A mathematical theory of true randomness

Alex Simpson

Faculty of Mathematics and Physics
University of Ljubljana, Slovenia

Seminar at UNISA Department of Decision Sciences
19th and 26th January 2023

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 731143

(Previously supported by a grant from the John Templeton Foundation 2013–2014.)

A mathematical theory of true randomness

Part 1

Motivation and axioms

A hierarchy of randomness notions

- Pseudo randomness (mainstream mathematics, computational complexity)

  Sieve methods in number theory, Szemerédi regularity lemma, expander graphs, pseudo-random-number generators, ...
  [Tao, Maynard, Szemerédi, Wigderson, ...]

- Algorithmic randomness (computability theory)

  Kolmogorov complexity, Martin-Löf statistical tests, Chaitin's Ω, Schnorr martingales, ...

- Set-theoretic randomness (set theory)

  Solovay random reals

- True randomness (physics? the Platonic universe!)

  The topic we address!

Prologue

Let $r, s \in \{0,1\}^\omega$ be two sequences generated independently by repeated (independent) tosses of a fair coin.

Consider the following statements relating r to probability 1 sets.

$$r \in \{0,1\}^\omega - \{r\} \qquad r \in \{0,1\}^\omega - \{0^\omega\} \qquad r \in \{0,1\}^\omega - \{s\}$$

The first is a trivial mathematical falsehood. The other two are facts of empirical experience, but are not normally considered as mathematical truths.

Including a primitive independence relation in the mathematical universe allows us to define randomness and to turn statements 2 and 3 into mathematical truths reflecting intrinsic properties of randomness.

A closely related programme was followed by Michiel van Lambalgen [JSL 1990 & 1992]. We discuss his work at the end.

Intuitions for independence

Intuitively, $x \perp\!\!\!\perp y$ means that x and y could be obtained respectively by two different mathematicians who tap into two independent random sources.

E.g., independently tossing a fair coin and a die:

$$0011011110010100010000\ldots \;\perp\!\!\!\perp\; 3266125134162511555412\ldots$$

Two sequences obtained from the above, by setting even positions to 1 in the first, and applying δ_6 to the second.

$$0111011111010101111010\ldots \;\perp\!\!\!\perp\; 0011000000001000000000\ldots$$

Anything in the universe with anything definable:

$$x \;\perp\!\!\!\perp\; \pi$$

Using independence, we give a definition of randomness.

Define $r \in \{0,1\}^\omega$ to be random if:

> for every probability 1 subset $X \subseteq \{0,1\}^\omega$ that is independent of r, we have $r \in X$.

In symbols:

$$\mathrm{Ran}(r) \iff \forall X \subseteq \{0,1\}^\omega.\;\; \lambda(X) = 1 \text{ and } X \perp\!\!\!\perp r \text{ implies } r \in X$$

where λ is the uniform probability measure on $\{0,1\}^\omega$.

Let $r, s \in \{0,1\}^\omega$ be two independent random sequences; that is, $\mathsf{Ran}(r)$, $\mathsf{Ran}(s)$ and $s \perp\!\!\!\perp r$. Then

$$\{0,1\}^\omega - \{0^\omega\} \perp\!\!\!\perp r \qquad\qquad \{0,1\}^\omega - \{s\} \perp\!\!\!\perp r$$

(applying the principle: $x \perp\!\!\!\perp y$ and f definable $\implies$ $f(x) \perp\!\!\!\perp y$).

So we indeed obtain:

$$r \in \{0,1\}^\omega - \{0^\omega\} \qquad\qquad r \in \{0,1\}^\omega - \{s\}$$

In contrast, since $r \notin \{0,1\}^\omega - \{r\}$, it follows that $\{0,1\}^\omega - \{r\} \not\perp\!\!\!\perp r$, whence $r \not\perp\!\!\!\perp r$.

For every random r, it holds that $r \not\perp\!\!\!\perp r$.

Axioms for independence

Axiom I1. $x \perp\!\!\!\perp 0$

Axiom I2. $x \perp\!\!\!\perp y$ implies $y \perp\!\!\!\perp x$

Axiom I3. For $y \in \{0,1\}^{\omega}$, if $(x,y) \perp\!\!\!\perp z$ and $x \perp\!\!\!\perp y$ then $x \perp\!\!\!\perp (y,z)$

Axiom I4.

$$(\exists y\ \phi(x,y)) \to \forall z\ (x \perp\!\!\!\perp z \to \exists y'\ (y' \perp\!\!\!\perp z\ \wedge\ \phi(x,y')))$$

(where property $\phi(x,y)$ depends only on x, y)

These axioms will be subsumed later by axioms for a more general conditional independence relation.

