Synthesising Random Variables

Alex Simpson

Institute for Mathematics, Physics and Mechanics (IMFM)
Faculty of Mathematics and Physics (FMF)
University of Ljubljana, Slovenia

Synthetic Mathematics, Logic-Affine Computation and Efficient Proof Systems
CIRM, Luminy, 9th September 2025

Synthetic probability theory

Goal: Provide a comprehensive set of axioms supporting the development the core definitions, constructions and results of probability theory in a simpler and more perspicuous way than the usual ZFC-based mathematical approach.

- The axioms should provide a mathematical framework capturing a mathematical idealisation of probability as it is experienced.
- Random variable should be a primitive notion with RVs axiomatised in terms of their interface (what one can do with them) rather than by means of a concrete set-theoretic implementation.

This is synthetic mathematics in the spirit of, e.g., synthetic differential geometry (Lawvere, Kock, Moerdijk & Reyes, ...), synthetic algebraic geometry (Kock, Blechschmidt, Coquand, Cherubini, ...), etc.

Not to be confused with

- synthetic probability theory meaning category-theoretic-based approaches to defining and reasoning about probabilistic maps (Markov kernels) using the machinery of Markov categories (Cho & Jacobs, Fritz, Perrone, ...).
- synthetic probability/measure theory meaning programming-language-based methods for defining and reasoning about (probability) measures (Staton).

Synthesising random variables

1. Synthesising an axiomatic theory of primitive RVs

   I shall present the axiomatisation by telling the story of its development, including some wrong turns.

2. Using the theory to synthesise individual RVs

   I shall illustrate the usefulness of the axioms for constructing random variables with interesting properties, for example how to define Brownian motion as a stochastic process.

Maxim: let the axioms be guided by a well-chosen model

Standard definition of random variable

A real-valued random variable is:

$$X : \Omega \to \mathbb{R}$$

where:

- the sample space Ω is a probability space (a set Ω with σ-algebra $\mathcal{E}$ and probability measure $\mathbf{P}_\Omega : \mathcal{E} \to [0,1]$); and
- X is a measurable function (for all Borel sets $B \subseteq \mathbb{R}$, $X^{-1}(B) \in \mathcal{E}$).

The presheaf of random variables

$$\mathrm{RV}(\mathbb{R})(\Omega) \;:=\; \{X : \Omega \to \mathbb{R} \mid X \text{ measurable}\}$$

For any measure-preserving $p : \Omega' \to \Omega$

$$\mathrm{RV}(\mathbb{R})(p) \;:=\; X \;\mapsto\; X \circ P \;:\; \mathrm{RV}(\mathbb{R})(\Omega) \to \mathrm{RV}(\mathbb{R})(\Omega')$$

Defines a presheaf

$$\mathrm{RV}(\mathbb{R}) \;:\; \mathbb{SBP}^{\mathrm{op}} \to \mathbf{Set}$$

($\mathbb{SBP}$ = standard Borel probability spaces with measure-preserving functions)

The sheaf of random variables (2013)

$$\mathrm{RV}(\mathbb{R})(\Omega) \; := \; \{X : \Omega \to \mathbb{R} \mid X \text{ measurable}\} \,/\, =_{\text{a.s.}}$$

For any measure-preserving $p : \Omega' \to \Omega$

$$\mathrm{RV}(\mathbb{R})(p) \; := \; [X] \mapsto [X \circ P] \; : \; \mathrm{RV}(\mathbb{R})(\Omega) \to \mathrm{RV}(\mathbb{R})(\Omega')$$

Defines an atomic sheaf

$$\mathrm{RV}(\mathbb{R}) \; : \; \mathbb{SBP}^{\mathrm{op}} \to \mathbf{Set}$$

($\mathbb{SBP}$ = standard Borel probability spaces with measure-preserving functions)

The category $\mathsf{Sh}(\mathbb{SBP})$

A well-chosen model?

