second union theorem. $\square$

Some Open Questions

Question

For r nonrandom, is there an intrinsic density r set which cannot compute a μ_r-random set?

Question

Given r, is there an r-MWC-stochastic set which cannot compute a μ_r-random set?

Question

Can we generalize the `Into` *and* `Within` *theorems to work for random sets?*