Determined and uncertain elements

We say x is determined if $x \perp\!\!\!\perp x$.
We say x is uncertain if $x \not\perp\!\!\!\perp x$.

Lemma A If x is definable (by a formula $\phi(z)$ s.t. $\exists! z\, \phi(z)$) then x is determined.

Lemma B If x is determined then $y \perp\!\!\!\perp x$, for all y.

Proof Suppose x is such that there exists y with $y \not\perp\!\!\!\perp x$. We show that x is uncertain.

By I4, for any z with $x \perp\!\!\!\perp z$, there exists y with $y \perp\!\!\!\perp z$ and $y \not\perp\!\!\!\perp x$.

Setting $z = x$, we have that $x \perp\!\!\!\perp x$ implies there exists y with $y \perp\!\!\!\perp x$ and $y \not\perp\!\!\!\perp x$, which is a contradiction.

So $x \not\perp\!\!\!\perp x$ as required. □

Lemma C Suppose $x \in X$ with $x \perp\!\!\!\perp X$. For any y, there exists $x' \in X$ with $x' \perp\!\!\!\perp y$.

Proof Suppose $x \in X$ and $x \perp\!\!\!\perp X$.

Suppose, for contradiction, that there exists y for which there is no $x' \in X$ with $x' \perp\!\!\!\perp y$

Since $X \perp\!\!\!\perp x$, by I4, there exists y such that $y \perp\!\!\!\perp x$ and there is no $x' \in X$ with $x' \perp\!\!\!\perp y$

But $x \in X$ and $x \perp\!\!\!\perp y$; a contradiction! □

Failure of AC

Theorem [cf. van Lambalgen] If there exists an uncertain $r \in \{0,1\}^\omega$ then the set $\{0,1\}^\omega$ has no well-ordering.

Proof Let $\mathrm{Unc} \subseteq \{0,1\}^\omega$ be the subset of uncertain sequences. By assumption there exists $r \in \mathrm{Unc}$. Since Unc is definable, we have $r \perp\!\!\!\perp \mathrm{Unc}$. So, by Lemma C, for any y, there exists $r' \in \mathrm{Unc}$ such that $r' \perp\!\!\!\perp y$.

In particular, for any well-order $\prec$ on $\{0,1\}^\omega$, there exists $s \in \mathrm{Unc}$ such that $s \perp\!\!\!\perp \prec$, hence there is a smallest such s under $\prec$. This gives a definable function mapping any well-order $\prec$ of $\{0,1\}^\omega$ to the $\prec$-smallest $s_\prec$ such that $s_\prec \in \mathrm{Unc}$ and $s_\prec \perp\!\!\!\perp \prec$.

Now suppose for contradiction that there exists a well-order $\prec'$ on $\{0,1\}^\omega$. We have $s_{\prec'} \in \mathrm{Unc}$ and $\prec' \perp\!\!\!\perp s_{\prec'}$. By I4, independence is preserved under application of the function $\prec \mapsto s_\prec$. Hence $s_{\prec'} \perp\!\!\!\perp s_{\prec'}$, which contradicts $s_{\prec'} \in \mathrm{Unc}$. □

We take ZF+DC as our ambient set theory, in the language with $\in, \perp\!\!\!\perp$ as primitive relations and with Axioms I1–I4 added.

The relaxation of AC to DC allows us to assume a probability measure $\lambda\colon \mathcal{P}(\{0,1\}^\omega) \to [0,1]$ defined on the full powerset.

Every $w \in \{0,1\}^*$ determines a cylinder set $\langle w \rangle \subseteq \{0,1\}^\omega$ by $\langle w \rangle := \{s \in \{0,1\}^\omega \mid s\restriction_{|w|} = w\}$. The cylinder sets form a basis for the product topology on $\{0,1\}^\omega$ (Cantor space). Every open set arises as a disjoint union of cylinders, and finite (disjoint) unions of cylinders are exactly the clopen subsets of $\{0,1\}^\omega$.