The category $\mathsf{Sh}(\mathbb{SBP})$ of atomic sheaves is

- a boolean Grothendieck topos (so models classical higher-order logic),
- models dependent choice (DC), although the full axiom of choice (AC) fails,
- contains a canonical sheaf $\mathsf{RV}(A)$ of random variables, for every standard Borel space A

Idea: consider $\mathsf{Sh}(\mathbb{SBP})$ as an ambient category of sets and add axioms for the $\mathsf{RV}(A)$ objects.

Monoidal structure

The presheaf category $\mathrm{Psh}(\mathbb{SBP})$ carries the Day monoidal structure

$$F \mathbin{\widehat{\otimes}} G \;:=\; \int^{\Omega,\Omega'} \mathbb{SBP}(-, \Omega \otimes \Omega') \times F(A) \times G(B)\,.$$

where $\Omega \otimes \Omega'$ is the product-measure probability space.

Using the associated sheaf functor $\mathsf{a} : \mathrm{Psh}(\mathbb{SBP}) \to \mathrm{Sh}(\mathbb{SBP})$, we obtain a monoidal structure on the sheaf category $\mathrm{Sh}(\mathbb{SBP})$

$$F \otimes^{\mathrm{Sh}} G \;:=\; \mathsf{a}\left(F \mathbin{\widehat{\otimes}} G\right)\;.$$

Both monoidal structures are symmetric, affine (the unit is terminal) and closed.

Monoidal structure

There is an evident faithful functor

$$\mathsf{RV} : \mathbb{SB} \to \mathsf{Sh}(\mathbb{SBP})$$

mapping any standard Borel space A to the sheaf $\mathsf{RV}(A)$ of A-valued random variables.

The monoidal structure satisfies

$$\big(\mathsf{RV}(A) \otimes^{\mathsf{Sh}} \mathsf{RV}(B)\big)\,(\Omega) \;\cong\; \{([X],[Y]) \in \mathsf{RV}(A)(\Omega) \times \mathsf{RV}(B)(\Omega) \mid X \perp\!\!\!\perp Y\}$$

where $\perp\!\!\!\perp$ is probabilistic independence.

Forget the monoidal structure!

The monoidal structure does not seem helpful for developing a useful axiomatisation of a primitive notion of random variable.

Independence needs to be a property that may or may not hold, depending on circumstance, rather than a feature that is enforced by a type constructor.

(A further, technical issue is that $\otimes^{\mathsf{Sh}}$ is not a fibred functor.)

Moral: do not be over-seduced by elegant category-theoretic structure.

RVs and their probability laws

Axiom There is a functor

$$\mathrm{RV} : \mathbb{SB} \to \mathbf{Set}$$

Axiom There is a natural transformation

$$\mathbf{P} \colon \mathrm{RV} \Rightarrow \mathrm{M}_1$$

where $\mathrm{M}_1 : \mathbb{SB} \to \mathbf{Set}$ is the probability-measure functor

$$\mathrm{M}_1(A) \;=\; \{\mu \colon \mathcal{B}_A \to [0,1] \mid \mu \text{ is a probability measure}\} \;.$$

Idea $\mathrm{RV}(A)$ is the set of A-valued random variables, and $\mathbf{P}_A : \mathrm{RV}(A) \to \mathrm{M}_1(A)$ maps a random variable $X \in \mathrm{RV}(A)$ to its probability law $\mathbf{P}_A(X)$.

Drawbacks

$\mathrm{RV}(A)$ is defined only for standard Borel spaces A, and $\mathbf{P}_A(X) : \mathcal{B}_A \to [0, 1]$ assigns probabilities to Borel sets only. This is both cumbersome and restrictive.

In synthetic mathematics, one need not be constrained by ZFC-orthodoxy.

Why not allow $\mathrm{RV}(A)$ for arbitrary sets A, and have probability laws of the form $\mathbf{P}_A(X) : \mathcal{P}(A) \to [0, 1]$, i.e., probability laws are powerset measures?