Definition A probability measure $\lambda\colon \mathcal{P}(\{0,1\}^\omega) \to [0,1]$ is near Borel if (the two statements are equivalent):

- for any $X \subseteq \{0,1\}^\omega$ with there exists Borel $B \subseteq \{0,1\}^\omega$ such that $\lambda(X \Delta B) = 0$; or equivalently,
- for any $X \subseteq \{0,1\}^\omega$ and $\epsilon > 0$, there exists clopen $A \subseteq \{0,1\}^\omega$ s.t. $\lambda(X \Delta A) < \epsilon$.

Axiom of near-Borel measurability

Axiom of near-Borel measurability

There exists a near-Borel measure $\lambda\colon \mathcal{P}(\{0,1\}^\omega) \to [0,1]$ satisfying: for every $w \in \{0,1\}^*$, $\lambda\langle w\rangle = 2^{-|w|}$.

Remarks

- The existence of a probability measure λ on the full powerset $\mathcal{P}(\{0,1\}^\omega)$ is a mathematical idealisation.
- The near-Borel condition, especially in its approximation form, tempers the idealisation with a connection to meaningful sets.
- The near-Borel condition is weaker than asking for every subset of $\{0,1\}^\omega$ to be Lebesgue measurable.
- λ is an extension of Lebesgue measure.

Randomness and statistical testability

Definition (randomness) We say that $r \in \{0,1\}^\omega$ is random (notation $\mathrm{Ran}(r)$) if (the two statements are equivalent):

- for any $X \subseteq \{0,1\}^\omega$ with $\lambda(X) = 1$, if $X \perp\!\!\!\perp r$ then $r \in X$;
- for any $X \subseteq \{0,1\}^\omega$, if $X \perp\!\!\!\perp r$ and $r \in X$ then $\lambda(X) > 0$.

A statistical non-randomness test is a sequence $(U_n)_{n \geqslant 0}$ of open subsets of $\{0,1\}^\omega$ such that $\lim_{n\to\infty} \lambda(U_n) = 0$. We say that $s \in \{0,1\}^\omega$ satisfies the test if $s \in \bigcap_n U_n$.

Proposition If $s \in \{0,1\}^\omega$ satisfies a statistical non-randomness test $(U_n)_{n \geqslant 0}$ for which $(U_n)_{n \geqslant 0} \perp\!\!\!\perp s$ then s is non-random.

Borel randomness

Definition (Borel randomness)

We say that $r \in \{0,1\}^\omega$ is Borel random if (all statements are equivalent):

- for any Borel $B \subseteq \{0,1\}^\omega$ with $\lambda(B) = 1$, if $B \perp\!\!\!\perp r$ then $r \in B$;
- for any F_σ-set $A \subseteq \{0,1\}^\omega$ with $\lambda(A) = 1$, if $A \perp\!\!\!\perp r$ then $r \in A$;
- for any statistical non-randomness test $(U_n)_{n \geqslant 0}$, if $(U_n)_{n \geqslant 0} \perp\!\!\!\perp r$ then r does not satisfy $(U_n)_{n \geqslant 0}$.

Proposition Randomness implies Borel randomness.

Axiom of statistical testability

Axiom of statistical testability

The following statements (which are equivalent) hold.

- If $s \in \{0,1\}^\omega$ is non-random then it satisfies some statistical non-randomness test $(U_n)_{n \geqslant 0}$ such that $(U_n)_{n \geqslant 0} \perp\!\!\!\perp s$.
- Borel randomness implies randomness.

Remarks

- The definition of randomness in terms of arbitrary subsets $X \subseteq \{0,1\}^\omega$ is a mathematical idealisation.
- The statistical testability axiom tempers the idealisation with a characterisation in more practical terms.

The existence of randomness

Axiom (Existence of enough random elements)

The following statements (which are all equivalent) hold.

1. For any closed $A \subseteq \{0,1\}^\omega$ with $\lambda(A) > 0$, there exists $r \in A$ such that $\mathrm{Ran}(r)$ and $A \perp\!\!\!\perp r$.
2. For any Borel $B \subseteq \{0,1\}^\omega$ with $\lambda(B) > 0$, there exists $r \in B$ such that $\mathrm{Ran}(r)$ and $B \perp\!\!\!\perp r$.
3. For any $X \subseteq \{0,1\}^\omega$ with $\lambda(X) > 0$, there exists $r \in X$ such that $\mathrm{Ran}(r)$ and $X \perp\!\!\!\perp r$.
4. For any z and $X \subseteq \{0,1\}^\omega$ with $\lambda(X) > 0$, there exists $r \in X$ such that $\mathrm{Ran}(r)$ and $r \perp\!\!\!\perp z$.

Proof that $2 \Rightarrow 3$

2. For any Borel $B \subseteq \{0,1\}^\omega$ with $\lambda(B) > 0$, there exists $r \in B$ such that $\mathrm{Ran}(r)$ and $B \perp\!\!\!\perp r$.
3. For any $X \subseteq \{0,1\}^\omega$ with $\lambda(X) > 0$, there exists $r \in X$ such that $\mathrm{Ran}(r)$ and $X \perp\!\!\!\perp r$.

Let $X \subseteq \{0,1\}^\omega$ be such that $\lambda(X) > 0$.

By the near-Borel property, there exists Borel $B \subseteq \{0,1\}^\omega$ such that $\lambda(B \Delta X) = 0$, so $\lambda(B) = \lambda(X) > 0$.

By 2, there exists $r \in B$ such that $\mathrm{Ran}(r)$ and $B \perp\!\!\!\perp r$. Applying Lemma C to the set $\{s \in B \mid \mathrm{Ran}(s)\}$, it follows that there exists random $r \in B$ with $(X, B) \perp\!\!\!\perp r$, hence also $X \perp\!\!\!\perp r$.

It remains to show that $r \in X$. If not, we have $r \in B - X$. Since $(X, B) \perp\!\!\!\perp r$, also $B - X \perp\!\!\!\perp r$. Because r is random, the conjunction $B - X \perp\!\!\!\perp r$ and $r \in B - X$ contradicts that $\lambda(B - X) = 0$. □

A mathematical theory of true randomness

Part 2

Relative randomness and consequences of the axioms

Review of Part 1

- Axiomatic setting ZF+DC together with an independence relation $\perp\!\!\!\perp$ satisfying axioms I1–I5.
- Axiom There exists a near Borel probability measure $\lambda\colon \mathcal{P}(\{0,1\}^\omega) \to [0,1]$ extending the uniform Borel measure.
- Definitions of random and Borel random element $r \in \{0,1\}^\omega$:
  - for any $X \subseteq \{0,1\}^\omega$ with $\lambda(X) = 1$, if $X \perp\!\!\!\perp r$ then $r \in X$
  - for any Borel $B \subseteq \{0,1\}^\omega$ with $\lambda(B) = 1$, if $B \perp\!\!\!\perp r$ then $r \in B$
- Axiom (testability) Borel random implies random
- Axiom (enough randomness) For any $X \subseteq \{0,1\}^\omega$ with $\lambda(X) > 0$ and any z, there exists random $r \in X$ with $r \perp\!\!\!\perp z$.

Null sets

A subset $X \subseteq \{0,1\}^\omega$ is null if $\lambda(X) = 0$.

- If X has Borel outer measure 0 then it is null.
- If X is null then it has Borel inner measure 0.

Neither of the above implications reverses unless all subsets are Lebesgue measurable.

Null sets have a characterisation in terms of random elements.

Proposition The following are equivalent, for any $X \subseteq \{0,1\}^\omega$.

1. $\lambda(X) = 0$.
2. There is no random $r \in X$ with $r \perp\!\!\!\perp X$.

Proof $1 \Rightarrow 2:$ by definition of randomness.

$2 \Rightarrow 1:$ by the existence of enough random points. □

Proposition Suppose λ, λ' are two near-Borel probability measures assigning measure $2^{-|w|}$ to every cylinder $\langle w \rangle$. Suppose also that the corresponding λ- and λ'-induced randomness notions satisfy the testability and enough randomness axioms. Then $\lambda = \lambda'$.

Proof λ and λ' agree on Borel sets. So Borel randomness with respect to λ and λ' coincide, hence the same for randomness. By the characterisation of null sets, it follows that a set is null with respect to λ if and only if it is null with respect to λ'.

Let $X \subseteq \{0,1\}^\omega$ be any subset. By the near-Borel property, there exists Borel $B \subseteq \{0,1\}^\omega$ such that $\lambda(X \Delta B) = 0$. By the coincidence of null sets, $\lambda'(X \Delta B) = 0$. So we have,

$$\lambda(X) \;=\; \lambda(B) \;=\; \lambda'(B) \;=\; \lambda'(X) \;.$$

□

Lemma Every ordinal α is determined (i.e., $\alpha \perp\!\!\!\perp \alpha$).