This is a natural mathematical idealisation of probabilistic experience.

A change of model

Let $(\mathbb{K}, J_\omega)$ be the site with:

- objects — standard Borel probability spaces;
- morphisms — nullset reflecting measurable functions;
- Grothendieck topology — the countable cover (up to a nullset) topology J_ω.

The random topos $\mathcal{R}\mathsf{an} := \mathsf{Sh}(\mathbb{K}, J_\omega)$ is a Boolean topos validating DC in which $\mathbb{R}^n$ carries a translation-invariant measure on all subsets.

A well-chosen model!

$$\mathsf{Sh}_{\mathcal{R}\mathsf{an}}(\mathbb{SBP}) \;:=\; \text{atomic sheaves over } \mathbb{SBP} \text{ relative to } \mathcal{R}\mathsf{an}\,.$$

RVs and their probability laws revisited

Axiom There is a functor

$$\mathrm{RV} : \mathbf{Set} \to \mathbf{Set}$$

Axiom There is a natural transformation

$$\mathbf{P} \colon \mathrm{RV} \Rightarrow \mathrm{M}_1$$

where $\mathrm{M}_1 : \mathbf{Set} \to \mathbf{Set}$ is the probability-measure functor

$$\mathrm{M}_1(A) \;=\; \{\mu \colon \mathcal{P}(A) \to [0,1] \mid \mu \text{ is a probability measure}\} \; .$$

Idea $\mathrm{RV}(A)$ is the set of A-valued random variables, and $\mathbf{P}_A : \mathrm{RV}(A) \to \mathrm{M}_1(A)$ maps a random variable $X \in \mathrm{RV}(A)$ to its probability law $\mathbf{P}_A(X)$.

Limit-structure axioms

Axiom RV : **Set** $\to$ **Set** preserves countable (including finite) products.

Axiom **P** : RV $\Rightarrow$ M_1 is taut; i.e., if $m\colon A \to B$ is a monomorphism then the naturality square below is a pullback.

$$\begin{array}{ccc} \mathrm{RV}(A) & \xrightarrow{\;\mathbf{P}_A\;} & \mathrm{M}_1(A) \\ {\scriptstyle \mathrm{RV}(m)}\big\downarrow & & \big\downarrow{\scriptstyle \mathrm{M}_1(m)} \\ \mathrm{RV}(B) & \xrightarrow{\;\mathbf{P}_B\;} & \mathrm{M}_1(B) \end{array}$$

Proposition RV : **Set** $\to$ **Set** preserves equalisers.

Exploiting the axioms

Define the equality-in-law relation for $X, Y \in \mathrm{RV}(A)$ by

$$X \sim Y \quad \Leftrightarrow \quad \mathbf{P}_X = \mathbf{P}_Y$$

(we write $\mathbf{P}_X$ as a shorthand for $\mathbf{P}_A(X)$).

Define independence between $X \in \mathrm{RV}(A)$ and $Y \in \mathrm{RV}(B)$ by

$$X \perp\!\!\!\perp Y \quad \Leftrightarrow \quad \forall A' \subseteq A, B' \subseteq B \quad \mathbf{P}_{(X,Y)}(A' \times B') = \mathbf{P}_X(A') \cdot \mathbf{P}_Y(B') \,.$$

Tautness

Tautness: Random variables restrict to probability-1 subsets.

Given $Y \in \mathrm{RV}(B)$ and $A \subseteq B$ with $\mathbf{P}_Y(A) = 1$, there exists a unique $X \in \mathrm{RV}(A)$ such that $Y = i(X)$, where $i \colon A \to B$ is the inclusion function.

Consequence: Equality of random variables is almost sure equality.