Proof Suppose not. Then "the smallest uncertain ordinal" defines an ordinal β. Since β is definable, it is determined! □

Proposition Suppose $(X_{\alpha'})_{\alpha'<\alpha}$ is a family of null subsets of $\{0,1\}^\omega$. Then $\bigcup_{\alpha'<\alpha} X_{\alpha'}$ is also null.

Proof Suppose $\lambda(\bigcup_{\alpha'<\alpha} X_{\alpha'}) > 0$. By enough randomness, there exists random $r \in \bigcup_{\alpha'<\alpha} X_{\alpha'}$ with $r \perp\!\!\!\perp (X_{\alpha'})_{\alpha'<\alpha}$. Let β be such that $r \in X_\beta$. Since β is determined, we have $r \perp\!\!\!\perp \beta, (X_{\alpha'})_{\alpha'<\alpha}$, whence $r \perp\!\!\!\perp X_\beta$ by (I4). So we have random $r \in X_\beta$ such that $r \perp\!\!\!\perp X_\beta$, contradicting that X_β is null, □

Corollary λ is $\aleph$-additive; i.e., for any aleph $\aleph_\alpha$ and family $(X_{\alpha'})_{\alpha'<\aleph_\alpha}$ of pairwise disjoint subsets of $\{0,1\}^\omega$,

$$\lambda\left(\bigcup_{\alpha'<\aleph_\alpha} X_\alpha\right) = \sum_{\alpha'<\aleph_\alpha} \lambda(X_{\alpha'}) \ .$$

$$
\begin{aligned}
\mathsf{Ran} &:= \{s \in \{0,1\}^\omega \mid \mathsf{Ran}(s)\} \\
\mathsf{Ind}_t &:= \{s \in \{0,1\}^\omega \mid s \perp\!\!\!\perp t\}
\end{aligned}
$$

Proposition $\lambda(\mathsf{Ran}) = 1$

Proof The complement $\lambda(\{0,1\}^\omega - \mathsf{Ran})$ contains no random elements so is null. □

Proposition $\lambda(\mathsf{Ind}_t) = 1$

Proof Suppose $\lambda(\mathsf{Ind}_t) < 1$. Then $\lambda(\{0,1\}^\omega - \mathsf{Ind}_t) > 0$, so (by existence of enough random elements) $\{0,1\}^\omega - \mathsf{Ind}_t$ contains a random element s with $s \perp\!\!\!\perp t$, a contradiction. □

Two notions of relative randomness

- Generative relative randomness.

  r is random and generated independently from z.

  $\mathrm{Ran}(r)$ and $r \perp\!\!\!\perp z$

- Observable relative randomness.

  r satisfies all probability 1 properties that are independent of r in the presence of t.

  $\mathrm{Ran}(r \mid t)$

To define the latter, we replace our independence relation $x \perp\!\!\!\perp y$ with a more general conditional independence relation $x \perp\!\!\!\perp y \mid z$.

Conditional independence

Intuitively, $x \perp\!\!\!\perp y \mid z$ means that x and y could be obtained respectively by two different mathematicians, who tap into two independent random sources, but who have shared knowledge of z.

E.g., three sequences obtained by independently tossing fair coins:

$$0011011110010\ldots \;\perp\!\!\!\perp\; 1000100111100\ldots \;\mid\; 0111101001011\ldots$$

Independence conditional on anything definable:

$$0011011110010\ldots \;\perp\!\!\!\perp\; 1000100111100\ldots \;\mid\; 0$$

is equivalent to unconditional independence:

$$0011011110010\ldots \;\perp\!\!\!\perp\; 1000100111100\ldots$$

There is no monotonicity with respect to conditioning.

We do have:

$$0011011110010\ldots \perp\!\!\!\perp 1000100111100\ldots$$

but we do not have:

$$0011011110010\ldots \perp\!\!\!\perp 1000100111100\ldots \mid 1011111001110\ldots$$

since each sequence can be obtained from the other two by xor.

We do not have:

$$0011011110010\ldots \perp\!\!\!\perp 1100100001101\ldots$$

since the sequences are bitwise complements, but we do have:

$$0011011110010\ldots \perp\!\!\!\perp 1100100001101\ldots \mid 1100100001101\ldots$$

Axioms for conditional independence

We axiomatise a conditional independence relation $x \perp\!\!\!\perp y \mid z$, where we require that $z \in (\{0,1\}^\omega)^n$ for $n \geqslant 0$.