For $X, Y \in \mathrm{RV}(A)$:

$$X = Y \quad \Leftrightarrow \quad \mathbf{P}_{(X,Y)}\{(x,y) \mid x = y\} = 1 \qquad \text{(official notation)}$$

$$\mathbf{P}[X = Y] = 1 \qquad \text{(informal notation)}$$

Deterministic random variables

Deterministic RVs exist

For every $x \in A$ there exists a unique random variable $\delta_x \in \mathrm{RV}(A)$ satisfying, for every $A' \subseteq A$:

$$\mathbf{P}_{\delta_x}(A') = \begin{cases} 1 & \text{if } x \in A' \\ 0 & \text{otherwise} \end{cases}$$

We write δ for the function $x \mapsto \delta_x : A \to \mathrm{RV}(A)$.

No other random variables can be proved to exist at this point, since the axioms thus far are compatible with RV being the identity functor.

Interlude: equality and equivalence

There are two equivalence relations of interest on random variables.

- Almost sure equality — in our setting this is just equality.

  This satisfies the usual (internal) substitutivity laws.

- The weaker equivalence relation: equality in law $\sim$.

Interlude: equality and equivalence

There are two equivalence relations of interest on random variables.

- Almost sure equality — in our setting this is just equality.

  This satisfies the usual (internal) substitutivity laws.

- The weaker equivalence relation: equality in law $\sim$.

  This satisfies a meta-theoretic substitutivity law: all definable properties are equidistribution invariant.

The invariance axiom

Every sentence of the form

$$\forall X, Y \in \mathrm{RV}(A), \quad \Phi(X) \ \wedge \ X \sim Y \ \rightarrow \ \Phi(Y)$$

is true.

The invariance axiom

Every sentence of the form

$$\forall X, Y \in \mathrm{RV}(A), \quad \Phi(X) \wedge X \sim Y \rightarrow \Phi(Y)$$

is true.

There is no evil!

Synthesising individual random variables

Fair coin axiom

There exists $K \in \mathrm{RV}\{0,1\}$ with $\mathbf{P}_K\{0\} = \frac{1}{2} = \mathbf{P}_K\{1\}$.

Independence axiom

For every $X \in \mathrm{RV}(A)$ and $Y \in \mathrm{RV}(B)$, there exists $X' \in \mathrm{RV}(A)$ such that:

$$X' \sim X \quad \text{and} \quad X' \perp\!\!\!\perp Y \ .$$

Existence of iid sequences

Proposition For every random variable $X \in \mathrm{RV}(A)$ there exists an infinite sequence $(X_i)_{i \geq 0}$ of mutually independent random variables with $X_i \sim X$ for every X_i.

Existence of iid sequences

Proposition For every random variable $X \in \mathrm{RV}(A)$ there exists an infinite sequence $(X_i)_{i \geq 0}$ of mutually independent random variables with $X_i \sim X$ for every X_i.

Proof Let $X_0 = X$.

Existence of iid sequences

Proposition For every random variable $X \in \mathrm{RV}(A)$ there exists an infinite sequence $(X_i)_{i \geq 0}$ of mutually independent random variables with $X_i \sim X$ for every X_i.

Proof Let $X_0 = X$.

Given $X_0, \ldots, X_{i-1}$, the independence axiom gives us X_i with $X_i \sim X$ such that $X_i \perp\!\!\!\perp (X_0, \ldots, X_{i-1})$.

Existence of iid sequences

Proposition For every random variable $X \in \mathrm{RV}(A)$ there exists an infinite sequence $(X_i)_{i \geq 0}$ of mutually independent random variables with $X_i \sim X$ for every X_i.

Proof Let $X_0 = X$.

Given $X_0, \ldots, X_{i-1}$, the independence axiom gives us X_i with $X_i \sim X$ such that $X_i \perp\!\!\!\perp (X_0, \ldots, X_{i-1})$.

This defines the required sequence $(X_i)_{i \geq 0}$ by DC. □

Existence of iid sequences

Proposition For every random variable $X \in \mathrm{RV}(A)$ there exists an infinite sequence $(X_i)_{i \geq 0}$ of mutually independent random variables with $X_i \sim X$ for every X_i.

Proof Let $X_0 = X$.

Given $X_0, \ldots, X_{i-1}$, the independence axiom gives us X_i with $X_i \sim X$ such that $X_i \perp\!\!\!\perp (X_0, \ldots, X_{i-1})$.

This defines the required sequence $(X_i)_{i \geq 0}$ by DC. $\square$

By the proposition there exists an infinite sequence $(K_i)_{i \geq 0}$ of independent random variables identically distributed to the fair coin K.

Laws of large numbers

$$\forall \epsilon > 0 \quad \lim_{n\to\infty} \mathbf{P}\left[\, \left| \left(\frac{\sum_{i=0}^{n-1} K_i}{n} \right) - \frac{1}{2} \right| < \epsilon \,\right] \;=\; 1 \qquad \text{(weak)}$$

$$\mathbf{P}\left[\, \lim_{n\to\infty} \left(\frac{\sum_{i=0}^{n-1} K_i}{n} \right) \;=\; \frac{1}{2} \,\right] \;=\; 1 \qquad \text{(strong)}$$

Everything thus far, up to and including the formulation of the weak law, only uses the preservation of finite products by RV. The formulation of the strong law, however, makes essential use of the preservation of countably infinite products to define:

$$\lambda \;:=\; \mathbf{P}_{(K_i)_i} \;\in\; \mathrm{M}_1(\{0,1\}^{\mathbb{N}})$$

The near-Borel axiom

We say that $\mu \in \mathrm{M}_1(A)$ is an RV-measure if there exists $X \in \mathrm{RV}(A)$ with $\mathbf{P}_X = \mu$. We write $\mathrm{M}_{\mathrm{RV}}(A)$ for the set of RV-measures on A.

Let $(A, \mathcal{B})$ be a standard Borel space. We say that a probability measure $\mu \in \mathrm{M}_1(A)$ is near Borel if: for every $A' \subseteq A$ there exists $B \in \mathcal{B}$ such that $\mu(A' \Delta B) = 0$.

Axiom Every RV-measure on a standard Borel space is near Borel.

Proposition Every Borel probability measure $\mu_{\mathcal{B}} \colon \mathcal{B} \to [0,1]$ on a standard Borel space $(A, \mathcal{B})$ extends to a unique $\mu \in \mathrm{M}_{\mathrm{RV}}(A)$.

Corollary The measure $\lambda \in \mathrm{M}_{\mathrm{RV}}(\{0,1\}^{\mathbb{N}})$ is translation invariant.

Universality of λ RVs

All randomness derives from coin tosses

We say that $Y \in \mathrm{RV}(B)$ is functionally dependent on $X \in \mathrm{RV}(A)$ (notation $Y \leftarrow X$) if there exists $f : A \to B$ such that $Y = f(X)$.

Axiom: Every random variable is functionally dependent on some $\{0,1\}^{\mathbb{N}}$-valued random variable with law λ.

For every $Y \in \mathrm{RV}(A)$ there exist a random variable $X \in \mathrm{RV}(\{0,1\}^{\mathbb{N}})$ with $\mathbf{P}_X = \lambda$ such that $Y \leftarrow X$.

Conditional expectation

$X \in \mathrm{RV}(\mathbb{R})$ is integrable if it has finite expectation

$$\mathbf{E}[X] := \int x \, d\mathbf{P}_X(x) \, .$$

Proposition (Conditional independence)

For $Y \in \mathrm{RV}(A)$ and integrable $X \in \mathrm{RV}(\mathbb{R})$, there exists a unique integrable random variable $Z \in \mathrm{RV}(\mathbb{R})$ satisfying:

- $Z \leftarrow Y$, and
- for all $A' \subseteq A$

$$\mathbf{E}[Z \cdot \mathbf{1}_{A'}(Y)] = \mathbf{E}[X \cdot \mathbf{1}_{A'}(Y)]$$

The unique such Z defines the conditional expectation $\mathbf{E}[X \mid Y]$.