Axiom CI1. $x \perp\!\!\!\perp z \mid z$

Axiom CI2. $x \perp\!\!\!\perp y \mid z$ implies $y \perp\!\!\!\perp x \mid z$

Axiom CI3. If $x \perp\!\!\!\perp y \mid z, w$ and $x \perp\!\!\!\perp z \mid w$ then $x \perp\!\!\!\perp y, z \mid w$

Axiom CI4. If $x \perp\!\!\!\perp y, z \mid w$ then $x \perp\!\!\!\perp y \mid z, w$

Axiom CI5.

$$(\exists y \ \phi(x,y,z)) \rightarrow \forall w \ (x \perp\!\!\!\perp w \mid z \rightarrow \exists y' \ (y' \perp\!\!\!\perp w \mid z \wedge \phi(x,y',z)))$$

(where property $\phi(x,y,z)$ depends only on x, y, z)

(Influenced by axiomatizations proposed in different contexts by Dawid, by Spohn and by Geiger, Paz & Pearl.)

Relative randomness via observability

Definition (relative randomness) We say that $r \in \{0,1\}^\omega$ is random relative to $t \in (\{0,1\}^\omega)^n$ (notation $\mathrm{Ran}(r \mid t)$) if (the two statements are equivalent):

- for any $X \subseteq \{0,1\}^\omega$ with $\lambda(X) = 1$, if $X \perp\!\!\!\perp r \mid t$ then $r \in X$;
- for any $X \subseteq \{0,1\}^\omega$, if $X \perp\!\!\!\perp r \mid t$ and $r \in X$ then $\lambda(X) > 0$.

Coincidence of relative randomness notions

Theorem $\mathrm{Ran}(r \mid t)$ iff both $\mathrm{Ran}(r)$ and $r \perp\!\!\!\perp t$.

Proof

$\Longleftarrow$ Suppose $\mathrm{Ran}(r)$ and $r \perp\!\!\!\perp t$. Let $X \subseteq \{0,1\}^\omega$ be such that $\lambda(X) = 1$ and $X \perp\!\!\!\perp r \mid t$. We need to show that $r \in X$.

We have $X, t \perp\!\!\!\perp r$ by CI3, hence $X \perp\!\!\!\perp r$. Since $\mathrm{Ran}(r)$ and $\lambda(X) = 1$, indeed $r \in X$.

$\Longrightarrow$ Suppose $\mathrm{Ran}(r \mid t)$. We need to show $\mathrm{Ran}(r)$ and $r \perp\!\!\!\perp t$.

Since $\mathrm{Ran} := \{s \in \{0,1\}^\omega \mid \mathrm{Ran}(s)\}$ is definable, we have $\mathrm{Ran} \perp\!\!\!\perp r \mid t$. As $\lambda(\mathrm{Ran}) = 1$ and $\mathrm{Ran}(r \mid t)$, it follows that $r \in \mathrm{Ran}$; i.e., $\mathrm{Ran}(r)$.

Similarly, since $\mathrm{Ind}_t := \{s \in \{0,1\}^\omega \mid s \perp\!\!\!\perp t\}$ is definable from t, we have $\mathrm{Ind}_t \perp\!\!\!\perp r \mid t$. As $\lambda(\mathrm{Ind}_t) = 1$ and $\mathrm{Ran}(r \mid t)$, it follows that $r \in \mathrm{Ind}_t$; i.e., $r \perp\!\!\!\perp t$. □

Axioms for relative randomness

A sequence $r \in \{0,1\}^\omega$ is Borel random relative to t if for every Borel $B \subseteq \{0,1\}^\omega$ with $\lambda(B) = 1$, if $B \perp\!\!\!\perp r \mid t$ then $r \in B$;

Testability axiom (full relative version) Relative Borel randomness implies relative randomness.

Proposition (Enough relative randomness)

For any z, t and any $X \subseteq \{0,1\}^\omega$ with $\lambda(X) > 0$, there exists $r \in X$ with $\mathrm{Ran}(r \mid t)$ and $r \perp\!\!\!\perp z \mid t$.

Proof

By enough randomness, there exists $r \in X$ with $\mathrm{Ran}(r)$ and $r \perp\!\!\!\perp z, t$. Since both $\mathrm{Ran}(r)$ and $r \perp\!\!\!\perp t$, we have $\mathrm{Ran}(r \mid t)$ by coincidence of relative randomness notions. Moreover $r \perp\!\!\!\perp z \mid t$ by (CI4). $\square$

Theorem. For Borel measurable $f\colon \{0,1\}^\omega \to \{0,1\}^\omega$, t.f.a.e.

1. f^{-1} preserves Borel nullsets.
2. f^{-1} preserves all nullsets.
3. $\mathrm{Ran}(r \mid f)$ implies $\mathrm{Ran}(f(r) \mid f)$.

   (N.b., f can be represented by an element of $\{0,1\}^\omega$.)

Proof of 1 $\Rightarrow$ 3. Suppose $\mathrm{Ran}(r \mid f)$.

Suppose B is Borel, $f(r) \in B$ and $B \perp\!\!\!\perp f(r) \mid f$.
By (CI5), $f^{-1}B \perp\!\!\!\perp f(r) \mid f$.
Since there exists s s.t. $\mathrm{Ran}(s \mid f)$ and $f(s) = f(r)$, it follows from (CI5) that there exists s s.t. $\mathrm{Ran}(s \mid f)$ and $f(s) = f(r)$ and $s \perp\!\!\!\perp f^{-1}B \mid f$.
As $s \in f^{-1}B$, we have $\lambda(f^{-1}B) > 0$ because $\mathrm{Ran}(r \mid f)$.
Since f^{-1} preserves nullsets, $\lambda(B) > 0$.

The above shows $f(r)$ is Borel random relative to f. Whence, by testability, $\mathrm{Ran}(r \mid f)$. □

Corollary. For Borel measurable $f\colon \{0,1\}^\omega \to \{0,1\}^\omega$, t.f.a.e.

1. f^{-1} preserves measure of Borel sets.
2. f^{-1} preserves measure of all subsets.

Proof of $1 \Rightarrow 2$. For any $X \subseteq \{0,1\}^\omega$, by the near-Borel property, there exists Borel B such that $\lambda(X \Delta B) = 0$. By the theorem, $\lambda((f^{-1}X)\Delta(f^{-1}B)) = \lambda(f^{-1}(X\Delta B)) = 0$. So:

$$\lambda(f^{-1}X) \ = \ \lambda(f^{-1}B) \ = \ \lambda(B) \ = \ \lambda(X) \ .$$

□

Corollary. The measure $\lambda\colon \mathcal{P}(\{0,1\}^\omega) \to [0,1]$ is translation invariant; i.e., for all $s \in \{0,1\}^\omega$ and $X \subseteq \{0,1\}^\omega$, we have $\lambda(X) = \lambda(s \oplus X)$ (where $\oplus$ is pointwise xor).

General probability measures

Let $\mu\colon \mathcal{P}(\{0,1\}^\omega) \to [0,1]$ be any powerset probability measure.

We cannot in general use:

$$\forall\, X \subseteq \{0,1\}^\omega.\ \ \mu(X) = 1 \text{ and } r \perp\!\!\!\perp X \text{ implies } r \in X$$

as the definition of the μ-randomness of $r \in X$ and simultaneously obtain enough μ-random elements in the sense that

$$\forall\, X \subseteq \{0,1\}^\omega.\ \ \mu(X) > 0 \text{ implies } \exists\ \mu\text{-random } r \in X \text{ s.t. } r \perp\!\!\!\perp X$$

Example: suppose $s \in \{0,1\}^\omega$ is (λ-)random and define $\mu := \delta_s$, where δ_s is the Dirac measure.

Then although $\mu(\{s\}) = 1$ and s is μ-random according to the above definition, we do not have $s \perp\!\!\!\perp \{s\}$.

The natural solution would be to use independence conditional on μ. But we can only condition by elements of $\{0,1\}^\omega$.

We instead condition on the Borel restriction $\mu_\mathcal{B}$ of μ,
which can indeed be represented as an element of $\{0,1\}^\omega$.

Define $r \in X$ to be μ-random (notation $\mathrm{Ran}_\mu(r)$) if:

$$\forall X \subseteq \{0,1\}^\omega.\;\; \mu(X) = 1 \;\text{ and }\; r \perp\!\!\!\perp X \mid \mu_\mathcal{B} \;\text{ implies }\; r \in X$$

Say that there are enough μ-random elements if

$$\forall X \subseteq \{0,1\}^\omega.\;\; \mu(X) > 0 \text{ implies } \exists\; \mu\text{-random } r \in X \text{ s.t. } r \perp\!\!\!\perp X \mid \mu_\mathcal{B}$$

The above definitions make good sense in situations in which $\mu_\mathcal{B}$ determines μ. This is the case if μ supports our three characteristic properties of well-behaved randomness.