Conditional probability

For $X \in \mathrm{RV}(A)$, $Y \in \mathrm{RV}(B)$ and $A' \subseteq A$ define:

$$\mathbf{P}[X \in A' \mid Y] \;:=\; \mathbf{E}[\mathbf{1}_{A'}(X) \mid Y] \;.$$

Conditional independence

For $X \in \mathrm{RV}(A)$, $Y \in \mathrm{RV}(B)$ and $Z \in \mathrm{RV}(C)$ define:

$$X \perp\!\!\!\perp Y \mid Z \;:\Leftrightarrow\; \text{for all } A' \subseteq A,\ B' \subseteq B$$
$$\mathbf{P}[(X, Y) \in A' \times B' \mid Z] \;=\; \mathbf{P}[X \in A' \mid Z] \cdot \mathbf{P}[Y \in B' \mid Z] \;.$$

Regular conditional probabilities

For $X \in \mathrm{RV}(A)$ and $Y \in \mathrm{RV}(B)$ a regular conditional probability (rcp) for Y conditioned on X is a random variable $Z \in \mathrm{RV}(\mathrm{M_{RV}}(B))$ such that:

- $Z \leftarrow X$ (so Z is induced from X by an RV-kernel $A \to \mathrm{M_{RV}}(B)$)
- For every $B' \subseteq B$,

$$Z(B') \;=\; \mathbf{P}[Y \in B' \,|\, X] \ ,$$

where $Z(B') \in \mathrm{RV}[0,1]$ abbreviates $(\mu \mapsto \mu(B'))(Z)$.

Theorem For every pair of random variables X, Y, there exists a unique rcp for Y conditioned on X. We write $P_{Y|X}$ for this rcp.

From kernels to RVs

Theorem

Suppose $k \colon A \to \mathsf{M}_{\mathsf{RV}}(B)$ is an RV-kernel where $|B| \leq 2^{\aleph_0}$. Then, for any $X \in \mathsf{RV}(A)$, there exists $Y \in \mathsf{RV}(B)$ such that:

$$P_{Y|X} \;=\; k(X) \;\; .$$

Simple illustrative application:

Using the RV-kernel $(\mu, \sigma) \mapsto \mathcal{N}_{\mu,\sigma^2} \colon \mathbb{R}^2 \to \mathsf{M}_{\mathsf{RV}}(\mathbb{R})$, we obtain for any $M, S \in \mathsf{RV}(\mathbb{R})$ a random variable Z such that

$$P_{Z\,|\,M,S} = \mathcal{N}_{M,S^2} \quad \text{(in statistician's notation } Z \sim \mathcal{N}_{M,S^2} \text{)}$$

Existence of conditionally independent RVs

Proposition

For every $X \in \mathrm{RV}(A)$, $Y \in \mathrm{RV}(B)$ and $Z \in \mathrm{RV}(C)$, there exists $X' \in \mathrm{RV}(A)$ such that:

$$(X', Z) \sim (X, Z) \quad \text{and} \quad X' \perp\!\!\!\perp Y \mid Z \; .$$

Stochastic processes: a myth

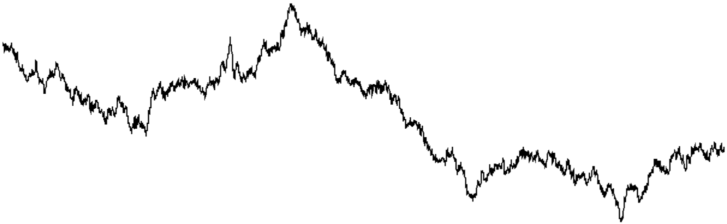
David Williams:

> " At the level of this book, the theory would be more elegant if we regarded a random variable as an *equivalence class* of measurable functions, two functions belonging to the same equivalence class if and only if they are equal almost everywhere. ... [In the] more interesting, and more important, theory where the parameter set of our process is uncountable ... the equivalence class formulation just will not work ... it loses the subtlety which is essential even for formulating the fundamental results on the existence of continuous modifications, etc. "

Probability with Martingales, 1990

Brownian motion

Example Brownian motion trajectory in $\mathbb{R}^{[0,1]}$.



$B \in \mathrm{RV}\left(\mathbb{R}^{[0,1]}\right)$ is a Brownian motion if:

- $B_0 = 0$;
- B has independent increments; i.e., for all $0 \leq t_0 < \cdots < t_n$

$$\coprod_{1 \leq i \leq n} B_{t_i} - B_{t_{i-1}} \quad ;$$

- B_T has stationary normal increments; i.e., for all $s, t \geq 0$

$$(B_{s+t} - B_s) \sim \mathcal{N}_{0,t} \quad ;$$

- $\mathbf{P}(B \text{ is continuous}) = 1\,.$

Construction of Brownian motion

Theorem A Brownian motion $B \in \mathrm{RV}\left(\mathbb{R}^{[0,1]}\right)$ exists.

Proof outline (following Levy's construction) Using DC, construct a sequence of random variables $(F^n \in \mathrm{RV}\left(\mathbb{R}^{\mathbb{D}_n}\right))_n$, where

$$\mathbb{D}_n \;:=\; \{q \in \mathbb{Q} \mid 0 \leq q \leq 1,\ \exists m \in \mathbb{Z}.\ q = \frac{m}{2^n}\}\ ,$$

$$F^0(0) \;:=\; 0 \qquad\qquad F^0(1) \;\sim\; \mathcal{N}_{0,1}$$

$$\begin{aligned} F^{n+1}(q) &:= F^n_q && \text{if } q \in \mathbb{D}_n \\ F^{n+1}\left(\frac{m}{2^{n+1}}\right) &\sim \mathcal{N}_{M,2^{-(n+2)}} && \text{if } m \text{ odd} \end{aligned}$$

where $M = \frac{1}{2}\left(F^n\left(\frac{m-1}{2^{n+1}}\right) + F^n\left(\frac{m+1}{2^{n+1}}\right)\right)$ and $\perp\!\!\!\perp_{q\in\mathbb{D}_{n+1}\setminus\mathbb{D}_n} F^{n+1}(q) \mid F_n$.

Define $F \in \mathrm{RV}\left(\mathbb{R}^{\mathbb{D}}\right)$, where $\mathbb{D} := \bigcup_n \mathbb{D}_n$ is the set of dyadic rationals in $[0,1]$, by

$$F\left(\frac{m}{2^n}\right) \;:=\; F^n\left(\frac{m}{2^n}\right) \;,$$

which is well defined.

Using a standard probabilistic argument prove that this dyadic-rational-indexed process is almost surely continuous at all real $t \in [0,1]$. Thus F restricts to a random variable F' on the set

$$\{f \in \mathbb{R}^{[0,\infty)\cap\mathbb{D}} \mid f \text{ is continuous at all } t \in [0,1]\} \;.$$

Now apply the function that maps each such f to its unique continuous extension in $\tilde{f} \in \mathbb{R}^{[0,1]}$. Define

$$B \;:=\; \widetilde{F'} \;.$$

Again using standard probabilistic arguments, one can show that B as defined above is a Gaussian process (all its finite dimensional distributions are multidimensional Gaussian) and that the covariance relation satisfies

$$\mathrm{Cov}[B_s, B_t] \;=\; \min(s, t)$$

Again, by a standard probabilistic argument, it follows that B is a Brownian motion.

□

Ongoing and future work

Fully work out and write up.

Develop substantial portions of probability theory in detail.

Transfer theorems.

Constructive and (hence) computable versions.

Type-theoretic formalised probability theory.

A convenient category for higher-order probability theory: **Set** !