Randomness supporting measures

Let $\mu\colon \mathcal{P}(\{0,1\}^\omega) \to [0,1]$ be a powerset probability measure.

μ is randomness supporting if the following three conditions hold.

- Near Borel

  μ is near Borel.

- Testable

  Borel μ-randomness implies μ-randomness

- Enough randomness

  There are enough μ-random elements.

Theorem Every Borel measure on $\{0,1\}^\omega$ extends to a unique randomness supporting powerset measure.

Further directions

A comprehensive theory of randomness-supporting measures

Preservation under pushforward; product measures and Fubini; interactions between randomness and stochastic processes.

Parallels with algorithmic randomness

Characterisations of randomness in terms of incompressibility and in terms of Martingales.

Foundational questions

Consistency?! Consistency with universal Lebesgue measurablility? Additional axioms, e.g., the axiom of statistical analysability:

> For every $s \in \{0,1\}^\omega$ there exists a determined probability measure μ on $\{0,1\}^\omega$ such that $\mathsf{Ran}_\mu(s)$.

Foundations for a synthetic probability theory

Summing up so far

We have extended set theory with conditional independence and used this to axiomatise randomness.

Philosophically, this builds predictive content into probability theory. ('Almost sure' is replaced with conditions under which genuine certainty applies.)

Technically, the approach leads to a theory of randomly supported probability measures, which is still at an early stage of development.

We now briefly discuss a potential model for our theory, and connections with previous work.

The random topos

The random topos is the topos of sheaves for the countable-cover (modulo a null set) Grothendieck topology on the monoid of null-set reflecting Borel-measurable endofunctions on $\{0,1\}^\omega$ with uniform Borel measure.

This is a boolean topos. It validates dependent choice.

I believe I can model the entire theory in this topos, but this is work in progress.

(I do not currently have a completed consistency proof.)

Dependence/independence logic

Dependence logic [Väänänen 2007] and independence logic [Grädel & Väänänen 2013] extend first-order logic with primitives expressing dependence and (conditional) independence.

The semantics is based on Hodges' team semantics for independence-friendly logic. However, the team semantics of dependence/independence logic does not validate classical logic!

In the random topos (and other related models), I use a sheaf semantics that is related to team semantics, but which does validate classical logic.

Algorithmic randomness

Question Can independence-based definitions of randomness be given in the context of algorithmic randomness?

An illustration of the sort of definition we have in mind

Define $s \perp\!\!\!\perp t$ for $s, t \in \{0,1\}^\omega$ to mean s and t have meet **o** in the partial order of Turing degrees.

Use an encoding of statistical non-randomness tests by sequences s, so that $s \mapsto T^s$ maps computable s to Martin-Löf tests.

Define r to be random if there is no s with $s \perp\!\!\!\perp r$ such that r satisfies T^s .

Does this or something similar give an interesting notion of randomness?

Randomness via independence *à la* van Lambalgen

van Lambalgen [JSL 1990 & 1992] also axiomatized properties of randomness based on a primitive relation of 'independence', and used his axioms to derive measure-theoretic consequences.

The approach of this talk has been heavily influenced by vL's work, and provides an alternative realisation of his programme.

The major technical difference is that van Lambalgen axiomatized a basic 'independence' relation $R(x, \vec{y})$, which expresses the relation $\mathrm{Ran}(x \mid \vec{y})$ in this talk. In his work, 'independence' is thus identified (one might say conflated) with relative randomness.

We use a neutral notion of independence and use this to define randomness. This is conceptually natural, and allows the smooth development of randomness for general probability measures.

Conclusions

We follow van Lambalgen in axiomatising randomness using a primitive notion of independence.

Where van Lambalgan identifies ‘independence’ with relative randomness, we instead axiomatise a neutral notion of independence, and use this to define randomness.

We believe our approach to be conceptually more perspicuous.

A technical advantage is that our approach accommodates randomness for general probability measures in a simple way.

There is potential for developing probability theory in our framework with the advantage that all sets are measurable.

The development and its consistency are work in progress!